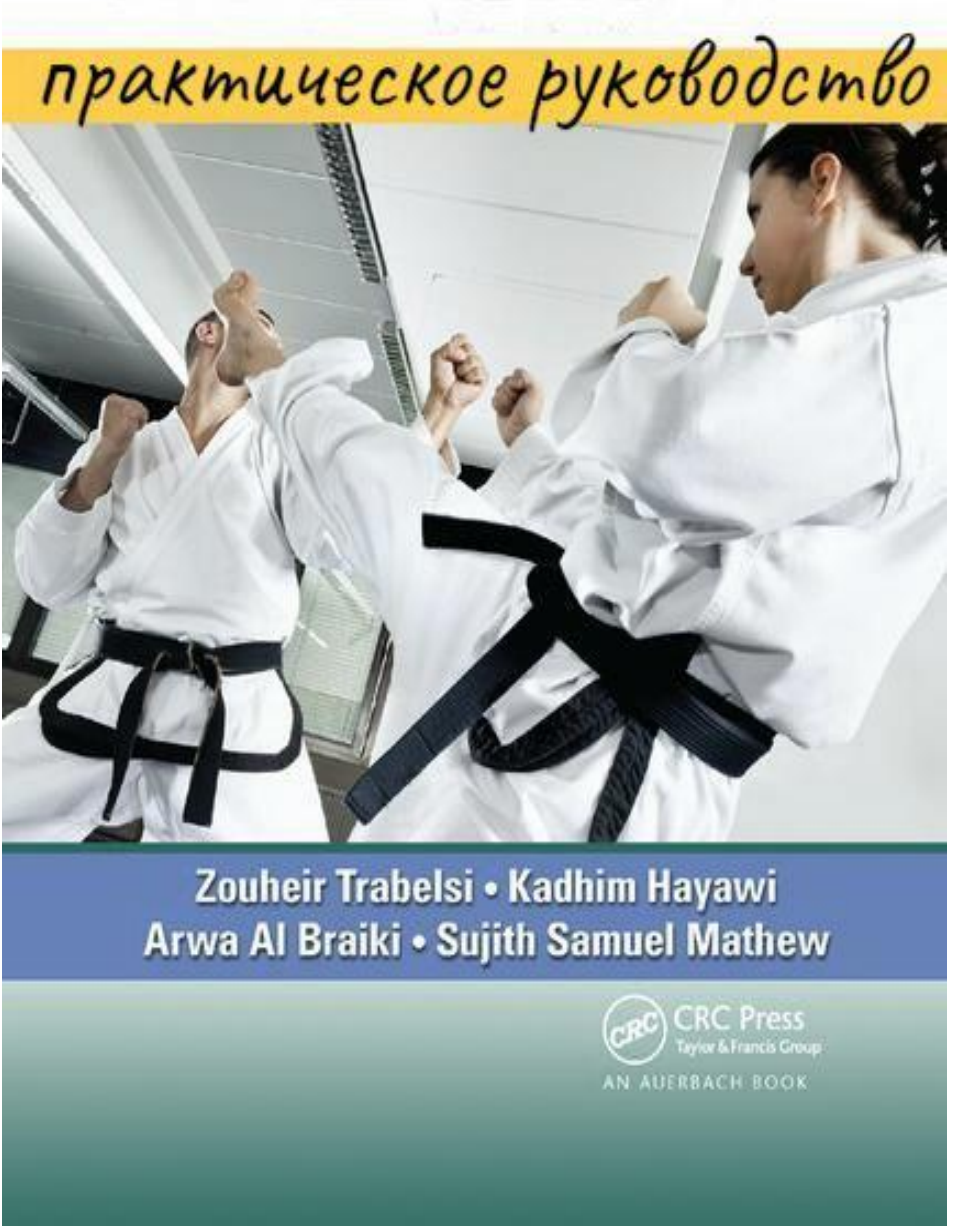
Сетевые атаки и защита



Сетевые атаки и защита

Практический подход

Перевод на русский Condor

Защита активов с помощью безопасности
Tyler Justin Speed
ISBN 978-1-4398-0982-2

Справочник CISO: практическое руководство по защите вашей компании
Michael Gentile, Ron Collette, and Thomas D. August
ISBN 978-0-8493-1952-5

Руководство CISO по тестированию на проникновение: структура для планирования, управления и максимизации преимуществ
James S. Tiller
ISBN 978-1-4398-8027-2

Кибербезопасность: угрозы и ответные меры государственного сектора
Kim J. Andreasson, Editor
ISBN 9781-4398-4663-6

Основы кибербезопасности
James Graham, Editor
ISBN 978-1-4398-5123-4

Кибербезопасность для промышленных систем управления: SCADA, DCS, PLC, HMI и SIS
Tyson Macaulay and Bryan L. Singer ISBN 978-1-4398-0196-3

Киберпространство и кибербезопасность
George Kostopoulos Request

ISBN 978-1-4665-0133-1

Инструменты интеллектуального анализа данных для обнаружения вредоносных программ
Mehedy Masud, Latifur Khan, and Bhavani Thuraisingham ISBN 978-1-4398-5454-9

Защита от чёрных хакеров: как хакеры делают то, что они делают, и как защититься от них
Jesse Varsalone and Matthew McFadden ISBN 978-1-4398-2119-0

Цифровая криминалистика для портативных устройств
Eamon P. Doherty
ISBN 978-1-4398-9877-2

Электронно хранимая информация: полное руководство по управлению, пониманию, приобретению, хранению, поиску
David R. Matthews
ISBN 978-1-4398-7726-5

Принципы и лучшие практики FISMA: за пределами соответствия
Patrick D. Howard
ISBN 978-1-4200-7829-9

Упрощенное управление информационной безопасностью: от зала заседаний до клавиатуры
Todd Fitzgerald
ISBN 978-1-4398-1163-4

Контроль и аудит информационных технологий, четвертое издание
Sandra Senft, Frederick Gallegos, and Aleksandra Davis Request ISBN 978-1-4398-9320-3

Управление инсайдерской угрозой: нет темных углов
Nick Catrantzos
ISBN 978-1-4398-7292-5

Бесшумная стеганография: ключ к скрытой коммуникации
Abdelrahman Desoky
ISBN 978-1-4398-4621-6

Безопасное и отказоустойчивое программное обеспечение: требования, тестовые примеры и методы тестирования
Mark S. Merkow
ISBN 978-1-4398-6621-4

Деинжиниринг безопасности: решение проблем управления информационными рисками
Ian Tibble
ISBN 978-1-4398-6834-8C

Руководство по оценке рисков безопасности: полное руководство по проведению оценок рисков безопасности, второе издание
Douglas Landoll
ISBN 978-1-4398-2148-0

7 качеств высоконадежного программного обеспечения
Mano Paul
ISBN 978-1-4398-1446-8

Smart Grid Security: сквозной взгляд на безопасность в новой электрической сети
Gilbert N. Sorebo and Michael C. Echols ISBN 978-1-4398-5587-4

AUERBACH PUBLICATIONS
www.auerbach-publications.com To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401 E-mail: orders@crcpress.com

Сетевые атаки и защита

Практический подход

Zouheir Trabelsi • Kadhim Hayawi Arwa Al Braiki • Sujith Samuel Mathew

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20120827

International Standard Book Number-13: 978-1-4665-1797-4 (eBook - PDF)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Содержание

Ведение
1. Атака отравления CAM таблицы.....1
1.1.Введение.....1
1.2.Лабораторное упражнение 1.1: отравление таблицы CAM коммутатора.....3
1.2.1. Результат.....3
1.2.2. Описание.....3
1.2.3. Эксперимент.....5
1.2.3.1.Шаг 1. Назначьте статические IP-адреса сетевым хостам.....5
1.2.3.2. Шаг 2: Просмотр содержимого таблицы CAM.....6
1.2.3.3. Шаг 3. Создайте вредоносный пакет, чтобы испортить таблицу CAM.....8
1.2.3.4. MAC Flood Attack для отслеживания трафика.....9
1.3. Лабораторное упражнение 1.2: Предотвращение атаки отравления таблицы CAM.....10
1.3.1. Результат.....10
1.3.2. Описание.....10
1.3.3. Эксперимент.....10
1.3.3.1. Шаг 1. Назначьте статические IP-адреса хостам сети.....11
1.3.3.2. Шаг 2. Настройте порт безопасности режима ограничения в коммутаторе.....11
1.3.3.3. Шаг 3. Создайте вредоносный пакет, чтобы испортить таблицу CAM.....12
1.3.3.4. Шаг 4: Настройте порт безопасности режима выключения на коммутаторе.....14
1.4. Краткое содержание главы.....15
2. ARP Cache Poisoning на основе MiM и DoS-атак.....17
2.1. Введение.....17
2.1.1. Протокол разрешения адресов (ARP).....17
2.1.2. ARP Cache.....18
2.2. Лабораторная работа 2.1: Атака отравления ARP кэша.....20
2.2.1. Результат.....20
2.2.2. Описание.....20
2.2.3. Обновление статического ARP Cache.....21
2.2.4. Эксперимент.....25
2.2..4.1. Архитектура сети.....25
2.2.4.2. Шаг 1. Назначьте статические IP-адреса хостам сети.....26
2.2.4.3. Шаг 2: Просмотр ARP-кэшей хостов.....26
2.2.4.4. Создайте вредоносный пакет ARP-запросов, чтобы повредить кэш ARP целевого хоста.....26
2.3. Лабораторная работа 2.2: DoS-атака на основе отравления ARP Cache.....28
2.3.1. Результат.....28
2.3.2. DoS-атака на основе отравления ARP Cache.....28
2.3.3. Эксперимент.....30
2.3.3.1. Шаг 1. Назначьте статические IP-адреса хостам сети.....30
2.3.3.2. Шаг 2. Просмотр ARP-кэша хоста A.....30

2.3.3.3. Шаг 3: Создайте пакет запроса вредоносного ARP.....31
2.3.3.4. Шаг 4: Проверьте DoS-атаку.....32
2.4. Лабораторная работа 2.3: MiM-атака на основе отравления ARP Cache.....33
2.4.1. Результат.....33
2.4.2. MiM Attack на основе отравления ARP Cache.....33
2.4.3. Эксперимент.....36
2.4.3.1. Шаг 1. Назначьте статические IP-адреса хостам сети.....37
2.4.3.2. Шаг 2. Включите IP-маршрутизацию на хосте C.....37
2.4.3.3. Шаг 3. Просмотр ARP-кэшей хоста A и хоста B.....39
2.4.3.4. Шаг 4: Создайте два вредоносных пакета запроса ARP.....39
2.4.3.5. Шаг 5: Проверьте атаку MiM.....41
2.4.3.6. Шаг 6: Сниффинг и анализирование трафика между хостами A и B.....41
2.5. Краткое содержание главы.....44
3. Обнаружение и предотвращение аномального трафика ARP.....45
3.1. Введение.....45
3.2. Аномальные пакеты ARP.....46
3.3. Эксперимент.....51
3.3.1. Межуровневая проверка ARP.....55
3.3.2. ARP Stateful Inspection.....55
3.3.3. Шторм ARP запросами и ARP сканирование.....56
3.3.3.1. Шторм ARP запросами.....56
3.3.3.2. ARP сканирование.....56
3.3.4. Анализ экспериментальных результатов.....57
3.4. Лабораторная работа 3.1: обнаружение аномального трафика ARP.....58
3.4.1. Результат.....58
3.4.2. Инструмент обнаружения XArp 2.....58
3.4.3. Эксперимент.....59
3.4.3.1. Архитектура сети.....59
3.4.3.2. Шаг 1. Назначьте статические IP-адреса хостам сети.....60
3.4.3.3. Шаг 2: Установите инструмент XArp 2.....60
3.4.3.4. Шаг 3: Настройте порт SPAN в коммутаторе Cisco.....61
3.4.3.5. Шаг 4. Создание и обнаружение аномальных пакетов ARP.....61
3.5. Лабораторная работа 3.2. Предотвращение аномального трафика ARP с использованием проверки динамического ARP для сетевой среды, отличной от DHCP.....69
3.5.1. Результат.....69
3.5.2. Динамическая проверка ARP.....69
3.5.3. Эксперимент.....70
3.5.3.1. Архитектура сети.....70
3.5.3.2. Шаг 1. Назначьте статические IP-адреса хостам сети.....71
3.5.3.3. Шаг 2. Настройка проверки динамического ARP для среды, отличной от DHCP, в коммутаторе Cisco Catalyst 3560.....71

3.5.3.4. Шаг 3. Создание и предотвращение неправильных пакетов ARP.....74
3.6. Лабораторная работа 3.3. Предотвращение аномального трафика ARP с использованием проверки динамического ARP и отслеживания DHCP для среды DHCP.....82
3.6.1. Результат.....82
3.6.2. DHCP Snooping.....82
3.6.3. Эксперимент.....83
3.6.3.1. Архитектура сети.....83
3.6.3.2. Шаг 1. Включите отслеживание DHCP.....84
3.6.3.3. Шаг 2. Настройка проверки динамического ARP для среды DHCP.....85
3.6.3.4. Шаг 3: Создание и предотвращение неправильного пакета ARP.....86
3.7. Краткое содержание главы.....88
4. Обнаружение сетевого трафика и обнаружение случайного режима.....89
4.1. Введение.....89
4.2. Лабораторная работа 4.1: Обнаружение случайного режима.....94
4.2.1. Результат.....94
4.2.2. Описание.....94
4.2.3. Тестирование.....95
4.2.4. Средства обнаружения случайного режима.....101
4.2.5. Эксперимент.....103
4.2.6. Архитектура сети.....103
4.2.7. Эксперимент.....103
4.2.7.1. Шаг 1. Назначьте статические IP-адреса хостам сети.....103
4.2.7.2. Шаг 2: Запустите сетевую карту хоста B в случайном режиме.....104
4.2.7.3. Шаг 3. Создание пакетов запросов ARP-ловушек.....104
4.2.7.4. Шаг 4: Анализ пакетов ответа ARP.....106
4.2.8. Обнаружение беспроводной сети.....110
4.2.8.1. Взлом ключа WEP и расшифровка сетевого трафика.....111
4.3. Краткое содержание главы.....116
5. IP-атаки типа «отказ в обслуживании».....117
5.1. Введение.....117
5.1.1. Распределенная атака типа «отказ в обслуживании» (DdoS).....118
5.2. Лабораторная работа 5.1: Land-атака.....120
5.2.1. Результат.....120
5.2.2. Описание.....120
5.2.3. Эксперимент.....120
5.2.3.1. Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks.....121
5.2.3.2. Шаг 2. Установите политики безопасности (правила фильтрации).....122
5.2.3.3. Шаг 3: Включить защиту от Land-атаки.....122
5.2.3.4. Шаг 4: Построить пакеты Land-атаки.....123
5.2.3.5. Шаг 5: Сниффинг сгенерированного трафика.....124
5.2.3.6. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....125
5.3. Лабораторная работа 5.2: SYN Flood Attack.....126
5.3.1. Результат.....126

5.3.2. Описание.....126
5.3.3. Эксперимент.....127
5.3.3.1. Шаг 3. Включите защиту от SYN-атаки.....128
5.3.3.2. Шаг 4: Создание пакетов SYN Flood Attack.....128
5.3.3.3. Шаг 5: сниффинг сгенерированного трафика.....131
5.3.3.4. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....132
5.4. Лабораторная работа 5.3: Атака Teardrop.....133
5.4.1. Результат.....133
5.4.2. Описание.....133
5.4.3. Эксперимент.....134
5.4.3.1. Шаг 3: Включить защиту от атаки Teardrop.....134
5.4.3.2. Шаг 4: Создание пакетов атаки Teardrop.....135
5.4.3.3. Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks.....137
5.5. Лабораторная работа 5.4: Атака на UDP.....138
5.5.1. Результат.....138
5.5.2. Описание.....138
5.5.3. Эксперимент.....139
5.5.3.1. Шаг 3. Включите защиту от UDP-атаки....139
5.5.3.2. Шаг 4: Построить UDP-пакеты Flood Attack.....140
5.5.3.3. Шаг 5: Сниффинг сгенерированного трафика.....142
5.3.3.4. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....143
5.6. Лабораторная работа 5.5: ненормальные IP-пакеты..143
5.6.1. Результат.....144
5.6.2. Описание.....144
5.6.2.1. Фрагментированный пакет ICMP.....144
5.6.2.2. Большой ICMP-пакет.....145
5.6.2.3. Пакет неизвестного протокола.....145
5.6.3. Эксперимент.....145
5.6.3.1. Шаг 3. Включите защиту от трех ненормальных пакетов.....146
5.6.3.2. Шаг 4: Генерация трех ненормальных пакетов.....147
5.6.3.3. Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks.....149
5.7. Краткое содержание главы.....149
6. Разведывательный трафик.....151
6.1. Введение.....151
6.2. Лабораторная работа 6.1: поиск IP-адресов.....151
6.2.1. Результат.....153
6.2.2. Описание.....153
6.2.3. Эксперимент.....153
6.2.3.1. Шаг 3. Включите защиту от очистки IP-адресов.....154
6.2.3.2. Шаг 4. Выполните очистку IP-адреса.....155
6.2.3.3. Шаг 5: Сниффинг сгенерированного трафика.....155
6.2.3.4. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....156

6.3. Лабораторная работа 6.2: сканирование портов TCP.....156
6.3.1. Результат.....156
6.3.2. Описание.....156
6.3.3. Эксперимент.....157
6.3.3.1. Включить защиту от сканирования портов.....158
6.3.3.2. Шаг 4. Выполните сканирование портов TCP.....159
6.3.3.3. Шаг 5: Сниффинг сгенерированного трафика.....160
6.3.3.4. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....161
6.4. Лабораторная работа 6.3: идентификация удаленной операционной системы.....161
6.4.1. Результат.....161
6.4.2. Описание.....161
6.4.2.1. NetScanTools Pro.....162
6.4.2.2. Nmap.....163
6.4.3. Эксперимент.....165
6.4.3.1. Шаг 3. Включите защиту от трех пакетов TCP.....167
6.4.3.2. Шаг 4: Сгенерируйте три пакета пробника TCP.....167
6.4.3.3. Шаг 5: Сниффинг сгенерированного трафика.....167
6.4.3.4. Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.....169
6.5. Лабораторная работа 6.4: трассировка.....170
6.5.1. Результат.....170
6.5.2. Описание.....171
6.5.3. Превентивные техники.....173
6.5.3.1. Эксперимент 6.4.1. Анализ трафика, генерируемого командой Tracert.....174
6.5.3.2. Эксперимент 6.4.2. Запретить трассировку трафика.....177
6.6. Краткое содержание главы.....179
7. Фильтрация пакетов и проверка.....181
7.1. Введение.....181
7.2. Лабораторная работа 7.1: базовая фильтрация пакетов.....182
7.2.1. Результат.....182
7.2.2. Базовая фильтрация пакетов.....183
7.2.3. Эксперимент.....184
7.2.4. Архитектура сети.....184
7.2.5. Шаги эксперимента.....185
7.2.5.1. Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks.....185
7.2.5.2. Шаг 2. Настройка серверов Web, FTP и Telnet.....185
7.2.5.3. Шаг 3. Реализация правил фильтрации для политик безопасности.....187
7.2.5.4. Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks.....190
7.3. Лабораторная работа 7.2: фильтрация нестандартных сервисов.....191
7.3.1. Результат.....191

7.3.2. Нестандартная фильтрация сервисов.....191
7.3.3. Эксперимент.....192
7.3.4. Архитектура сети.....193
7.3.5. Шаги эксперимента.....193
7.3.5.1. Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks.....193
7.3.5.2. Шаг 2: Настройте нестандартный веб-сервер, работающий на порте 3000.....193
7.3.5.3. Шаг 3. Создайте нестандартный сервисный профиль в устройстве Juniper Networks.....194
7.3.5.4. Шаг 4. Внедрение правил фильтрации для фильтрации трафика с нестандартной службой.....195
7.3.5.5. Шаг 5: Протестируйте правила фильтрации и просмотрите результаты в журнале событий Juniper Networks D.....196
7.4. Лабораторная работа 7.3: проверка согласованности и эффективности правил фильтрации брандмауэра.....197
7.4.1. Результат.....197
7.4.2. Согласованность и эффективность правил фильтрации.....197
7.4.3. Важность порядка правил фильтрации.....201
7.4.4. Эксперимент: устройство Juniper Networks.....203
7.4.5. Архитектура сети.....203
7.4.6. Шаги эксперимента.....203
7.4.6.1. Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks.....203
7.4.6.2. Шаг 2. Внедрение непоследовательных и неэффективных правил фильтрации.....204
7.4.6.3. Шаг 3. Проверка согласованности и эффективности правил фильтрации.....204
7.4.7. Эксперимент: FirePAC Tool.....205
7.4.8. Шаги эксперимента.....205
7.4.8.1. Шаг 1: Получить файл конфигурации брандмауэра.....206
7.4.8.2. Шаг 2. Проверка согласованности и эффективности правил фильтрации.....207
7.4.8.3. Шаг 3: Анализ результатов FirePAC Tool...207
7.5. Лабораторная работа 7.4: фильтрация содержимого пакетов.....211
7.5.1. Результат.....211
7.5.2. Фильтрация содержимого пакета.....211
7.5.3. Эксперимент.....213
7.5.4. Архитектура сети.....214
7.5.5. Шаги эксперимента.....214
7.5.5.1. Шаг 1: Настройте сетевые интерфейсы на сетевом устройстве Juniper.....215
7.5.5.2. Шаг 2. Настройка веб-серверов, FTP-серверов и почтовых серверов.....215
7.5.5.3. Шаг 3. Реализация правил фильтрации для политик безопасности.....215
7.5.5.4. Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks.....218
7.6. Лабораторная работа 7.5: фильтрация пакетов без сохранения состояния и против состояния.....224
7.6.1. Результат.....224
7.6.2. Проблемы безопасности с фильтрацией пакетов без сохранения состояния.....224
7.6.3. Контроль состояния фильтрации TCP пакетов..230
7.6.4. Контроль состояния фильтрации UDP пакетов.232

7.6.5. Контроль состояния фильтрации ICMP пакетов....234
7.6.6. Эксперимент....237
7.6.7. Архитектура сети....237
7.6.8. Шаги эксперимента....238
7.6.8.1. Часть 1. Полноценное тестирование TCP пакетов....238
7.6.9. Часть 2: Тестирование фильтрации пакетов ICMP с сохранением состояния....242
7.7. Лабораторная работа 7.6: активные и пассивные режимы FTP....245
7.7.1. Результат....245
7.7.2. Активные и пассивные режимы FTP....246
7.7.2.1. Активный режим FTP....246
7.7.2.2. Активная фильтрация трафика FTP....247
7.7.2.3. Реализация правил фильтрации для активного FTP-трафика....248
7.7.2.4. Проблема безопасности с активным режимом FTP....253
7.7.3. Пассивный режим FTP....253
7.7.3.1. Пассивная фильтрация трафика FTP....254
7.7.3.2. Реализация правил фильтрации для пассивного FTP-трафика....256
7.7.3.3. Проблема безопасности с пассивным режимом FTP....258
7.7.4. Эксперимент: активный анализ трафика FTP и анализ....260
7.7.5. Архитектура сети....260
7.7.6. Шаги эксперимента - часть 1: активный сеанс FTP....260
7.7.6.1. Шаг 1. Подключитесь к FTP-серверу, используя активный режим FTP, и перехватите сессионные пакеты....261
7.7.6.2. Шаг 2. Анализ пакетов активного сеанса FTP....261
7.7.7. Шаги эксперимента. Часть 2. Пассивный режим FTP....265
7.7.7.1. Шаг 1. Настройте LeapFTP в качестве пассивного FTP-клиента....265
7.7.7.2. Шаг 2. Подключитесь к FTP-серверу и прослушайте сессионные пакеты....266
7.7.7.3. Шаг 3: Анализ пассивных пакетов сеанса FTP....266
7.8. Краткое содержание главы....271
8. Безопасность маршрутизатора....273
8.1. Введение....273
8.2. Лабораторная работа 8.1: Основы модели AAA....275
8.2.1. Результат....275
8.2.2. Описание....275
8.2.3. Эксперимент....277
8.2.4. Архитектура сети....277
8.2.5. Шаги эксперимента....277
8.2.5.1. Шаг 1: Основные команды настройки маршрутизатора....278
8.2.5.2. Шаг 2: Настройте интерфейс обратной связи....279
8.2.5.3. Шаг 3: Консольная аутентификация и авторизация по умолчанию....280

8.2.5.4 Шаг 4: VTY (Telnet) аутентификация и авторизация по умолчанию.....280
8.2.5.5. Шаг 5: Настройте модель AAA: аутентификация.....281
8.2.5.6. Шаг 6: применить аутентификацию к VTY.....281
8.2.5.7. Шаг 7: применить аутентификацию к консоли.....282
8.2.5.8. Шаг 8: Проверьте консольную и Telnet аутентификацию.....282
8.2.5.9. Шаг 9: Настройте модель AAA: авторизация.....283
8.2.5.10. Шаг 10: применить авторизацию к VTY.....283
8.2.5.11. Шаг 11: применить авторизацию к консоли.....284
8.2.5.12. Шаг 12: Проверьте консоль и авторизацию Telnet.....284
8.2.5.13. Шаг 13: Настройте ведение журнала консоли.....285
8.3. Лабораторная работа 8.2: безопасные сетевые службы.....286
8.3.1. Результат.....286
8.3.2. Описание.....286
8.3.3. Эксперимент.....288
8.3.4. Архитектура сети.....288
8.3.5. Шаги эксперимента.....289
8.3.5.1. Шаг 1: Инициализация ПК и маршрутизатора.....289
8.3.5.2. Шаг 2: Сниффинг ICMP трафика.....291
8.3.5.3. Шаг 3: Сниффинг Telnet трафика.....293
8.3.5.4. Шаг 4: Сниффинг SSH трафика.....297
8.3.5.5. Шаг 5: Сниффинг HTTP трафика.....299
8.3.5.6. Шаг 6: Сниффинг HTTPS трафика.....301
8.4. Лабораторная работа 8.3: фильтрация пакетов на пограничном маршрутизаторе.....303
8.4.1. Результат.....303
8.4.2. Описание.....303
8.4.3. Эксперимент.....305
8.4.4. Архитектура сети.....305
8.4.5. Шаги эксперимента.....305
8.4.5.1. Шаг 1: Основные команды настройки маршрутизатора.....306
8.4.5.2. Шаг 2. Включите буферизованное ведение журнала на уровне отладки.....306
8.4.5.3. Шаг 3. Инициализация маршрутизаторов и ПК: IP-адреса и имена хостов.....307
8.4.5.4. Шаг 4: Запустите динамическую маршрутизацию: область OSPF 0 с перераспределением.....311
8.4.5.5. Шаг 5: Запустите серверы HTTP и Telnet на обоих маршрутизаторах.....315
8.4.5.6. Шаг 6: Реализация политик безопасности на пограничном маршрутизаторе FW.....318
8.4.5.7. Шаг 7: Тестирование политик безопасности, созданных на шаге 6.....320
8.5. Краткое содержание главы.....323
9. Реализация VPN-туннеля типа "сеть-сеть" для защиты от подслушивающих атак.....325

9.1. Введение.....325
9.1.1. Фазы протокола IKE.....327
9.1.2. Режимы Ipsec.....328
9.1.3. Протоколы Ipsec.....328
9.1.4. Типы VPN.....328
9.2. Лабораторная работа 9.1: VPN типа «сеть-сеть» - первая реализация.....329
9.2.1. Результат.....329
9.2.2. Описание.....330
9.2.3. Эксперимент.....330
9.2.3.1. Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию.....331
9.2.3.2. Шаг 2. Назначьте IP-адреса компьютеров и интерфейсов брандмауэра для обоих сайтов.....332
9.2.3.3. Шаг 3. Назначьте сетевые IP-адреса двух локальных сетей (Аль-Айн и Дубай) для обоих сайтов.....338
9.2.3.4. Шаг 4. Настройте VPN с сайта Al-Ain на сайт в Дубае и наоборот.....341
9.2.3.5. Шаг 5: Маршрут от площадки в Аль-Айне до шлюза в Дубае и обратно.....346
9.2.3.6. Шаг 6: Установите политики для обоих сайтов.....348
9.2.3.7. Шаг 7. Отправьте эхо-запрос из Аль-Айна в Дубай и наоборот, чтобы проверить создание VPN-туннеля.....351
9.2.3.8. Шаг 8: Проверьте Установление VPN-туннеля.....351
9.3. Лабораторная работа 9.2: VPN типа «сеть-сеть» - вторая реализация.....353
9.3.1. Результат.....353
9.3.2. Описание.....353
9.3.3. Эксперимент.....353
9.3.3.1. Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию для обоих сайтов.....354
9.3.3.2. Шаг 2. Назначьте IP-адреса компьютерам и интерфейсу брандмауэра для обоих сайтов.....355
9.3.3.3. Шаг 3: Определите трафик, который должен быть защищен.....356
9.3.3.4. Шаг 4: Создайте статический маршрут от сайта Аль-Айн до сайта в Дубае и наоборот.....357
9.3.3.5. Шаг 5: Включите протокол IKE на обоих сайтах.....357
9.3.3.6. Шаг 6: Определите параметры фазы 1 IKE.....358
9.3.3.7. Шаг 7: Определите предварительный общий ключ, который будет использоваться обоими сайтами.....358
9.3.3.8. Шаг 8: Определите параметры фазы IKE 2 протокола Ipsec.....359
9.3.3.9. Шаг 9: свяжите параметры двух фаз друг с другом.....359
9.3.3.10. Шаг 10. Применение криптокарты на внешнем интерфейсе (GigabitEthernet0/0).....360
9.3.3.11. Шаг 11: Пинг с сайта Al-Ain на сайт в Дубае и наоборот.....360
9.3.3.12. Шаг 12: Изучите параметры, которые установлены в ассоциации безопасности.....361
9.4. Краткое содержание главы.....365
10. Внедрение VPN-туннеля удаленного доступа

против подслушивающих атак.....367
10.1. Введение.....367
10.2. Лабораторная работа 10.1: VPN с удаленным доступом - первая реализация.....369
10.2.1. Результат.....369
10.2.2. Описание.....369
10.2.3. Эксперимент.....370
10.2.3.1. Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию.....371
10.2.3.2. Шаг 2. Назначьте IP-адреса компьютерам и интерфейсу брандмауэра.....371
10.2.3.3. Шаг 3: Создание пользователей.....375
10.2.3.4. Шаг 4: Сконфигурируйте предложение Фазы 1.....378
10.2.3.5. Шаг 5: Настройте предложение фазы 2.....380
10.2.3.6. Шаг 6: создайте политику безопасности.....381
10.2.3.7. Шаг 7. Настройте удаленный VPN-клиент Juniper NetScreen и проверьте подключение.....382
10.2.3.8. Шаг 8: Проверьте Установление VPN-туннеля.....391
10.3. Лабораторная работа 10.2: VPN с удаленным доступом - вторая реализация.....392
10.3.1. Результат.....392
10.3.2. Описание.....392
10.3.3. Эксперимент.....392
10.3.3.1. Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию.....394
10.3.3.2. Шаг 2. Назначьте IP-адреса компьютерам и интерфейсам брандмауэра.....394
10.3.3.3. Шаг 3. Выберите тип VPN-туннеля для удаленного доступа и выберите клиенты для удаленного доступа.....397
10.3.3.4. Шаг 4: Укажите имя группы туннелей VPN и метод аутентификации.....399
10.3.3.5. Шаг 5. Настройка учетных записей пользователей.....400
10.3.3.6. Шаг 6: Настройте пул адресов.....401
10.3.3.7. Шаг 7: Настройте атрибуты клиента.....401
10.3.3.8. Шаг 8. Настройте политику IKE.....402
10.3.3.9. Шаг 9. Настройка параметров шифрования и аутентификации Ipsec.....402
10.3.3.10. Шаг 10: Исключение трансляции адресов и разделенное туннелирование.....403
10.3.3.11. Шаг 11. Установите клиентское программное обеспечение Cisco VPN.....404
10.3.3.12. Шаг 12: Запустите программное обеспечение и проверьте подключение.....405
10.3.3.13. Шаг 13: Проверьте Установление VPN-туннеля.....410
10.3.3.14. Шаг 14: Контролируйте VPN-туннель в ASA.....412
10.4. Краткое содержание главы.....419

Введение

Важность экспериментального обучения давно признана и подчеркнута среди педагогических методов. Эта книга предназначена для ознакомления читателя с экспериментами по атакам и защите сетевой безопасности с использованием простого пошагового и практического подхода. Цель этой книги - научить читателя тому, как выполнить несколько хорошо известных сетевых атак и реализовать соответствующие меры сетевой безопасности. Эта книга является катализатором для представления образовательного подхода, который основан только на защитных методах, чтобы позволить студентам лучше анатомировать и развивать как наступательные, так и защитные методы. В нем также описаны типовые сценарии, которые преподаватели могут использовать для разработки и реализации инновационных практических упражнений по обеспечению безопасности.

Курсы по сетевой безопасности часто преподаются как концепции на относительно абстрактных уровнях. Учебная программа, которая охватывает концепции сетевой безопасности без надлежащего охвата практической реализацией, лишает ученика возможности испытать технологии и методы, необходимые для обеспечения безопасности. Практический подход к распространению знаний о сетевой безопасности подготовит студента к сложностям проведения исследований и разработок в этой области. Такой подход редко встречается в большинстве курсов для аспирантов и студентов. Даже когда некоторые пропагандируют практический подход, в нем обычно преобладают упражнения с использованием защитных приемов. Тем не менее, в настоящее время методы нападения, изначально разработанные хакерами, получают всеобщее одобрение и интерес. Часто критикуют, что оскорбительные методы не следует преподавать студентам, поскольку это только увеличивает популяцию «злонамеренных хакеров». Многие преподаватели в этой области считают, что практические курсы, в которых подробно описываются атаки на безопасность, неэтичны и создают потенциал для некоторых, чтобы использовать инструменты и методы безответственно. Социальное значение состоит в том, чтобы ограничить внедрение новых хакеров в общество. Тем не

менее, другие утверждают, что обучение методам нападения дает лучших специалистов по безопасности, чем тех, кто обучается только методам защиты. Здесь важно отметить, что корпоративные предприятия нанимают экспертов, которые используют оскорбительные методы для тестирования на проникновение, чтобы обеспечить свою безопасность. Использование оскорбительных методов для обеспечения безопасных сред для крупных корпоративных организаций создало новый жанр хакеров, «этический хакер!». Очевидно, что оскорбительные методы имеют ключевое значение для лучшего понимания нарушений безопасности и сбоев системы. Обучение сетевым атакам с помощью практических экспериментов является необходимым компонентом обучения сетевой безопасности. Более того, мы считаем, что учащиеся, занимающиеся вопросами безопасности, должны экспериментировать с методами атак, чтобы иметь возможность внедрять соответствующие и эффективные решения для обеспечения безопасности. Такой подход к обучению позволит студенту обеспечить конфиденциальность, целостность и доступность компьютерных систем, сетей, ресурсов и данных. Никто не может идеально спроектировать или построить защиту для атак, которые на самом деле не испытывали из первых рук. Наступательные и оборонительные приемы должны преподаваться с равной важностью на курсах по безопасности информационных технологий (информационных технологий). Кроме того, каждый курс по информационной безопасности должен сопровождаться обсуждением правовых последствий и охватывать этические обязанности студентов по отношению к своему сообществу и обществу в целом.

В сетевой безопасности недостаточно современных учебников и технических документов, в которых подробно описываются учебные практические упражнения, включающие как наступательные, так и защитные приемы. Чтобы внести свой вклад в заполнение этого пробела в обучении безопасности, в этой книге предлагается ряд комплексных упражнений, которые необходимы студентам по сетевой безопасности.

Эта книга не претендует на включение всех методов нападения и защиты. В отличие от других связанных учебников по безопасности, в этой книге обсуждаются как генерация нескольких известных сетевых атак, так и методы для реализации соответствующих методов защиты. Практические процессы,

участвующие в генерации атак, распространяются с целью ознакомить читателя со сложностью того же самого, а не пропагандировать использование готовых инструментов для атак и проникновения в систему безопасности. Книга предназначена для сопровождения и дополнения существующих торговых или академических печатных текстов и может быть предложена студентам, обучающимся на курсах сетевой безопасности.

В качестве предпосылки для этой книги авторы предполагают, что читатель обладает знаниями об основных сетевых протоколах и принципах. Аппаратная сеть и устройства безопасности, используемые в упражнениях, принадлежат Juniper Networks и Cisco. Тем не менее, лаборатории могут быть легко перестроены с использованием любых доступных сетевых и защитных устройств или программного обеспечения от других поставщиков, предлагающих аналогичные функциональные возможности.

Книга организована следующим образом:

В главе 1 описана атака отравления таблицы CAM (Content Addressable Memory) на сетевые коммутаторы. Эта атака намеревается повредить записи в таблице CAM коммутатора, так что сетевой трафик будет перенаправлен, что приведет к ситуации атаки DoS (отказ в обслуживании). Эта глава включает в себя практические занятия по созданию атаки отравления таблицей CAM и функции безопасности для предотвращения отравления таблицей CAM, доступные на современных коммутаторах.

Глава 2 посвящена атаке отравления кэша ARP (Address Resolution Protocol). Эта атака является злонамеренным действием хоста в локальной сети (LAN) по введению ложного IP-адреса в соответствие MAC-адресу (Media Access Control) в кеше ARP другого хоста. Отравление ARP-кеша - легкая атака, очень вредная и представляет очень серьезную угрозу. Отравление кэша ARP позволяет генерировать атаки DoS и MiM (Man-in-the-Middle). DoS-атака состоит в том, чтобы не дать хосту-жертве связаться с одним или несколькими хостами в локальной сети. Атака MiM является распространенным методом, используемым для перехвата сетевого трафика в коммутируемых локальных сетях. Эта глава включает

практические занятия по созданию атак DoS и MiM с использованием метода отравления кэша ARP.

Глава 3 посвящена обнаружению и предотвращению ненормального трафика ARP. Отравление кэша ARP является примером атак, которые используют ненормальный трафик ARP для повреждения кэшей ARP целевого хоста. Атаки, основанные на аномальном трафике ARP, представляют интерес, потому что они являются преднамеренными и обычно должны инициироваться, поддерживаться и контролироваться людьми. Эти атаки могут выполняться новичками или сценаристами с использованием широко доступных и простых в использовании инструментов, специально разработанных для этой цели. Из-за важности этой проблемы в нескольких типах решений безопасности интегрированы механизмы, позволяющие справляться с ненормальным трафиком ARP. В этой главе оцениваются общие решения безопасности с точки зрения их способности обнаруживать аномальный трафик ARP и проводится анализ, основанный на тяжелых практических экспериментах. Глава включает практические упражнения по обнаружению и предотвращению аномального трафика ARP.

В главе 4 обсуждается анализ сетевого трафика и обнаружение сетевых интерфейсных плат (NIC), работающих в случайном режиме. В локальных сетях нюхательная деятельность с злонамеренными целями может быть очень вредной. Обнаружение сетевого трафика позволяет злоумышленникам легко похищать конфиденциальные данные, пароли и конфиденциальность любого лица. Используя примеры, эта глава объясняет, как работает анализ сетевого трафика. В этой главе также обсуждаются концепции аппаратного фильтра сетевых плат и программного фильтра системного ядра, а также описывается общая методика обнаружения плат сетевых карт, работающих в случайном режиме. Глава включает практическое упражнение о том, как генерировать и вручную перехватывать пакеты запросов ARP для обнаружения плат NIC, работающих в случайном режиме..

В главе 5 описываются атаки типа «отказ в обслуживании», основанные на протоколе Интернета (на основе IP). DoS-атака - это атака, которая пытается сделать систему непригодной для использования или существенно замедлить работу системы для законных пользователей путем перегрузки ресурсов, чтобы никто другой не мог получить к ней доступ. Эта глава включает

практические упражнения по генерации и обнаружению четырех известных DoS-атак, а именно: наземная атака, SYN-атака, Teardrop-атака и UDP-атака. Кроме того, в этой главе представлена практическая работа по созданию и предотвращению ненормального IP-трафика.

Глава 6 обсуждает разведывательный трафик. Прежде чем злоумышленник сможет запустить эксплойт, он должен понять среду, на которую он нацелен. При этом ему необходимо собрать предварительную информацию о количестве машин, типах машин, операционных системах и т. Д. Вся собранная информация помогает составить представление об окружающей среде, которая будет подвергаться тестированию или атаке. Эта глава включает практические упражнения по генерации и обнаружению четырех общих разведывательных действий, а именно: сканирование IP-адреса, сканирование порта TCP (Transmission Control Protocol), идентификация удаленной ОС (операционной системы) и Traceroute.

В главе 7 рассматривается фильтрация и проверка сетевого трафика. Фильтрация и проверка трафика являются средством контроля доступа к сетям. Концепция заключается в определении того, разрешено ли пакету входить или выходить из сети организации, используя набор правил фильтрации, которые отражают и обеспечивают соблюдение политики безопасности организации. Технология фильтрации трафика может быть найдена в операционных системах, программных и аппаратных брандмауэрах, а также в качестве функции безопасности большинства маршрутизаторов и некоторых современных коммутаторов. В этой главе представлен ряд практических упражнений по внедрению правил фильтрации для базовых политик безопасности, фильтрации служб, работающих на нестандартных портах TCP и UDP (User Datagram Protocol), проверке согласованности и эффективности правил фильтрации межсетевого экрана, содержимого пакетов. фильтрация, фильтрация пакетов без учета состояния и состояния, а также активный и пассивный режимы FTP (File Transfer Protocol).

Глава 8 знакомит с некоторыми общими механизмами, используемыми для обеспечения безопасности маршрутизатора и защиты устройств. Маршрутизатор представляет собой единую точку входа для каждой сети. Следовательно, защита пограничного маршрутизатора является важной частью любого

решения сетевой безопасности. В этой главе представлены практические занятия, демонстрирующие следующие функции безопасности маршрутизатора: модель аутентификации, авторизации и аудита (ВА), безопасность доступа к управлению, фильтрация трафика с использованием списков контроля доступа (ACL) и проверка с отслеживанием состояния. Мы применяем на практике фильтрацию трафика на основе стандарта IETF, установленного Запросом комментариев (RFC), и отраслевых стандартов. Маршрутизатор Cisco используется потому, что он является наиболее распространенным устройством для пересылки пакетов между различными сетями. Однако большинство концепций и методов безопасности, описанных здесь, можно безопасно применять к продуктам других поставщиков.

В главе 9 изложены основы протоколов, стандартов, типов и развертываний решений для безопасности виртуальной частной сети (IPsec VPN). IPsec VPN - это открытый стандарт, определенный IETF для обеспечения безопасной связи между двумя конечными точками в общедоступной сети с использованием технологий конфиденциальности, целостности и аутентификации. IPsec VPN становится неотъемлемой частью любой корпоративной сети; Однако реализация IPsec VPN может быть очень утомительной и сложной задачей, особенно для начинающих. Эта глава проведет читателя через простые практические лабораторные занятия по развертыванию IPsec VPN-решений «сайт-сайт» с использованием различных иллюстраций, снимков экрана и шагов настройки.

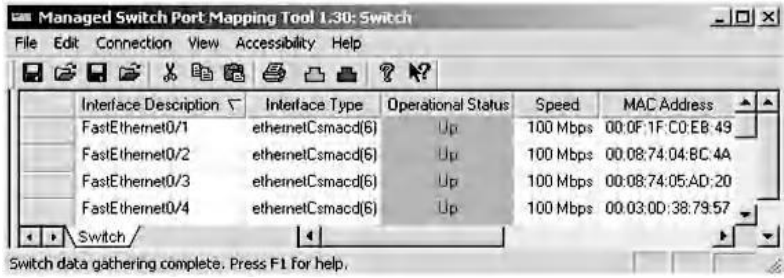
В главе 10 обсуждается архитектура решения безопасности IPsec VPN для удаленного доступа и описываются его структура, компоненты, приложения и реализации. VPN с удаленным доступом позволяет пользователям получать доступ к частным данным и защищенным сетевым ресурсам центрального сайта через защищенный туннель IPsec VPN. Из-за растущего числа приложений удаленного доступа IPsec VPN большинство поставщиков операционных систем, брандмауэров и маршрутизаторов включают поддержку VPN в свои продукты. В этой главе представлены практические лабораторные реализации решения IPsec VPN для удаленного доступа от двух лидеров в этой области. Лаборатории служат для расширения знаний читателей о лучших практиках VPN

Глава 1

Атака отравления таблицы CAM коммутатора

1.1 Введение

Локальные сети (LAN) настроены на использование коммутаторов, которые поддерживают таблицу, называемую Content Addressable Memory (CAM), которая используется для сопоставления отдельных MAC-адресов (Media Access Control) в сети с физическими портами на коммутаторе. Таблица CAM позволяет коммутатору направлять данные из физического порта именно туда, где находится получатель, в отличие от беспорядочной широковещательной передачи данных из всех портов, таких как концентратор. Преимущество этого метода заключается в том, что данные соединяются исключительно с сегментом сети, содержащим компьютер, для которого эти данные специально предназначены. На следующем снимке экрана показан пример записей в таблице CAM коммутатора, где четыре коммутатора подключены к коммутатору. Например, первый хост (чей MAC-адрес 00: 0F: 1F: C0: EB: 49) подключен к порту № 1 (интерфейс: Fast Ethernet 0/1) на коммутаторе.



Когда коммутатор получает пакет от хоста, он сначала извлекает MAC-адрес назначения из заголовка кадра Ethernet. Используя этот MAC-адрес, коммутатор получает соответствующий номер порта из таблицы CAM. Затем пакет отправляется только на хост, подключенный к этому порту. Таким образом, анализ сетевого трафика кажется трудным в коммутируемой локальной сети. Тем не менее, в главе 2 подробно рассматриваются методы перехвата сетевого трафика в коммутируемых локальных сетях.

Атака отравления таблицей CAM коммутатора является злонамеренным действием, приводящим к повреждению записей в таблице CAM коммутатора, так что сетевой трафик будет перенаправлен от предполагаемых хостов. Эта злонамеренная деятельность может создать ситуацию DoS (отказ в обслуживании), так как коммутатор становится неспособным пересылать пакеты в их реальные и законные места назначения.

Эта глава включает в себя два практических упражнения. Первый описывает, как выполнить атаку отравления таблицей CAM. Второй касается реализации доступных функций безопасности на коммутаторах для предотвращения атаки отравления таблицей CAM.

В упражнениях используются следующие аппаратные устройства и программные средства:

* Cisco Catalyst 3650 Switch Series*
* CommView Visual Packet Builder†: Graphical User Interface (GUI) based packet generator

* http://www.cisco.com
† http://www.tamos.com

1.2 Лабораторное упражнение 1.1: Отравление CAM таблицы коммутатора

1.2.1 Результат

Цель этого практического упражнения состоит в том, чтобы учащиеся узнали, как выполнить атаку отравления таблицей CAM коммутатора.

1.2.2 Описание

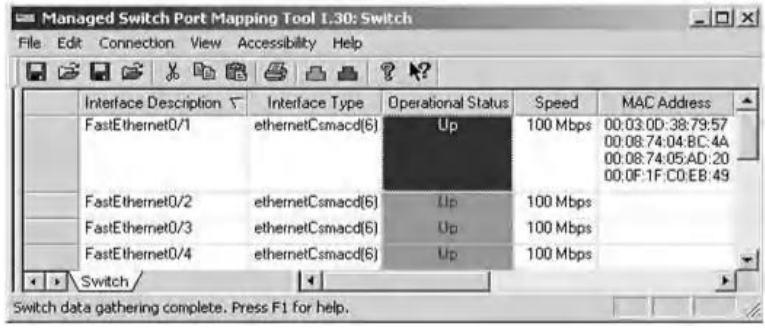
Атака отравления таблицы CAM коммутатора намерена испортить записи в таблице, чтобы сетевой трафик был перенаправлен. Рассмотрим два хоста, подключенных к коммутатору, один на порт a, а другой на порт b. Вредоносный хост (подключенный к порту a) отправляет поддельный пакет с MAC-адресом источника в заголовке Ethernet пакета, равным MAC-адресу целевого хоста (подключенного к порту b). MAC-адрес назначения в заголовке пакета может быть любым MAC-адресом. Как только коммутатор получает пакет, он обновляет свою таблицу CAM. Поэтому запись таблицы CAM для MAC-адреса этого целевого хоста будет повреждена. Следовательно, целевой хост будет считаться хостом, подключенным к порту a. Любой пакет, отправленный целевому хосту (MAC-адрес назначения в заголовке Ethernet пакета равен MAC-адресу целевого хоста), будет перенаправлен на Порт a, то есть на вредоносный хост.

В качестве примера атаки с отравлением таблицей CAM на предыдущем рисунке показано, что в таблице CAM коммутатора имеется четыре хоста, подключенных к коммутатору. Хост № 1, злонамеренный хост, атакует таблицу CAM коммутатора, используя три поддельных пакета. Пакеты почти одинаковы, но имеют разные MAC-адреса источника в заголовках Ethernet. Информация о пакетах выглядит следующим образом:

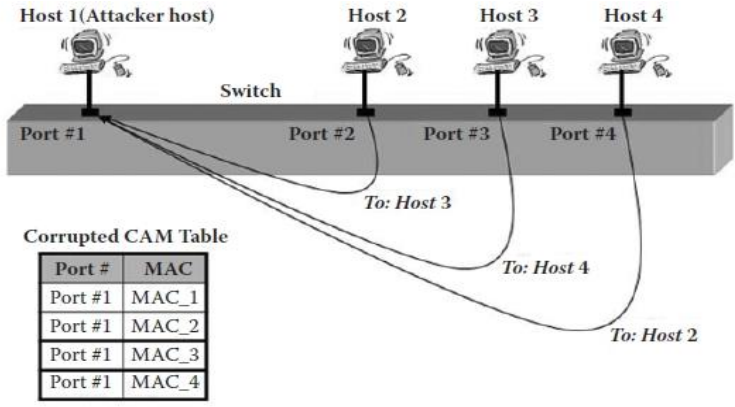
1. Первый поддельный пакет: MAC-адрес источника в заголовке Ethernet = 00: 08: 74: 04: BC: 4A (хост № 2).

2. Второй поддельный пакет: MAC-адрес источника в заголовке Ethernet = 00: 08: 74: 05: AD: 20 (хост № 3).
3. Третий поддельный пакет: MAC-адрес источника в заголовке Ethernet = 00: 03: 0D: 38: 79: 57 (хост № 4).

После этой атаки таблица CAM коммутатора становится поврежденной, как показано на следующем снимке экрана. Таблица CAM показывает, что все четыре хоста подключены к порту 1 коммутатора (FastEthernet 0/1). Физически, однако, только порт № 1 подключен к порту № 1.



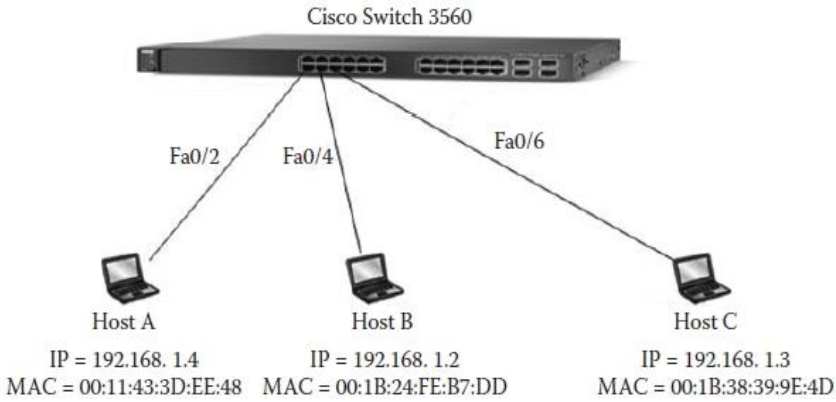
После отправки пакета на один из этих трех хостов-жертв (хост № 2, хост № 3 или хост № 4) коммутатор направит его на порт № 1, то есть на хост № 1. Эта ситуация может создать ситуацию DoS, потому что коммутатор не пересылает пакеты, предназначенные этим трем хостам, их законным адресатам (см. Рисунок ниже).



1.2.3 Эксперимент

В следующем эксперименте описано, как просмотреть и повредить содержимое таблицы CAM. Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Три хоста подключены к коммутатору Cisco следующим образом:

1. Хост A подключен к порту #2 коммутатора.
2. Хост B подключен к порту #4 коммутатора.
3. Хост C подключен к порту #6 коммутатора.



Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса сетевым хостам.
Шаг 2: Просмотрите содержимое таблицы CAM.
Шаг 3: Создайте вредоносный пакет для повреждения таблицы CAM

1.2.3.1 Шаг 1. Назначьте статические IP-адреса сетевым хостам

Шаги, необходимые для назначения статических IP-адресов хостам, очень похожи в большинстве операционных систем Windows и Linux.

Например, в Windows XP, чтобы назначить IP-адреса хостам, выполните следующие действия:

Откройте панель управления и выберите «Сетевое подключение» (Network Connection). Дважды щелкните значок «Подключение по локальной сети» (Local Area Network connection). Выберите «Протокол Интернета (TCP / IP)» (Internet Protocol (TCP/IP)) и нажмите кнопку «Свойства» (Properties).

Выберите опцию «Использовать следующий IP-адрес» (Use the following IP address) и заполните записи (см. Следующий снимок экрана).

Затем нажмите “OK.”

Чтобы проверить назначенный статический IP-адрес, введите следующую команду в окне cmd:

```
C:\>ipconfig/all
```

1.2.3.2 Шаг 2: Просмотр содержимого таблицы CAM

Чтобы просмотреть содержимое таблицы CAM, выполните следующие действия:

Подключите хост к консольному порту на коммутаторе.

* Запустите приложение терминала (например, HyperTerminal) на хосте.

* Под опцией «Connect Using:» выберите один из соответствующих коммуникационных портов (COM1, COM2 и т. д.), К которому подключен консольный кабель.

* Выберите «OK», и появится окно «Настройки порта» (Port Settings), предлагающее вам определить скорость передачи данных и параметры связи, как определено поставщиком. (Большинство поставщиков имеют следующие настройки: 9600 бит в секунду, 8 бит данных, нет четности, 1 стоповый бит и нет управления потоком.)

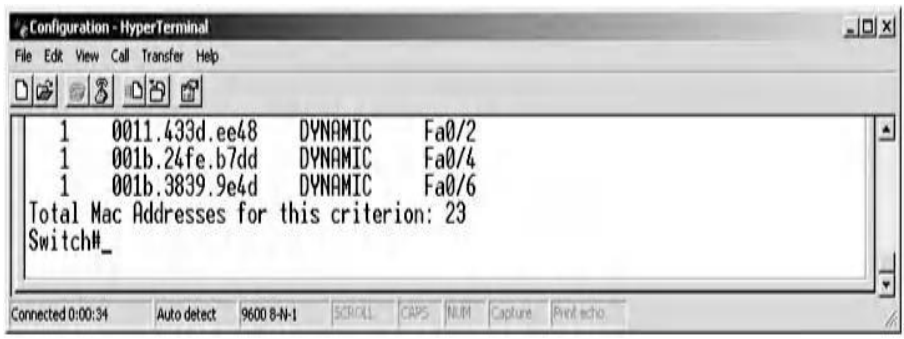
* Выберите «OK». Это поместит вас в окно терминала. Нажмите клавишу «Enter» несколько раз, пока в окне терминала не появится меню с переключателя.

* Если появится меню, то вы готовы настроить коммутатор по мере необходимости.

* Введите следующую команду, чтобы просмотреть содержимое таблицы CAM:

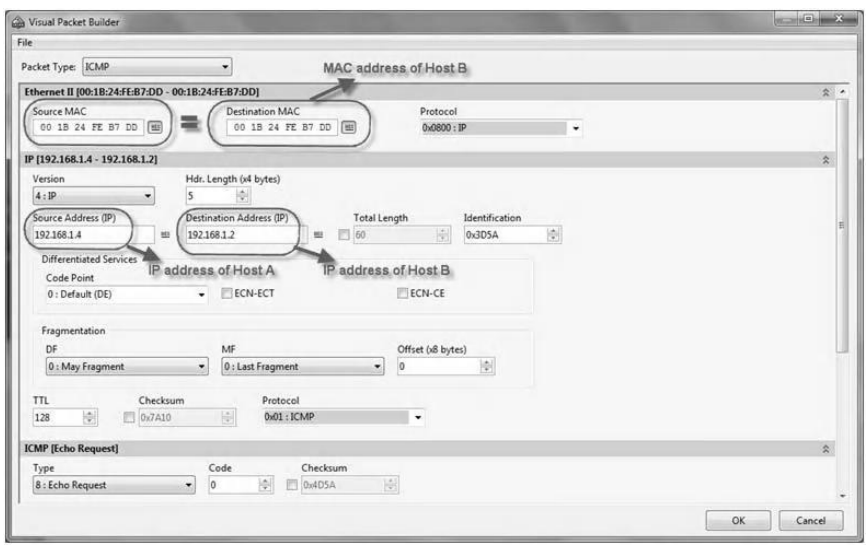
```
Switch> enable//введите команду enable для
доступа в привилегированный режим EXEC
Switch# show mac-address-table
```

* Содержимое таблицы CAM показано на следующем снимке экрана. Три хоста, MAC-адреса которых отображаются, подключены к порту № 2, порту № 4 и порту № 6 соответственно.

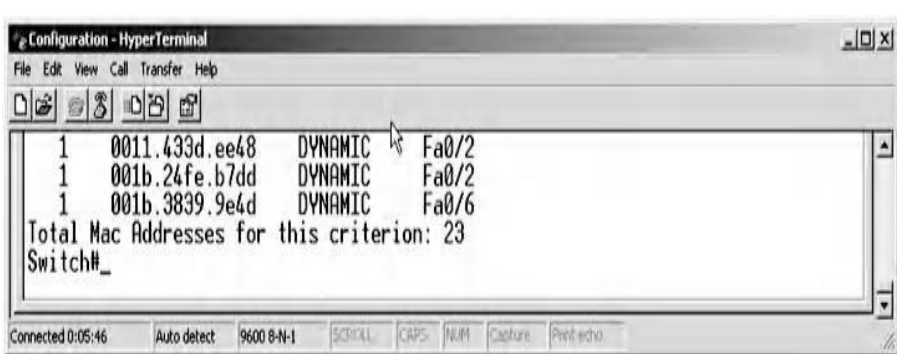


1.2.3.3 Шаг 3. Создание вредоносного пакета для повреждения таблицы CAM

Используйте любой генератор пакетов, например CommView Visual Packet Builder, для создания вредоносного пакета, чей MAC-источник в кадре Ethernet равен MAC-адресу хоста-жертвы. Например, мы предполагаем, что узел A генерирует ложный ICMP-эхо-пакет, чей MAC-источник равен MAC-адресу хоста B. Используя CommView Visual Packet Builder, на следующем снимке экрана представлен снимок экрана, показывающий содержимое ложного ICMP-эхо-пакета.



А следующий снимок экрана - это снимок содержимого поврежденной таблицы CAM после отправки поддельного эхо-пакета ICMP.



Этот экран показывает, что хост B подключен к порту № 2. Однако физически хост B все еще подключен к порту № 4. Следовательно, когда хост C отправляет пакеты хосту B, коммутатор не будет пересылать их хосту B; они будут перенаправлены на хост A. Это ситуация атаки DoS, так как хост C не может правильно связаться с хостом B

Важно указать, что, как только узел B отправляет пакет адресату, коммутатор автоматически обновляет свою таблицу CAM. Следовательно, запись, соответствующая хосту B в таблице CAM, становится не поврежденной. Однако, чтобы сохранить таблицу CAM поврежденной, злонамеренный узел A должен продолжать вводить поддельный эхо-пакет ICMP

1.2.3.4 Атака MAC Flood для отслеживания трафика

Старая техника атаки для перехвата трафика в коммутируемой сети LAN основана на затоплении MAC. MAC-флудинг - это метод, используемый для нарушения безопасности сетевых коммутаторов. В типичной атаке с MAC-адресами злоумышленник получает от коммутатора множество фреймов Ethernet, каждый из которых содержит свой MAC-адрес источника. Намерение состоит в том, чтобы использовать ограниченную память, выделенную в коммутаторе, для хранения таблицы CAM. То есть, когда некоторые таблицы CAM старых моделей коммутаторов переполняются, коммутаторы возвращаются в широковещательный режим (также известный как режим концентратора или режим аварийного открытия). Как следствие, анализ сетевого трафика может быть легко выполнен. Следовательно, после запуска успешной атаки MAC-наводнения злонамеренный пользователь может использовать анализатор пакетов (анализатор) для сбора важных данных, передаваемых между хостами других сетей, которые не будут доступны при нормальной работе коммутатора.

1.3 Лабораторное упражнение 1.2: Предотвращение атаки отравления таблицы CAM

1.3.1 Результат

Цель этого практического упражнения состоит в том, чтобы учащиеся узнали, как предотвратить повреждение содержимого таблицы CAM коммутатора.

1.3.2 Описание

Чтобы предотвратить отравление таблиц CAM, администраторы безопасности обычно полагаются на наличие функции «безопасности порта» коммутаторов. Большинство коммутаторов можно настроить для ограничения количества MAC-адресов, которые можно узнать на портах, подключенных к конечным станциям. Меньшая таблица «безопасных» MAC-адресов поддерживается в дополнение (и в качестве подмножества) к традиционной таблице CAM.

Например, коммутаторы Cisco Catalyst серии 3560 позволяют ограничить количество допустимых MAC-адресов на порту (или интерфейсе) с помощью функции безопасности порта. Когда это число превышено, нарушение безопасности будет вызвано, и действие нарушения будет выполнено на основе режима, настроенного на этом порту. Следовательно, любой неавторизованный MAC-адрес не сможет получить доступ и повредить таблицу CAM коммутатора. Интерфейс может быть настроен для одного из трех режимов нарушения в зависимости от действия, которое должно быть выполнено в случае нарушения:

1. Защита. Когда число защищенных MAC-адресов достигает максимально допустимого для интерфейса предела, пакеты с неизвестными исходными MAC-адресами отбрасываются до тех пор, пока администратор коммутатора не удалит достаточное количество защищенных MAC-адресов, чтобы опуститься ниже максимального значения или увеличить количество максимально допустимых адресов. Администратор коммутатора не уведомляется о нарушении безопасности.

2. Ограничение: этот режим аналогичен предыдущему режиму. Однако в этом режиме администратор коммутатора уведомляется о нарушении безопасности.
3. Завершение работы: нарушение безопасности порта приводит к немедленному завершению работы интерфейса. Администратор коммутатора может вывести его из этого состояния и настроить время восстановления. Это режим "по умолчанию".

1.3.3 Эксперимент

В следующем эксперименте описывается, как настроить и протестировать функции безопасности портов в коммутаторах Cisco Catalyst серии 3560, чтобы предотвратить повреждение содержимого таблицы CAM. Эксперимент использует ту же сетевую архитектуру, которая описана в предыдущей лабораторной работе, и состоит из следующих шагов:

Шаг 1. Назначьте статические IP-адреса хостам сети
Шаг 2: Настройте порт безопасности режима ограничения в коммутаторе
Шаг 3: Создайте вредоносный пакет для повреждения таблицы CAM
Шаг 4: Настройте порт безопасности режима выключения на коммутаторе

1.3.3.1 Шаг 1. Назначьте статические IP-адреса хостам сети

Обратитесь к шагу 1 в предыдущей лабораторной работе.

1.3.3.2 Шаг 2. Настройте порт безопасности режима ограничения в коммутаторе

Чтобы настроить порт безопасности режима ограничения:

* Подключите хост к консольному порту на коммутаторе

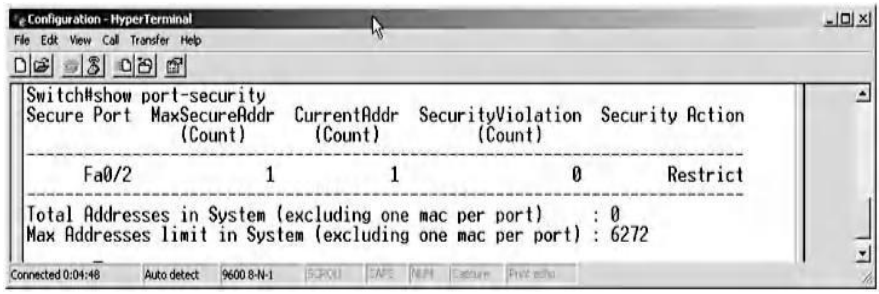
* Запустите приложение терминала на хосте. Введите следующие команды:

```
Switch> enable//введите команду enable для
доступа в привилегированный режим EXEC
Switch# Configure terminal
Switch(config)#      interface      fastethernet
0/2//Функция безопасности порта применяется на
хосте, подключенном к Port #2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security
violation restrict
Switch(config-if)# end
Switch# copy running-config startup-config
```

* Чтобы отобразить режим безопасности порта, введите следующую команду:

```
Switch# show port-security
```

На снимке экрана ниже показан режим безопасности порта до попытки повреждения



1.3.3.3 Шаг 3. Создайте вредоносный пакет, чтобы испортить таблицу CAM

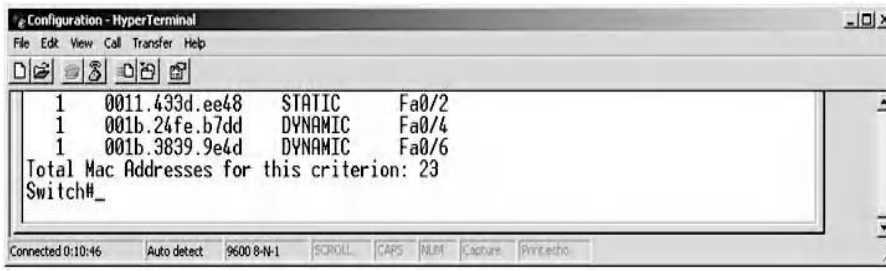
Используйте любой генератор пакетов, например CommView Visual Packet Builder, для создания вредоносного пакета, для которого в качестве MAC-источника в заголовке Ethernet задан поддельный MAC-адрес. Например,

можно использовать тот же поддельный эхо-пакет ICMP, сгенерированный в предыдущей лабораторной работе.

* Введите следующую команду, чтобы просмотреть содержимое таблицы CAM после попытки повреждения:

```
Switch# show mac-address-table.
```

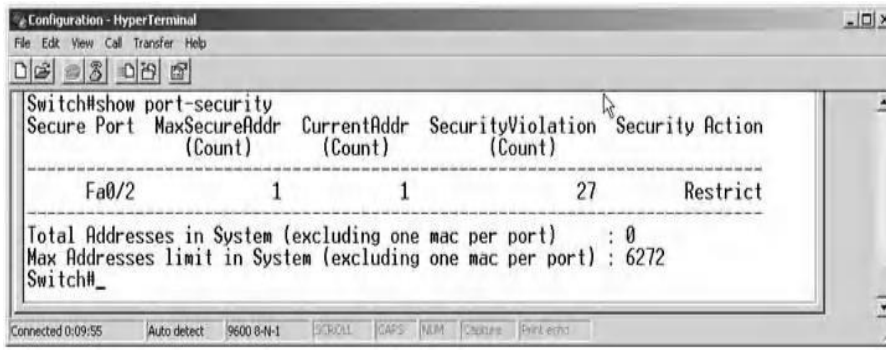
Следующий скриншот ясно показывает, что таблица CAM не была повреждена.



* Введите следующую команду, чтобы снова отобразить режим безопасности порта:

```
Switch# show port-security.
```

Снимок экрана ниже ясно показывает, что было двадцать семь пакетов, которые пытались нарушить функцию безопасности, реализованную на порту № 2 (Fa0 / 2). Эти пакеты попытались повредить таблицу CAM; однако коммутатор заблокировал их.



1.3.3.4 Шаг 4: Настройте порт безопасности режима выключения на коммутаторе

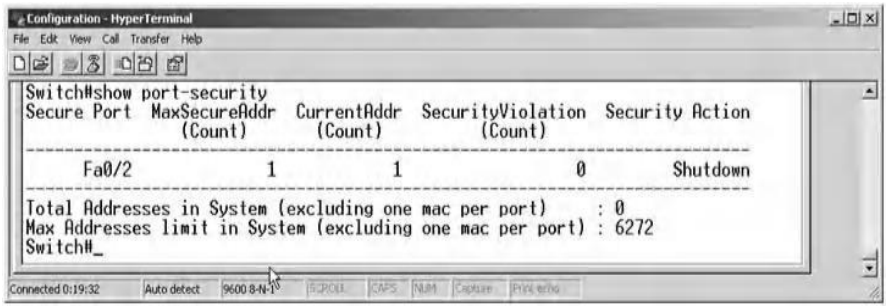
Введите следующие команды для настройки порта безопасности режима выключения:

```
Switch(config)# interface fastethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security
violation shutdown
Switch(config-if)# end
```

Switch# скопируйте running-config startup-config

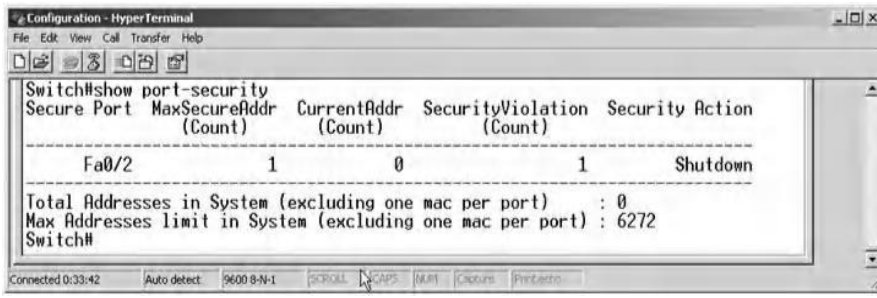
* Показать режим безопасности порта.

На следующем снимке экрана показан режим безопасности порта до попытки повреждения.



* Сгенерируйте тот же поддельный ICMP-пакет из предыдущего теста, а затем отобразите режим безопасности порта.

Следующий снимок экрана ясно показывает, что был пакет, который пытался нарушить функцию безопасности, реализованную на порту № 2. Коммутатор заблокировал вредоносный пакет и закрыл порт.



На следующем снимке экрана четко видно, что узел A потерял соединение с коммутатором (интерфейс 0/2 был отключен), и на рабочем столе узла A появилось предупреждающее сообщение.

1.4 Краткое содержание главы

В этой главе описывается создание и предотвращение атаки отравления таблицей CAM коммутатора. Атака заключается в повреждении записей в таблице CAM для создания ситуации DoS. После атаки целевой коммутатор становится неспособным пересылать пакеты в их законные места назначения. Практические упражнения главы позволяют пользователям узнать, как выполнить и предотвратить атаку отравления таблицей CAM коммутатора.

Глава 2

Отравление ARP кэша на основе MiM и DoS-атак

2.1 Введение

2.1.1 Address Resolution Protocol (ARP)

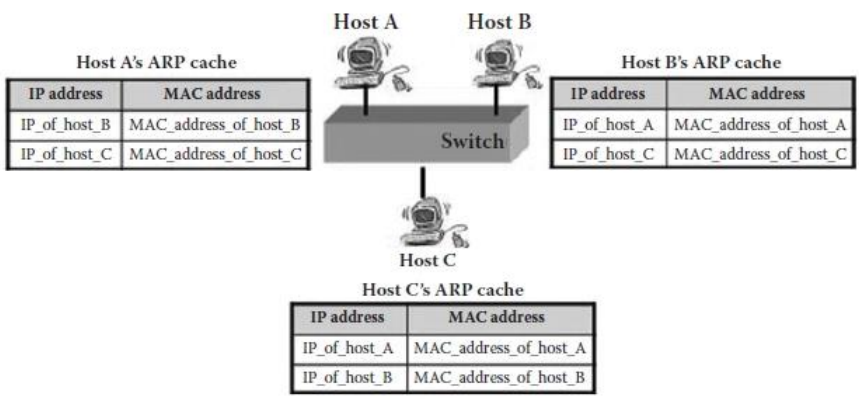
ARP используется для сопоставления IP-адреса с заданным MAC-адресом (Media Access Control), чтобы пакеты могли передаваться по локальной сети. Сообщения ARP обмениваются, когда один хост знает IP-адрес (адрес интернет-протокола) удаленного хоста и хочет определить MAC-адрес удаленного хоста. Например, в локальной сети для получения MAC-адреса хоста 2 хосту 1 необходимо сначала отправить сообщение запроса широковещательного ARP всем хостам в сети. Затем узел 2 отправит ответное сообщение одноадресной ARP обратно узлу 1, содержащему его MAC-адрес. Сообщение ARP в сети Ethernet / IP имеет восемь параметров, а именно:

ARP Header
Operation code (1: for ARP request, 2: for ARP response)
Source IP address
Source MAC address
Destination IP address
Destination MAC address
Ethernet Header
Source MAC address
Destination MAC address
Ethernet Type (= 0x0806 for ARP message)

ARP не определяет никаких правил для поддержания согласованности между заголовком ARP и заголовком Ethernet. Это означает, что можно указать некоррелированные адреса между этими двумя заголовками. Например, MAC-адрес источника в заголовке Ethernet может отличаться от MAC-адреса источника в заголовке ARP.

2.1.2 ARP кэш

Каждый хост в сегменте LAN имеет таблицу, которая называется ARP-кеш, которая сопоставляет IP-адреса с соответствующими им MAC-адресами, как показано на рисунке ниже.



Существует два типа записей в кэше ARP, а именно: (1) статические записи: в зависимости от операционной системы (ОС) записи остаются в кэше ARP постоянно или до перезагрузки системы; и (2) динамические записи: записи остаются в кэше ARP в течение нескольких минут (в зависимости от ОС), а затем удаляются, если на них нет ссылок. К сожалению, механизм статических записей используется только в небольших локальных сетях. Однако в больших сетях развертывание и обновление статических записей в кэшах ARP не являются обычной практикой.

В принципе, в зависимости от операционной системы, сообщения запроса или ответа ARP позволяют нам создавать новые записи и обновлять существующие записи в кэше ARP. То есть, если запись не существует в кэше ARP, ответное сообщение ARP позволяет нам создать запись в кэше ARP. Кроме того, когда хост получает сообщение с запросом ARP, он полагает, что соединение будет выполнено. Следовательно, чтобы минимизировать трафик ARP, он создает новую запись в своем кэше ARP для адресов, предоставленных в сообщении запроса ARP. Если запись уже существует в кэше ARP, то сообщения запроса или ответа ARP разрешают ее обновление по адресам (исходным MAC-адресам и IP-адресам), указанным в заголовках ARP.

В этой главе рассматриваются три практических упражнения. Первый описывает технику отравления кэша ARP. Другие посвящены реализации атак DoS и MiM, соответственно, с использованием метода отравления кэша ARP.

Используются следующие аппаратные устройства и программные средства:

* Cisco switch*
* CommView tool†: Network monitor and analyzer tool (Sniffer)
* CommView Visual Packet Builder‡: A Graphical User Interface (GUI) based packet generator

2.2 Лабораторная работа 2.1: Атака отравление ARP кэша

2.2.1 Результат

Цель этого упражнения состоит в том, чтобы учащиеся узнали, как повредить кэши ARP хостов в локальной сети.

2.2.2 Описание

Атака с отравлением ARP-кеша является злонамеренным действием (со стороны хоста в локальной сети) введения ложного IP-адреса в сопоставление MAC-адреса в ARP-кэше другого хоста. Это может быть сделано путем прямого манипулирования кэшем ARP целевого хоста независимо от сообщений ARP, отправленных целевым хостом. Для этого злонамеренный хост может либо добавить новую поддельную запись в кэш ARP целевого хоста, либо обновить уже существующую запись поддельными IP-адресами и MAC-адресами. Эти два метода объясняются следующим образом:

1. **Создайте новую поддельную запись:** Для этого целевому хосту отправляется сообщение запроса ARP с поддельными IP-адресами источника и MAC-адресами в заголовке ARP. Когда целевой хост

* http://www.cisco.net
† http://www.tamos.com
‡ http://www.tamos.com

получает сообщение запроса ARP, он полагает, что соединение должно быть выполнено, и затем создает новую запись в своем кэше ARP, используя поддельные адреса источника (IP и / или MAC), предоставленные в ARP сообщения. заголовок.

2. **Обновите запись с поддельными адресами:** Для этого целевому хосту отправляется запрос ARP или ответное сообщение с поддельными IP-адресами и MAC-адресами. Таким образом, даже если запись уже существует в кэше ARP целевого хоста, она будет обновлена с использованием поддельных IP / MAC-адресов.

2.2.3 Обновление статического ARP кэша

Эффективный способ защиты кэша ARP от атак отравления состоит в использовании статических записей в кэше ARP. Записи не могут быть обновлены пакетами запросов и ответов ARP и не имеют срока действия, если они статичны. Однако это может обеспечить ложное чувство безопасности в некоторых ОС. Фактически, существуют ОС, которые отмечают статические записи в своих кэшах ARP, но авторизуют свои обновления с помощью пакетов запросов и ответов ARP. Следовательно, такие записи нельзя рассматривать как статические записи, а скорее как постоянные записи в кэшах ARP. Несколько распространенных ОС были протестированы на предмет повреждения их статических записей с помощью ARP-запросов и ответных сообщений. В качестве примеров ниже показано, что уязвимы только ARP-кэш Windows 2000 и SunOS Solaris 5.9. Следовательно, Windows 2000 и SunOS Solaris 5.9 не защищают злоумышленника от повреждения статических записей. Оставшиеся протестированные ОС предотвратили повреждение и обновление статических записей в кешах ARP. Поэтому в этих ОС статическая запись является постоянной и не может быть обновлена с помощью ARP-запросов и ответных сообщений.

Обновление статических записей в кэшах ARP с использованием сообщений запросов и ответов ARP

	Can an ARP request update a static entry in the ARP cache?	*Can an ARP response update a static entry in the ARP cache?*	*Status of the entry*
Windows 7 Home Premium	No	No	Permanent and static
Windows Vista	No	No	Permanent and static
Windows XP	No	No	Permanent and static
Windows Server 2003 Enterprise Edition	No	No	Permanent and static
Windows 2000	Yes	Yes	Permanent but **not static**
Ubuntu 8.10, Kernel 2.6.27-7 generic	No	No	Permanent and static
Red Hat Enterprise 7.2, Kernel 2.4.9-e.12	No	No	Permanent and static
Free BSD 5.0	No	No	Permanent and static
SunOS Solaris 5.9	Yes	Yes	Permanent but **not static**

В принципе, чтобы повредить записи в кэше ARP целевого хоста, вредоносный хост генерирует сообщения запроса или ответа ARP, включая поддельные IP и MAC-адреса.

Однако на практике успех этой вредоносной активности зависит от операционной системы целевого хоста. Вредоносный узел может попытаться отправить поддельные ответные сообщения ARP целевому узлу, даже если злонамеренный узел не получил никакого сообщения запроса ARP от целевого узла. Если ОС целевого хоста принимает поддельное ответное сообщение ARP от вредоносного хоста, не проверяя, было ли ранее сгенерировано сообщение запроса ARP, то полученное ответное сообщение ARP повредит кэш ARP целевого хоста. Однако новые ОС более устойчивы и не подвержены этой атаке. Альтернативно, злонамеренный хост может попытаться отправить сообщения запроса ARP вместо сообщений ответа ARP. В следующей таблице приведены результаты эксперимента, проведенного на нескольких распространенных ОС. Целью эксперимента было выявить, какие ОС с динамическими записями в кешах ARP были уязвимы для атаки отравления кешами ARP.

Обновление записей кэша ARP с использованием сообщений запросов и ответов ARP

Operating Systems	*Windows Vista*		*Windows 7 Home Premium*		*Windows XP*		*Windows Server 2003 Enterprise Edition*		*Windows 2000*	
Does the entry exist in the ARP cache?	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
ARP request	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ARP reply	✓	X	✓	X	✓	X	✓	X	✓	✓

Update of ARP Cache Entries Using ARP Request and Response Messages

Operating Systems	Mac OS X Version 10.7.3		Red Hat Enterprise 7.2, Kernel 2.4.9-e.12		Ubuntu 8.10, Kernel 2.6.27-7 generic		Free BSD 5.0		SunOS Solaris 5.9	
Does the entry exist in the ARP cache?	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No
ARP request	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
ARP response	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Примечание: ✓ = запрос или ответное сообщение ARP принимается системой и, следовательно, позволяет обновить или создать запись; и X = запрос или ответное сообщение ARP отклонено системой и, следовательно, не позволяет обновлять и создавать запись.

Предыдущая таблица четко указывает на то, что:

* Если запись уже существует в кэше ARP, все протестированные ОС разрешают ее обновление по ответу ARP (даже при отсутствии запроса ARP) или сообщениям запроса.
* Если запись не существует в кэше ARP, многие протестированные ОС не позволяют создавать новую запись с помощью ответного сообщения ARP. Однако все протестированные ОС допускают создание новой записи с помощью сообщения запроса ARP.

Поэтому, когда используются только ответные сообщения ARP, атаку с отравлением кэша ARP становится трудно реализовать для нескольких ОС, как показано в предыдущей таблице.

Тем не менее, остается возможность при использовании сообщений запроса ARP. В заключение, наиболее распространенные ОС по-прежнему уязвимы для атаки отравления кэшем ARP. Вредоносные пользователи могут использовать сообщения запроса ARP для создания или обновления поддельных записей MAC / IP в кэшах ARP своих целевых хостов. Кроме того, ARP-запрос или ответные сообщения могут использоваться для поддержания существования поддельных записей MAC / IP в кэшах ARP целевых хостов.

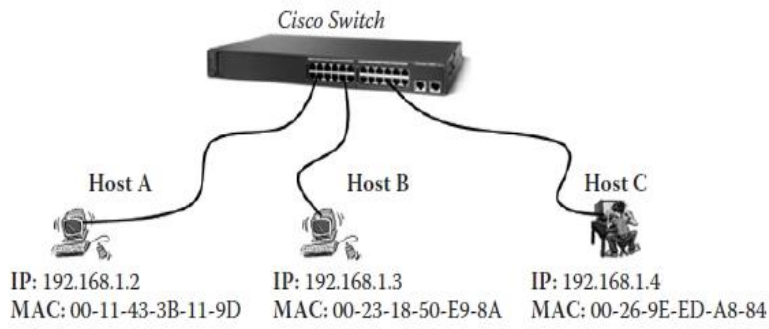
2.2.4 Эксперимент

Следующий эксперимент описывает, как повредить кэш ARP целевого хоста. Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2: Просмотр ARP-кэшей хостов.
Шаг 3: Создайте вредоносный пакет запроса ARP, чтобы повредить кэш ARP целевого хоста.

2.2.4.1 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке; три хоста подключены к коммутатору Cisco.

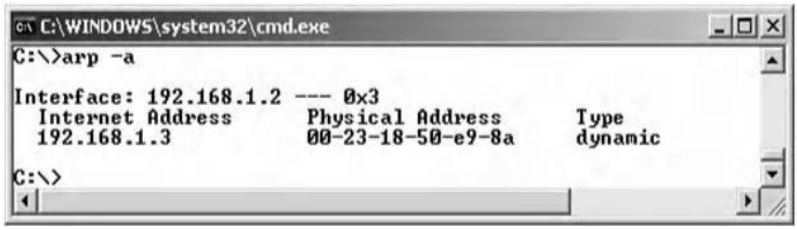


2.2.4.2 Шаг 1. Назначьте статические IP-адреса хостам сети.

Обратитесь к Главе 1.

2.2.4.3 Шаг 2: Просмотр ARP-кэшей хостов

Чтобы отобразить содержимое кэша ARP хоста, введите онлайн команду: «*C:> arp –a*». Например, на снимке экрана ниже показано содержимое кэша ARP хоста A (192.168.1.2).

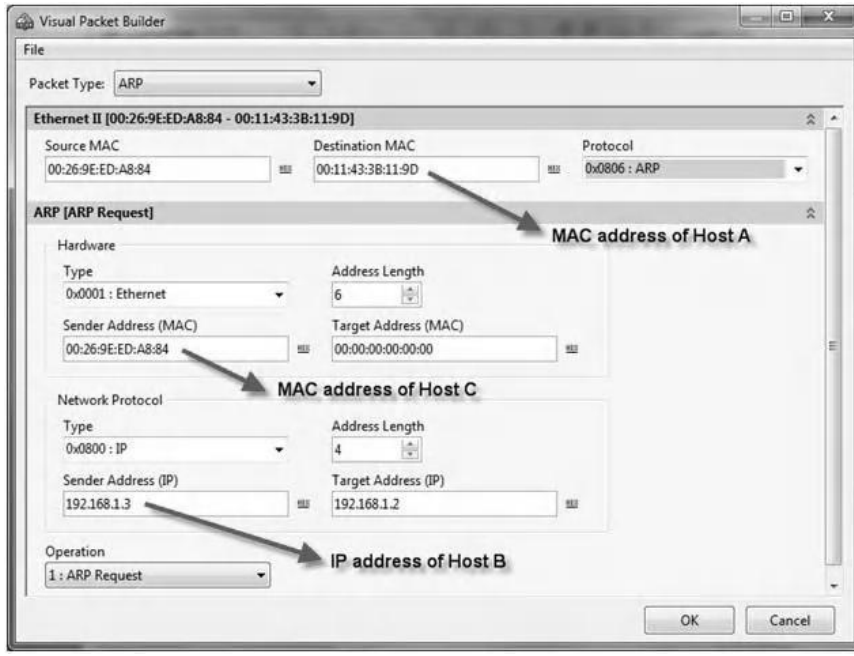


2.2.4.4 Создайте вредоносный пакет ARP-запросов, чтобы повредить кэш ARP целевого хоста

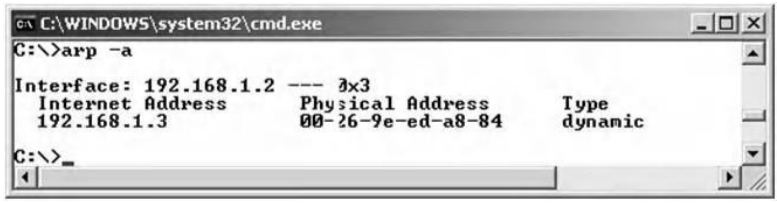
Мы предполагаем, что хост C хочет отравить кэш ARP хоста A, вставив следующую недопустимую запись: IP-адрес хоста B <-> MAC-адрес хоста C. Следовательно, хост C должен отправить хосту A следующий поддельный одноадресный ARP-запрос

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host B**
Source MAC address	**MAC address of Host C**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	Any MAC address
Destination MAC address	**MAC address of Host A**
Ethernet Type	0x0806 for ARP message

Используя любой инструмент построения пакетов, вышеуказанный поддельный ARP-запрос может быть легко создан. CommView Visual Packet Builder предоставляет очень удобный графический интерфейс для создания пакетов ARP. На следующем снимке экрана показано содержимое пакета поддельного одноадресного ARP-запроса, созданного для повреждения кэша ARP узла A.



После отправки вышеуказанного поддельного пакета ARP на хост A, кэш ARP хоста A будет поврежден из-за неверной записи, как показано ниже.



Следовательно, до тех пор, пока ARP-кэш узла A остается поврежденным, весь трафик, отправляемый узлом A на узел B, будет перенаправляться на узел C. Следующие два упражнения описывают атаки DoS и MiM, основанные на отравлении кэша ARP.

2.3 Лабораторная работа 2.2: DoS-атака на основе отравления ARP кэша

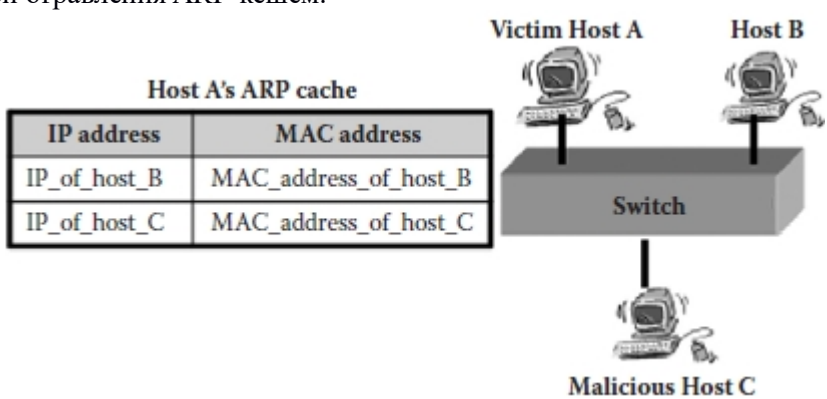
2.3.1 Результат

Цель этого практического упражнения - научить студентов выполнять DoS-атаку, основанную на методе отравления кэша ARP, в сети LAN.

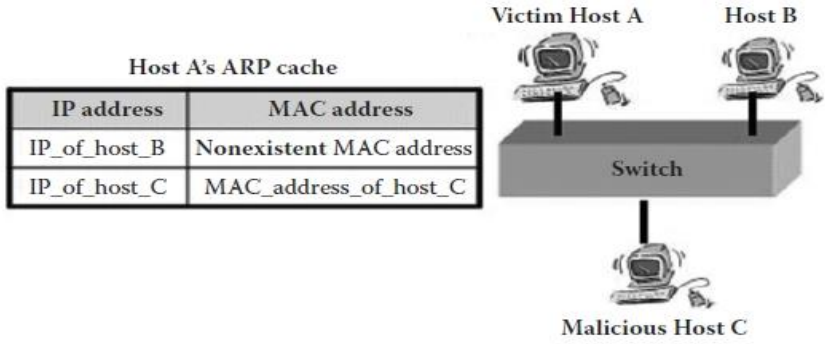
2.3.2 DoS-атака на основе отравления ARP кэша

DoS-атака, основанная на отравлении кэша ARP, состоит в том, чтобы не дать хосту-жертве связаться с одним или несколькими хостами в локальной сети. Во-первых, вредоносный хост повреждает кэш ARP хоста-жертвы, используя метод отравления кеша ARP (описанный в лабораторной работе 2.1). Таким образом, кэш ARP хоста жертвы обновляется поддельными записями (IP-адресом и MAC-адресом), что соответствует неверной ассоциации IP-адресов и несуществующих MAC-адресов. Позже, когда хост-жертва пытается отправить пакеты на хост, пакет будет отправлен на несуществующий хост, вызывая ситуацию атаки DoS. Следовательно, хост-жертва не сможет отправлять пакеты законному хосту-получателю.

На следующем рисунке показан ARP-кэш хоста A жертвы перед атакой отравления ARP-кешем.



А на следующем рисунке показан ARP-кэш хоста A после атаки отравления ARP-кешем.



Кэш содержит поддельную запись, соответствующую сопоставлению IP-адреса хоста B с несуществующим MAC-адресом. Следовательно, любой пакет, отправленный хосту B хостом A, будет перенаправлен на несуществующий хост. Это ситуация DoS, так как пакеты хоста A не могут достигнуть хоста B. Следовательно, хост A и хост B не могут обмениваться данными должным образом, пока не будет удалена поддельная запись в ARP-кэше хоста A. Это может быть сделано, когда узел A обновляет свое содержимое кэша ARP или обновляет его, когда получен законный запрос ARP или пакет ответа. Однако злонамеренный хост C может продолжать отправлять поддельный запрос ARP на хост A, и, следовательно, поддельная запись остается в кэше ARP, и ситуация с DoS сохранится.

Чтобы отравить кэш ARP хоста A, атакующий хост C должен отправить на хост жертвы A следующий поддельный пакет одноадресного ARP-запроса:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host B**
Source MAC address	**Nonexistent MAC address**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00

Ethernet Header	
Source MAC address	Any MAC address
Destination MAC address	**MAC address of Host A**
Ethernet Type	0x0806 for ARP message

2.3.3 Эксперимент

Этот эксперимент описывает, как практически выполнять DoS-атаки на основе метода отравления кэша ARP. В эксперименте используется та же сетевая архитектура, которая описана в лабораторной работе 2.1. Кроме того, мы предполагаем, что хост C является вредоносным хостом и планирует запретить хосту A (жертве) обмениваться данными с хостом B. Чтобы выполнить эту DoS-атаку, хосту C необходимо повредить кэш ARP хоста A, вставив фальшивый файл. запись в ARP-кэше хоста A. Поддельная запись - это IP-адрес хоста B, связанный с несуществующим MAC-адресом. Эксперимент состоит из следующих этапов:

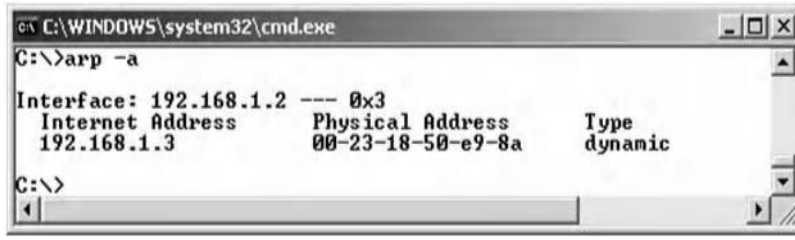
Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2. Просмотр ARP-кэша хоста A.
Шаг 3: Создайте вредоносный пакет ARP-запроса.
Шаг 4: Проверьте DoS-атаку.

2.3.3.1 Шаг 1. Назначьте статические IP-адреса хостам сети

Обратитесь к Главе 1.

2.3.3.2 Шаг 2. Просмотр ARP-кэша хоста A

На следующем снимке экрана показано содержимое кэша ARP узла A до атаки отравления кэшем ARP.

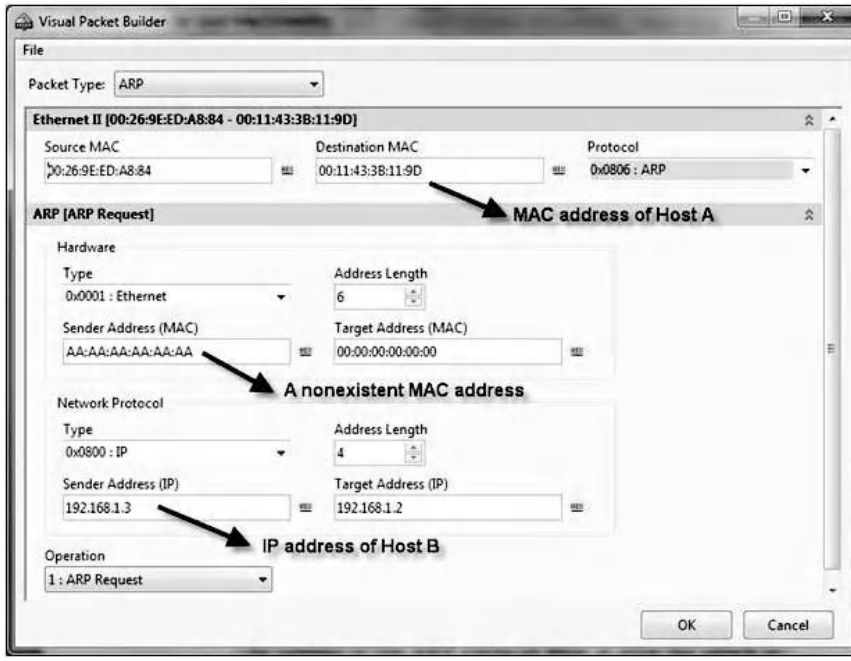


2.3.3.3 2. Шаг 3. Создайте пакет запроса вредоносного ARP

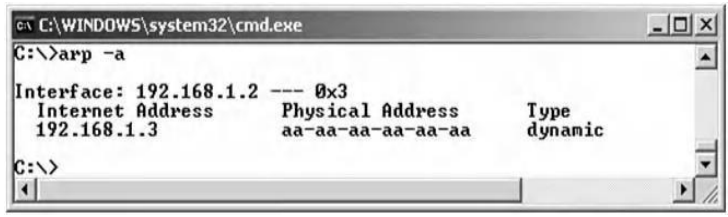
Вредоносный пакет ARP, выпущенный с хоста C, намерен испортить кэш ARP хоста A. Поля заголовков вредоносного пакета запроса ARP устанавливаются следующим образом:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host B**
Source MAC address	**AA:AA:AA:AA:AA:AA (Nonexistent fake MAC address)**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	Any MAC address
Destination MAC address	**MAC address of Host A**
Ethernet Type	0x0806 for ARP message

CommView Visual Packet Builder используется для создания вредоносного пакета одноадресного ARP-запроса для повреждения кэша ARP узла A. На следующем снимке экрана показано содержимое вредоносного пакета одноадресного ARP-запроса.



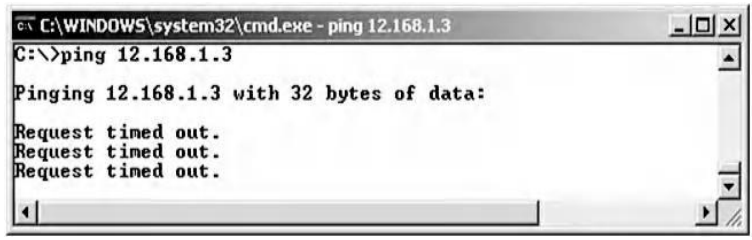
На следующем снимке экрана показано поврежденное содержимое кэша ARP узла A после атаки.



2.3.3.4 Шаг 4: Проведите DoS-атаку

Чтобы провести DoS-атаку, хост A пингует хост B из командного окна MS-DOS (*C: \> ping 192.168.1.3*). На следующем снимке экрана четко видно, что узел A не получает никакого ответа Ping от узла B. Это не потому, что узел B не подключен к сети или отклоняет запросы Ping от узла A с помощью брандмауэра. Скорее, это связано с тем, что кэш ARP хоста A поврежден, и запрос Ping

(эхо-пакет ICMP) не достиг хоста B для генерации ответа Ping (пакет ответа ICMP). Запрос Ping был отправлен на несуществующий хост, чей MAC-адрес является «aa-aa-aa-aa-aa-aa». Следовательно, узел B не генерирует ответный пакет ICMP.



2.4 Лабораторная работа 2.3: MiM-атака на основе отравления ARP Cache

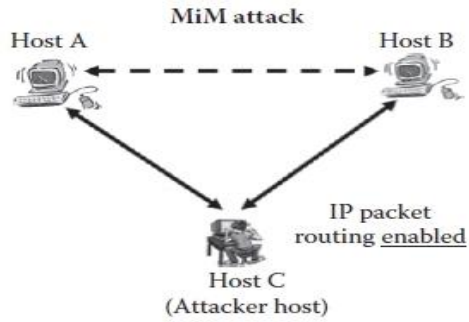
2.4.1 Результат

Цель этого практического упражнения состоит в том, чтобы студенты научились выполнять MiM-атаку в локальной сети на основе метода отравления кэша ARP.

2.4.2 MiM-атака на основе отравления ARP-кэша

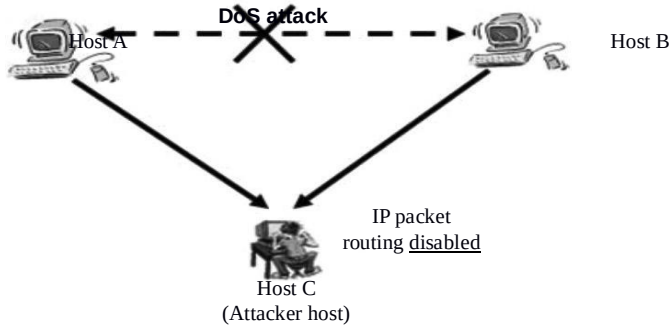
Атака MiM является распространенным методом, используемым для прослушивания сетевого трафика в коммутируемых локальных сетях, и основана на поддельных сообщениях ARP. Эта атака состоит в перенаправлении (перенаправлении) сетевого трафика между двумя целевыми узлами на вредоносный узел. Затем злонамеренный хост перенаправит полученные пакеты в исходное место назначения, так что связь между двумя целевыми хостами не будет прервана, и пользователи двух хостов не заметят, что их трафик прослушивается злоумышленником.

При такого рода атаках злонамеренный пользователь сначала включает маршрутизацию IP-пакетов своего хоста, чтобы действовать в качестве маршрутизатора и иметь возможность пересылать перенаправленные пакеты, как показано на следующем рисунке.



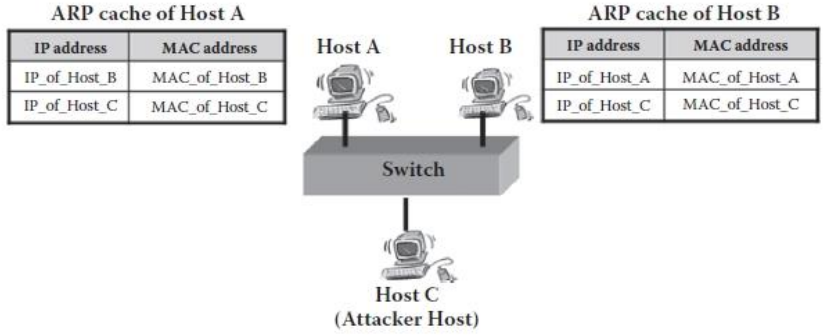
Затем, используя технику отравления кэша ARP, злонамеренный пользователь повреждает кэши ARP двух целевых хостов, чтобы заставить два хоста переслать все свои пакеты вредоносному хосту. Это чрезвычайно эффективно, если учесть, что могут быть отравлены не только хосты, но и маршрутизаторы / шлюзы. Весь интернет-трафик для хоста может быть перехвачен с помощью атаки MiM на хост и маршрутизатор локальной сети.

Важно отметить, что если злонамеренный хост повреждает кэши ARP двух целевых хостов, не включив свою маршрутизацию IP-пакетов, то эти два хоста не смогут обмениваться пакетами, и это будет ситуация атаки DoS, как показано в следующая цифра В этом случае злонамеренный хост не пересылает полученные пакеты их законным адресатам.

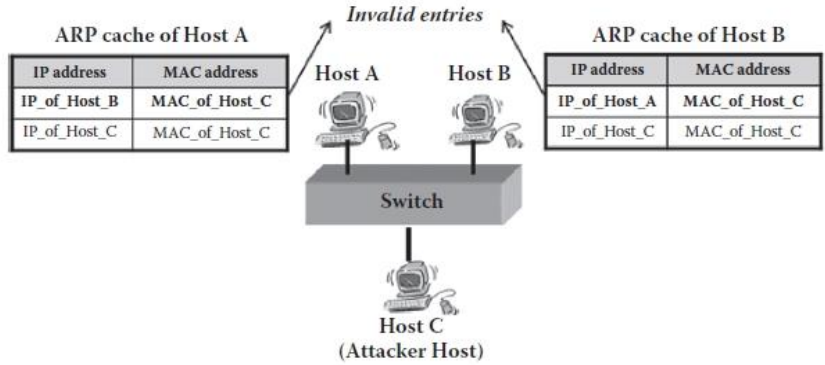


Атака MiM, как показано выше (то есть второй предыдущий рисунок), где хост С является вредоносным хостом, а хосты А и В являются двумя целевыми хостами, выполняется следующим образом. Во-первых, Host C включает маршрутизацию своих IP-пакетов,

а затем разрушает кэши ARP хостов A и B, используя метод отравления кэша ARP. На рисунке ниже показаны начальные записи в кэшах ARP хостов A и B до атаки отравления кешем ARP.



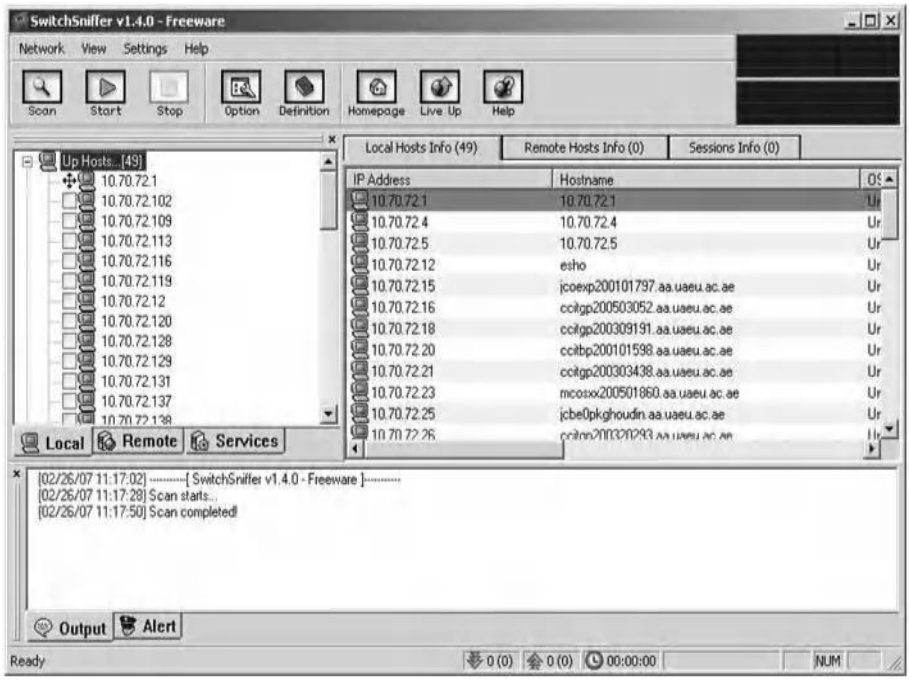
После атаки на следующем рисунке показаны недопустимые записи в кэшах ARP хостов A и B.



То есть хост A связывает IP-адрес хоста B с MAC-адресом хоста C, а хост B связывает IP-адрес хоста A с MAC-адресом хоста C. Следовательно, все пакеты, отправленные хостом A на хост B, сначала будут отправлены на хост C. Затем хост C перенаправит их на хост B, так как маршрутизация IP-пакетов на хосте C включена. Точно так же все пакеты, отправленные хостом B хосту A, сначала будут отправлены хосту C; затем узел C перенаправляет их на узел A.

Существует множество простых в использовании инструментов, которые позволяют проводить атаку MiM, используя в основном описанную выше технику. Примерами таких инструментов являются *ARP Spoof Tool, Winarp_mim, SwitchSniffer, WinArpSpoof, WinArpAttacker и Cain & Abel*. Однако, используя эти готовые к использованию инструменты, студенты не смогут узнать, как практически выполняется атака MiM. Таким образом, только для образовательных целей в приведенном ниже эксперименте описываются действия по выполнению атаки MiM.

В качестве примера на следующем снимке экрана представлен снимок экрана с графическим интерфейсом инструмента *SwitchSniffer*. Пользователь сначала сканирует LAN, чтобы определить подключенные узлы, а затем просто выбирает целевые узлы. Затем инструмент повредит кэши ARP выбранных целевых хостов, что позволит пользователю прослушивать их трафик.



2.4.3 Эксперимент

В следующем эксперименте описывается, как практически выполнить атаку MiM с использованием метода отравления кэша ARP. В эксперименте используется та же сетевая архитектура которая описана

в лабораторной работе 2.1. Кроме того, мы предполагаем, что хост C является вредоносным хостом и намеревается перехватить трафик, которым обмениваются хост A и хост B, используя атаку MiM. Чтобы выполнить эту атаку с прослушиванием, хосту C необходимо повредить кэши ARP хостов A и B, вставив поддельные записи в их кэши ARP.

Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2. Включите IP-маршрутизацию на хосте C.
Шаг 3: Просмотр ARP-кэшей хостов A и B.
Шаг 4: Создайте два вредоносных пакета запроса ARP.
Шаг 5: Проверьте атаку MiM.
Шаг 6: Сниффим и анализируем трафик между хостами A и B.

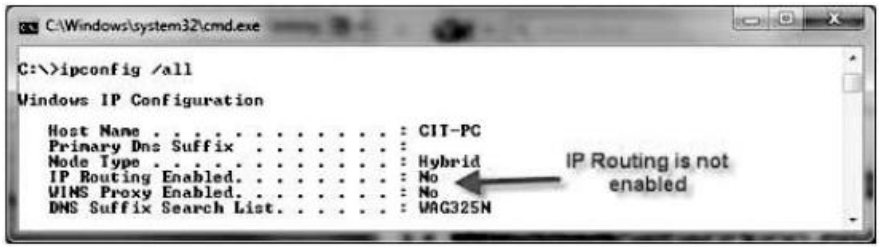
2.4.3.1 Шаг 1. Назначьте статические IP-адреса хостам сети

Обратитесь к Главе 1.

2.4.3.2 Шаг 2. Включите IP-маршрутизацию на хосте C

По умолчанию IP-маршрутизация отключена. Вредоносный узел C должен включить маршрутизацию IP-пакетов, чтобы действовать в качестве маршрутизатора и иметь возможность пересылать перенаправленные IP-пакеты, которые он получает.

Команда «*C:>ipconfig/all*» позволяет проверить, включена ли IP-маршрутизация на хосте. На следующем снимке экрана показано, что IP-маршрутизация отключена на хосте C.

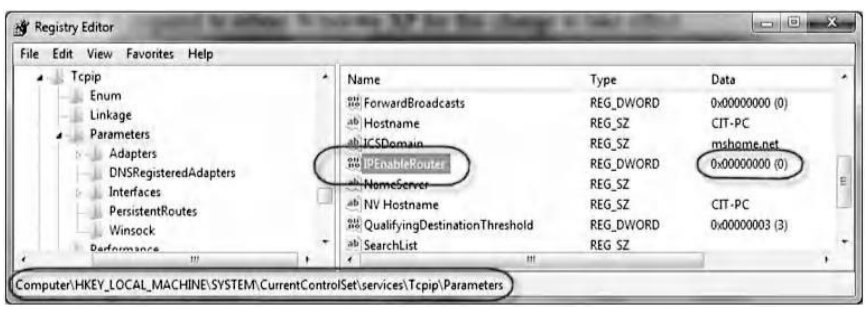


Мы предполагаем, что хост C работает под управлением Windows XP или Windows 7. Чтобы включить IP-маршрутизацию, необходимо изменить значение системной регистрации, связанной с IP-маршрутизацией, следующим образом:

1. В меню «Пуск» (Start) выберите «Выполнить» (Run).
2. Введите regedt32.exe или regedit.exe и нажмите кнопку OK.
3. В редакторе реестра перейдите к:

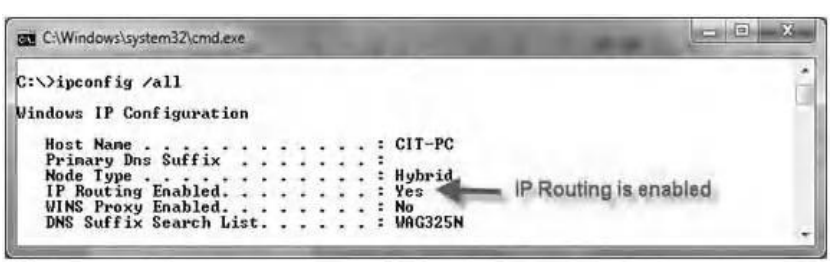
```
HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\
Services\Tcpip \Parameters
```

4. Выберите запись «*IPEnableRouter*» (см. следующий снимок экрана для включения IP-маршрутизации в Windows XP или Windows 7).



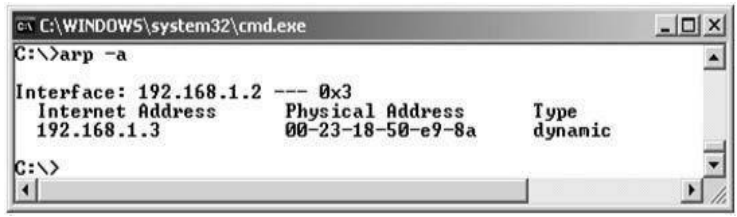
5. Чтобы включить IP-маршрутизацию, присвойте значение 1 записи «*IPEnableRouter*».
6. Закройте редактор реестра.

Необходимо перезагрузить Хост C, чтобы это изменение вступило в силу. Следующий снимок экрана показывает, что IP-маршрутизация включена на хосте C.



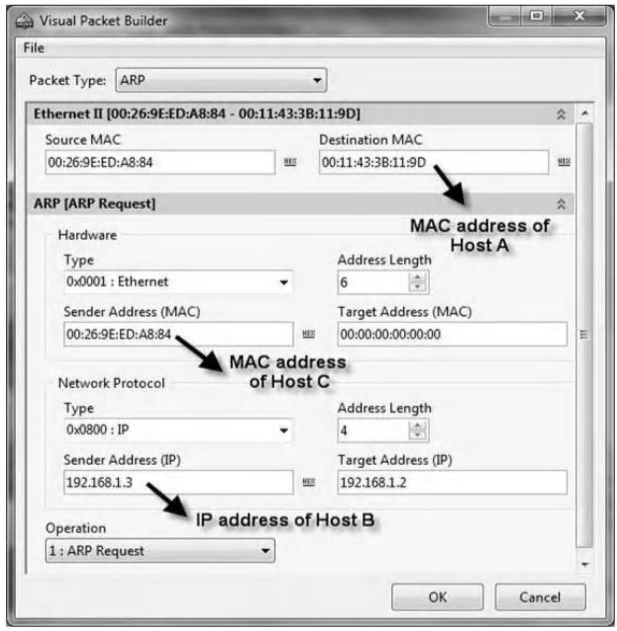
2.4.3.3 Шаг 3. Просмотр ARP-кэшей хоста A и хоста B

С хоста A, пинг хоста B и наоборот; затем просмотрите их кэши ARP. Например, на следующем снимке экрана показано содержимое ARP-кэша хоста A.

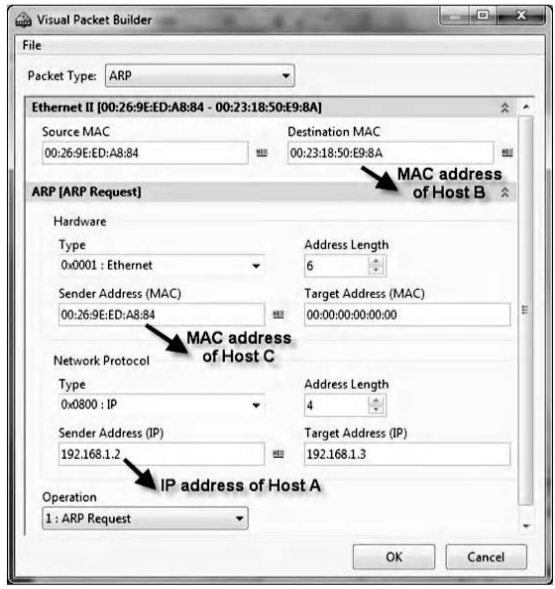


2.4.3.4 Шаг 4: Создайте два вредоносных пакета запроса ARP

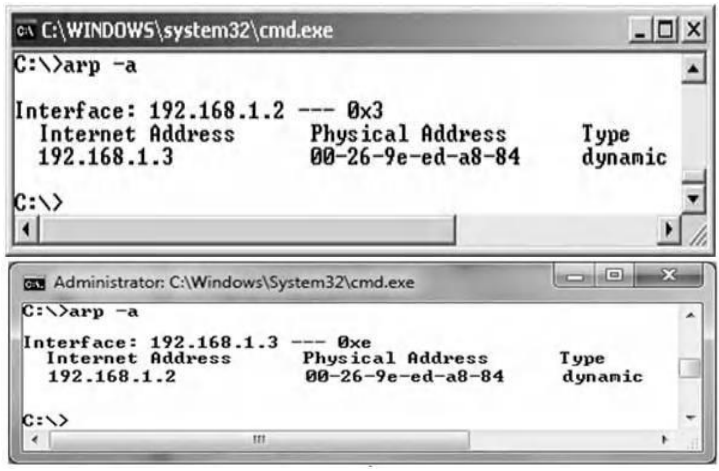
Чтобы отравить кэши ARP хоста A и хоста B, с помощью CommView Visual Packet Builder создаются два поддельных пакета одноадресных ARP-запросов. Сначала узел C отправляет поддельный пакет ARP-запроса одноадресной передачи на узел A, чтобы повредить его кэш ARP (как показано на следующем снимке экрана).



Затем узел C отправляет другой поддельный пакет запроса ARP одноадресной передачи узлу B, чтобы повредить его кэш ARP (см. Снимок экрана ниже).



На следующих снимках экрана показаны поврежденные кэши ARP хостов A (верхний экран) и B (нижний экран), соответственно, после отправки двух вышеупомянутых поддельных пакетов одноадресного ARP-запроса.

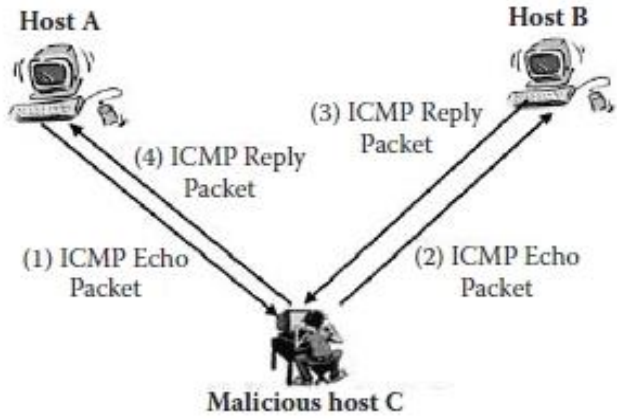


2.4.3.5 Проведите атаку MiM

Если предыдущие шаги выполнены правильно, то, когда хост A пингует хост B, хост A обычно получает ответ эхо-запроса от хоста B (ответное сообщение ICMP). Однако трафик, которым обмениваются хосты A и B, сначала перенаправляется на хост C, а затем отправляется в его законный пункт назначения, и все это без их ведома. Это связано с тем, что кэши ARP хостов A и B повреждены.

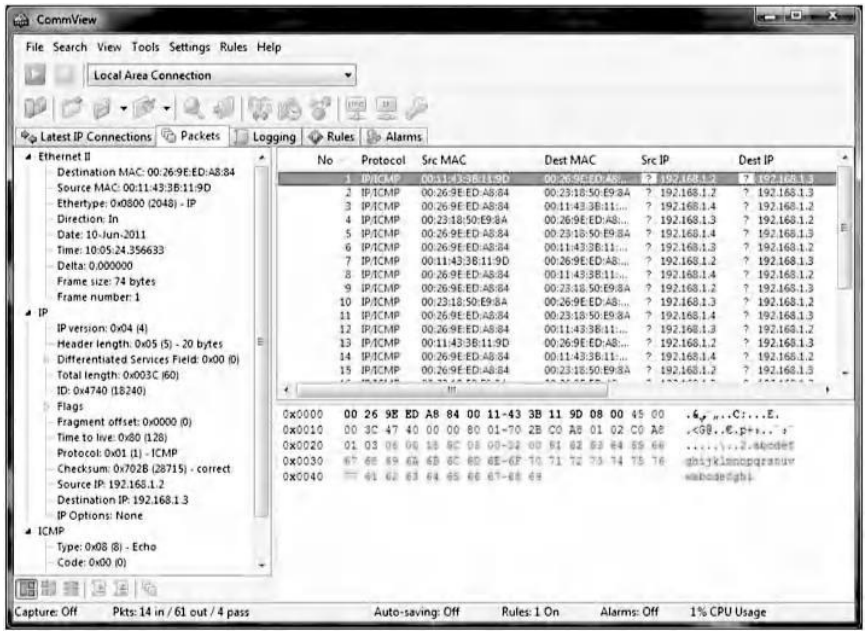
2.4.3.6 Сниффим и анализируем трафик между хостами A и B

Обычно, когда узел A проверяет связь с узлом B, эхо-пакет ICMP отправляется узлом A на узел B. Затем узел B отвечает, отправляя узлу A ответный пакет ICMP. Следовательно, два пакета обмениваются. Однако в атаке MiM, описанной в этом практическом упражнении, происходит обмен четырьмя пакетами. То есть первый пакет - это эхо-пакет ICMP, отправленный хостом A на хост C. Второй пакет - это эхо-пакет ICMP, пересланный хостом C на хост B. Третий пакет - это ответный пакет ICMP, отправленный хостом B на хост C Четвертый пакет - это ответный пакет ICMP, пересылаемый хостом C хосту A, как показано на следующем рисунке.

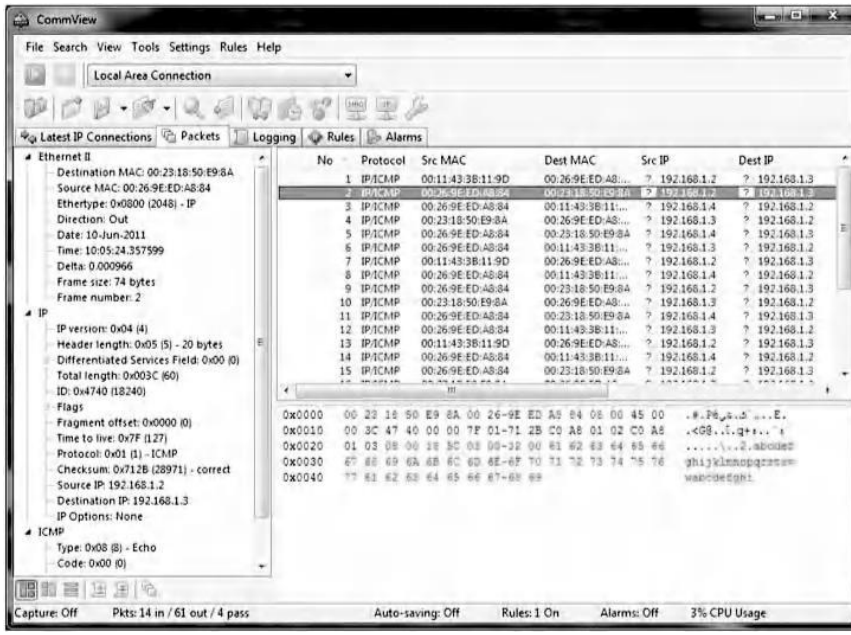


На хосте C сниффер *CommView* используется для захвата четырех обмененных пакетов. Анализ MAC-адресов источника и назначения четырех захваченных пакетов ясно показывает, что обмененный трафик ping между хостом A и хостом B был перенаправлен на хост C.

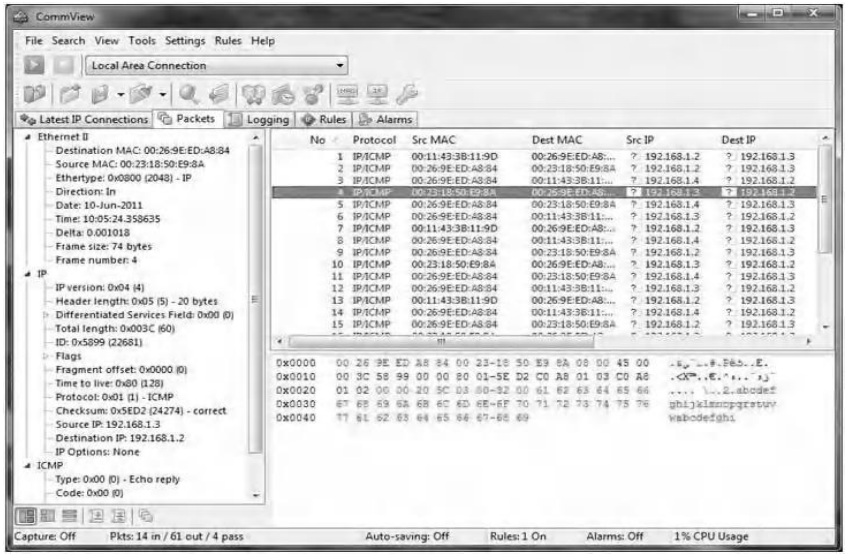
На следующем снимке экрана показано, что эхо-пакет ICMP (Packet # 1) был отправлен хостом A на хост C, хотя IP-адресом пакета является IP-адрес хоста B.



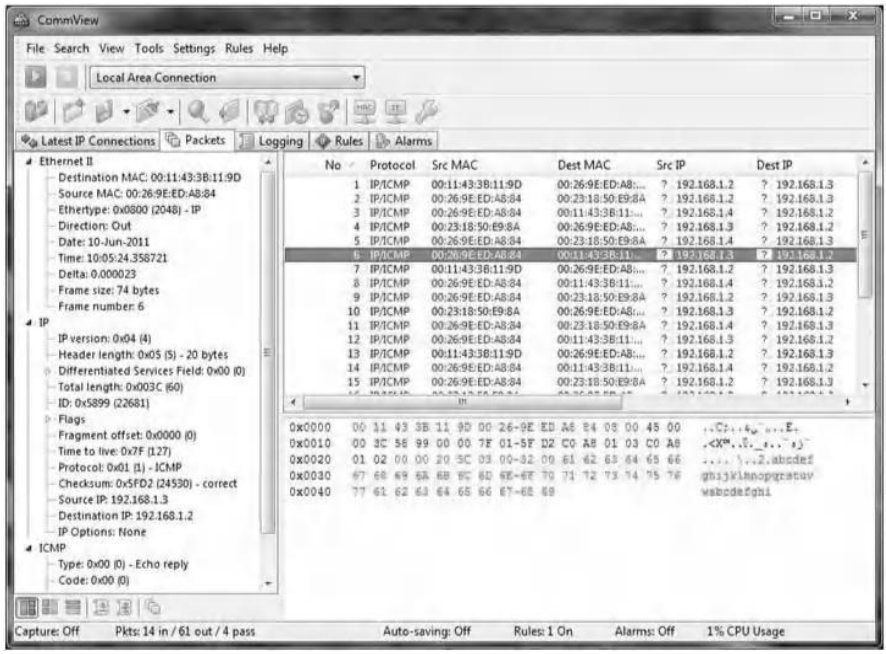
На следующем снимке экрана показано, что эхо-пакет ICMP (Packet # 2) был перенаправлен хостом C на хост B, хотя IP-адрес источника пакета является IP-адресом хоста A.



И на следующем снимке экрана показано, что ответный пакет ICMP (Packet # 4) был отправлен хостом B на хост C, хотя IP-адресом пакета является IP-адрес хоста A.



Ниже приведен снимок экрана, показывающий, что ответный пакет ICMP (Packet#6) был переслан хостом C на хост A, хотя исходный IP-адрес пакета является IP-адресом хоста B.



2.5 Резюме главы

В этой главе обсуждалось создание DoS- и MiM-атак на основе метода отравления кэша ARP. DoS-атака не позволяет хосту-жертве обмениваться данными с одним или несколькими хостами в локальной сети. Атака MiM использовалась для перехвата сетевого трафика между хостами в коммутируемой локальной сети. Студенты узнали, как выполнять атаки DoS и MiM на основе технологии отладки кэша ARP в коммутируемых локальных сетях.

Глава 3

Обнаружение и предотвращение аномального трафика ARP

3.1 Введение

Пакеты ненормального ARP (Address Resolution Protocol) обычно вводятся в сеть для повреждения кэшей ARP целевых хостов. Атака отравления ARP, описанная в главе 2, является примером атак, которые используют ненормальные пакеты ARP для прослушивания и манипулирования данными, проходящими через локальную сеть (Local Area Network). Аномальные атаки на основе пакетов ARP представляют особый интерес, поскольку они являются высоко намеренными и обычно инициируются, поддерживаются и контролируются людьми. Эти атаки могут выполняться новичками с использованием широко доступных и простых в использовании инструментов, специально разработанных для этой цели. Более опытные пользователи со злым умыслом могут использовать генераторы пакетов для создания ненормальных пакетов ARP для выполнения атак. Из-за высокой актуальности этой проблемы несколько решений для обеспечения безопасности, начиная от дорогостоящих коммутаторов ЛВС, аппаратных и программных средств обнаружения

и предотвращения вторжений (IDS / IPS) и заканчивая устройствами Unified Threat Management (UTM *), которые объединяют механизмы для управления ими с ненормальным трафиком ARP.

Эта глава сначала оценивает общие решения безопасности относительно их способности обнаруживать и предотвращать ненормальный трафик ARP. Затем в главе описываются три практических занятия. Первая практическая лаборатория (Lab 3.1) посвящена обнаружению аномального трафика ARP с использованием XArp 2. Вторая практическая лаборатория (Lab 3.2) посвящена предотвращению аномального ARP-трафика с использованием функции безопасности Dynamic ARP Inspection (DAI). реализованого на коммутаторе Cisco Catalyst 3560 для среды без DHCP. Третья практическая работа (лабораторная работа 3.3) посвящена предотвращению ненормального трафика ARP с использованием функций безопасности Dynamic ARP Inspection (DAI) и DHCP Snooping, реализованных на коммутаторе Cisco Catalyst 3560 для среды DHCP.

В практических упражнениях используются следующие аппаратные устройства и программные средства:

* Cisco Catalyst 3650 Switch†
* XArp 2‡: Abnormal ARP traffic detection tool
* CommView Visual Packet Builder§: A Graphical User Interface (GUI) based packet generator
* DHCP Turbo¶: a DHCP server tool

3.2 Аномальные пакеты ARP

Существуют различные типы ненормальных пакетов ARP. Некоторые пакеты вредны и представляют очень серьезную угрозу. Другие не так вредны, но могут иметь скрытый контент, который является частью потенциальной вредоносной деятельности. Было идентифицированно

* UTM (Unified Threat Management): используется для описания устройства безопасности, имеющего множество функций в одном блоке, включая брандмауэр, систему IDS или IPS, фильтрацию спама в электронной почте, антивирусную защиту и фильтрацию содержимого в World Wide Web.

† http://www.cisco.com

‡ http://www.chrismc.de § http://www.tamos.com

¶ http://www.weird-solutions.com

четыре возможных типа аномальных пакетов запроса ARP и шесть возможных типов аномальных пакетов ответа ARP. В таблицах 3.1 и 3.2 перечислены идентифицированные типы аномальных пакетов запросов и ответов ARP соответственно. Детали заключаются в следующем.

P#1, P#5, и P#7: Устройства безопасности должны отслеживать сопоставления адресов IP-to-MAC (Internet Protocol-to-Media Access Control). Каждый пакет ARP содержит сопоставление адреса IP-MAC. Пакет запроса ARP содержит сопоставление IP-MAC отправителя. Пакет ответа ARP содержит сопоставление IP-MAC разрешенного компьютера. Каждое отображение вставляется в базу данных. Если отслеживаемое сопоставление нарушает текущие сопоставления, должно быть сгенерировано предупреждение. База данных сопоставлений IP-MAC-адресов может быть заполнена автоматически или вручную.

P#2, P#6, и P#8: Пакеты ARP имеют особые ограничения. В пакете запроса и ответа ARP MAC-адрес источника Ethernet должен соответствовать MAC-адресу источника ARP. В ответе ARP MAC-адрес назначения Ethernet должен совпадать с MAC-адресом назначения ARP.

P#3: Обычный ARP-запрос должен быть отправлен на широковещательный MAC-адрес, а не на одноадресный MAC-адрес. Такие пакеты используются программным обеспечением отравления ARP для атаки только на конкретную машину, а не на все машины в локальной сети.

P#9: Обычный ответный пакет ARP должен быть отправлен на одноадресный MAC-адрес, а не на широковещательный MAC-адрес. Такие пакеты используются программным обеспечением отравления ARP для атаки на все машины в локальной сети.

P#4 и P#10: В пакете ARP есть поля, которые имеют ограничения относительно значений, которые они могут принять. Эти значения должны быть проверены на правильность. Отображения ARP могут не содержать определенные IP-адреса. К ним относятся широковещательная и многоадресная рассылка, а также нулевые адреса.

Таблица 3.1 Список возможных ненормальных пакетов запросов ARP

Packet Identifier	*P#1*	*P#2*	*P#3 (Unicast ARP request)*	*P#4 (Unexpected IP or MAC address in ARP request packets)*
ARP Header				
ARP Operation	Request	Request	Request	Request
Source IP	IP address of a host A	IP address of a host A		0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Source MAC	MAC address of a non-existent host	MAC address of a host A		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination IP				0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Destination MAC				
Ethernet Header				
Source MAC		MAC address of a nonexistent host		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast MAC
Destination MAC			Unicast	00-00-00-00-00-00 Unicast or Multicast
Does the packet corrupt the ARP cache?	Yes	No	No	No

Таблица 3.2 Список возможных неправильных пакетов ответа ARP (продолжение)

Packet Identifier	*P#5*	*P#6*	*P#7*	*P#8*	*P#9 (Broadcast ARP reply)*	*P#10 (Unexpected IP or MAC address)*
ARP Header						
Operation	Reply	Reply	Reply	Reply	Reply	Reply
Source IP	IP address of a host A	IP address of a host A				0.0.0.0 255.255.255.255 Multicast Not in the network subnet
Source MAC	MAC address of a nonexistent host	MAC address of a host A				00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination IP			IP_B	IP_B		0.0.0.0 255.255.255.255 Multicast Not in the network subnet

Таблица 3.2 Список возможных неправильных пакетов ответа ARP (продолжение)

Packet Identifier	*P#5*	*P#6*	*P#7*	*P#8*	*P#9 (Broadcast ARP reply)*	*P#10 (Unexpected IP or MAC address)*
ARP Header						
Destination MAC			MAC address of a nonexistent host	MAC address of a host B		00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Ethernet Header						
Source MAC		MAC address of a nonexistent host				00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Destination MAC				MAC address of a nonexistent host	ff-ff-ff-ff-ff-ff	00-00-00-00-00-00 ff-ff-ff-ff-ff-ff Multicast
Does the packet corrupt the ARP cache?	Yes	No	No	No	No	No

Некоторые MAC-адреса в пакетах ARP очень подозрительны. Например, никакое сопоставление IP-MAC не должно иметь назначенного широковещательного, многоадресного или нулевого адреса MAC. IP-адреса каждого пакета ARP должны находиться в одной подсети. Пакеты ARP с IP-адресами, которые не принадлежат подсети сетевых интерфейсов, являются подозрительными и должны быть предупреждены.

Таблицы 3.1 и 3.2 показывают, что только ненормальные пакеты P # 1 и P # 5 могут повреждать кэши ARP целевых хостов с поддельными записями IP-MAC. Оставшиеся ненормальные пакеты ARP не повреждают кэши ARP. Однако они все еще могут быть вредными и скрывать потенциальную атаку, такую как DoS (отказ в обслуживании). Следовательно, необходимость реализации эффективных решений безопасности, способных обнаруживать все виды ненормальных пакетов ARP, становится необходимостью.

3.3 Эксперимент

Эксперименты были проведены широко, чтобы оценить эффективность общих решений безопасности в обнаружении и предотвращении аномального трафика ARP. Выбранные решения безопасности подразделяются на четыре категории, а именно:

* Коммутаторы локальной сети
  — Cisco Switch 3560 Series
  — Juniper Switches EX3200
  * Серия программного обеспечения IDS / IPS
  — Snort IDS
  — XArp 2
  — Sax2 NIDS
* Аппаратные средства DS / IPS
  — Cisco IPS 4255 Series
  — TopLayer Model 5000
  — IBM ISS Proventia Model GX4004C
  — SourceFire
  — TippingPoint 50

* Устройства унифицированного управления угрозами (UTM)
  — Juniper Netscreen 50

Таблица 3.3 показывает решения безопасности, которые включают механизмы проверки ARP, независимо от типа проверки.

В последующих экспериментах устройство «IPS TippingPoint 50» исключается, поскольку оно включает проверку ARP, которая не связана с обнаружением действий по отравлению кэша ARP. Устройство использует три подписи ARP, чтобы проверить, содержат ли поля «Тип оборудования» и «Тип протокола» в заголовке Ethernet допустимые значения.

Среди решений безопасности, которые включают механизмы проверки ARP (таблица 3.3), в таблице 3.4 показаны те, которые могут полностью или частично обнаружить ненормальные пакеты ARP, перечисленные в таблицах 3.1 и 3.2. Используя данные, представленные в таблице 3.4, становится очевидным, что ни одна система не предлагает идеального решения для обнаружения отравления ARP. Из протестированных систем XArp 2 является идеальным с точки зрения количества обнаруженных ненормальных пакетов ARP. Snort IDS является хорошей альтернативой, но оба они выполняют только обнаружение и не способны предотвратить ARI-атаки. Системы предотвращения или блокировки, такие как коммутаторы Cisco серии 3560 или Juniper Switch серии EX3200, являются наиболее амбициозными, но обычно требуют сложных процедур установки. Кроме того, высокая стоимость этих коммутаторов делает это решение недоступным для многих компаний. Cisco IPS является системой предотвращения и является ограниченным альтернативным решением, поскольку он может работать с несколькими типами ненормальных пакетов ARP (P # 1 и P # 5). Тем не менее, важно помнить, что пакеты P # 1 и P # 5 являются наиболее используемыми пакетами ARP во время атаки отравления кэшем ARP, поскольку они являются единственными пакетами, которые могут повредить кэши ARP целевых хостов.

Sax2 NIDS не может обнаружить какой-либо ненормальный пакет, описанный в таблицах 3.1 и 3.2. Однако он может обнаруживать штормовой трафик ARP-запросов и трафик сканирования ARP. Этот тип трафика атаки использует обычные пакеты ARP.

Талица 3.3 Решения безопасности, выполняющие ARP Inspection

	Type	*Performing ARP Inspection? (Yes or No)*	*Detection or Prevention Solution?*
Cisco 3560 Switch Series	Switch	Yes	Prevention
Juniper Switches EX3200 Series	Switch	Yes	Prevention
Snort IDS	IDS software tool	Yes	Detection
XArp 2	IDS software tool	Yes	Detection
Sax2 NIDS	IDS software tool	Yes	Detection
Cisco IPS 4425 Series	IPS appliance	Yes	Detection
TopLayer Model 5000	IPS appliance	No	Detection
IBM ISS Proventia			
Model GX4004C	IPS appliance	No	Detection
SourceFire	IPS appliance	No	Detection
TippingPoint 50	IPS appliance	Yes	Detection
Juniper Netscreen 50	UTM	No	Detection

В таблице 3.4 «частично обнаруженный» означает, что устройство обнаруживает все или некоторые пакеты запроса или ответа ARP, которые имеют неожиданные IP-адреса и / или MAC-адреса источника или назначения.

Таблица 3.4 Обнаружение неправильных пакетов ARP запросов и ответов

	P#1	*P#2*	*P#3*	*P#4*	*P#5*	*P#6*	*P#7*	*P#8*	*P#9*	*P#10*
Cisco 3560 Switch Series	Detected	Detected	Not detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
Juniper Switches EX3200 Series	Detected	Detected	Not detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
Snort IDS	Detected	Detected	Detected	Not detected	Detected	Detected	Detected	Detected	Not detected	Not detected
XArp 2 tool	Detected	Detected	Detected	Partially detected	Detected	Detected	Detected	Detected	Detected	Partially detected
Sax2 NIDS	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected	Not detected
Cisco IPS Series 4255	Detected	Not detected	Not detected	Partially detected	Detected	Not detected	Detected	Not detected	Not detected	Partially detected

3.3.1 Межуровневая проверка ARP

Для обнаружения ненормальных пакетов ARP P#2, P#6 и P#8, описанных в таблицах 3.1 и 3.2, механизм проверки ARP должен иметь возможность выполнять межуровневую проверку ARP между заголовками Ethernet и ARP. В пакетах запросов и ответов ARP MAC-адрес источника Ethernet должен совпадать с MAC-адресом источника ARP. Однако в ответном пакете ARP MAC-адрес назначения Ethernet должен совпадать с MAC-адресом назначения ARP. В таблице 3.5 перечислены решения безопасности, которые включают межуровневые механизмы проверки ARP.

3.3.2 Проверка состояния ARP

Ответы ARP должны обычно следовать за запросами ARP. Процесс обнаружения с полным состоянием должен запоминать все запросы ARP и сопоставлять их с ответами ARP. Многие инструменты отравления ARP отправляют ответы ARP, которые не запрашиваются. В таблице 3.6 приведен список решений безопасности, которые выполняют проверки состояния ARP для запросов ARP на ответы ARP. Механизмы проверки ARP могут выдавать ложные отчеты об обнаружении в некоторых случаях, так как машины хотят распространять свое сопоставление IP-MAC-адресов на другие машины.

Таблица 3.5 Решения безопасности, выполняющие межуровневую проверку ARP

	Performing Cross-Layers ARP Inspections?
Cisco Catalyst 3560 Switch Series	Yes
Juniper Switches EX3200 Series	Yes
Snort IDS	Yes
XArp 2	Yes
Sax2 NIDS	No
Cisco IPS 4425 Series	No

Таблица 3.6 Решения безопасности, выполняющие проверку ARP

	Performing ARP Stateful Inspections?
Cisco Catalyst 3560 Switch Series	No
Juniper Switches EX3200 Series	No
Snort IDS	No
XArp 2	Yes
Sax2 NIDS	Yes
Cisco IPS 4425 Series	No

Среди вышеупомянутых проверенных решений безопасности инструмент XArp 2 и Sax2 IDS являются единственными решениями, которые выполняют проверку состояния ARP.

3.3.3 Штурм ARP запросами и ARP сканирование

3.3.3.1 Штурм ARP запросами

Динамические записи ARP остаются в кэше ARP в течение нескольких минут, а затем удаляются, если на них нет ссылок. Следовательно, чтобы сохранить кэш ARP целевого хоста поврежденным поддельными записями, злонамеренные пользователи могут штурмовать целевой хост пакетами запросов ARP. Другими словами, злонамеренный хост продолжает непрерывно отправлять пакеты с поддельными ARP-запросами на целевой хост. Если количество пакетов запроса ARP в секунду превышает порог запроса ARP, это указывает на то, что происходит шторм запроса ARP.

3.3.3.2 ARP сканирование

Возможная причина сканирования ARP в локальных сетях - из-за активного программного обеспечения для наблюдения или вируса, выполняющего сканирование ARP.

Таблица 3.7 Решения по обеспечению безопасности, включая ARP Request Storm и / или механизмы обнаружения ARP-сканирования

	Detect ARP Request Storm?	*Detect ARP Scan?*
Cisco Catalyst 3560 Switch Series	No	No
Juniper Switches EX3200 Series	No	No
Snort IDS	No	No
XArp 2	No	No
Sax2 NIDS	Yes	Yes
Cisco IPS 4425 Series	No	No

В таблице 3.7 показаны решения безопасности, которые включают механизмы для обнаружения штормов запросов ARP и / или сканирования ARP. Среди протестированных решений безопасности Sax2 NIDS является единственным решением, которое способно обнаруживать штормы запросов ARP и сканирование ARP.

3.3.4 Анализ экспериментальных результатов

Приведенные выше экспериментальные результаты ясно показывают, что аномальный трафик ARP не полностью обнаружен и предотвращен протестированными решениями безопасности. Очевидно, что в этих решениях отсутствуют эффективные механизмы обнаружения и предотвращения.

В дополнение к базовым функциям проверки ненормального ARP, для решения безопасности:

* Выполните межуровневую проверку ARP между заголовками Ethernet и ARP. Среди протестированных решений безопасности только межсетевой контроль ARP выполняют коммутаторы Cisco серии 3560, Juniper Switch EX3200, Snort IDS и XArp 2.

* Выполните проверку состояния ARP, чтобы запомнить запросы ARP и сопоставить их с ответами ARP. XArp 2 и Sax2 NIDS являются единственными решениями безопасности, которые выполняют проверку состояния ARP.
* Справиться с ARP-запросом штормового трафика и ARP-сканированием трафика. Sax2 NIDS является единственным решением безопасности, способным обнаруживать штормы запросов ARP и сканирование ARP.

Исходя из результатов вышеупомянутых экспериментов, «XArp 2» является наиболее эффективным из доступных решений безопасности, чтобы справиться с ненормальным трафиком ARP. Однако, по сравнению с другими протестированными решениями безопасности, улучшения могут быть сделаны путем добавления механизмов безопасности для обнаружения штормов запросов ARP и сканирования ARP. С другой стороны, коммутатор Cisco Catalyst 3560 и коммутаторы Juniper серии EX3200 являются примерами дорогостоящих коммутаторов, которые используют эффективную расширенную функцию безопасности, называемую динамической проверкой ARP (DAI), для предотвращения ненормального трафика ARP.

3.4 Лабораторная работа 3.1: обнаружение аномального трафика ARP

3.4.1 Результат

Цель этого практического упражнения - научить студентов генерировать и обнаруживать аномальный трафик ARP с использованием XArp 2 в локальной сети.

3.4.2 Инструмент обнаружения XArp 2

XArp 2 - это эффективный инструмент, который обеспечивает решение безопасности для обнаружения ненормального трафика ARP. XArp 2 отслеживает действия Ethernet, ведет базу данных пар MAC-адресов Ethernet / IP-адресов и обнаруживает неожиданные изменения ассоциации MAC / IP и другой ненормальный трафик ARP.

XArp 2 пассивно проверяет сетевой трафик в поисках признаков атак ARP. XArp 2 предполагает, что хост, на котором работает XArp 2, имеет доступ к порту мониторинга на коммутаторе (обычно называемом портом SPAN или портом зеркального отображения).

Существуют и другие инструменты, которые включают механизмы обнаружения аномального трафика ARP. Например, Snort - это система обнаружения вторжений в сеть с открытым исходным кодом, способная обнаруживать некоторые типы ненормальных пакетов ARP. Подобно XArp 2, Snort - это датчик, который должен иметь доступ к порту мониторинга или находиться в месте, где он может видеть весь сетевой трафик. Короче говоря, такие решения, как XArp 2 и Snort, пытаются обнаружить вредоносное поведение, а не предотвратить его.

3.4.3 Эксперимент

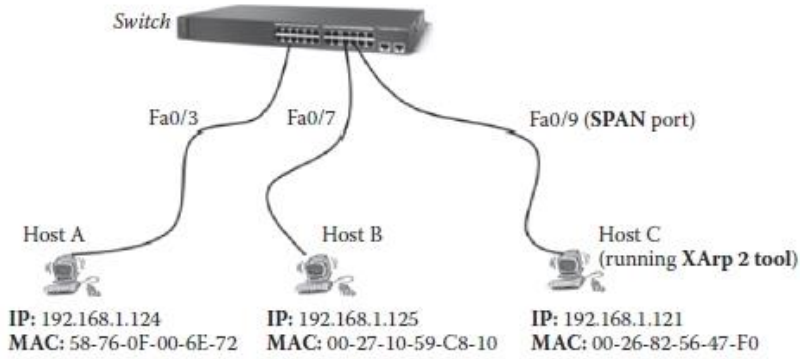
В следующем эксперименте описывается, как обнаружить ненормальные пакеты ARP с использованием XArp 2 в локальной сети. В эксперименте приводятся примеры предупреждающих сообщений XArp 2, генерируемых после введения различных типов ненормальных пакетов ARP.

Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2: Установите инструмент XArp 2.
Шаг 3: Настройте порт SPAN в коммутаторе Cisco.
Шаг 4: Генерация и обнаружение ненормальных пакетов ARP

3.4.3.1 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на рисунке ниже. Три хоста подключены к коммутатору Cisco. XArp 2 установлен на хосте C, а порт коммутатора, к которому подключен хост C, является портом SPAN (Fa0/9).

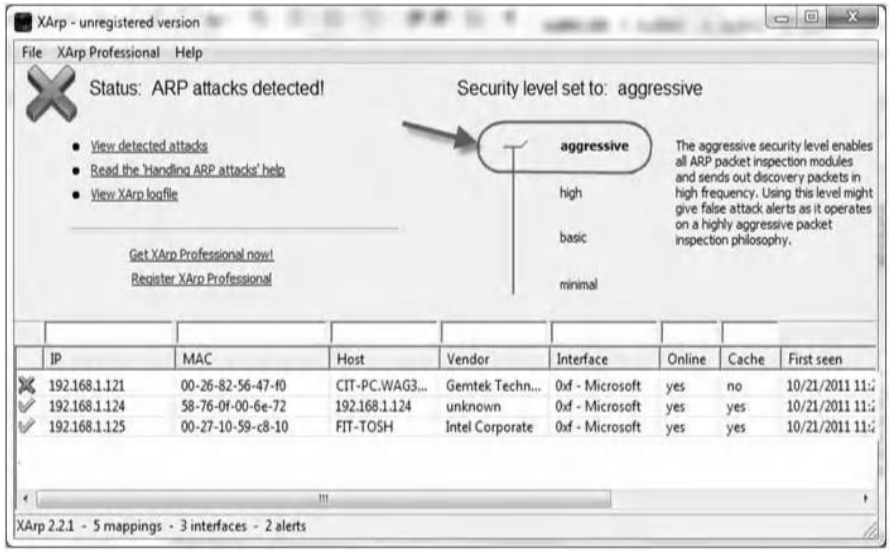


3.4.3.2 Шаг 1. Назначьте статические IP-адреса хостам сети

Обратитесь к Главе 1.

3.4.3.3 Шаг 2: Установите инструмент XArp 2

Этот шаг состоит из установки XArp 2 на хосте C и последующего выбора агрессивного уровня безопасности, как показано на следующем снимке экрана, для обнаружения большинства типов ненормальных пакетов ARP.



3.4.3.4 Шаг 3: Настройте порт SPAN в коммутаторе Cisco

Следующие шаги показывают, как настроить порт Fa0 / 9 на коммутаторе как порт SPAN:

* Подключите хост C к консольному порту на коммутаторе.
* Запустите настройку с помощью инструмента HyperTerminal. (Обратитесь к Главе 1 для получения дополнительной информации об инструменте HyperTerminal.)
* Введите следующую команду для настройки порта SPAN:

```
Switch> enable//введите команду enable для
доступа к привилегированному режиму EXEC.
Switch(conf)#monitor session 1 source interface
fastethernet 0/3 both
Switch(conf)#monitor session 1 source interface
fastethernet 0/7 both
Switch(conf)#monitor session 1 destination
interface fastethernet 0/9
Switch(conf)#exit
Switch# copy running-config startup-config
```

После ввода вышеуказанных команд весь трафик, исходящий от хоста A (Fa0 /3) и хоста B (Fa/07), будет прослушиваться хостом C (Fa0/9).

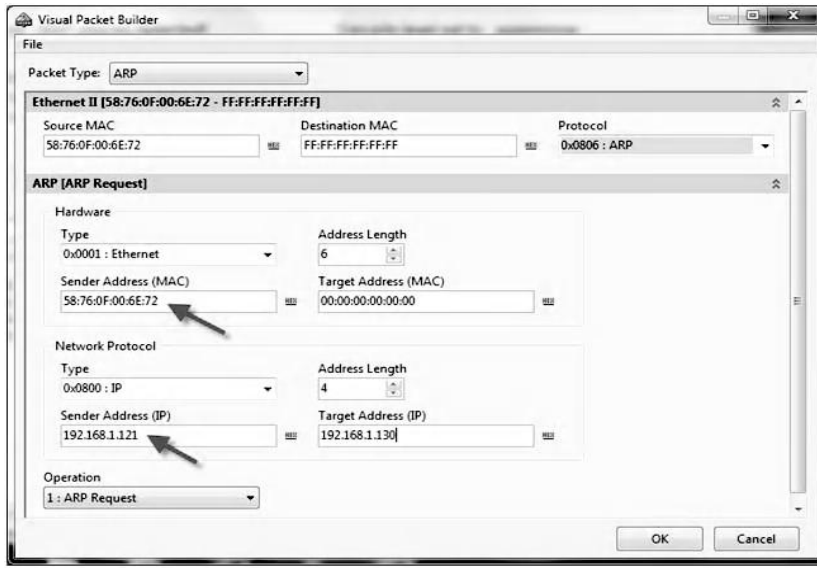
3.4.3.5 Шаг 4. Создание и обнаружение аномальных пакетов ARP

Пакет, выпущенный от хоста A, должен использоваться для генерации ненормальных пакетов ARP. Поскольку XArp 2 отслеживает трафик хоста A и хоста B, ожидается, что сгенерированные ненормальные пакеты ARP будут проверены XArp 2. В этом эксперименте с помощью CommView Visual Packet Builder создаются четыре типа ненормальных пакетов ARP:

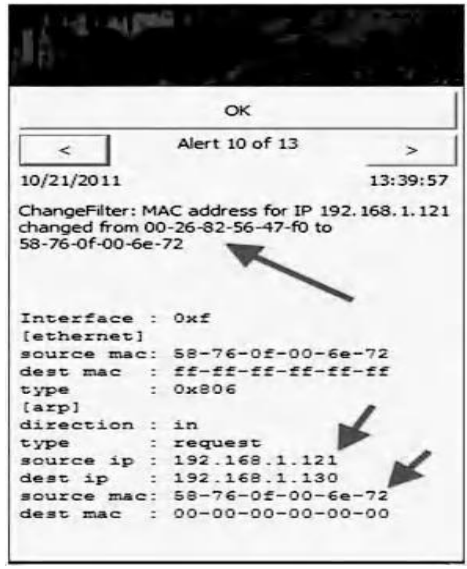
* *Packet#1*: Хост A отправляет широковещательный пакет запроса ARP. Пакет нарушает действительное сопоставление IP / MAC-адреса, поскольку пара IP-адрес источника / MAC-адрес в заголовке ARP является недопустимой, как показано здесь:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host C**
Source MAC address	**MAC address of Host A**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	Broadcast MAC address
Ethernet Type	0x0806 for ARP message

CommView Visual Packet Builder позволяет генерировать вышеуказанный ненормальный пакет ARP (*Packet#1*; см. Снимок экрана ниже).



После введения ненормального пакета ARP в сеть XArp 2 сгенерировал предупреждающее сообщение ChangeFilter, показанное на следующем снимке экрана.



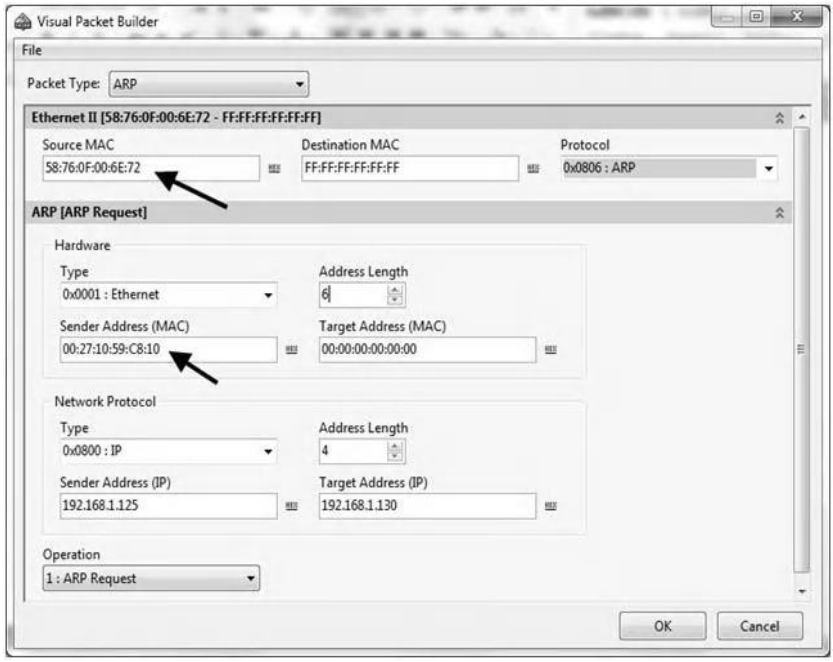
Предупреждение XArp 2 ChangeFilter указывает на то, что пакет нарушает текущие сопоставления. XArp 2 отслеживает сопоставления IP-адресов и MAC-адресов. Запросы ARP содержат сопоставление IP-MAC отправителя. Ответы ARP содержат сопоставление IP-MAC разрешенного хоста. Каждый пинг карты вставляется в базу данных. Если отслеживаемое сопоставление нарушает текущие сопоставления, генерируется предупреждение.

* *Packet #2*: Хост A отправляет широковещательный пакет запроса ARP. Пакет имеет MAC-адрес источника Ethernet, который не соответствует MAC-адресу источника ARP, как показано здесь:

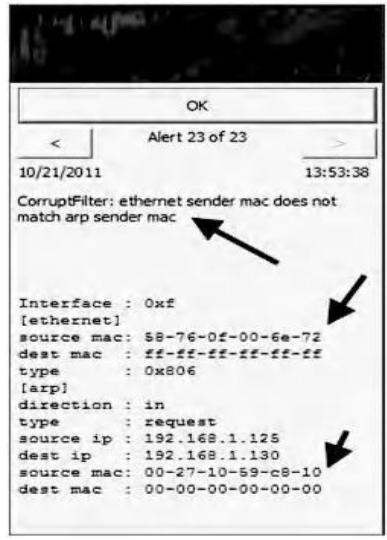
ARP Header	
Operation code	1 (for ARP request)
Source IP address	IP address of Host B
Source MAC address	**MAC address of Host B**

ARP Header	
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	**MAC address of Host A**
Destination MAC address	Broadcast MAC address
Ethernet Type	0x0806 for ARP message

CommView Visual Packet Builder позволяет генерировать вышеупомянутый ненормальный пакет ARP (*Packet #2*; см. Снимок экрана ниже).



После внедрения указанного выше ненормального пакета ARP в сеть XArp 2 сгенерировал предупреждающее сообщение CorruptFilter, показанное на следующем снимке экрана.

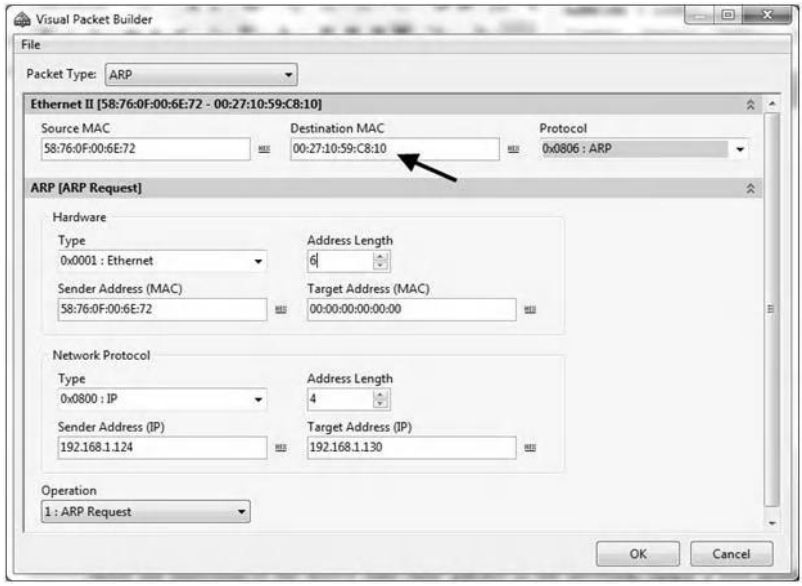


Предупреждение XArp 2 CorruptFilter указывает, что пакет ARP содержит неправильные значения. То есть MAC-адрес источника Ethernet не соответствует MAC-адресу источника ARP. XArp 2 проверяет эти значения на правильность.

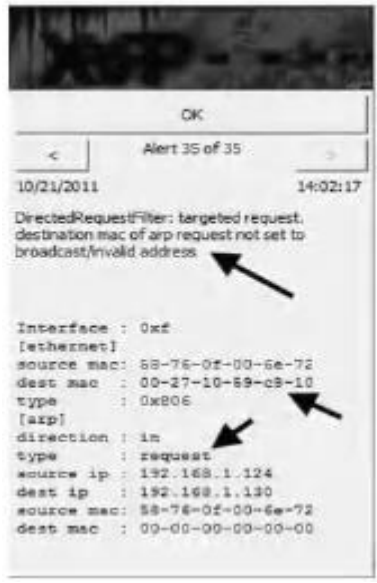
* *Packet #3*: Узел A отправляет ненормальный пакет запроса одноадресной ARP на узел B. Пакет запроса ARP необходимо отправить на широковещательный MAC-адрес. Однако в этом эксперименте сгенерированный пакет запроса ARP был отправлен на одноадресный MAC-адрес (MAC-адрес хоста B), как показано здесь:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	IP address of Host A
Source MAC address	MAC address of Host A
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	**MAC address of Host B**
Ethernet Type	0x0806 for ARP message

CommView Visual Packet Builder позволяет генерировать вышеупомянутый ненормальный пакет одноадресной передачи ARP (*Packet #3*), как показано на следующем снимке экрана.



После внедрения вышеуказанного ненормального пакета запроса ARP в сеть XArp 2 сгенерировал предупреждающее сообщение DirectedRequestFilter инструмента следующим образом.

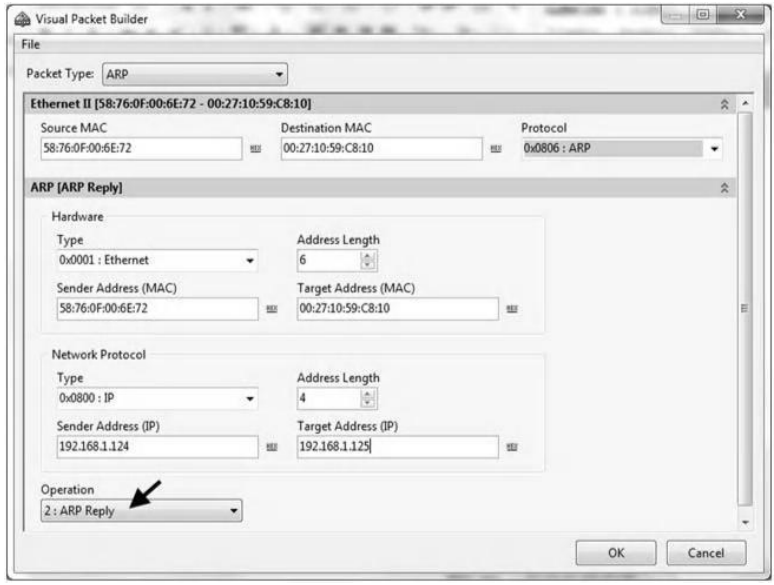


В предупреждающем сообщении XArp 2 DirectedRequestFilter указывается, что пакет запроса ARP отправляется на одноадресный MAC-адрес. Однако запросы ARP должны отправляться на широковещательный MAC-адрес.

* *Packet #4*: Хост A отправляет пакет ответа ARP, который не запрашивается, на хост B. То есть хост A отправляет пакет ответа ARP на хост B, несмотря на тот факт, что хост B не отправил ни одного пакета запроса ARP. Ответы ARP должны обычно следовать запросам ARP. Следующий ненормальный пакет ответа ARP, который не запрошен, был отправлен узлом A на узел B:

ARP Header	
Operation code	1 (for **ARP reply**)
Source IP address	IP address of Host A
Source MAC address	MAC address of Host A
Destination IP address	IP address of Host B
Destination MAC address	MAC address of Host B
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	MAC address of Host B
Ethernet Type	0x0806 for ARP message

CommView Visual Packet Builder позволяет генерировать вышеупомянутый ненормальный ответный пакет ARP (*Packet #4*; см. Скриншот ниже).



После внедрения вышеуказанного ненормального пакета запроса ARP в сеть XArp 2 сгенерировал предупреждающее сообщение RequestedResponseFilter инструмента, показанное на следующем снимке экрана.

В предупреждающем сообщении XArp 2 RequestedResponseFilter указывается, что был сгенерирован ответный пакет ARP, который не был запрошен. XArp 2 запоминает все исходящие запросы ARP и сопоставляет их с ответами ARP.

3.5 Лабораторная работа 3.2. Предотвращение аномального трафика ARP с использованием проверки динамического ARP для сетевой среды, отличной от DHCP

3.5.1 Результат

Цель данного практического упражнения состоит в том, чтобы учащиеся узнали, как предотвратить ненормальный трафик ARP, с помощью функции безопасности Dynamic ARP Inspection для среды без DHCP в локальной сети.

3.5.2 Динамическая проверка ARP

Усовершенствованные коммутаторы, такие как коммутаторы Cisco Catalyst 3560 и коммутаторы серии Juniper EX, используют функцию безопасности, называемую Dynamic ARP Inspection, для отклонения ненормальных пакетов ARP, главным образом с недопустимыми привязками IP-MAC-адресов. Динамическая проверка ARP обеспечивает ретрансляцию только действительных запросов и ответов ARP. Эта функция помогает предотвратить злонамеренные атаки, не передавая недопустимые запросы ARP и ответы на другие порты в той же локальной сети. Эта возможность защищает сетевые узлы от атак DoS и MiM, использующих технику отравления кэша ARP. Динамическая проверка ARP опирается на использование списка контроля доступа ARP (ACL), который включает в себя действительные привязки IP-MAC-адресов. Список ACL ARP создается вручную для сетевой среды, отличной от DHCP, и автоматически для сетевой среды DHCP.

Например, мы предполагаем, что четыре хоста (A, B, C и D) подключены к коммутатору. В коммутаторах Cisco Catalyst 3560 для защиты вышеуказанных хостов от атаки отравления кэшем ARP создается следующий список ACL ARP:

```
Permit ip host Sender-IP-A mac host Sender-MAC-A
Permit ip host Sender-IP-B mac host Sender-MAC-B
Permit ip host Sender-IP-C mac host Sender-MAC-C
Permit ip host Sender-IP-D mac host Sender-MAC-D Deny
ip any mac any log
```

Динамическая проверка ARP также может быть настроена для отбрасывания пакетов ARP, когда IP-адреса недействительны или когда MAC-адреса в заголовке ARP не совпадают с адресами, указанными в заголовке Ethernet.

Важно отметить, что большинство коммутаторов используют списки ACL ARP для проверки правильности только пары IP-адреса источника и MAC-адреса в заголовке ARP. Они не используются для проверки правильности определения пары IP и MAC в заголовке ARP. Это связано с тем, что неверные пары IP-адресов назначения и MAC-адресов в заголовке ARP не повреждают кэши ARP целевых хостов.

3.5.3 Эксперимент

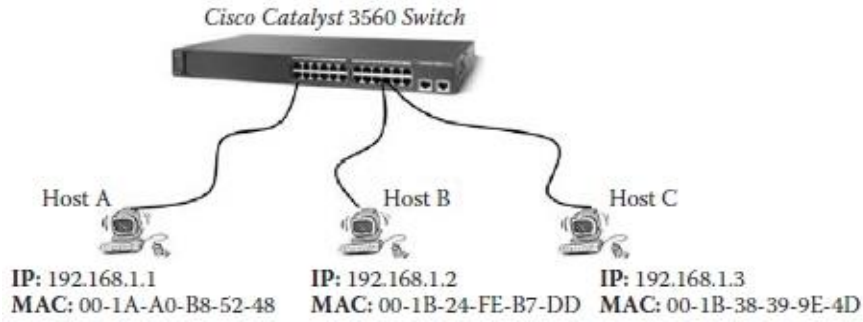
В следующем эксперименте описывается, как предотвратить ненормальные пакеты ARP с помощью проверки динамического ARP для среды, отличной от DHCP, в локальной сети.

3.5.3.1 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Три хоста подключены к коммутатору Cisco Catalyst 3560.

Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2. Настройте проверку динамического ARP для среды, отличной от DHCP, в коммутаторе Cisco Catalyst 3560.
Шаг 3: Генерация и предотвращение ненормальных пакетов ARP.



3.5.3.2 Шаг 1. Назначьте статические IP-адреса хостам сети.

Обратитесь к Главе 1.

3. 5.3.3 Шаг 2. Настройте проверку динамического ARP для среды без DHCP в коммутаторе Cisco Catalyst 3560

* Подключите хост A к консольному порту на коммутаторе.
* Запустите настройку с помощью инструмента HyperTerminal. (Обратитесь к Главе 1 для получения дополнительной информации об использовании инструмента HyperTerminal.)
* Введите следующие команды, чтобы создать список ACL ARP для сети, показанной на предыдущем рисунке:

```
Switch>enable //введите команду enable для
доступа в привилегированный режим EXEC
Switch#configure terminal //включить режим
глобальной конфигурации
Switch(config)# ip arp inspection vlan 1//включить
динамический контроль ARP в VLAN 1
Switch(config)# ip arp inspection vlan 1 logging
acl-match matchlog //включите динамическую проверку
ARP на vlan 1, и пакеты ARP, разрешенные или
запрещенные ACL, регистрируются.
Switch(config)#arp access-list
ZouheirACL//определить ARP ACL и войти в режим
настройки списка доступа ARP.
```

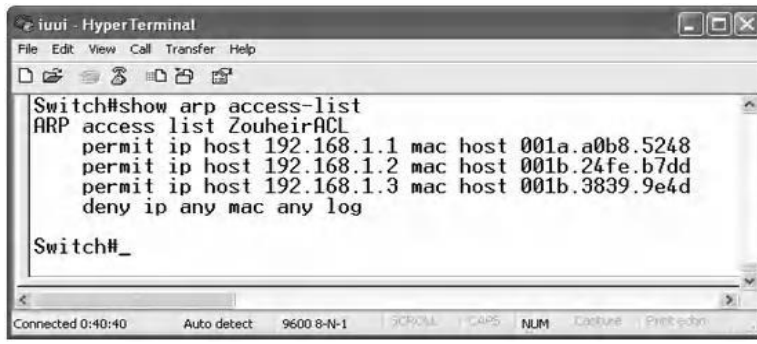
```
Для этого примера имя списка доступа -
«ZouheirACL»
Switch(config-arp-nacl)# permit ip host
192.168.1.1 mac host 00-1A-A0-B8-52-48 log
Switch(config-arp-nacl)# permit ip host
192.168.1.2 mac host 00-1B-24-FE-B7-DD log
Switch(config-arp-nacl)# permit ip host
192.168.1.3 mac host 00-1B-38-39-9E-4D log
Switch(config-arp-nacl)# deny ip any log
Switch(config-arp-nacl)# exit Switch(config)# ip
arp inspection filter ZouheirACL vlan 1 static
//применить ARP ACL (ZouheirACL) к VLAN 1
Switch(config)# exit
Switch# copy running-config startup-config//эта
команда позволяет нам сохранить конфигурацию
```

Важно указать, что коммутатор использует список ACL ARP для проверки только IP-адреса источника и MAC-адреса хоста отправителя в пакете ARP. Он не проверяет IP-адреса и MAC-адреса назначения.

Чтобы проверить записи созданного списка ACP ARP «ZouheirACL», введите следующую команду:

```
Switch# show arp access-list
```

На следующем снимке экрана показано содержимое списка ARP ACL «ZouheirACL».



Кроме того, чтобы настроить коммутатор на выполнение дополнительных проверок MAC-адреса источника, MAC-адреса назначения, IP-адреса источника и IP-адреса назначения, введите следующие команды:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
dst-mac ip
```

В приведенной выше команде параметры «src-mac», «dst-mac» и «ip» позволяют коммутатору выполнять дополнительные проверки, а именно:

1. Опция «src-mac» позволяет сверять MAC-адрес источника в заголовке Ethernet с MAC-адресом источника в заголовке ARP. Эта проверка выполняется как для запросов ARP, так и для ответов.
2. Опция «dst-mac» позволяет сверять MAC-адрес назначения в заголовке Ethernet с MAC-адресом назначения в заголовке ARP. Эта проверка выполняется для ответов ARP.
3. Опция «ip» позволяет проверять заголовок ARP на наличие недействительных и неожиданных IP-адресов. Адреса включают 0.0.0.0, 255.255.255.255 и все IP-адреса многоадресной рассылки. IP-адреса источника проверяются во всех ARP-запросах и ответах, а IP-адреса назначения проверяются только в ARP-ответах.

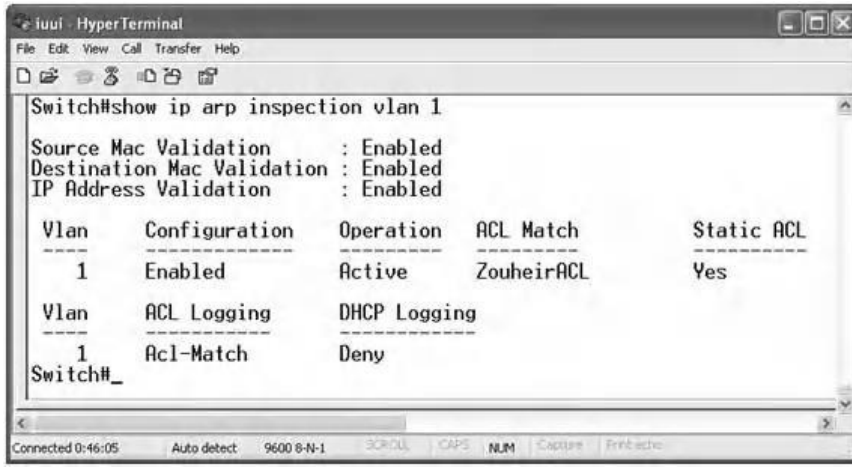
Введите следующую команду, чтобы указать количество записей, которые должны быть зарегистрированы в буфере:

```
Switch(config)# ip arp inspection log-buffer
entries 200
```

Чтобы отобразить конфигурацию и рабочее состояние проверки динамического ARP для VLAN 1, введите следующую команду:

```
Switch# show ip arp inspection vlan 1
```

На приведенном ниже снимке экрана показана конфигурация и рабочее состояние Dynamic ARP Inspection для VLAN 1.



3. 5.3.4 *Шаг 3. Создание и предотвращение неправильных пакетов ARP*

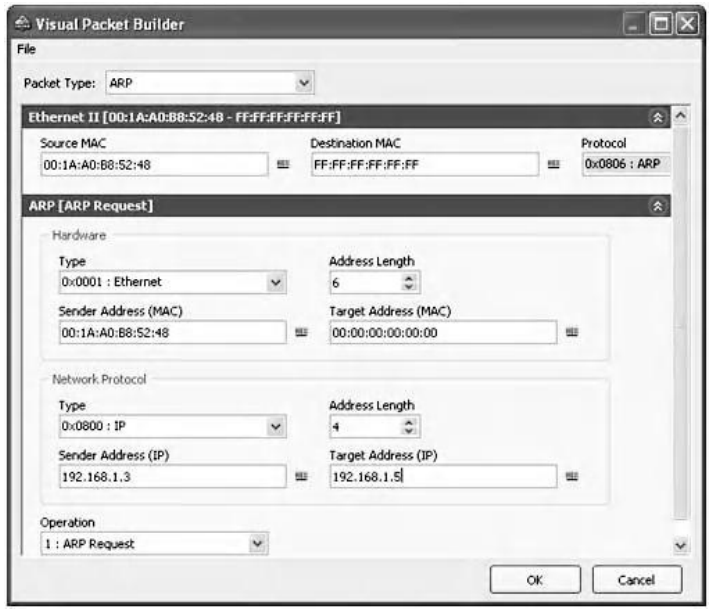
Мы предполагаем, что проверка динамического ARP включена на коммутаторе Cisco. На хосте A генерируются четыре типа аномальных пакетов ARP:

* Packet #1: Хост A отправляет следующий широковещательный пакет запроса ARP. Пакет нарушает действительное сопоставление IP / MAC-адреса, поскольку пара IP-адрес источника / MAC-адрес в заголовке ARP является недопустимой, как показано здесь:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host C**
Source MAC address	**MAC address of Host A**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00

Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	Broadcast MAC address
Ethernet Type	0x0806 for ARP message

На следующем снимке экрана показан сгенерированный выше ненормальный пакет ARP с использованием CommView Visual Packet Builder.

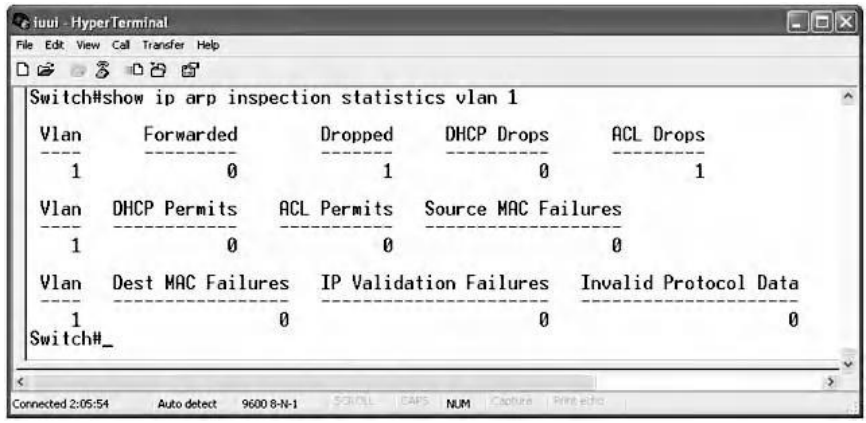


После внедрения вышеупомянутого ненормального пакета запроса ARP в сеть коммутатор Cisco отклонил пакет. Чтобы отобразить статистику о потерянных пакетах ARP, введите следующую команду:

```
Switch# show ip arp inspection statistics vlan 1
```

На следующем снимке экрана показано, что сгенерированный выше ненормальный пакет запроса ARP был отброшен механизмом «ACL Drop» коммутатора Cisco, поскольку он

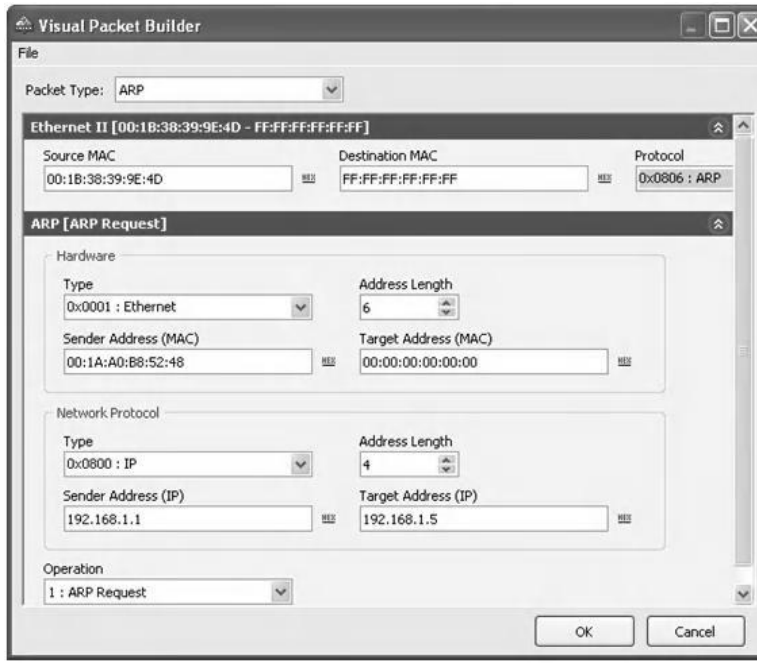
содержит недопустимую IP-адрес источника / пару MAC-адресов (192.168.1.3/00-11-43-3D-EE-48).



* Packet #2: Узел A отправляет следующий ненормальный пакет запроса ARP на узел B. Пакет ARP имеет MAC-адрес источника в заголовке Ethernet, отличный от MAC-адреса источника в заголовке ARP, как показано ниже:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	IP address of Host A
Source MAC address	**MAC address of Host A**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	**MAC address of Host C**
Destination MAC address	Broadcast MAC address
Ethernet Type	0x0806 for ARP message

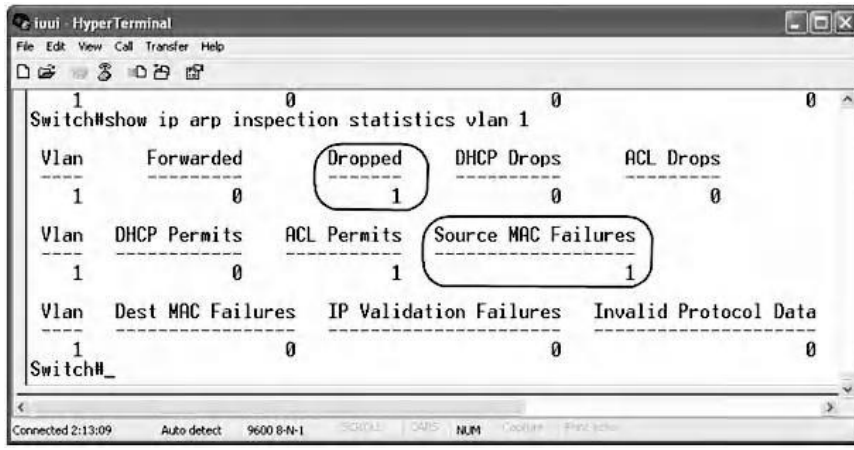
На следующем снимке экрана показан сгенерированный выше ненормальный пакет ARP с использованием CommView Visual Packet Builder.



После внедрения вышеупомянутого ненормального пакета запроса ARP в сеть коммутатор Cisco отклонил пакет. Чтобы отобразить статистику о потерянных пакетах ARP, введите следующую команду:

```
Switch# show ip arp inspection statistics vlan 1
```

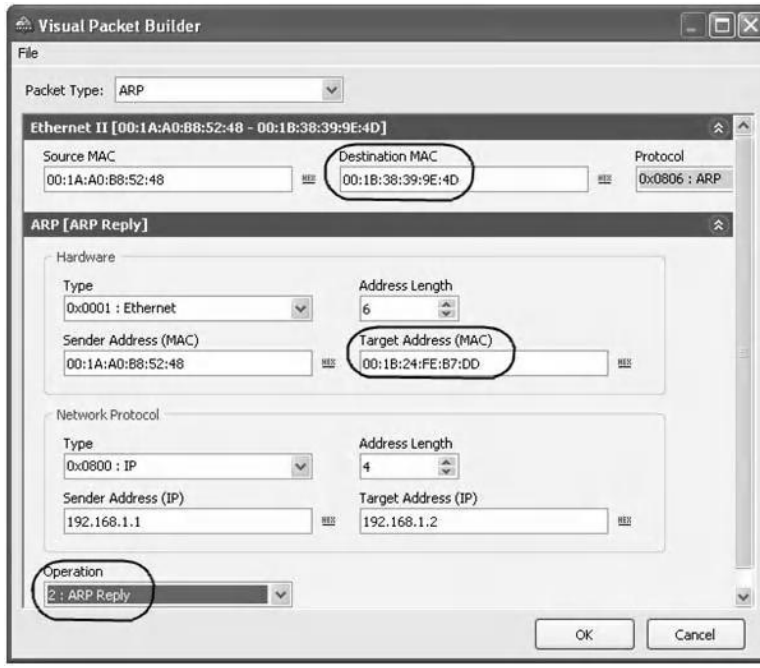
На приведенном ниже снимке экрана показано, что сгенерированный ненормальный пакет ARP был отброшен механизмом «Source MAC Failures”» коммутатора Cisco, поскольку MAC-адрес отправителя в заголовке Ethernet не соответствует MAC-адресу отправителя в заголовке ARP.



* Packet #3: Узел A отправляет следующий ненормальный ответный пакет ARP на узел B. Пакет ARP имеет MAC-адрес назначения в заголовке Ethernet, отличный от MAC-адреса назначения в заголовке ARP, как показано здесь:

ARP Header	
Operation code	2 (for **ARP reply**)
Source IP address	IP address of Host A
Source MAC address	MAC address of Host A
Destination IP address	IP address of Host B
Destination MAC address	**MAC address of Host B**
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	**MAC address of Host C**
Ethernet Type	0x0806 for ARP message

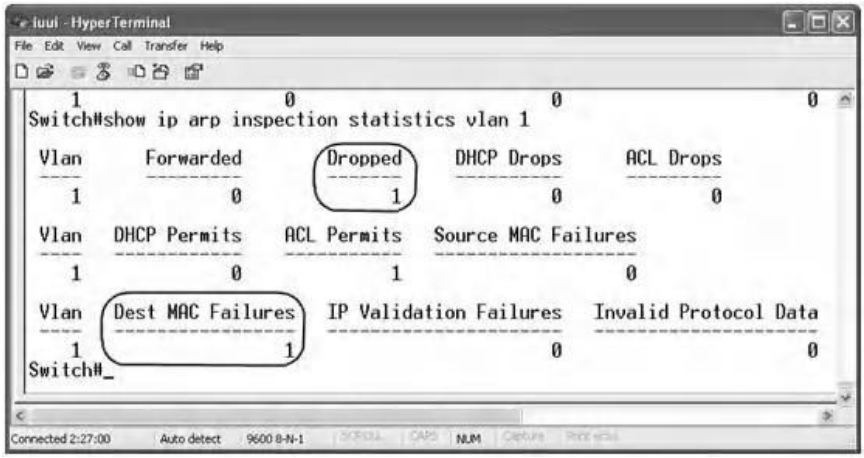
На следующем снимке экрана показан сгенерированный выше ненормальный ответный пакет ARP с использованием CommView Visual Packet Builder.



После введения вышеуказанного ненормального пакета ответа ARP в сеть коммутатор Cisco отбрасывает пакет. Чтобы отобразить статистику о потерянных пакетах ARP, введите следующую команду:

```
Switch# show ip arp inspection statistics vlan 1
```

Ниже приведен снимок экрана, показывающий, что сгенерированный выше ненормальный ответный пакет ARP был отброшен механизмом «MAC MAC Failures» коммутатора Cisco, поскольку MAC-адрес назначения в заголовке Ethernet не соответствует MAC-адресу назначения в заголовке ARP.



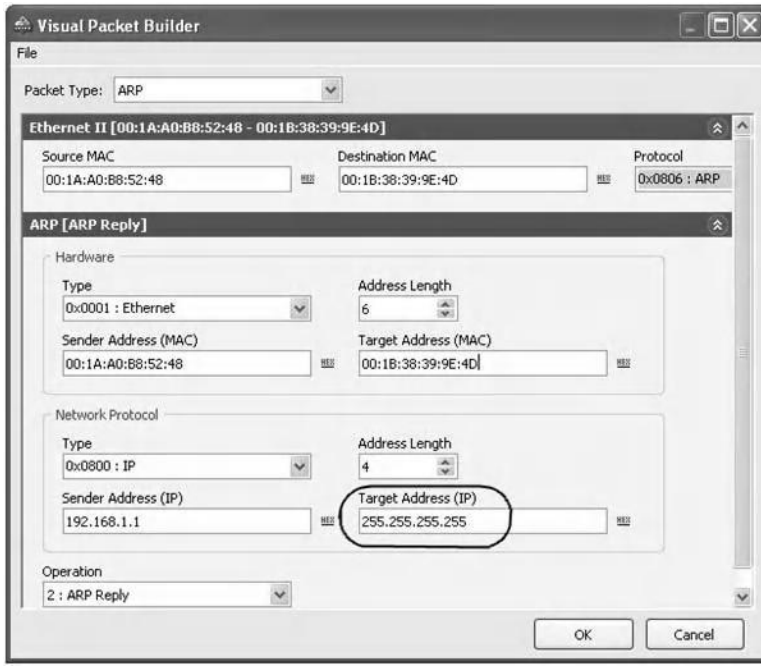
❿ *Packet #4*: Хост A отправляет следующий неправильный пакет ответа ARP. Пакет содержит недопустимый IP-адрес назначения (255.255.255.255) в заголовке ARP, как показано ниже:

ARP Header	
Operation code	2 (for ARP reply)
Source IP address	IP address of Host A
Source MAC address	MAC address of Host A
Destination IP address	255.255.255.255
Destination MAC address	MAC address of Host C
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	MAC address of Host C
Ethernet Type	0x0806 for ARP message

Коммутатор использует ACL ARP для проверки правильности только пары исходного IP и MAC в заголовке пакета ARP. Он не проверяет действительность IP-адреса и MAC-адреса назначения в заголовке пакета ARP. Это связано с тем, что неверные пары

пары IP-адресов и MAC-адресов назначения не повреждают кэши ARP целевых хостов. Однако механизм «Ошибки валидации IP» позволяет проверять заголовок ARP на наличие недопустимых и неожиданных IP-адресов, таких как IP-адрес «255.255.255.255».

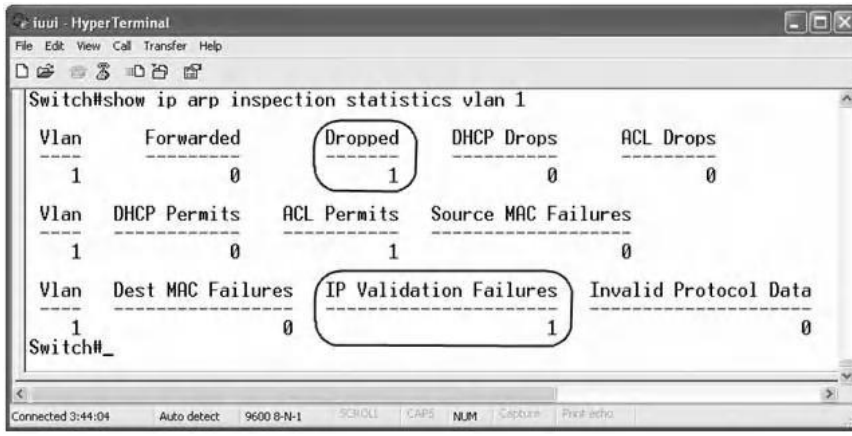
На следующем снимке экрана показан сгенерированный выше ненормальный ответный пакет ARP с использованием CommView Visual Packet Builder.



После введения вышеуказанного ненормального пакета ответа ARP в сеть коммутатор Cisco отбрасывает пакет. Чтобы отобразить статистику о потерянных пакетах ARP, введите следующую команду:

```
Switch# show ip arp inspection statistics vlan 1
```

Вот снимок экрана, показывающий, что сгенерированный ненормальный ответный пакет ARP был отброшен механизмом Cisco «IP Validation Failures», потому что он содержит недопустимый IP-адрес назначения.



3.6 Лабораторная работа 3.3. Предотвращение аномального трафика ARP с использованием проверки динамического ARP и отслеживания DHCP для среды DHCP

3.6.1 Результат

Цель данного практического упражнения - научить студентов генерировать и предотвращать ненормальный трафик ARP с помощью функций проверки Dynamic ARP Inspection и DHCP Snooping для среды DHCP в локальной сети.

3.6.2 DHCP Snooping (отслеживание DHCP)

В сетевой среде DHCP серверы DHCP автоматически назначают IP-адреса узлам, подключенным к сети, из определенного диапазона IP-адресов. Это очень часто используется в призовых сетях для сокращения усилий по настройке.

В среде DHCP функция безопасности Dynamic ARP Inspection в коммутаторах Cisco позволяет определять достоверность пакетов ARP на основе действительных привязок IP-MAC-адресов, хранящихся в доверенной базе данных, базе данных привязки отслеживания DHCP. Эта база данных построена с помощью механизма, называемого DHCP

snooping (отслеживание DHCP). Когда пакет ARP получен на доверенном интерфейсе, коммутатор передает пакет без какой-либо проверки. На ненадежных интерфейсах коммутатор пересылает пакет, только если он действителен.

3.6.3 Эксперимент

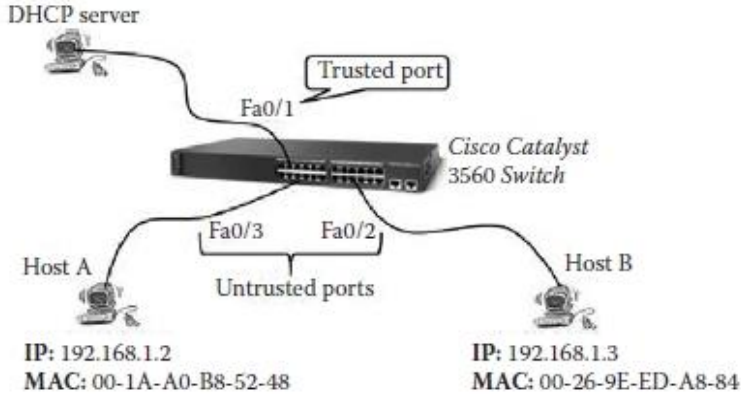
В следующем эксперименте описывается, как предотвратить ненормальные пакеты ARP с помощью Dynamic ARP Inspection и DHCP snooping для среды DHCP в локальной сети.

Эксперимент состоит из следующих этапов:

Шаг 1. Включите отслеживание DHCP.
Шаг 2: Настройте проверку динамического ARP для среды DHCP.
Шаг 3: Генерация и предотвращение ненормальных пакетов ARP.

3.6.3.1 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Два хоста подключены к коммутатору Cisco Catalyst 3560 через два ненадежных порта. Третий хост размещает DHCP-сервер. Пользователь может использовать любое доступное программное обеспечение DHCP-сервера. В этом эксперименте используется инструмент DHCP Turbo Server.



3.6.3.2 Шаг 1. Включите отслеживание DHCP

Чтобы включить отслеживание DHCP и настроить порт коммутатора Cisco Catalyst 3560, к которому подключен сервер DHCP, в качестве доверенного порта (по умолчанию порты коммутатора ненадежны), необходимо выполнить следующие действия:

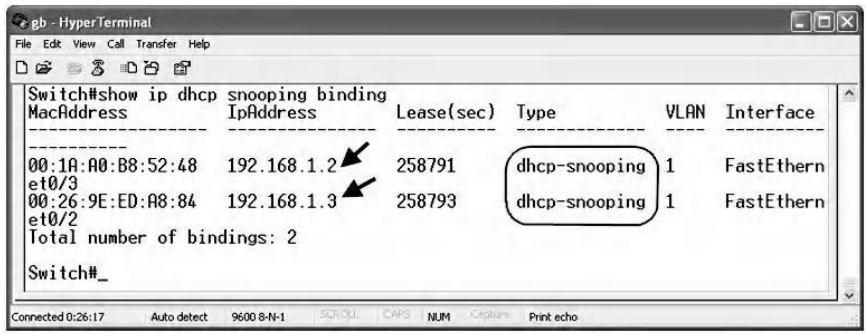
* Подключите хост A к консольному порту на коммутаторе.
* Запустите настройку с помощью инструмента HyperTerminal (дополнительную информацию об использовании инструмента HyperTerminal см. В главе 1).
* Введите следующие команды:

```
Switch>enable//введите команду enable для
доступа в привилегированный режим EXEC
Switch#configure terminal//войти в режим
глобальной конфигурации
Switch(config)#ip dhcp snooping//включить DHCP,
отслеживающий глобально
Switch(config)#ip dhcp snooping vlan 1//включить
отслеживание DHCP на VLAN 1
Switch(config)#interface FastEthernet 0/1//войти в
режим настройки интерфейса для интерфейса
FastEthernet 0/1(Port#1)
Switch(config-if)#ip dhcp snooping trust//
настроить интерфейс как доверенный. По умолчанию это
ненадежно.
Switch(config-if)#end
Switch#copy running-config startup-config//сохранить
записи в файле конфигурации
```

Перезагрузите сервер DHCP и коммутатор Cisco, чтобы разрешить создание базы данных связывания отслеживания DHCP. Затем введите следующую команду, чтобы отобразить содержимое базы данных привязки DHCP snooping:

```
Switch#show ip dhcp snooping binding
```

На следующем снимке экрана показано содержимое базы данных DHCP Snooping.



3.6.3.3 Шаг 2. Настройка проверки динамического ARP для среды DHCP

Чтобы настроить проверку динамического ARP, введите следующие команды:

```
Switch>enable//введите команду enable для доступа в
привилегированный режим EXEC
Switch#configure terminal//войти в режим
глобальной конфигурации
Switch(config)#ip arp inspection vlan 1//включить
динамический контроль ARP на VLAN 1
Switch(config)#end//вернуться в привилегированный режим
EXEC
Switch#show ip arp inspection vlan 1//проверить
конфигурацию динамического контроля ARP
Switch#show ip arp inspection statistics vlan 1//
проверить статистику проверки динамического ARP
Switch#configure terminal
Switch(config)#ip arp inspection validate src-mac dst-mac
ip//выполнить определенную проверку входящих пакетов ARP.
Обратитесь к Лаборатории № 3.2 для получения
дополнительной информации.
Switch(config)#ip arp inspection log-buffer entries
200//укажите количество записей, которые будут
зарегистрированы в буфере. Диапазон составляет от 0 до
1024.
```

```
Switch(config)#ip arp inspection log-buffer logs 0
interval 1//это означает, что запись помещается в буфер
журнала, но системное сообщение не генерируется.
```

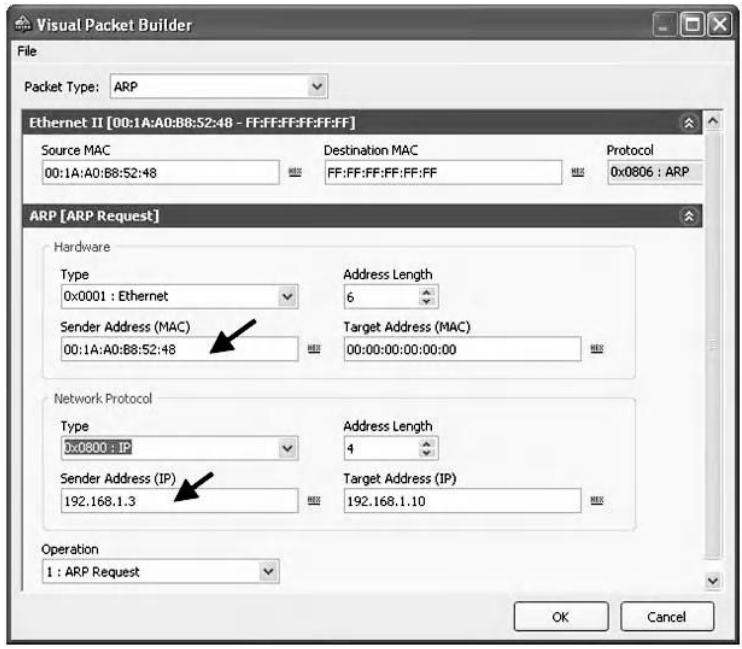
3.6.3.4 Шаг 3: Создание и предотвращение неправильного пакета ARP

Поскольку отслеживание DHCP и проверка динамического ARP включены, коммутатор должен отбрасывать аномальные пакеты ARP с неверным отображением IP / MAC-адреса. В этом эксперименте пользователь может использовать те же четыре ненормальных пакета ARP из предыдущей лабораторной работы. Например, мы генерируем только следующий ненормальный пакет ARP:

* *Packet#1*: Хост A отправляет следующий широковещательный пакет запроса ARP. Пакет нарушает действительное сопоставление IP/MAC-адреса, поскольку пара IP-адрес источника/MAC-адрес в заголовке ARP является недопустимой, как показано здесь.

ARP Header	
Operation code	1 (for ARP request)
Source IP address	**IP address of Host B**
Source MAC address	**MAC address of Host A**
Destination IP address	Any IP address
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	Broadcast MAC address
Ethernet Type	0x0806 for ARP message

На следующем снимке экрана показан вышеупомянутый ненормальный пакет ARP, сгенерированный с помощью CommView Visual Packet Builder.



После внедрения вышеупомянутого ненормального пакета запроса ARP в сеть коммутатор Cisco отклонил пакет. Чтобы отобразить статистику о потерянных пакетах ARP, введите следующую команду:

```
Switch#show ip arp inspection statistics vlan 1
```

На следующем снимке экрана показано, что сгенерированный выше ненормальный пакет запроса ARP был отброшен механизмом «DHCP Deny» коммутатора Cisco, поскольку он содержит недопустимую пару IP-адрес источника/MAC-адресов (192.168.1.3/00-1A-A0-B8-52-48).

3.7 Краткое содержание главы

В этой главе были проанализированы и оценены решения безопасности, которые обнаруживают и предотвращают аномальный трафик ARP на основе практических экспериментов. Ясно, что обнаружению и предотвращению аномального трафика ARP не уделялось достаточного внимания большинством распространенных решений безопасности, даже если некоторый ненормальный трафик ARP может представлять серьезные угрозы.

В этой главе описаны три практических упражнения: (1) обнаружение аномального ARP-трафика с использованием XArp 2, (2) предотвращение аномального ARP-трафика с использованием функции безопасности Dynamic ARP Inspection (DAI) для среды без DHCP. в коммутаторах Cisco Catalyst 3560 и (3) предотвращение ненормального трафика ARP с использованием функций безопасности Dynamic ARP Inspection и DHCP snooping для среды DHCP в коммутаторах Cisco Catalyst 3560.

Глава 4

Обнаружение сетевого трафика и обнаружение случайного режима

4.1 Введение

Сниффинг-атака с использованием анализатора среди различных типов атак на локальные сети (ЛВС) - это простая атака, которая может быть очень опасной. Обнаружение сетевого трафика позволяет злоумышленникам легко красть конфиденциальные данные, пароли и конфиденциальность всех. Поскольку многие базовые службы, такие как FTP (протокол передачи файлов), Telnet и электронная почта (SMTP / POP3), отправляют пароли и данные в виде открытого текста, злоумышленники могут легко шпионить за пользователями сети, анализируя содержимое соответствующих перехваченных сетевой трафик. Для других сервисов может потребоваться программа дешифрования для извлечения паролей из потоков данных. Весь незащищенный сетевой трафик может быть уязвим для прослушивания.

Обнаружение сетевого трафика можно сделать, просто загрузив бесплатную программу-сниффер из Интернета и установив ее на компьютер. Кроме того, в коммутируемой ЛВС (не вещательная сеть) атака с использованием сниффинга требует, чтобы хост-сниффер был либо подключен к порту SPAN (анализатор коммутируемых портов) на коммутаторе сети, либо использовал метод, такой как MiM (Man In-the-Middle) атака, описанная в главе 2,

для перенаправления целевого трафика. Однако в широковещательных локальных сетях нет необходимости перенаправлять трафик на хост-анализатор или подключать хост-анализатор к порту SPAN, поскольку сетевой трафик передается на все хосты сети.

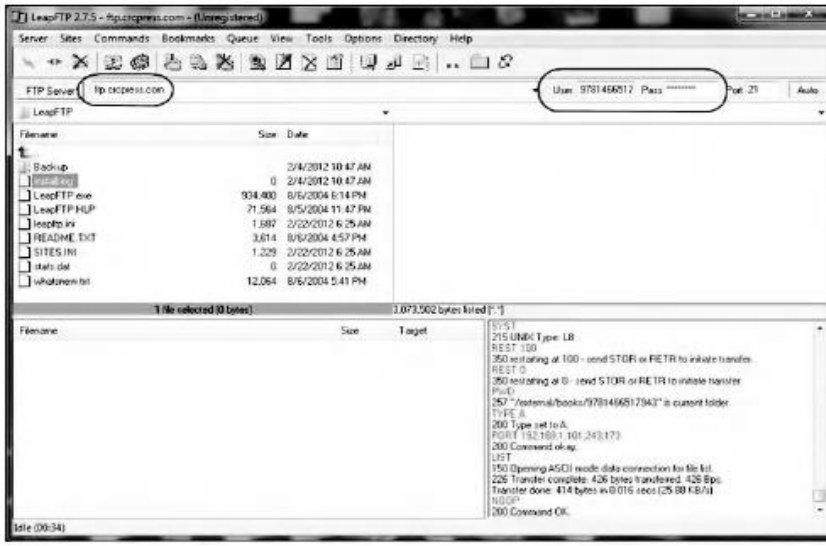
Анализаторы - это программы, которые позволяют хосту захватывать и отображать содержимое любого пакета, который проходит через сетевую интерфейсную карту (NIC) хоста, также известную как сетевой адаптер, даже если он не предназначен для хоста. Это может быть сделано путем перевода сетевого адаптера хоста в режим, называемый «смешанным режимом». Этот режим позволяет сетевому адаптеру получать вслепую любой пакет, а не только предназначенные для него пакеты, в сети Ethernet без проверки MAC-адреса назначения (Media Access). Контрольный адрес) и передать его ядру системы. Следовательно, пакеты, которые не должны поступать на хост-анализатор, больше не блокируются сетевым адаптером хоста. По умолчанию для сетевых карт установлен режим, называемый «нормальный режим». Когда сетевой адаптер хоста находится в нормальном режиме, он захватывает только пакеты, предназначенные для хоста, используя механизм фильтрации, известный как аппаратный фильтр сетевой карты. Таким образом, NIC хоста принимает только пакеты, чьи MAC-адреса назначения отправляются на MAC-адрес NIC хоста. Фактически, сетевые адаптеры представлены 6-байтовым аппаратным адресом (MAC-адрес Ethernet). Производители карт назначают уникальный MAC-адрес для каждой карты, так что каждый MAC-адрес является уникальным во всем мире. Все коммуникации в сети Ethernet основаны на этом аппаратном MAC-адресе одноадресной рассылки. Однако NIC может установить дополнительные аппаратные фильтры для приема пакетов разных типов. В обычном режиме NIC фильтрует пакеты на основе настроенного аппаратного фильтра. Ниже приведены возможные дополнительные аппаратные фильтры:

* *Broadcast (широковещательная рассылка)*: этот фильтр позволяет сетевой карте принимать широковещательные пакеты, для которых MAC-адрес назначения установлен на "*FF:FF:FF:FF:FF:FF*".

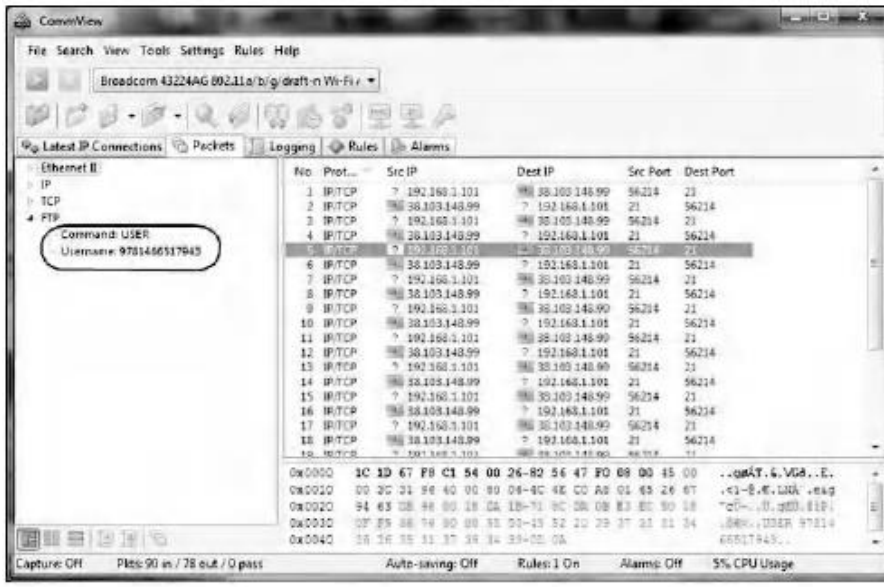
* *Multicast (многоадресная рассылка)*: этот фильтр позволяет сетевой карте принимать все пакеты, которые специально настроены для получения адресов некоторых групп многоадресной рассылки. NIC может принимать только пакеты с аппаратных адресов многоадресной рассылки, предварительно зарегистрированных в списке многоадресной рассылки. Пакеты многоадресной рассылки имеют адрес MAC назначения, установленный на "*01:00:5E:xx:xx:xx*".

All Multicast: этот фильтр позволяет NIC принимать все многоадресные пакеты, для которых установлен групповой бит "*01:xx:xx:xx:xx:xx*".

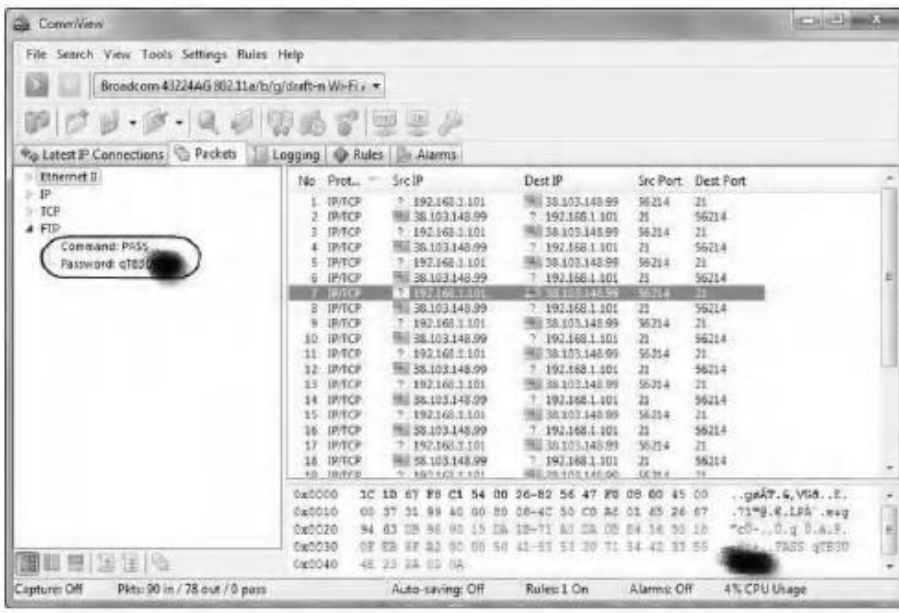
Следующие три снимка экрана являются примерами прослушивания пароля сеанса FTP. Анализатор CommView используется для захвата трафика сеанса FTP. На первом снимке экрана показан графический интерфейс пользователя (графический пользовательский интерфейс) инструмента LeapFTP (клиент FTP), подключенного к серверу FTP (ftp.crcpress.com) с использованием имени пользователя и пароля.



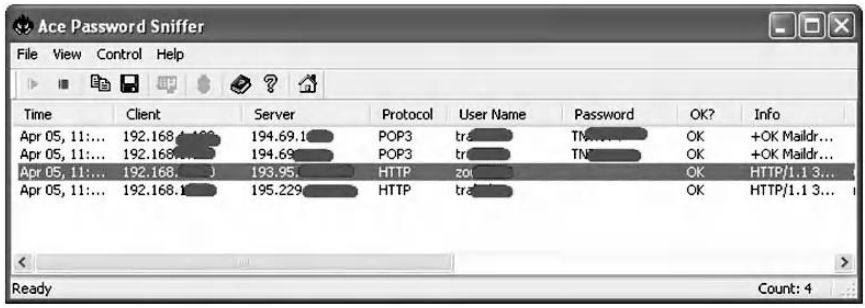
На следующем снимке экрана показано имя пользователя («9781466517943») сеанса FTP, захваченного анализатором CommView.



А на следующем снимке экрана показан пароль сеанса FTP, записанный анализатором CommView.



Существует множество готовых к использованию программ для анализа паролей, которые поддерживают мониторинг паролей через FTP, POP3 (Post Office Protocol 3), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol) и Telnet. Примеры перехватчиков паролей включают Ace Password Sniffer (http://www.effetech.com/aps/), Password Sniffer (htt://www.packet-sniffer.net/password-sniffer.htm), и SniffPass (http://www.nirsoft.net/utils/password_sniffer.html). В общем, анализаторы паролей - это небольшое программное обеспечение для мониторинга, которое прослушивает сети, захватывает пароли, которые проходят через сетевые адаптеры, и мгновенно отображает их на экране. На следующем снимке экрана показан пример прослушанных паролей, сгенерированных инструментом Ace Password Sniffer.



Атаки с использованием сетевого трафика обычно трудно обнаружить, потому что они вообще не влияют на сетевой трафик. На практике обнаружение узлов сети в сети состоит из обнаружения узлов с сетевыми картами, работающими в произвольном режиме. Узлы сети с сетевыми картами, работающими в случайном режиме, можно считать подозрительными узлами. Важно отметить, что некоторые программы, однажды установленные на хосте, могут установить сетевой адаптер хоста в беспорядочный режим, не имея намерения выполнять какие-либо злонамеренные действия по прослушиванию. Кроме того, пользователь хоста не знает о том, что установленная программа установила сетевой адаптер его хоста в случайный режим. Такой хост будет идентифицирован как подозрительный хост, поскольку его сетевой адаптер работает в случайном режиме. В таком случае администратор сети должен предпринять соответствующие действия.

В этой главе обсуждается практическое упражнение о том, как обнаружить сетевой адаптер, работающий в случайном режиме. Используются следующие программные инструменты:

* NetScanTools Pro *: случайный инструмент обнаружения
* PromiScan †: случайный инструмент обнаружения
* Инструмент CommView ‡: инструмент для мониторинга и анализа сети (анализатор)(sniffer)
* CommView Visual Packet Builder§: генератор пакетов на основе графического интерфейса пользователя (GUI)

4.2 Лабораторная работа 4.1: Обнаружение случайного режима

4.2.1 Результат

Цель этого упражнения состоит в том, чтобы учащиеся узнали, как обнаружить NICb, работающий в беспорядочном режиме.

4.2.2 Описание

Когда сетевой адаптер работает в беспорядочном режиме, пакеты, которые должны фильтроваться аппаратным фильтром сетевого адаптера, теперь передаются ядру системы. Поэтому, если мы настроим пакет запроса ARP (Address Resolution Protocol) таким образом, чтобы он не имел широковещательного MAC-адреса в качестве MAC-адреса назначения в заголовке Ethernet пакета, отправим его подозрительному узлу в сети и обнаружим, что хост отвечает на это, затем хост работает в беспорядочном режиме.

Следовательно, этот метод обнаружения состоит в проверке того, реагирует ли подозрительный хост на пакеты запросов ARP с перехватом, которые не должны обрабатываться подозрительным хостом. Поскольку

*http://www.netscantools.com
†http://www.securityfriday.com
‡http://www.tamos.com
§http://www.tamos.com

хост, принимающий анализ, получает пакеты, которые не нацелены на него, он может совершать ошибки, такие как ответ на пакет запроса ARP, который первоначально должен был фильтроваться аппаратным фильтром сетевого адаптера хоста. Следовательно, обнаружение выполняется путем проверки пакетов ответа ARP, когда пакеты запроса ARP отправляются подозрительному узлу в сети.

Например, MAC-адрес назначения пакета запроса прерывания ARP установлен на MAC-адрес, который не существует, такой как «00-00-00-00-00-01». Когда сетевой адаптер работает в обычном режиме, пакет прерывания ARP считается пакетом «для другого хоста» и отклоняется аппаратным фильтром сетевого адаптера. Однако, когда сетевой адаптер работает в случайном режиме, его аппаратный фильтр отключен. Затем пакет запроса прерывания ARP сможет передать ядру системы. Ядро системы предполагает, что пакет прибыл, потому что это было разрешено аппаратным фильтром NIC, и, следовательно, должен быть сгенерирован ответный пакет. Однако это не так. В ядре системы существует своего рода дополнительный программный фильтр, называемый программным фильтром. После аппаратного фильтра пакеты фактически снова фильтруются программным фильтром ядра системы. Поэтому, когда сетевая карта работает в обычном режиме, включаются аппаратные и программные фильтры. Однако, когда сетевая карта работает в случайном режиме, аппаратный фильтр отключен, но программный фильтр ядра системы остается включенным. Типы фильтров, выполняемых программным фильтром, зависят от ядра операционной системы (ОС).

4.2.3 Тесты

Целью тестов является выявление механизмов фильтрации, используемых программными фильтрами ядер нескольких распространенных ОС. Для каждого ядра ОС тесты состоят из определения специальных MAC-адресов, которые будут использоваться пакетами ARP-ловушек для обнаружения сетевых адаптеров, работающих в случайном режиме. Если ответ ARP получен в результате тестового пакета запроса ARP, то специальный MAC-адрес назначения, включенный в пакет запроса ARP, может быть использован для идентификации сетевых адаптеров, работающих в смешанном режиме. В следующем списке перечислены специальные MAC-адреса, используемые в тестах.

* FF:FF:FF:FF:FF:FF (Br): Это широковещательный MAC-адрес, который должны получать все хосты в локальной сети. Этот адрес не фильтруется аппаратными и программными фильтрами. Он используется для проверки того, поддерживает ли хост широковещательный MAC-адрес Br.

* FF:FF:FF:FF:FF:FE (Br47), FF:FF:00:00:00:00 (Br16), и FF:00:00:00:00:00 (Br8): Это поддельные широковещательные MAC-адреса. Они используются для проверки того, проверяет ли программный фильтр все биты данного MAC-адреса, чтобы классифицировать его как широковещательный MAC-адрес.

* 01:00:00:00:00:00 групповой бит адрес (Gr): это MAC-адрес, для которого установлен только групповой бит. Он используется для проверки того, считает ли программный фильтр MAC-адрес многоадресной рассылки.

* 01:00:5E:00:00:00 адрес многоадресной рассылки 0 (M0): Этот многоадресный MAC-адрес обычно не используется. Он используется для проверки того, считает ли программный фильтр MAC-адрес многоадресной рассылки.

* 01:00:5E:00:00:01 адрес многоадресной рассылки 1 (M1): Это MAC-адрес многоадресной рассылки, который должны получать все хосты в локальной сети. Этот адрес не фильтруется аппаратными и программными фильтрами. Он используется для проверки того, поддерживает ли хост MAC-адреса многоадресной рассылки.

➓ 01:00:5E:00:00:02 адрес многоадресной рассылки 2 (M2): Этот многоадресный MAC-адрес называется адресом многоадресной группы «Все маршрутизаторы». Он адресован всем маршрутизаторам в одном сегменте сети. Следовательно, это пример многоадресных MAC-адресов, которые не зарегистрированы в многоадресных списках сетевых адаптеров. Он используется для проверки того, считает ли программный фильтр MAC-адрес многоадресной рассылки.

* 01:00:5E:00:00:03 адрес многоадресной рассыки 3 (M3): Этот многоадресный MAC-адрес является примером многоадресных адресов, которые не назначены. Он используется для проверки того, считает ли программный фильтр MAC-адрес многоадресной рассылки.

В таблице 4.1 и таблице 4.2 показаны результаты испытаний для нескольких ОС. После отправки пакета запроса ARP, если ответный пакет ARP не получен, в столбце помещается «-». Если получен допустимый ответный пакет ARP, в столбце помещается буква «O». Однако, если получен недопустимый пакет ответа ARP, в столбце помещается символ «X». Ответ ARP считается недопустимым, когда предполагается, что соответствующий ему пакет запроса ARP заблокирован аппаратными или программными фильтрами, и, следовательно, пакет ответа ARP не должен приниматься. Однако, когда сетевая карта работает в случайном режиме, результаты теста показывают, что программные фильтры ядра протестированной ОС неправильно фильтруют MAC-адреса нескольких типов, в основном адреса Br47 и Br16.

MAC-адрес Br и многоадресный MAC-адрес M1, когда сетевой адаптер работает в обычном режиме. Однако, когда сетевой адаптер работает в случайном режиме, результаты теста выполняются в операционной системе. Это,

* В случае Windows 7, Windows Vista, Mac OS 10.7.3, Ubuntu 8.10, Red Hat Enterprise 7.2 и FreeBSD 5.0 их системные ядра отвечали на все поддельные широковещательные MAC-адреса (Br47, Br16 и Br8) и на MAC адреса с установленным групповым битом (Gr, M0, M2 и M3). Следовательно, вышеупомянутые MAC-адреса могут использоваться для идентификации сетевых адаптеров, работающих в случайном режиме. Широковещательный MAC-адрес Br и многоадресный MAC-адрес M1 не рассматриваются, поскольку они являются адресами, которые должны получать все узлы в локальной сети. Для вышеупомянутых ОС на следующем рисунке показано, что поддельные широковещательные MAC-адреса Br47, Br16 и Br8 фильтруются.

Таблица 4.1. Обнаружение случайного режима для операционных систем Windows

Operating Systems / *MAC Addresses*		*Windows 7 Home Premium*		*Windows XP*		*Windows Server 2003 Enterprise Edition*		*Windows Vista*		*Windows 2000/NT*	
		Normal	*Promiscuous*	*Normal*	*Promiscuous*	*Normal*	*Promiscuous*	*Normal*	*Promiscuous*	*Normal*	*Promiscuous*
FF:FF:FF:FF:FF:FF	Br	O	O	O	O	O	O	O	O	O	O
FF:FF:FF:FF:FF:FE	Br47	—	X	—	X	—	X	—	X	—	X
FF:FF:00:00:00:00	Br16	—	X	—	X	—	X	—	X	X	X
FF:00:00:00:00:00	Br8	—	X	—	—	—	—	—	X	—	—
01:00:00:00:00:00	Gr	—	X	—	—	—	—	—	X	—	—
01:00:5E:00:00:00	M0	—	X	—	—	—	—	—	X	—	—
01:00:5E:00:00:01	M1	O	O	O	O	O	O	O	O	O	O
01:00:5E:00:00:02	M2	—	X	—	—	—	—	—	X	—	—
01:00:5E:00:00:03	M3	—	X	—	—	—	—	—	X	—	—

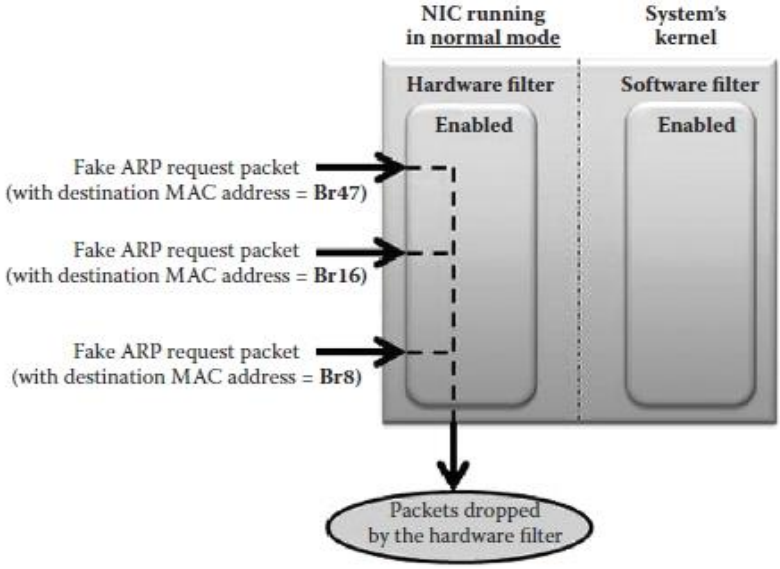
Примечание: O: легальный ответ, X: нелегальный ответ, —: нет ответа.

Таблица 4.2 Обнаружение случайного режима для других операционных систем

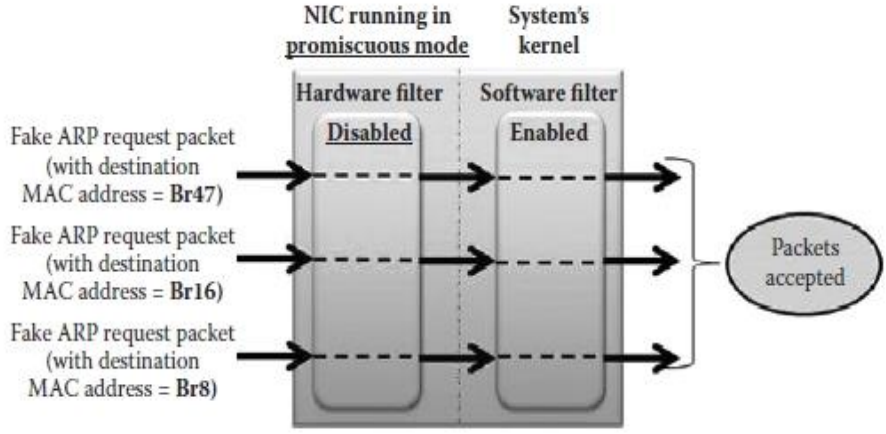
Operating Systems / *MAC Addresses*		*Mac OS X Version 10.7.3*		*Ubuntu 8.10, Kernel 2.6.27-7 generic*		*Red Hat Enterprise 7.2, Kernel 2.4.9-e.12*		*FreeBSD 5.0*	
		Normal	*Promiscuous*	*Normal*	*Promiscuous*	*Normal*	*Promiscuous*	*Normal*	*Promiscuous*
FF:FF:FF:FF:FF:FF	Br	O	O	O	O	O	O	O	O
FF:FF:FF:FF:FF:FE	Br47	—	X	—	X	—	X	—	X
FF:FF:00:00:00:00	Br16	—	X	—	X	—	X	—	X
FF:00:00:00:00:00	Br8	—	X	—	X	—	X	—	X
01:00:00:00:00:00	Gr	—	X	—	X	—	X	—	X
01:00:5E:00:00:00	M0	—	X	—	X	—	X	—	X
01:00:5E:00:00:01	M1	O	O	O	O	O	O	O	O
01:00:5E:00:00:02	M2	—	X	—	X	—	X	—	X
01:00:5E:00:00:03	M3	—	X	—	X	—	X	—	X

Примечание: O: легальный ответ, X: нелегальный ответ, —: нет ответа.

аппаратный фильтр, когда сетевая карта работает в обычном режиме.



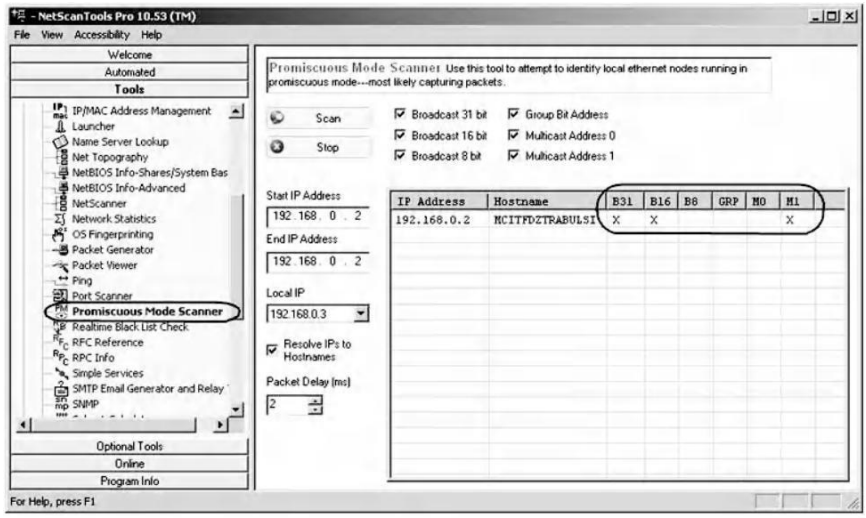
Однако они принимаются и отправляются ядру системы, когда сетевая карта работает в случайном режиме, как показано на рисунке ниже.

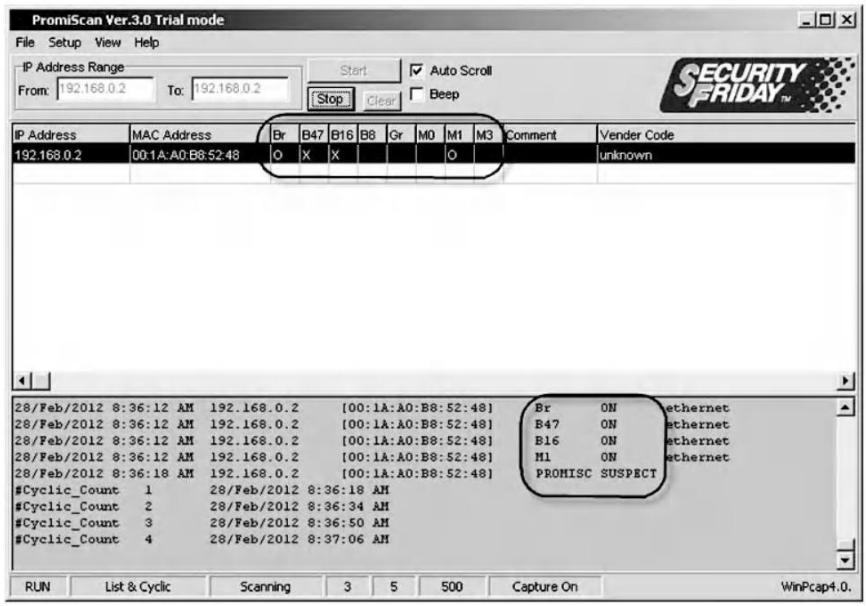


* В случае Windows XP и Windows Server 2003 их системные ядра отвечали только на поддельные широковещательные MAC-адреса Br47 и Br16. Следовательно, программные фильтры определяют широковещательный MAC-адрес, проверяя только первые 2 байта. Следовательно, адреса Br47 и Br16 могут использоваться для идентификации того, работает ли сетевой адаптер в случайном режиме.
* В случае Windows 2000 / NT ядра системы реагировали только на ложные широковещательные MAC-адреса Br47 и Br16. Следовательно, программные фильтры Windows 2000 / NT идентифицируют широковещательный MAC-адрес, проверяя только первые 2 байта. Важно отметить, что когда сетевая карта работает в обычном режиме, Windows 2000 / NT также отвечала на ложную трансляцию MAC Br16. Следовательно, только поддельный широковещательный MAC-адрес Br47 может быть использован для идентификации того, работает ли NIC в случайном режиме.

4.2.4 Средства обнаружения случайного режима

Доступен ряд готовых к использованию инструментов для обнаружения случайных ошибок, таких как PMD (http://webteca.altervista.org/index.htm), PromiScan (http://www.securityfriday.com), Nmap (http://www.nmap.org), и NetScanTools Pro (http://www.netscantools.com).. Инструменты используются для определения наличия устройства, прослушивающего пакеты, которое не должно прослушивать пакеты. Большинство из этих инструментов основаны на вышеописанной методике обнаружения. Например, на следующих двух снимках экрана показаны результаты сканирования случайного режима целевого хоста с использованием инструментов NetScanTools Pro и PromiScan соответственно. MAC-адреса, используемые этими двумя инструментами, также показаны. В NetScanTools Pro поддельная трансляция B31 соответствует поддельной трансляции Br47 (FF:FF:FF:FF:FF:FE).





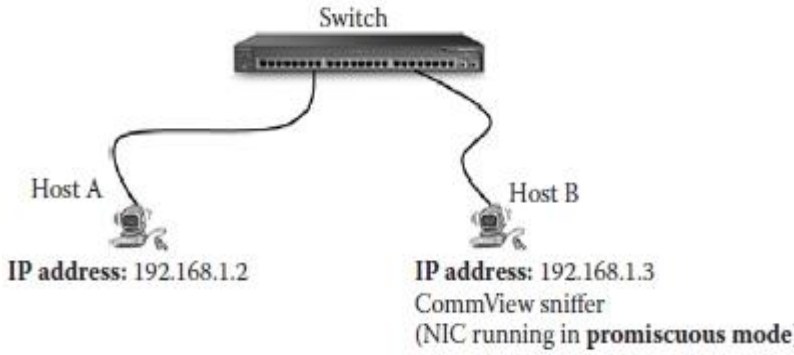
Основное ограничение этого метода обнаружения состоит в том, что, если узел перехвата перестает отвечать на сообщения запроса ARP во время перехвата сетевого трафика, используя, например, локальный межсетевой экран, тогда метод становится бесполезным, поскольку он опирается на сообщения ответа ARP, сгенерированные анализатором хоста.

4.2.5 Эксперимент

Поскольку эта книга имеет образовательную цель, в следующем эксперименте описывается, как вручную генерировать пакеты запросов ARP-ловушек для идентификации сетевых адаптеров, работающих в случайном режиме в локальной сети.

4.2.6 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Два хоста, A и B, подключены к коммутатору и работают под управлением операционной системы Windows 7.



4.2.7 Эксперимент

Эксперимент состоит из следующих этапов:

Шаг 1: Назначьте статические IP-адреса хостам сети.
Шаг 2: Запустите NIC хоста B в случайном режиме.
Шаг 3: Сгенерируйте пакеты запроса ARP прерывания.
Шаг 4: Анализ пакетов ответа ARP.

4. *2.7.1 Шаг 1. Назначьте статические IP-адреса хостам сети*

Обратитесь к Главе 1.

4.2.7.2 Шаг 2: Запустите сетевую карту хоста B в случайном режиме

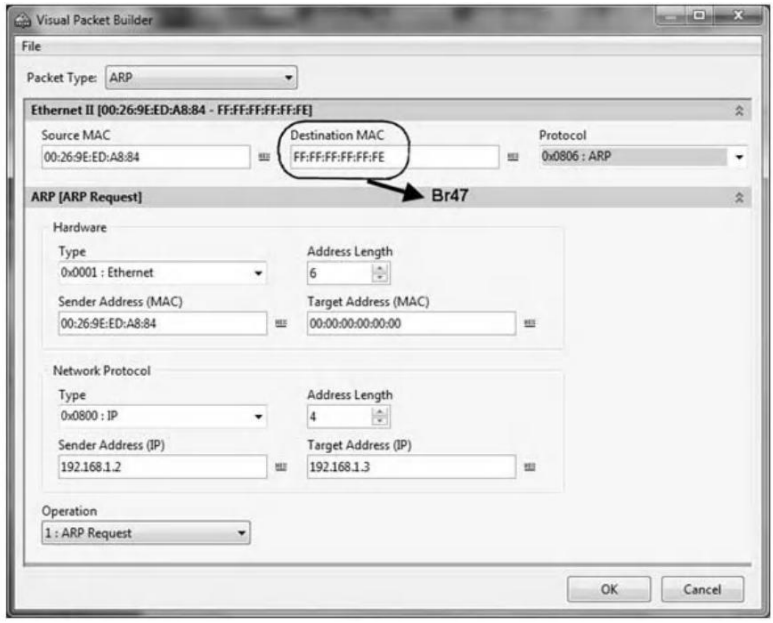
Установите сниффер CommView (или любой доступный инструмент сниффера) на хосте B, чтобы его сетевой адаптер работал в случайном режиме.

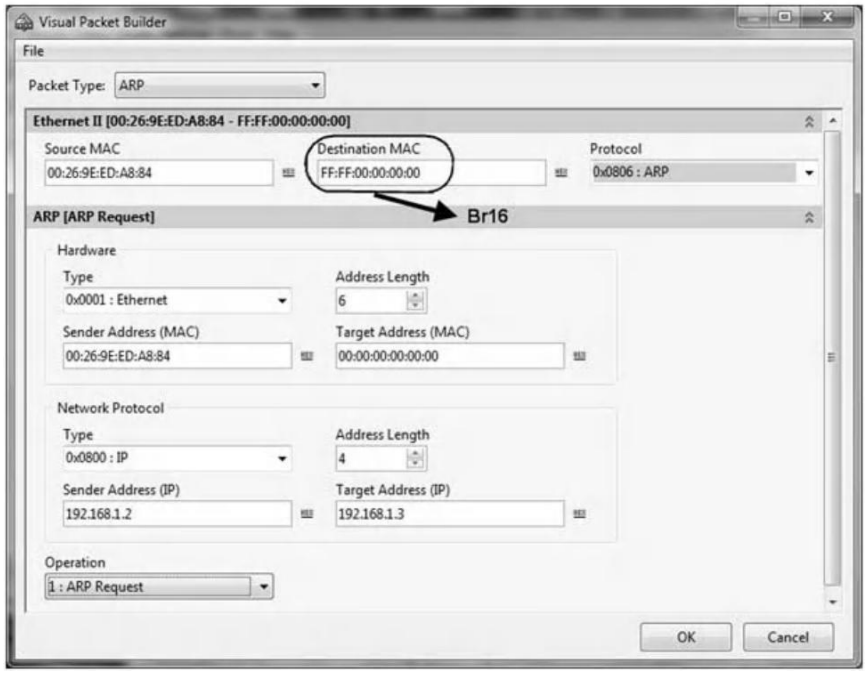
4.2.7.3 Шаг 3. Создание пакетов запросов ARP-ловушек

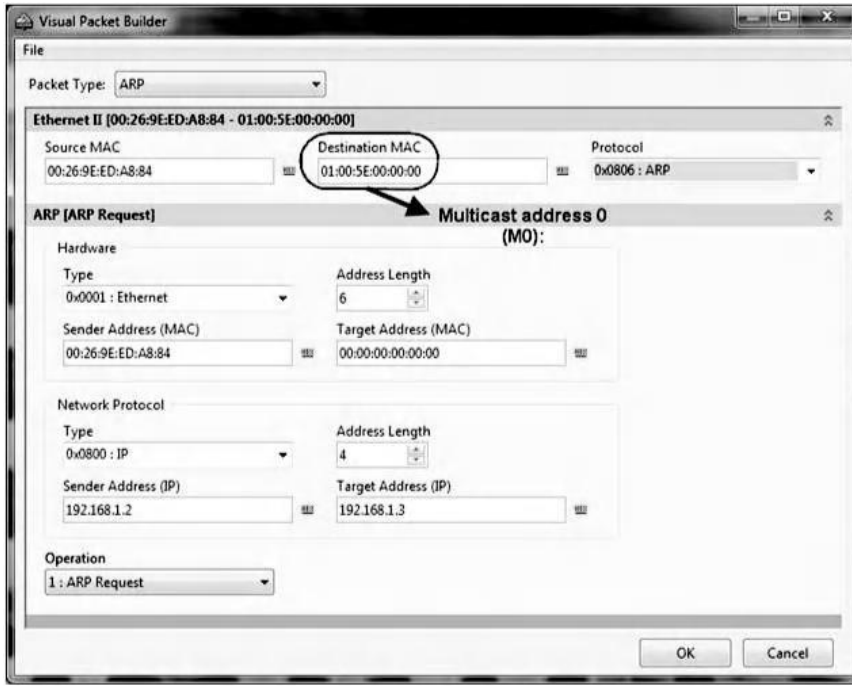
На хосте A проводятся тесты, чтобы определить, работает ли сетевой адаптер хоста B в случайном режиме. Следовательно, хост A продолжит отправку нескольких пакетов запроса ARP с перехватом на хост B, используя поддельные широковещательные MAC-адреса Br47 и Br16 и многоадресные MAC-адреса M0, M2 и M3. Пакеты запроса прерывания ARP будут выглядеть следующим образом:

ARP Header	
Operation code	1 (for ARP request)
Source IP address	IP address of Host A
Source MAC address	MAC address of Host A
Destination IP address	IP address of Host B
Destination MAC address	00:00:00:00:00:00
Ethernet Header	
Source MAC address	MAC address of Host A
Destination MAC address	Br47, Br16, M0, M2, M3
Ethernet type	0x0806 for ARP message

Используя любой инструмент построения пакетов, вышеупомянутые запросы ARP могут быть легко созданы. CommView Visual Packet Builder предоставляет очень удобный графический интерфейс для создания пакетов ARP. Три снимка экрана, которые следуют, показывают содержание примеров пакетов запроса ARP-прерывания с MAC-адресами назначения Br47, Br16 и M0 соответственно.

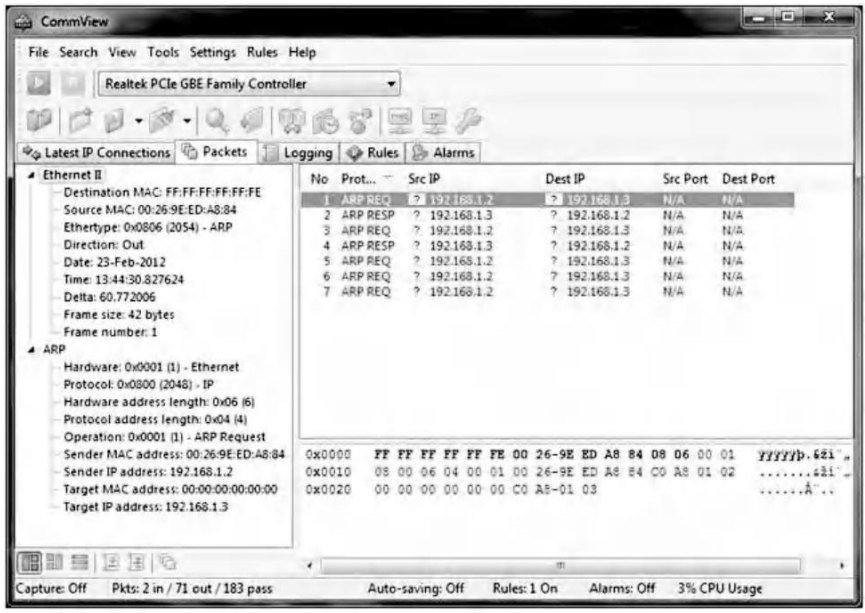

Visual Packet Builder
File
Packet Type: ARP
Ethernet II [00:26:9E:ED:A8:84 - FF:FF:FF:FF:FF:FE]
Source MAC
00:26:9E:ED:A8:84
Destination MAC
FF:FF:FF:FF:FF:FE
Protocol
0x0806 : ARP
Br47
ARP [ARP Request]
Hardware
Type
0x0001 : Ethernet
Address Length
6
Sender Address (MAC)
00:26:9E:ED:A8:84
Target Address (MAC)
00:00:00:00:00:00
Network Protocol
Type
0x0800 : IP
Address Length
4
Sender Address (IP)
192.168.1.2
Target Address (IP)
192.168.1.3
Operation
1 : ARP Request
OK
Cancel

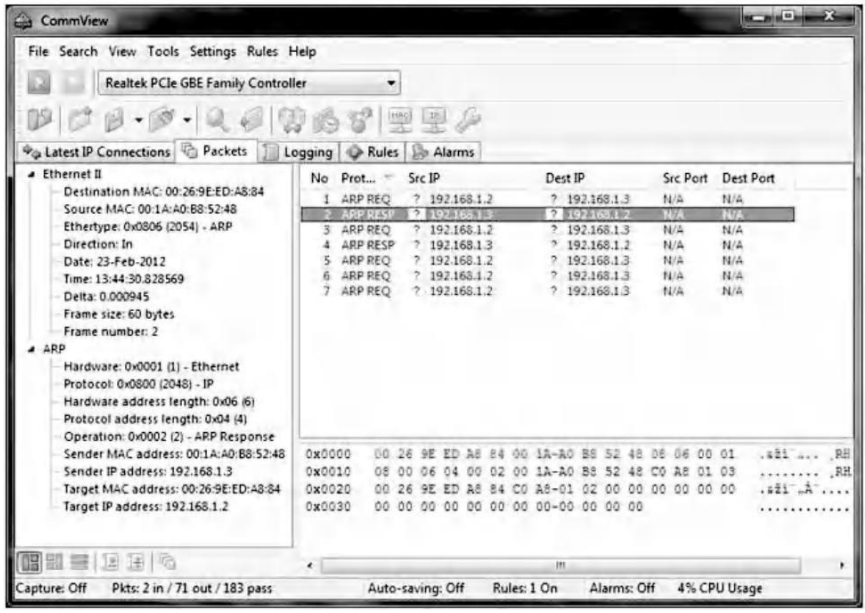

Visual Packet Builder
File
Packet Type: ARP
Ethernet II [00:26:9E:ED:A8:84 - FF:FF:00:00:00:00]
Source MAC
00:26:9E:ED:A8:84
Destination MAC
FF:FF:00:00:00:00
Protocol
0x0806 : ARP
Br16
ARP [ARP Request]
Hardware
Type
0x0001 : Ethernet
Address Length
6
Sender Address (MAC)
00:26:9E:ED:A8:84
Target Address (MAC)
00:00:00:00:00:00
Network Protocol
Type
0x0800 : IP
Address Length
4
Sender Address (IP)
192.168.1.2
Target Address (IP)
192.168.1.3
Operation
1 : ARP Request
OK
Cancel



4.2.7.4 Шаг 4: Анализ пакетов ответа ARP

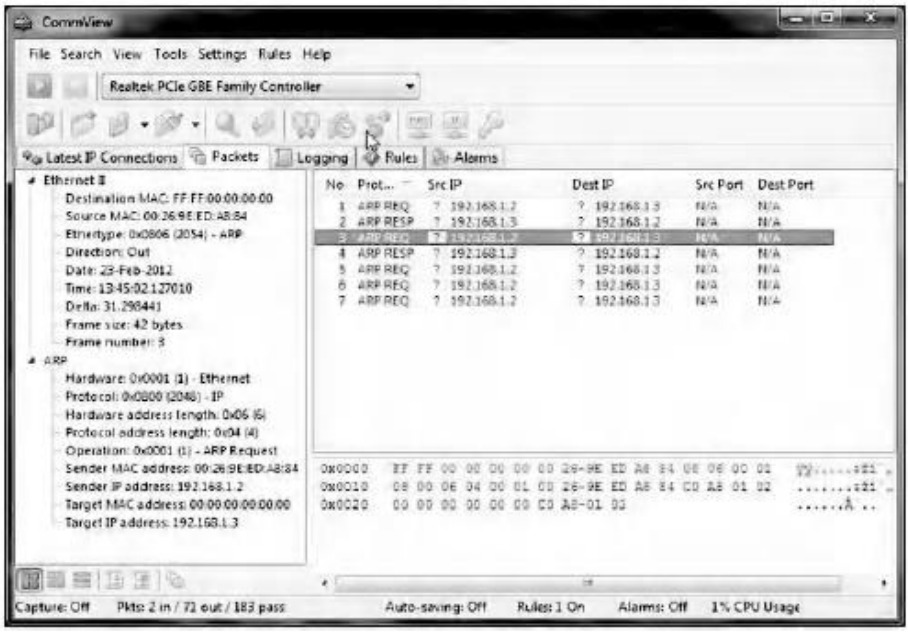
Узел A использует анализатор CommView для сбора любых пакетов ответа ARP, сгенерированных узлом B после получения пакетов запросов ARP прерывания. На следующем снимке экрана анализатора CommView показано содержимое сгенерированного пакета запроса ARP прерывания с MAC-адресом назначения Br47. И следующий снимок экрана ясно показывает, что пакет ответа ARP был получен от хоста B после отправки вышеупомянутого пакета запроса ARP прерывания.

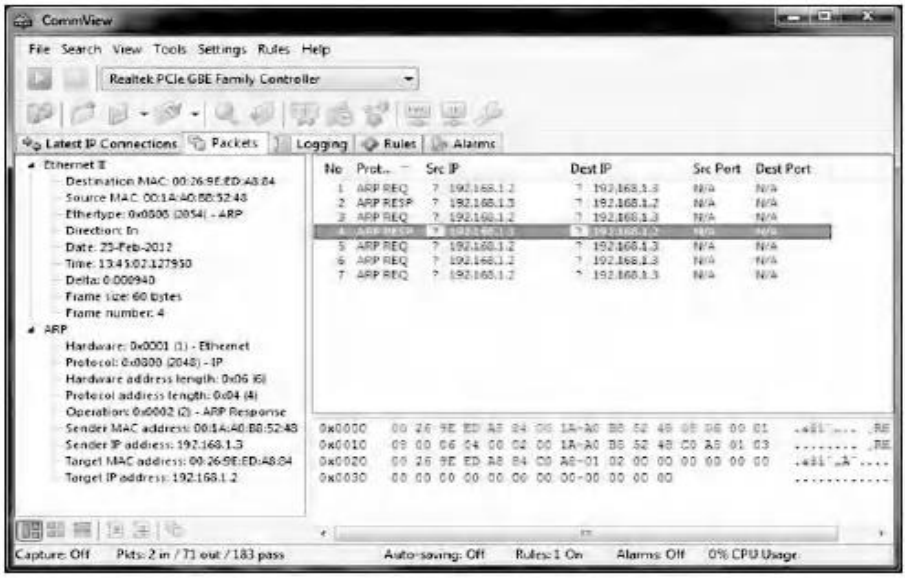




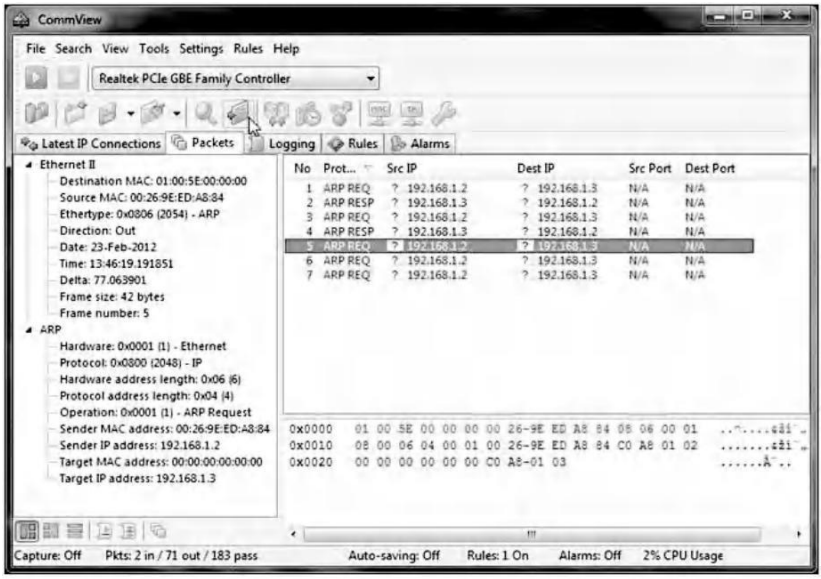
На следующем снимке экрана показано содержимое сгенерированного пакета запроса ARP прерывания с MAC-адресом назначения Br16. И на следующем снимке экрана

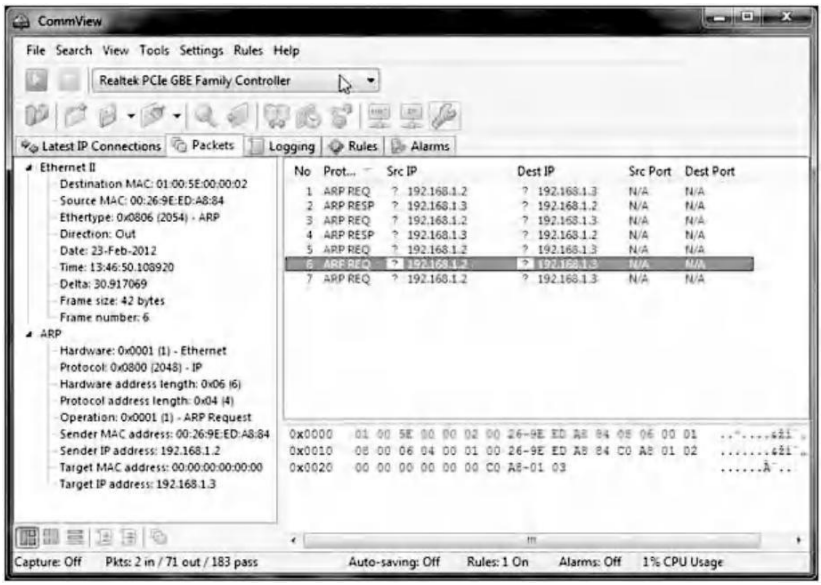
показано, что ответный пакет ARP был получен от хоста B после отправки вышеупомянутого пакета запроса прерывания ARP.

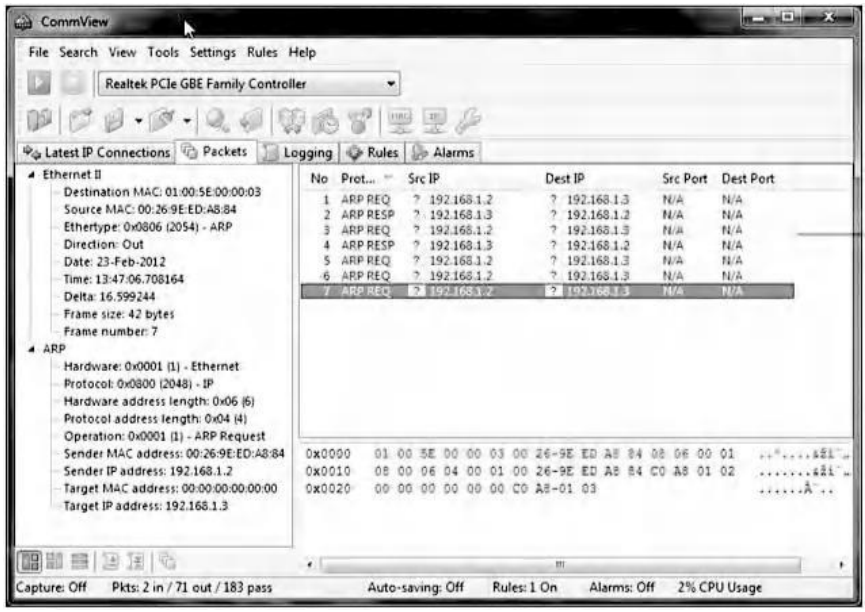




Тем не менее, три следующих снимка экрана показывают, что анализатор CommView не перехватил ни один ответный пакет ARP, выданный хостом B, после отправки пакетов запросов ARP прерывания с MAC-адресами многоадресной рассылки назначения M0, M2 и M3 соответственно.







Следовательно, ядро системы хоста B отвечало на ложные широковещательные MAC-адреса Br47 и Br16 и не отвечало на многоадресные MAC-адреса M0, M1 и M2. Следовательно, основываясь на результатах, показанных в таблицах 4.1 и 4.2, сетевая карта хоста B работает в беспорядочном режиме, а операционная система хоста B в основном представляет собой систему на базе Windows.

4.2.8 Сниффинг беспроводной сети

В беспроводных локальных сетях (WLAN) беспроводные сетевые карты не поддерживают случайный режим, но могут работать в шести режимах: Master (действующий как точка доступа), Managed/управляемый (клиент, также известный как станция), Ad-hoc, Mesh, Повторитель(Repeater) и режим RF Monitor.

Режим RF Monitor позволяет беспроводным сетевым картам захватывать пакеты без необходимости предварительно связываться с точкой доступа или специальной сетью. Режим RF Monitor также позволяет беспроводной сетевой карте пассивно захватывать пакеты без передачи каких-либо пакетов. Анализатор беспроводной сети может начать мониторинг беспроводных сетей только после установки

беспроводной карты в режим RF Monitor. Когда работает беспроводной анализатор, единственное, что требуется для мониторинга беспроводной сети, - это находиться в пределах диапазона сигнала. Затем анализатор перехватывает и отображает беспроводные пакеты и может отображать узлы, точки доступа (AP), идентификатор набора служб (SSID), уровень сигнала и другие важные статические параметры сети. В режиме RF Monitor беспроводная карта не проверяет правильность значений циклического избыточного кода (CRC) для перехваченных пакетов, поэтому некоторые перехваченные пакеты могут быть повреждены. Хакеры могут использовать режим RF Monitor для злонамеренных целей, таких как сбор трафика для взлома WEP.

Обнаружение беспроводных сетевых карт, работающих в режиме RF Monitor, представляет собой сложную задачу, отличающуюся от задачи обнаружения проводных сетевых карт, работающих в случайном режиме. Трудность заключается в том, что при настройке в режиме радиочастотного монитора беспроводная карта прекращает передачу данных. Традиционные методы обнаружения обычно полагаются на использование пакетов-ловушек для идентификации проводных сетевых карт, работающих в случайном режиме. Однако, когда беспроводная карта не передает данные, становится, следовательно, трудно определить, обнаруживает ли она сеть или нет, и установлен ли он в режим RF Monitor.

4.2.8.1 Взлом WEP-ключа и расшифровка сетевого трафика

Wired Equivalent Privacy (WEP) - это протокол безопасности, определенный в стандарте IEEE Wireless Fidelity (Wi-Fi) 802.11, который предназначен для обеспечения защиты беспроводных локальных сетей. WEP обеспечивает безопасность сетей Wi-Fi 802.11 на канальном уровне (модель OSI уровень 2). WEP стремится установить защиту, аналогичную той, которую обеспечивают меры физической безопасности проводной сети, путем шифрования данных, передаваемых через WLAN.

WEP использует потоковый шифр RC4 для конфиденциальности и контрольную сумму CRC-32 для целостности. WEP использует 64-битный (или 128-битный) ключ шифрования. Ключ состоит из

24-битного вектора инициализации (IV) и 40-битного (или 104-битного) ключа WEP. Из-за уязвимостей WEP ключ WEP можно легко взломать с помощью инструментов с открытым исходным кодом. WEP амортизировался в 2004 году и был заменен на WPA.

Взлом WEP включает в себя следующие этапы: отслеживание, анализ сетевого трафика, взлом ключа WEP и дешифрование захваченного трафика с использованием ключа взлома WEP.

4.2.8.1.1 Вардрайвинг и сниффинг

Wardriving - это процесс сканирования обнаруженных точек доступа вокруг здания или в другом месте с помощью компьютера. Существует много доступных инструментов, таких как CommView for WiFi *, Cain и Abel †, KisMAC ‡, Kismet§ и Wireshark¶, которые можно использовать для выполнения вардрайвинга. Wardriving собирает и регистрирует такую информацию, как SSID беспроводных сетей, используемый протокол безопасности (например, WEP, WPA и т. Д.), MAC-адрес точки доступа и список клиентов, подключенных к ней в настоящее время, а также их MAC-адреса. Например, после выполнения wardriving с использованием CommView для инструмента WiFi на следующем снимке экрана показан список идентифицированных SSID и MAC-адреса точек доступа и клиентов станции по каналам.

---

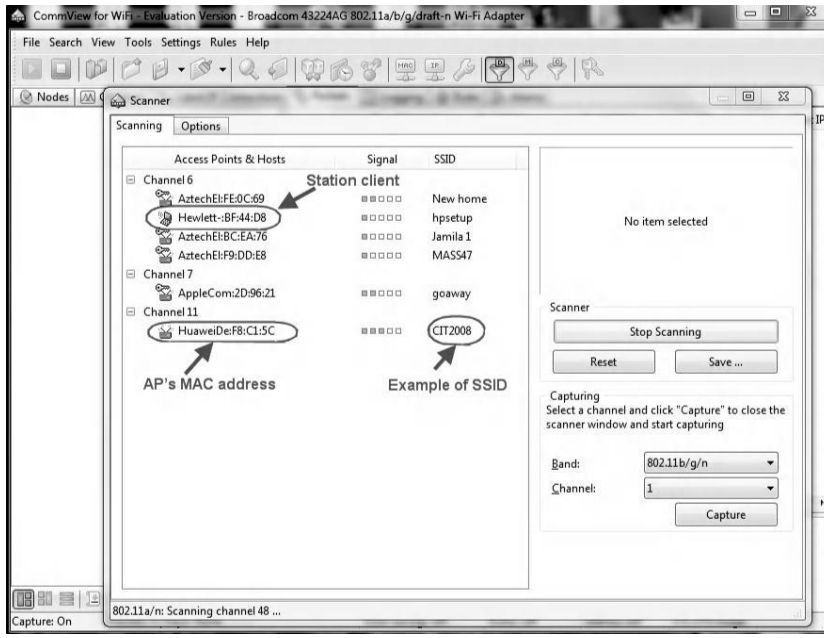
*http://www.tamos.com

† http://www.oxid.it/cain.html

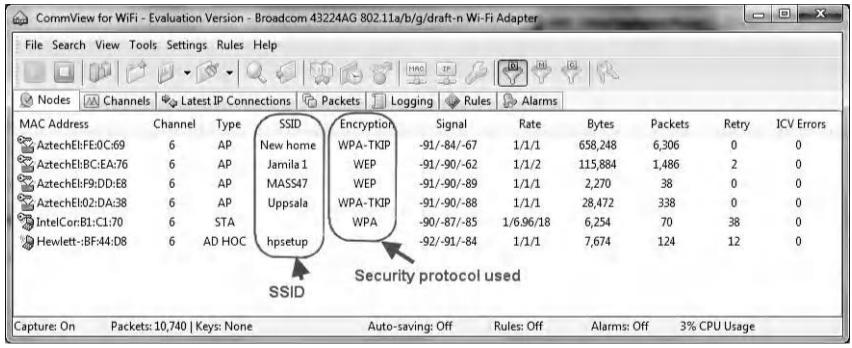
‡ http://kismac-ng.org

§ http://www.kismetwireless.net ¶

http: //www.Wireshark.org



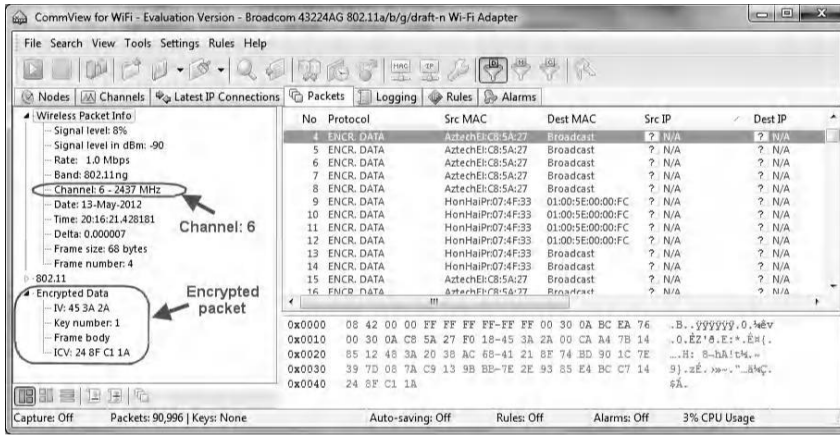
На следующем снимке экрана показан протокол безопасности (например, WEP, WPA и т. д.) для каждой точки доступа канала 6.



Беспроводной сниффер позволяет настроить сетевую карту на определенный канал и собирать все радиосигналы в пределах диапазона сетевой карты. Примерами таких снифферов являются CommView for WiFi, Kismet, Wireshark и Airodump * (который является частью пакета Aircrack). Пакеты, полученные с помощью этих снифферов, обычно

* http: //www.aircrack-ng.org

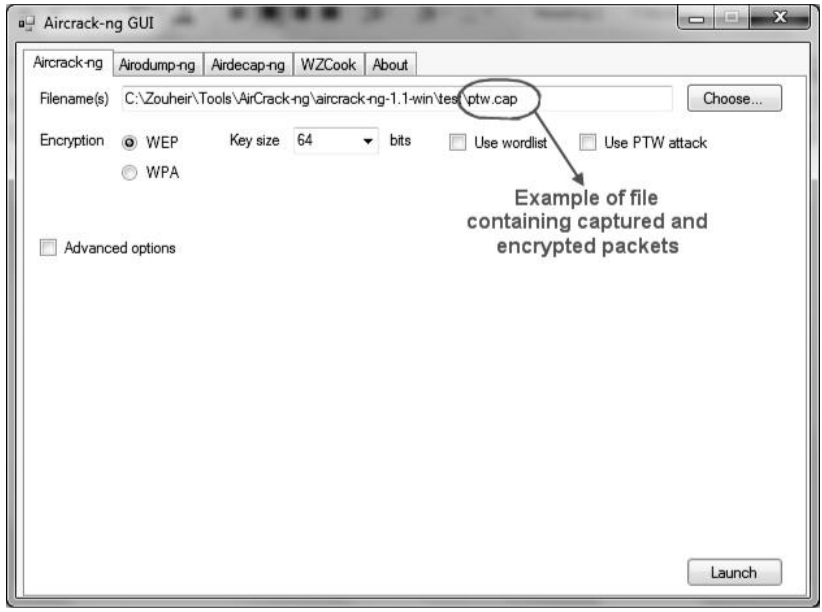
сохраняются в файлах с расширением .cap. Данные в пакетах захвата могут быть использованы в ряде атак позже. На следующем снимке экрана показаны зашифрованные пакеты, захваченные CommView для инструмента WiFi для канала 6.



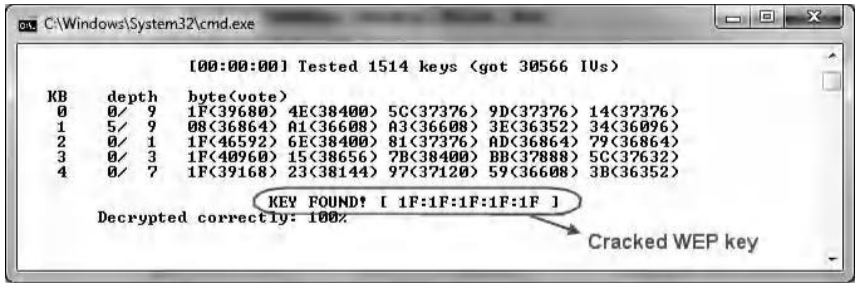
4.2.8.1.2 Взлом WEP-ключа

Когда достаточное количество зашифрованных пакетов собрано с помощью сниффинга, пользователь может приступить к взлому ключа WEP. IV в пакетах необходимы для взлома ключа WEP. Количество захваченных IV, необходимых для взлома ключа, зависит от размера ключа AP. Для 64-битного шифрования требуется от 250 000 до 500 000 IV, в зависимости от сложности ключа. Ключ состоит из десяти цифр со значениями A-F и 0-9. Для взлома 128-битного шифрования требуется от 500 000 до 1 миллиона IV. Примеры программ, способных взламывать ключи WEP, включают KisMAC, Aircrack, Cain и Abel и AirSnort *. На следующем снимке экрана показан графический интерфейс инструмента Aircrack-ng, используемого для взлома ключа WEP.

* http://airsnort.shmoo.com

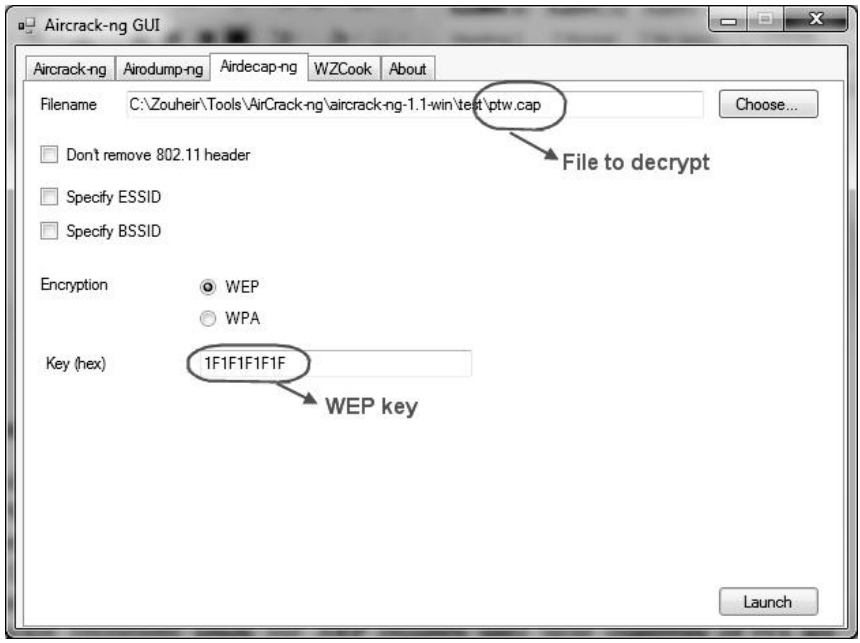


На следующем снимке экрана показан результат взлома ключа WEP с помощью инструмента Aircrack-ng. Найден ключ WEP «1F:1F:1F:1F:1F».



4.2.8.1.3 Расшифровка сетевого трафика

После взлома ключа WEP пользователь может использовать ключ для расшифровки захваченного сетевого трафика с помощью такого инструмента, как Airdecap-ng (часть пакета Aircrack). На следующем снимке экрана показан интерфейс графического интерфейса инструмента Airdecap-ng, используемого для дешифрования зашифрованного файла с помощью ключа WEP «1F: 1F: 1F: 1F: 1F».



4.3 Краткое содержание главы

В этой главе обсуждались атаки с прослушиванием и обнаружением сетевых карт, работающих в беспорядочном режиме. В локальных сетях сниффинг с злонамеренными целями может нанести вред. Это позволяет злоумышленникам легко красть конфиденциальные данные, пароли и личную информацию. В этой главе также разъясняются концепции аппаратного фильтра NIC и программного фильтра ядра системы и описывается общая методика обнаружения сетевых карт в случайном режиме. Практическое упражнение главы было посвящено внедрению метода обнаружения и тому, как вручную генерировать пакеты запросов ARP с прерыванием для обнаружения сетевых адаптеров, работающих в случайном режиме.

Глава 5

IP-атаки типа «отказ в обслуживании»

5.1 Введение

Это очень расстраивает, когда некоторые услуги недоступны, а недоступность не объясняется. Когда система перегружает все свои ресурсы, она становится непригодной для использования или обеспечивает очень низкую производительность для законных пользователей. Эта атака на системные ресурсы называется атакой отказа в обслуживании (DoS). DoS-атаки могут быть направлены на систему, чтобы предотвратить сетевое взаимодействие, или могут быть нацелены на всю организацию, чтобы предотвратить исходящий или входящий трафик к определенным сетевым службам, таким как веб-сайт организации или службы электронной почты.

Суровая правда в том, что организовать эти DoS-атаки гораздо проще, чем удаленно получить доступ к целевой системе. Следовательно, DoS-атаки стали очень распространенным явлением в Интернете. Они либо преднамеренные, либо случайные. DoS-атака вызывается преднамеренно, когда неавторизованный пользователь активно перегружает ресурс, и случайно, когда авторизованный пользователь непреднамеренно делает что-то, что делает службы недоступными.

DoS-атаки можно условно разделить на два типа. Первый тип вызывает системный сбой или сбой сети. Когда злоумышленник направляет данные или пакеты в систему (жертву), это может привести к сбою или перезагрузке системы. Следовательно, ресурсы системы недоступны. Второй тип атаки включает в себя заполнение системы или сети большими объемами информации и тем самым делает ее не отвечающей. Следовательно, когда законные пользователи пытаются подключиться к системе, им отказывают в доступе, потому что все ресурсы были исчерпаны. В последнем случае злоумышленник должен постоянно заполнять систему информационными пакетами на время атаки. После прекращения наводнения атака заканчивается, и система возобновляет работу.

К сожалению, DoS-атаки не могут быть полностью предотвращены. Всегда существует вероятность того, что злоумышленник отправит избыточную информацию в систему, которую он не сможет обработать. Угроза DoS-атак может быть сведена к минимуму путем увеличения пропускной способности сети и использования исправлений производителя, брандмауэров, систем предотвращения вторжений (IPS) и правильной конфигурации сети. Тем не менее, злоумышленник всегда может использовать дополнительные ресурсы, чтобы затопить целевую систему или сеть и изобрести новые типы DoS-атак.

Большинство DoS-атак основаны на слабых сторонах протоколов TCP / IP. Ниже приведены некоторые из классических DoS-атак: Ping of Death, Land, Smurf, SYN Flood, UDP Flood, SSPing, ICMP Flood, ICMP Fragment, ICMP-пакет большого размера, CPU Hog, Win Nuke, RPC Locator, Jolt2 и Bubonic.

5.1.1 Распределенная атака типа «отказ в обслуживании» (DDoS)

Распределенная атака типа «отказ в обслуживании» (DDoS) - это DoS-атака, которая монтируется из большого количества мест в сети. Атаки обычно проводятся с нескольких скомпрометированных систем. Эти системы могли быть скомпрометированы троянским конем или червем, или они могли быть скомпрометированы путем взлома вручную.

Эти скомпрометированные системы обычно управляются с помощью довольно сложного программного обеспечения клиент-сервер, такого как Trinoo, Tribe Flood Network, Stacheldraht, TFN2K или Shaft. DDoS-атаки очень трудно защитить.

Эта глава включает в себя четыре практических упражнения по генерации и обнаружению четырех распространенных DoS-атак, а именно: наземная атака, SYN-атака Flood, Teardrop-атака и UDP-Flood-атака. Кроме того, эта глава включает практическое упражнение о создании и обнаружении ненормальных IP-пакетов, которые могут содержать скрытые угрозы или DoS-трафик

В этих практических упражнениях используются следующие аппаратные устройства и программные средства:

* Беспроводное устройство Juniper Networks SSG20 (устройство Juniper Networks): устройство обнаружения вторжений
* Инструмент CommView †: инструмент сетевого мониторинга и анализатора (сниффер)
* CommView Visual Packet Builder ‡: генератор пакетов на основе графического интерфейса пользователя (GUI)
* FrameIP Packet Generator§: онлайн генератор пакетов
* Advanced Port Scanner¶: инструмент для сканирования портов
* Fast Port Scanner**: инструмент для сканирования портов

* http://www.juniper.net
† http://www.tamos.com
‡ http://www.tamos.com
§ http://www.frameip.com¶
http://www.radmin.com
* http://www.globalwebmonitor.com

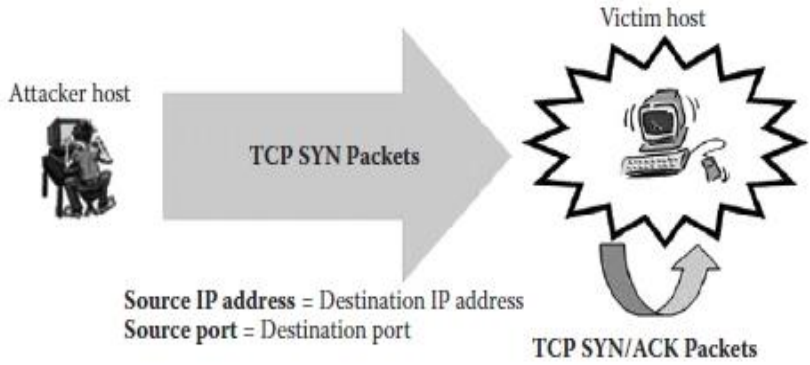
5.2 Лабораторная работа 5.1: Land-атака

5.2.1 Результат

Цель этого упражнения состоит в том, чтобы учащиеся научились генерировать и обнаруживать Land-атаки.

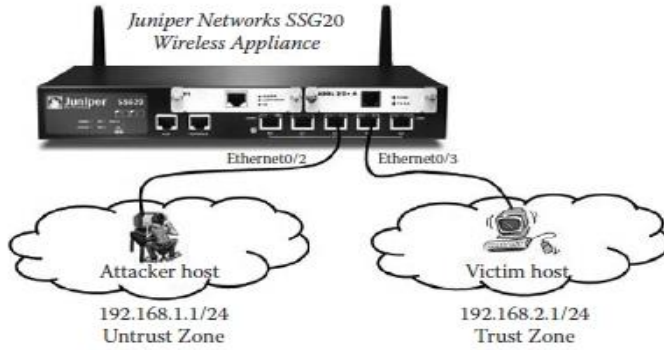
5.2.2 Описание

Атака Land происходит, когда злоумышленник отправляет поддельные пакеты TCP SYN (TCP = протокол управления передачей; SYN = синхронизация) (инициирование соединения) с тем же IP-адресом источника и назначения, а также с одинаковым номером порта источника и назначения. Целевой хост отвечает, отправляя пакет SYN ACK самому себе, создавая пустое соединение, которое продолжается до достижения значения времени простоя. Переполнение системы пустыми запросами на подключение приведет к ее перегрузке и вызовет отказ в услугах, которые она предлагает, как показано на следующем рисунке.



5.2.3 Эксперимент

Чтобы исследовать, как генерировать, а затем обнаруживать Land-атаку, проводится эксперимент с использованием устройства Juniper Networks в качестве устройства обнаружения. Пошаговое описание процесса приведено ниже. На следующем рисунке показана сетевая архитектура, использованная в эксперименте. Хост злоумышленника и хост жертвы подключены к интерфейсам ethernet 0/2 и ethernet 0/3 устройства Juniper Networks соответственно.

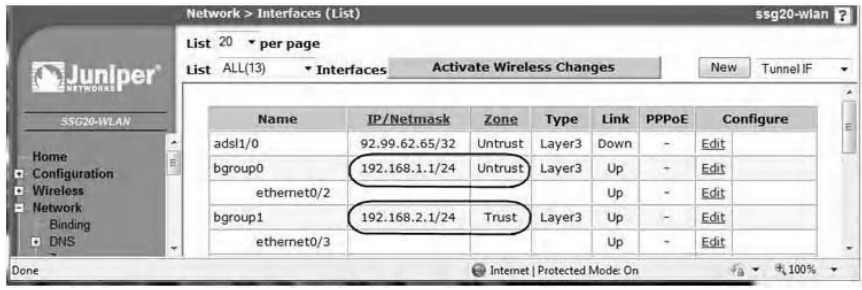


Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от Land-атаки.
Шаг 4: Построить пакеты атаки Land.
Шаг 5: Сниффинг сгенерированного трафика.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

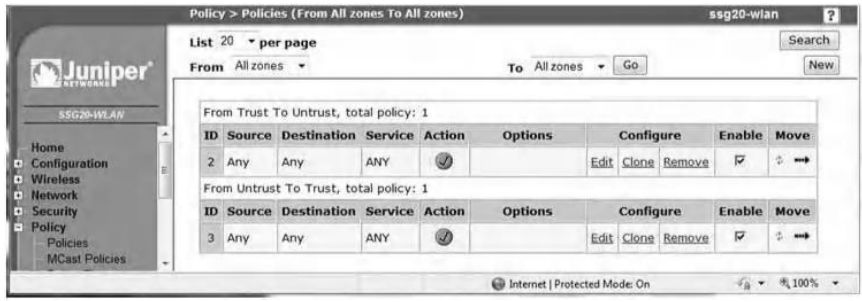
5. *2.3.1 Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks*

Мы предполагаем, что хост злоумышленника находится в недоверенной зоне / сети (сетевой адрес: 192.168.1.1/24) и подключен к интерфейсу ethernet0 / 2 устройства Juniper Networks. Хост-жертва находится в зоне доверия / сети (сетевой адрес: 192.168.2.1/24) и подключена к интерфейсу ethernet0 / 3, как показано на следующем снимке экрана, который иллюстрирует конфигурацию сетевых интерфейсов в устройстве Juniper Networks (см. также предыдущий рисунок).



5.2.3.2 Шаг 2. Установите политики безопасности (правила фильтрации)

Используя веб-интерфейс пользователя (WebUI) устройства Juniper Networks, политика по умолчанию между двумя хостами установлена на “Allow All/Permit” (Разрешить все/разрешить), чтобы разрешить все типы трафика между двумя хостами, как показано на следующем снимке экрана



5. 2.3.3 Шаг 3: Включить защиту от Land-атаки

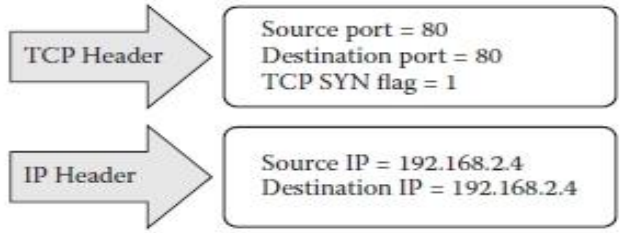
Чтобы включить защиту от атаки Land на устройстве Juniper Networks, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите Screening и установите следующие параметры, как показано на следующем снимке экрана
* Установите для зоны значение «Untrust” (Недоверие), поскольку трафик атаки с земли будет генерироваться из недоверенной зоны

* Выберите опцию Защита от Land-атак.
* Затем нажмите “Apply” (Применить).

5.2.3.4 Шаг 4: Построить пакеты Land-атаки

Land-атака разворачивается путем заполнения целевой системы поддельными пакетами SYN, содержащими IP-адрес хоста-жертвы в качестве IP-адреса назначения и источника. Кроме того, такие пакеты будут иметь одинаковый номер порта как для порта источника, так и для порта назначения. На рисунке ниже представлен пример, показывающий значения основных полей пакета Land-атаки.

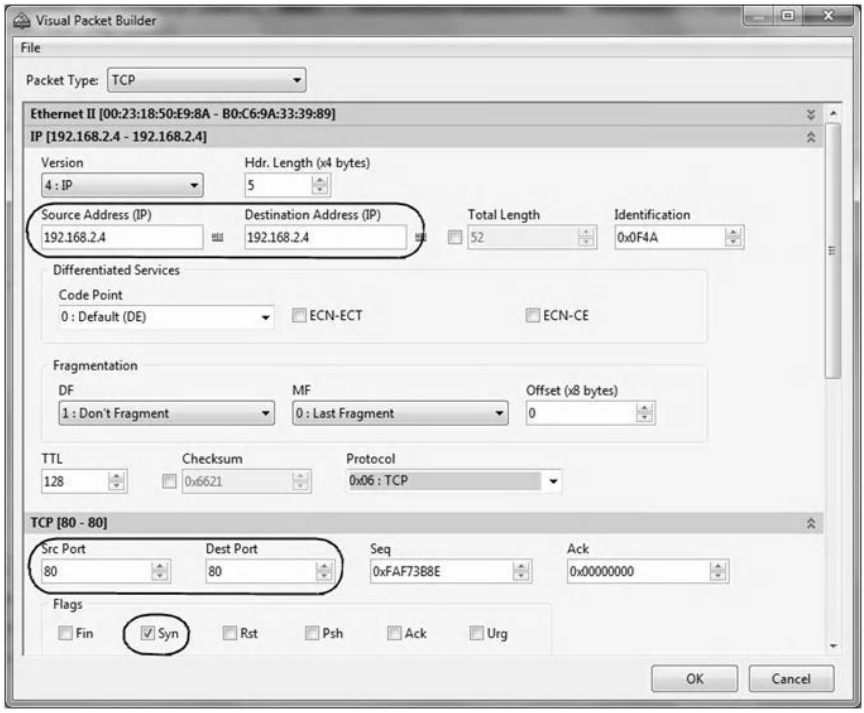


Пользователь может использовать инструмент генератора пакетов для создания пакетов, которые производят Land-атаку. Например, пользователь может использовать интерактивный командный инструмент, такой как FrameIP Packet Generator, или более дружественный и простой в использовании инструмент с графическим интерфейсом, такой как Engage Packet Builder * или CommView Visual Packet Builder.

* http://www.engagesecurity.com

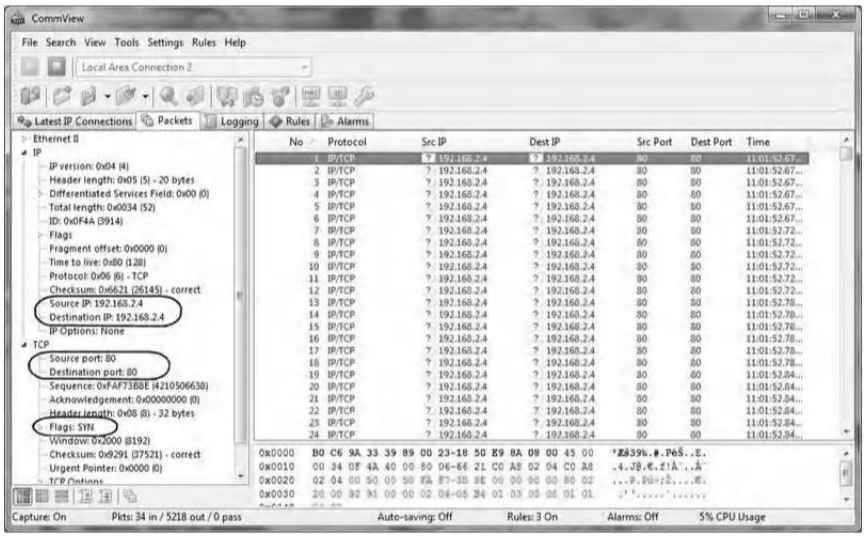
5.2.3.4.1 CommView Visual Packet Builder

CommView Visual Packet Builder используется для генерации атаки Land. На приведенном ниже снимке экрана показано, как поддельный пакет TCP SYN используется для создания атаки Land. Пакет имеет IP-адрес источника, установленный на IP-адрес назначения, номер порта источника, установленный на номер порта назначения, и MAC-адрес назначения, установленный на MAC-адрес шлюза хоста злоумышленника (192.168.1.1).



5.2.3.5 Шаг 5: Сниффим сгенерированный трафик

На хосте жертвы можно использовать программу перехвата (анализатор сети) для захвата сгенерированного трафика. Цель этого шага - проанализировать и проверить, был ли намеченный трафик сформирован адекватно. Например, используя CommView Sniffer, на следующем снимке экрана показаны пакеты Land-атаки, сгенерированные на шаге 4. Он также показывает, что хост жертвы (192.168.2.4) залит пакетами Land-атаки.



5. 2.3.6 *Шаг 6. Просмотр результатов в файле журнала устройства Juniper Networks*

Журнал событий (как показано на следующем снимке экрана) записывает события в устройстве Juniper Networks после обнаружения трафика Land-атакb. Шаги для просмотра содержимого журнала событий на устройстве Juniper Networks включают в себя:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* На левой панели разверните Reports (Отчеты), затем разверните System Log (Системный журнал) и выберите Event (Событие).

5.3 Лабораторная работа 5.2: SYN Flood Attack

5.3.1 Результат

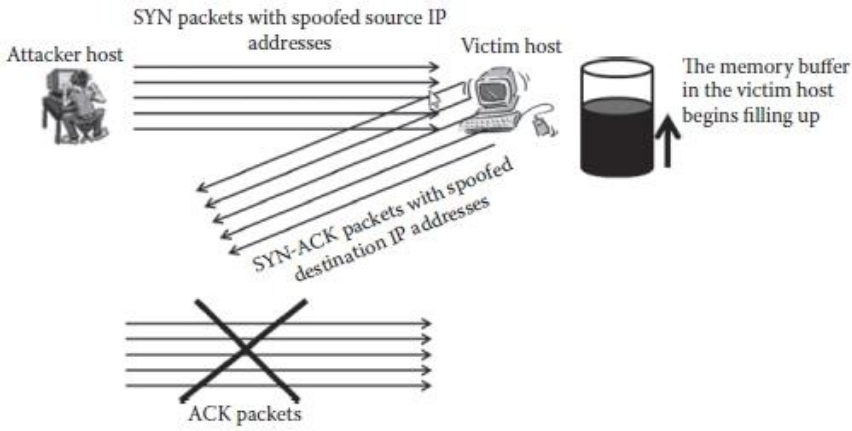
Цель этого практического эксперимента - научить студентов генерировать и обнаруживать атаку SYN Flood

5.3.2 Описание

Атака SYN Flood происходит, когда хост становится настолько перегруженным пакетами TCP SYN, инициирующими неполные запросы на соединение, что он больше не может обрабатывать законные запросы на соединение. Когда клиентская система пытается установить TCP-соединение с системой, предоставляющей услугу (сервер), клиент и сервер обмениваются последовательностью сообщений, и этот процесс называется трехсторонним рукопожатием.

Клиентская система начинает с отправки сообщения SYN (синхронизация) на сервер. Затем сервер подтверждает сообщение SYN, отправляя клиенту сообщение SYN-ACK (подтверждение). Затем клиент завершает установление соединения, отвечая сообщением ACK. Соединение между клиентом и сервером затем открывается, и между клиентом и сервером могут обмениваться специфичными для службы данными.

Возможность злоупотребления возникает в тот момент, когда сервер отправил подтверждение (SYN-ACK) обратно клиенту, но еще не получил окончательное сообщение ACK. Это называется полуоткрытым соединением. Сервер имеет в своей системной памяти встроенную структуру данных, описывающую все ожидающие соединения. Эта структура данных имеет конечный размер, и она может находиться в состоянии переполнения, преднамеренно создавая слишком много частично открытых соединений (как показано на следующем рисунке). Создание полуоткрытого соединения легко достигается с помощью IP-спуфинга. Система злоумышленника отправляет сообщения SYN на сервер жертвы, которые кажутся законными, но на самом деле адрес источника подделан системе, которая не подключена к сети. Это означает, что окончательное ACK-сообщение никогда не отправляется на сервер жертвы. Поскольку исходный адрес подделан, очень трудно определить личность истинного злоумышленника, когда пакет поступает в систему жертвы.



5.3.3 Эксперимент

Чтобы определить, как генерировать и обнаруживать атаку SYN Flood, проводится эксперимент с использованием устройства Juniper Networks в качестве устройства обнаружения. В этом эксперименте используется та же сетевая архитектура, которая описана в упражнении «Land-атака» выше (Лаборатория 5.1).

Эксперимент состоит из следующих этапов:

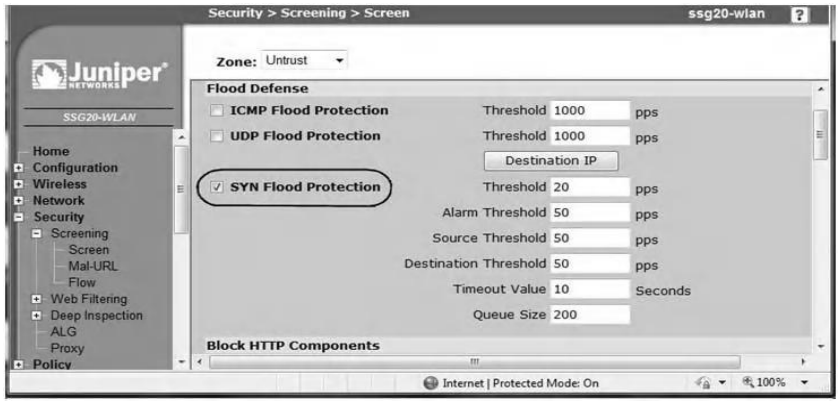
Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от атаки SYN Flood.
Шаг 4: Создайте пакеты атаки SYN Flood.
Шаг 5: Сниффинг сгенерированного трафика.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте практической лаборатории по атаке со стороны Земли (Лаборатория 5.1).

5. 3.3.1 Шаг 3. Включите защиту от SYN-атаки

Чтобы включить защиту от атаки SYN Flood на устройстве Juniper Networks, выполните следующие действия:

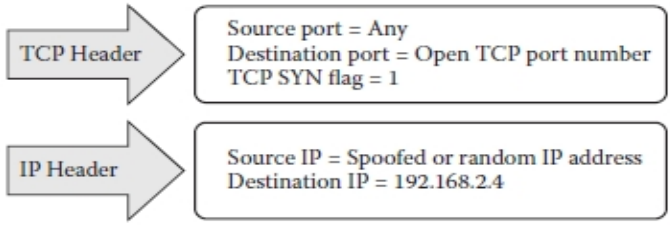
* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите Screening и установите следующие параметры, как показано на следующем скриншоте.
* Установите Zone в Untrust, потому что трафик атаки SYN Flood генерируется из ненадежных зон.
* Выберите опцию SYN Flood Protection.
* Существует ряд пороговых значений, которые можно установить, но основной порог связан с количеством пакетов SYN в секунду, которым разрешено проходить через устройство Juniper Networks (см. Следующий снимок экрана). Пользователь должен выбрать минимальные пороговые значения, чтобы атака SYN Flood обнаруживалась быстро
* Затем нажмите “Apply.”



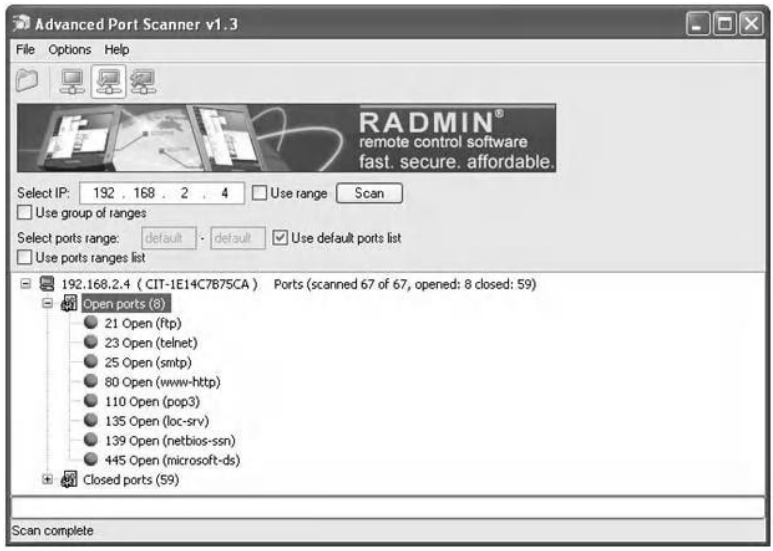
5.3.3.2 Шаг 4: Создание пакетов SYN Flood Attack

Есть много доступных готовых к использованию инструментов атаки SYN Flood. Однако, учитывая образовательный контекст этой книги, мы призываем пользователей научиться создавать собственные пакеты для атак SYN Flood.

Заголовки TCP и IP пакетов атаки SYN Flood должны быть установлены в значения, показанные на следующем рисунке, где показан пример пакета атаки SYN Flood. Исходный IP-адрес должен быть установлен на поддельный или случайный IP-адрес. Порт назначения должен быть установлен на номер открытого TCP-порта на хосте жертвы.



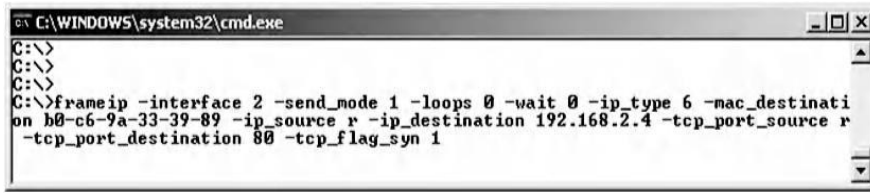
Злоумышленник может использовать любой инструмент сканирования портов, чтобы определить список открытых портов TCP на хосте жертвы. Затем злоумышленник может выбрать один открытый номер порта TCP и использовать его в качестве номера порта назначения tar-get в пакетах атаки SYN Flood. Например, на следующем снимке экрана показаны результаты сканирования TCP-порта целевого хоста с использованием инструмента Advanced Port Scanner.



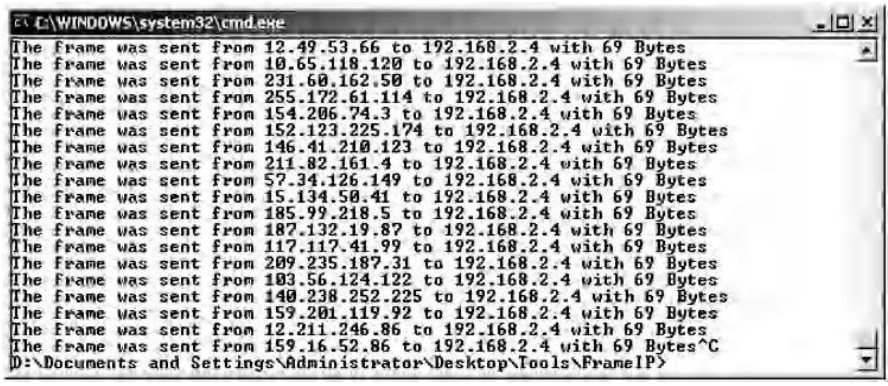
Для создания пакетов атаки SYN Flood инструмент компоновщика пакетов должен разрешать включение поддельных или случайных IP-адресов источника в заголовок IP.

5.3.3.2.1 Генератор фреймов IP-пакетов

Генератор пакетов FrameIP является примером инструментов, которые позволяют отправлять пакеты TCP SYN со случайными номерами портов источника и / или случайными IP-адресами источника. На приведенном ниже снимке экрана показана онлайн-команда FrameIP, которая позволяет генерировать поток трафика TCP SYN на порт назначения 80 целевого хоста с IP-адресом 192.168.2.4. Каждый генерируемый пакет TCP SYN будет иметь случайный поддельный номер порта источника и случайный поддельный IP-адрес источника.



На следующем снимке экрана показан сгенерированный FrameIP трафик TCP SYN Flood, созданный FrameIP в результате выполнения вышеуказанной онлайн-команды FrameIP.

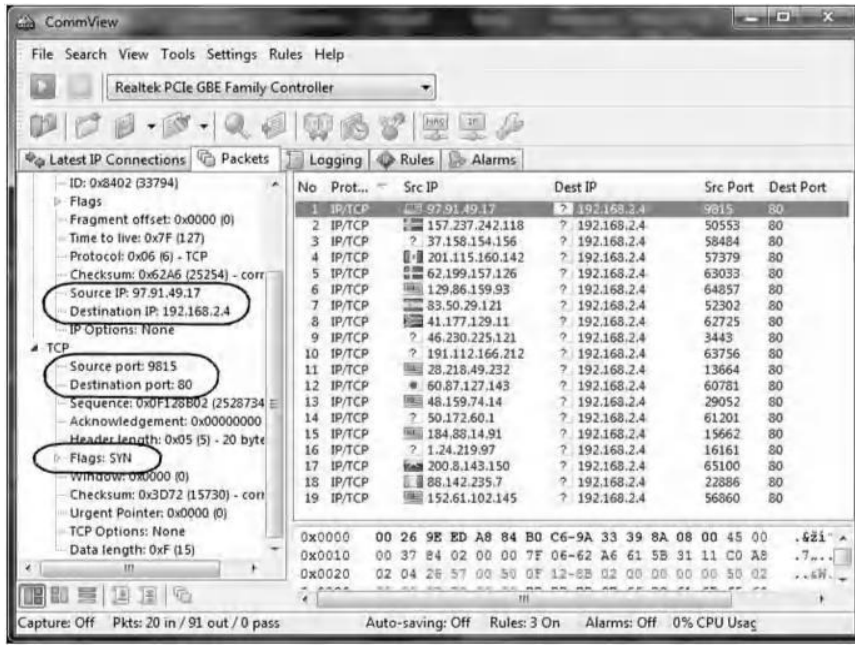


Параметры для команды, изображенной выше, следующие:

Параметры команды	Описание
-interface 2	Используемый интерфейс (см. Справку инструмента)
-send_mode 1	Тип используемой библиотеки (см. Справку инструмента)
-loops 0	Количество петель (0 = без остановки)
-wait 0	Время ожидания после каждого пакета
-ip_type 6	Тип пакета (6 = TCP пакет)
-mac_destination	MAC-адрес интерфейса шлюза
-ip_source r	IP-адрес случайного источника (r = случайный адрес)
-ip_destination 192.168.2.4	IP-адрес получателя
-tcp_port_source r	Случайные номера портов источника TCP
-tcp_port_destination 80	Номер порта назначения TCP
-tcp_flag_syn 1	Установлен бит флага TCP SYN

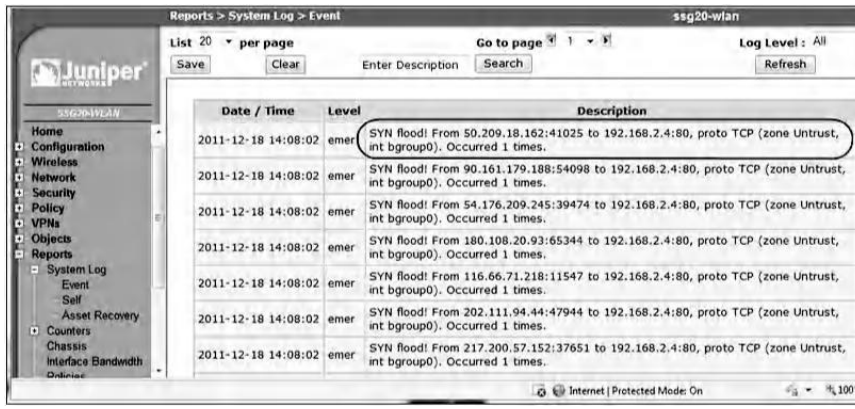
5.3.3.3 Шаг 5: Сниффинг сгенерированного трафика

На хосте жертвы можно использовать анализатор для захвата генерируемого трафика. Целью этого шага является анализ и проверка того, что предполагаемый трафик был сгенерирован адекватно. Например, используя CommView Sniffer, на следующем снимке экрана показано, что хост жертвы (192.168.2.4) находится под атакой SYN Flood и целевой порт TCP равен 80.



5.3.3.4 Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks

Устройство Juniper Networks записывает сигнал тревоги в журнал событий, когда количество пакетов SYN из одного или нескольких источников в один пункт назначения превышает пороговые значения. На следующем снимке экрана показано содержимое журнала событий после обнаружения трафика атаки SYN Flood.



5.4 Лабораторная работа 5.3: Атака Teardrop (слезинки)

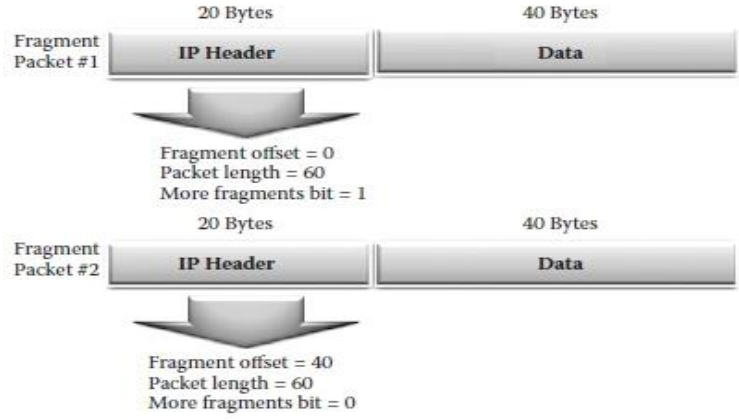
5.4.1 Результат

Цель этого практического эксперимента - научить студентов генерировать и обнаруживать атаку Teardrop.

5.4.2 Описание

Атака Teardrop направлена на процесс повторной сборки фрагментированных IP-пакетов. Фрагментация необходима, когда дейтаграммы IP больше, чем максимальная единица передачи (MUT) сегмента сети, по которому дейтаграммы должны проходить. Чтобы успешно повторно собрать пакеты на принимающей стороне, заголовок IP для каждого фрагмента включает в себя смещение, чтобы идентифицировать положение фрагмента в исходном нефрагментированном пакете. При атаке Teardrop фрагменты пакетов преднамеренно изготавливаются с перекрывающимися полями смещения, что приводит к зависанию или сбою хоста при попытке их повторной сборки.

На следующем рисунке показано, что второй фрагментный пакет (Packet #2) имеет намерение начинаться на 20 байтов раньше (на 40), чем заканчивается первый пакетный фрагмент (Packet #1) (на 60). Смещение Packet #2 не соответствует длине пакета Packet #1. Это несоответствие может привести к сбою некоторых систем во время попытки повторной сборки.



5.4.3 Эксперимент

Чтобы определить, как генерировать и обнаруживать атаку Teardrop, проводится эксперимент с использованием устройства Juniper Networks в качестве устройства обнаружения. Ниже приводится описание и этапы эксперимента. В эксперименте используется та же сетевая архитектура, которая описана в практической лаборатории Land-атак (лабораторная работа 5.1), и состоит из следующих этапов:

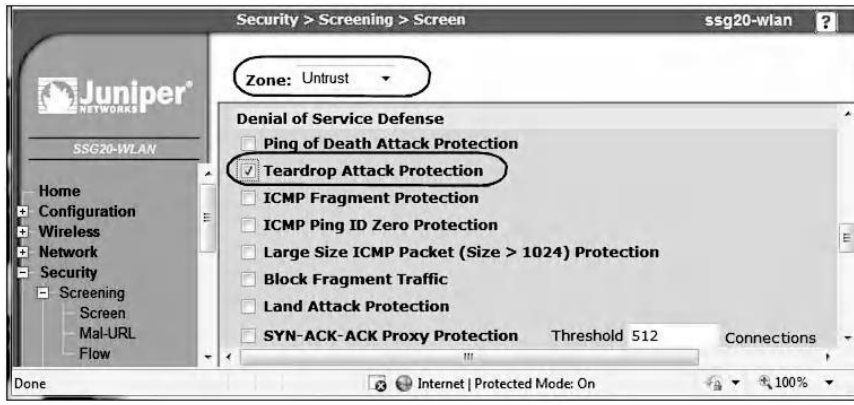
Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от атаки Teardrop.
Шаг 4: Создайте пакеты атаки Teardrop.
Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks.

Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте по Land-атаке в Лаборатории 5.1.

5.4.3.1 Шаг 3: Включить защиту от атаки Teardrop

Чтобы включить защиту от атаки Teardrop на устройстве Juniper Networks, выполните следующие действия:

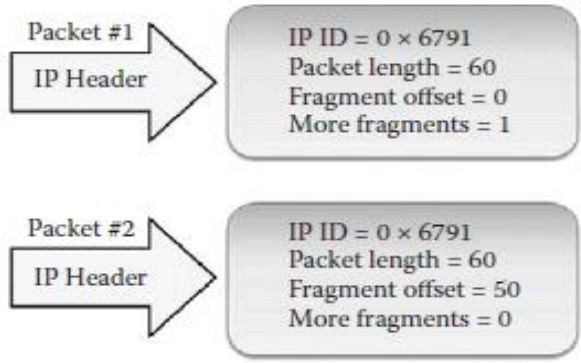
* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите Screening и установите следующие параметры, как показано на следующем снимке экрана, чтобы включить защиту от атаки Teardrop.



* Установите для Zone значение Untrust, поскольку трафик атаки Teardrop будет генерироваться из ненадежной зоны.
* Выберите опцию Teardrop Attack Protection.
* Затем нажмите “Apply.”

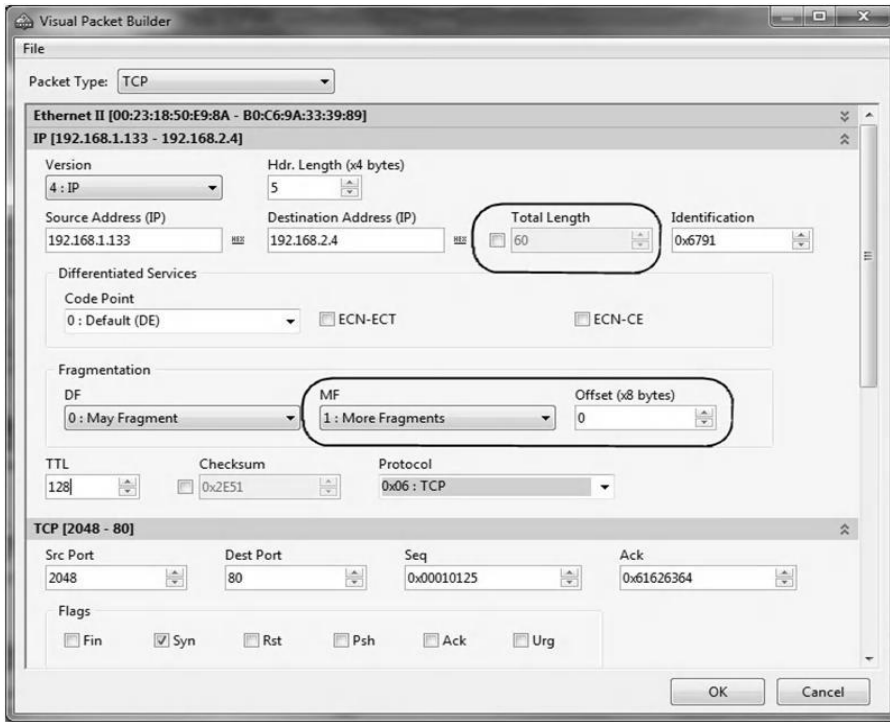
5.4.3.2 Шаг 4: Создание пакетов атаки Teardrop

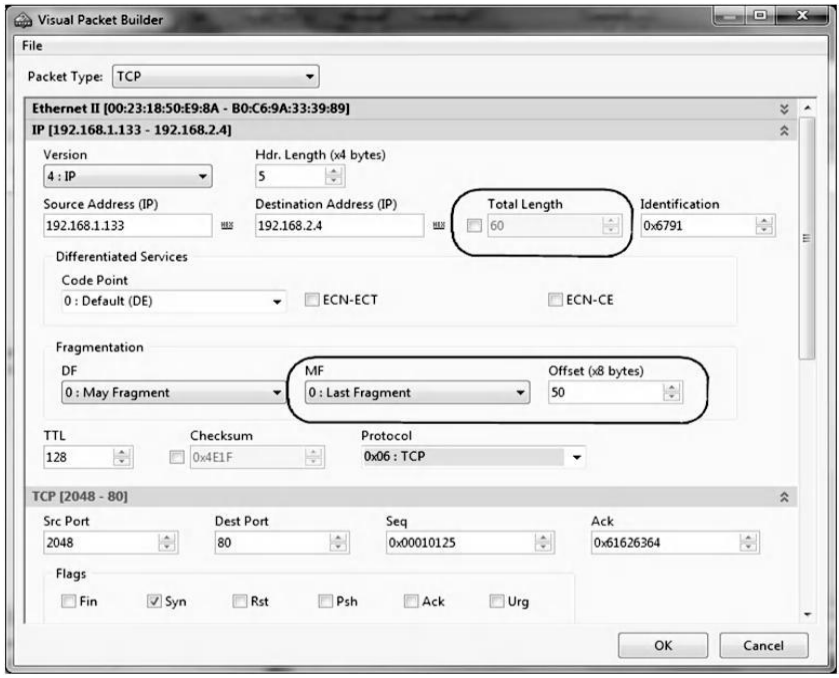
Для генерации атаки Teardrop необходимо собрать два фрагментированных пакета. Пакеты принадлежат одному и тому же исходному пакету и имеют одинаковую идентификацию (ID) IP. Идентификатор поля включает в себя идентифицирующее значение, назначаемое хостом отправителя для помощи в сборке фрагментов дейтаграммы. Однако два фрагментированных пакета имеют перекрывающиеся значения смещения. В качестве примера, значения IP-заголовка двух пакетов атаки Teardrop показаны на следующем рисунке.



5.4.3.2.1 CommView Visual Packet Builder

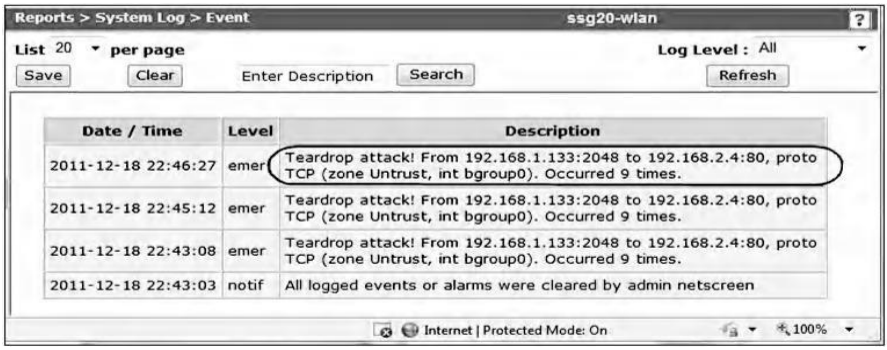
Используя CommView Visual Packet Builder, на следующих двух снимках экрана показаны первый и второй фрагментированные пакеты с перекрывающимися значениями смещения, приводящими к атаке Teardrop.





5.4.3.3 Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks

Содержимое журнала событий в устройстве Juniper Networks после обнаружения трафика атаки Teardrop показано на следующем снимке экрана.



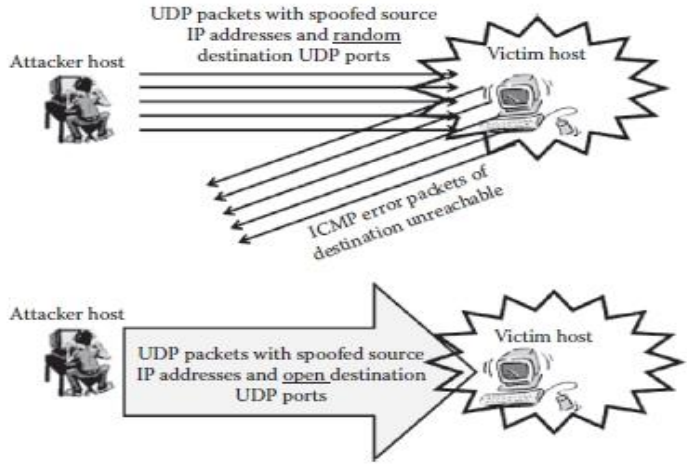
5.5 Лабораторная работа 5.4: Атака UDP Flood

5.5.1 Результат

Цель данного практического упражнения - научить студентов генерировать и обнаруживать атаки UDP Flood.

5.5.2 Описание

UDP (Протокол пользовательских датаграмм) является протоколом без установления соединения и не требует какой-либо процедуры установки соединения для передачи данных. Атака UDP Flood возможна, когда злоумышленник наводняет целевые порты в системе-жертве пакетами UDP. Когда система-жертва получает пакет UDP, она определяет, какое приложение ожидает порт назначения UDP. Существуют две возможности. Во-первых, если на порту нет ожидающего приложения (закрытый порт UDP), хост-жертва сгенерирует пакет ошибок ICMP (пункт назначения недоступен) по поддельному адресу источника. Во-вторых, если на конечном порту UDP запущено приложение, приложение обрабатывает пакет UDP. В обоих случаях, если достаточное количество UDP-пакетов доставлено на конечные UDP-порты, хост-жертва или приложение могут замедлиться или отключиться. Сценарий показан на следующем рисунке.



5.5.3 Эксперимент

Чтобы определить, как генерировать и обнаруживать атаку UDP Flood, проводится эксперимент с использованием устройства Juniper Networks в качестве устройства обнаружения. В этом эксперименте используется та же сетевая архитектура, которая описана в практической лаборатории Land-атак (лаборатория 5.1)

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от атаки UDP Flood.
Шаг 4: Построить пакеты атаки UDP Flood.
Шаг 5: Сниффинг сгенерированного трафика.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

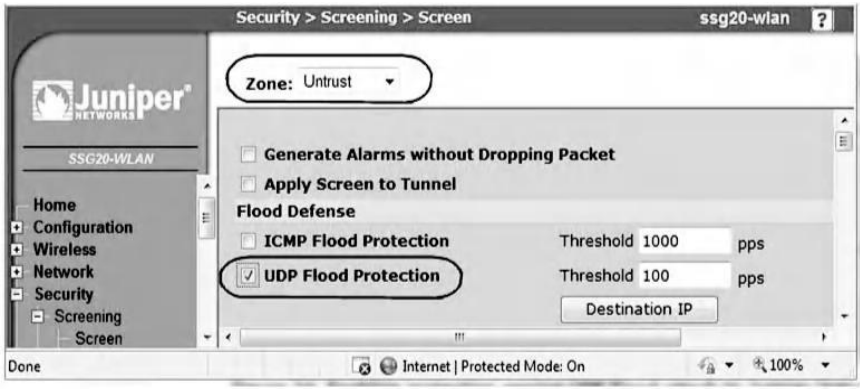
Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте по Land-атаке в Лаборатории 5.1.

5. 5.3.1 Шаг 3: Включите защиту от UDP Flood Attack

Чтобы включить защиту от атаки UDP Flood на устройстве Juniper Networks, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.

* Выберите Screening и установите следующие параметры, как показано на следующем снимке экрана, чтобы включить защиту от атаки UDP Flood.



* Установите Zone в Untrust, потому что трафик атаки UDP Flood будет генерироваться из ненадежных зон.

* Выберите опцию защиты от наводнений UDP.

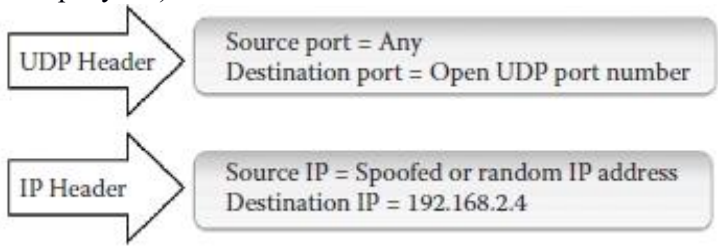
* становите порог. Порог - это количество пакетов UDP в секунду, которое устройство Juniper Networks может принять до того, как атака UDP Flood будет обнаружена и зарегистрирована. Пороговое значение по умолчанию составляет 1000 пакетов в секунду. Пользователь должен установить пороговое значение, чтобы атака UDP Flood обнаруживалась быстро.

* Затем нажмите “Apply.”

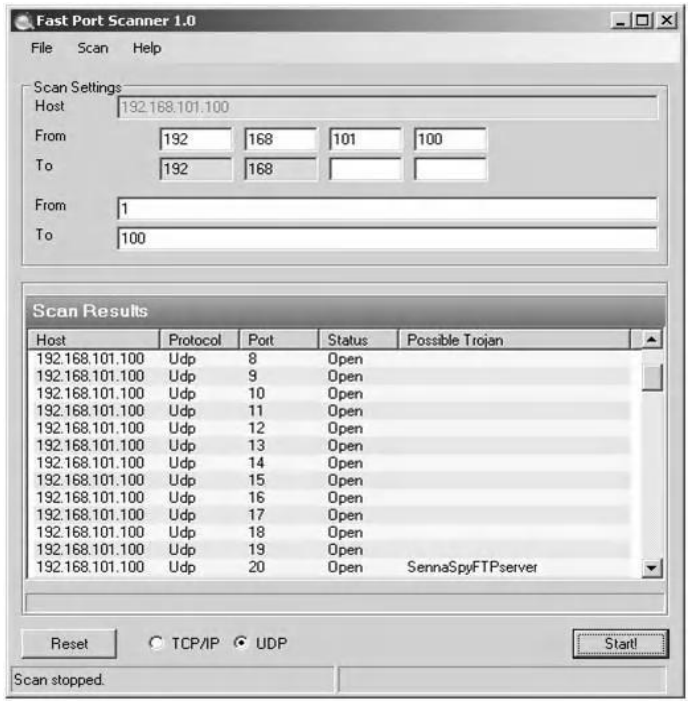
5.5.3.2 Шаг 4: Построить UDP-пакеты Flood Attack

Есть много доступных готовых к использованию инструментов атаки UDP Flood. Однако, учитывая образовательный контекст этой книги, мы призываем пользователей научиться создавать свои собственные пакеты UDP Flood.

В пакете атаки UDP Flood исходный IP-адрес должен быть установлен на поддельный или случайный IP-адрес. Порт назначения должен быть установлен на номер открытого UDP-порта на хосте жертвы (см. Следующий рисунок).



Злоумышленник может использовать любое средство сканирования портов, чтобы идентифицировать список открытых портов UDP на узле-жертве. Затем выбирается один открытый номер порта UDP, который используется в качестве номера порта назначения в пакетах атаки UDP Flood. Пример на следующем снимке экрана показывает результат сканирования UDP-порта целевого хоста с использованием инструмента Fast Port Scanner.

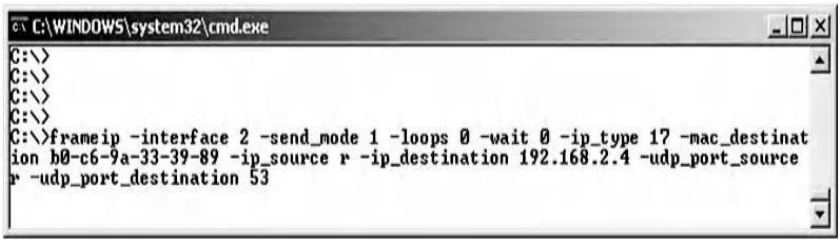


Для создания пакетов атаки UDP Flood пользователь должен использовать инструмент построения пакетов, который позволяет включать поддельные или случайные IP-адреса в поле исходного IP-адреса заголовка IP. Случайные или поддельные IP-адреса источника позволяют скрыть реальный IP-адрес источника хоста злоумышленника.

5.5.3.2.1 Генератор фреймов IP-пакетов

Генератор пакетов FrameIP может генерировать пакеты UDP со случайными или поддельными исходными IP-адресами. Следующий снимок экрана — это снимок сетевой команды FrameIP, которая

позволяет генерировать поток UDP-трафика на целевой UDP-порт 53 целевого хоста с IP-адресом 192.168.2.4.

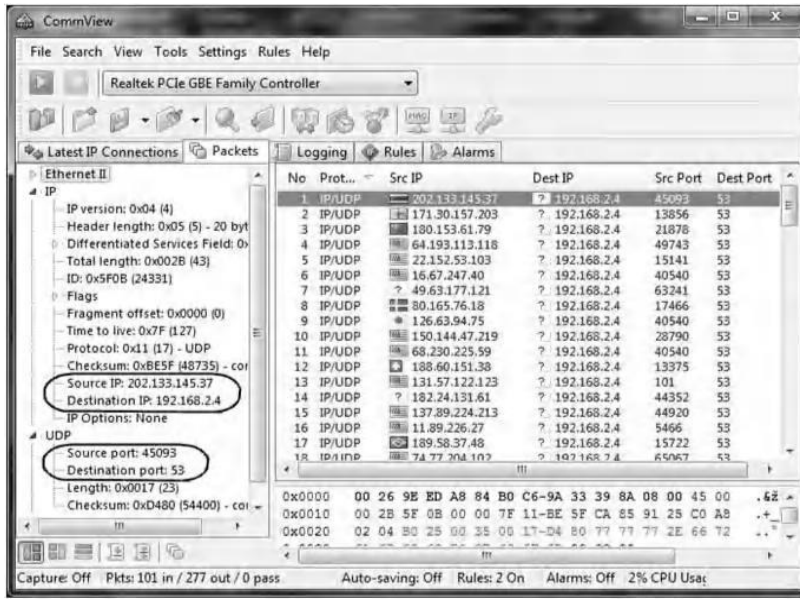


где

Параметры команды	Описание
- nterface 2	Используемый интерфейс (см. Справку инструмента)
-send_mode 1	Тип используемой библиотеки (см. Справку инструмента)
-loops 0	Количество петель (0 = без остановки)
-wait 0	Время ожидания после каждого пакета
-ip_type 17	Тип пакета (17 = UDP-пакет)
-mac_destination	MAC-адрес интерфейса шлюза
-ip_source r	IP-адрес случайного источника (r = случайный
-ip_destination 192.168.2.4	IP-адрес получателя
-udp_port_source r	Случайные номера портов источника UCP
-udp_port_destination 53	Номер порта назначения UCP

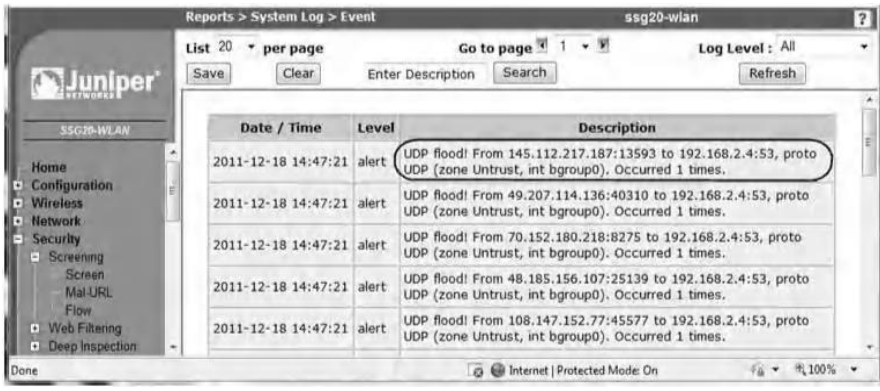
5.5.3.3 Шаг 5: Сниффинг сгенерированного трафика

На хосте жертвы можно использовать анализатор для захвата генерируемого трафика. Например, используя сниффер CommView, на следующем снимке экрана показано, что хост жертвы (192.168.2.4) находится под атакой UDP Flood и целевой порт UDP равен 53.



5. *5.3.4 Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks*

Устройство Juniper Networks записывает тревогу в журнал событий, когда количество пакетов UDP от одного или нескольких источников к одному месту назначения превышает пороговое значение. Содержимое журнала событий в устройстве Juniper Networks после обнаружения трафика атаки UDP Flood показано на следующем снимке экрана.



5.6 Лабораторная работа 5.5: ненормальные IP-пакеты

5.6.1 Результат

Цель этого практического упражнения состоит в том, чтобы учащиеся узнали, как создавать и обнаруживать ненормальные IP-пакеты, которые могут содержать скрытые угрозы или DoS-трафик.

5.6.2 Описание

Злоумышленники могут отправлять ненормальные пакеты, которые могут содержать скрытые угрозы или вызывать DoS-ситуацию в целевой системе.
В большинстве случаев неясно, каково намерение генерировать ненормальные пакеты. Тем не менее, ненормальные пакеты, как правило, являются ярким свидетельством существования злонамеренных действий. Поэтому важно блокировать ненормальные пакеты от достижения их целей. Обычно ненормальные пакеты - это пакеты, которые включают неожиданные значения полей, имеют неожиданно большие размеры или являются фрагментированными пакетами, которые обычно не должны быть фрагментированы. Здесь представлены три примера ненормальных пакетов.

5.6.2.1 Фрагментированный пакет ICMP

CMP-пакеты используются для отправки сообщений об ошибках и контроля. Например, когда пакет отбрасывается маршрутизатором, на исходный хост обычно отправляется пакет с ошибкой ICMP. Эхо-пакет ICMP является контрольным пакетом и используется для идентификации живого удаленного хоста.

ICMP-пакеты имеют небольшой размер, поскольку содержат очень короткие сообщения. Следовательно, нет законных причин для фрагментации пакетов ICMP. Пакет ICMP считается фрагментированным пакетом, когда установлен его флаг «Больше фрагментов», или он имеет значение смещения, указанное в поле смещения. Необычно видеть фрагментированные пакеты ICMP.

5.6.2.2 Большой ICMP-пакет

Как уже отмечалось, пакеты ICMP малы, поскольку содержат очень короткие сообщения. Следовательно, не существует законных оснований для существования больших пакетов ICMP. Необычно видеть большие пакеты ICMP. Если пакет ICMP такой большой, значит, что-то не так. Это также может указывать на некоторые другие виды сомнительной деятельности.

5.6.2.3 Пакет неизвестного протокола

Поле Protocol в заголовке IP идентифицирует протокол более высокого уровня (обычно протокол транспортного уровня или инкапсулированный протокол сетевого уровня), переносимый в графе данных. Значения этого поля были первоначально определены стандартом IETF (Internet Engineering Task Force) «Назначенные номера», RFC 1700, и теперь поддерживаются Управлением по назначению номеров Интернета (IANA). Эти протоколы более высокого уровня с идентификационными номерами 137 или более зарезервированы и не определены в данный момент. Поэтому в обычной ситуации пакеты, которые используют неизвестные протоколы (с идентификационным номером 137 или более), являются подозрительными и должны быть заблокированы для входа в сеть, если сеть не использует нестандартные протоколы.

5.6.3 Эксперимент

Чтобы узнать, как генерировать и обнаруживать три вышеупомянутых ненормальных IP-пакета, проводится эксперимент с использованием устройства Juniper Networks в качестве устройства обнаружения. Ниже приведено описание и этапы эксперимента. В этом эксперименте используется та же сетевая архитектура, которая описана в практической лаборатории Land-атак (лаборатория 5.1)

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).

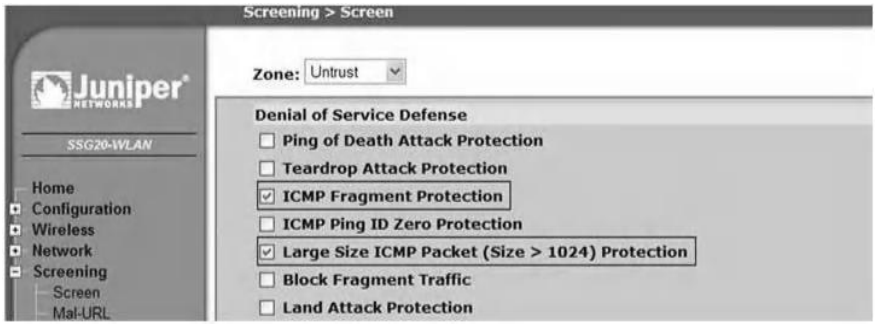
Шаг 3: Включите защиту от трех ненормальных пакетов.
Шаг 4: Генерация трех ненормальных пакетов.
Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks.

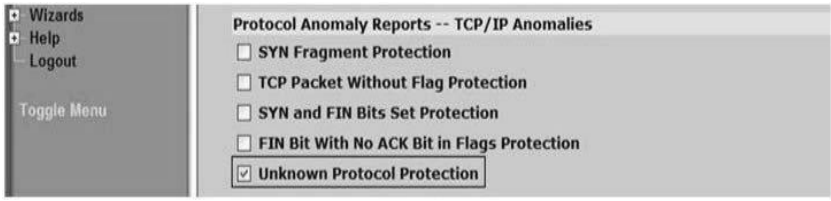
Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте по Land-атаке в Лаборатории 5.1.

5.6.3.1 Шаг 3. Включите защиту от трех ненормальных пакетов

Чтобы включить защиту от фрагментированных ICMP-пакетов, больших ICMP-пакетов и неизвестных протокольных пакетов в устройстве Juniper Networks, выполните следующие действия:

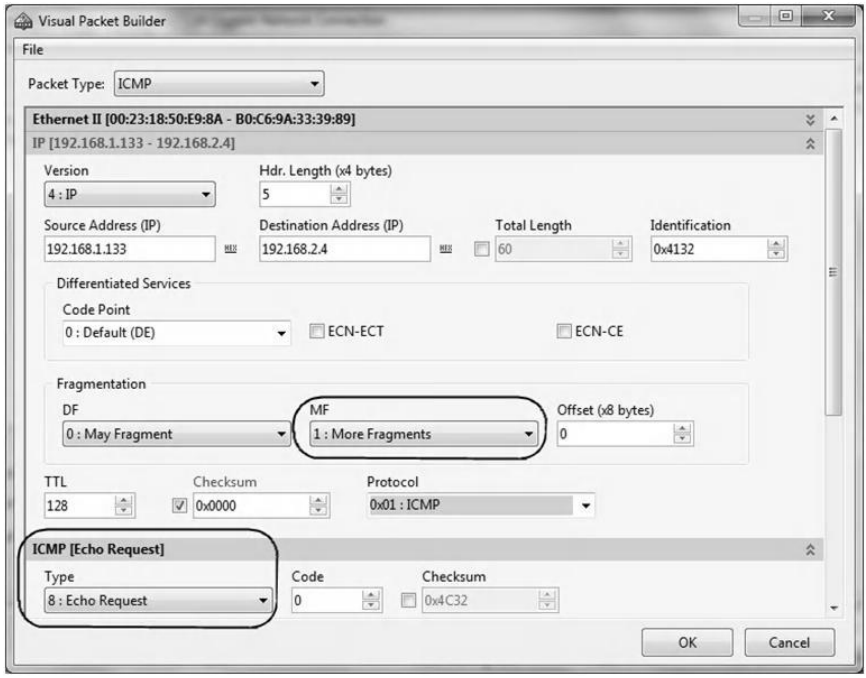
* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите Screening и установите следующие параметры.
* Установите Zone в Untrust, потому что ненадежные пакеты генерируются из ненадежной зоны.
* Установите Защита от фрагментации ICMP, Большая защита ICMP, Защита от неизвестного протокола, как показано на следующих двух снимках экрана. Первый снимок экрана иллюстрирует защиту от фрагментированных пакетов ICMP и пакетов большого размера, а второй снимок экрана иллюстрирует защиту от неизвестных пакетов протокола.
* Затем нажмите “Apply.”

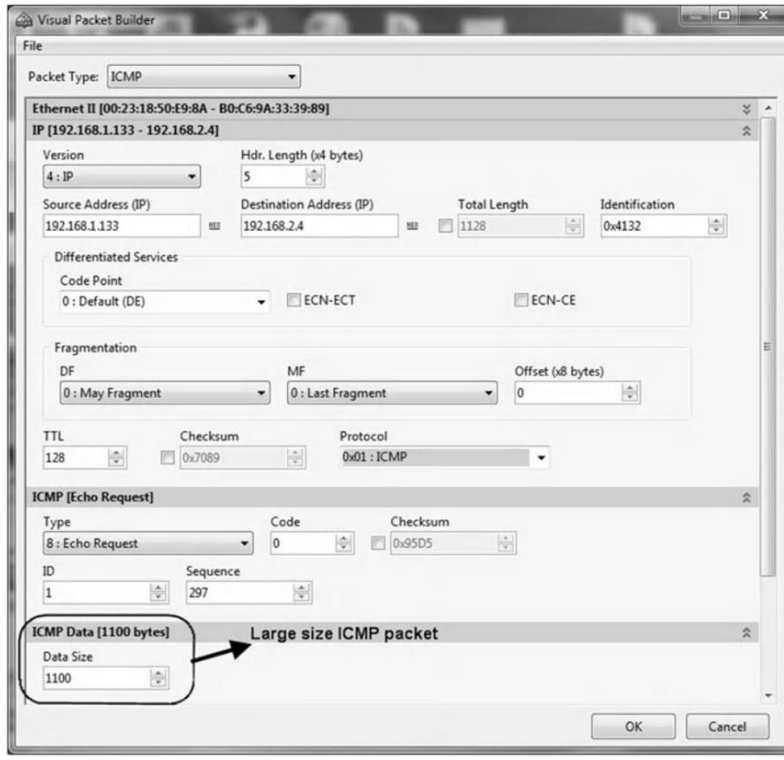


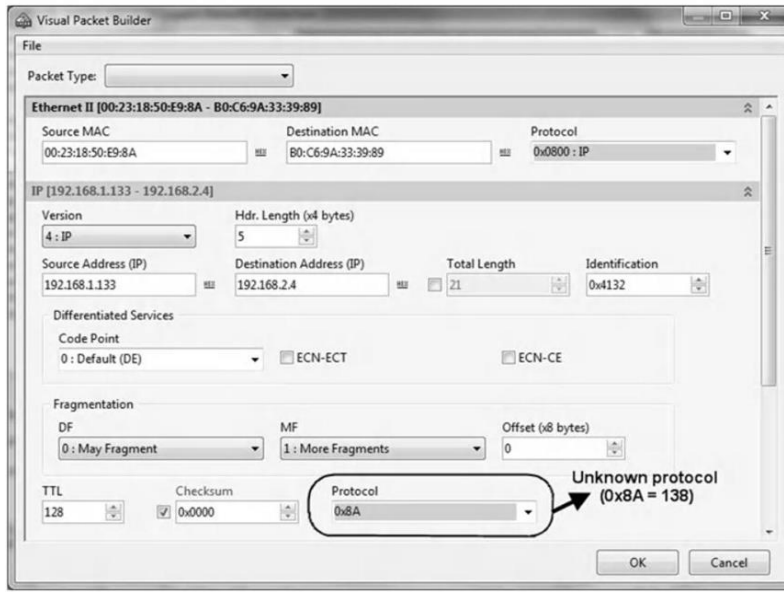


5.6.3.2 Шаг 4: Генерация трех ненормальных пакетов

Используя CommView Visual Packet Builder, на следующих трех снимках экрана показаны три ненормальных IP-пакета: фрагментированный пакет ICMP, пакет ICMP большого размера и неизвестный пакет протокола соответственно.

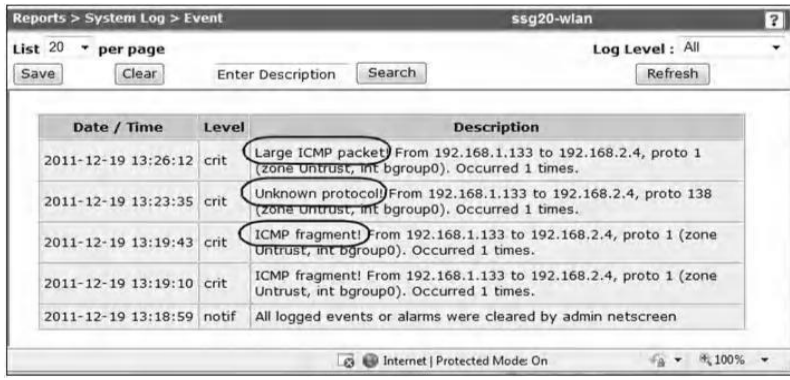



Visual Packet Builder
File
Packet Type: ICMP
Ethernet II [00:23:18:50:E9:8A - B0:C6:9A:33:39:89]
IP [192.168.1.133 - 192.168.2.4]
Version
4 : IP
Hdr. Length (x4 bytes)
5
Source Address (IP)
192.168.1.133
Destination Address (IP)
192.168.2.4
Total Length
1128
Identification
0x4132
Differentiated Services
Code Point
0 : Default (DE)
ECN-ECT
ECN-CE
Fragmentation
DF
0 : May Fragment
MF
0 : Last Fragment
Offset (x8 bytes)
0
TTL
128
Checksum
0x7089
Protocol
0x01 : ICMP
ICMP [Echo Request]
Type
8 : Echo Request
Code
0
Checksum
0x95D5
ID
1
Sequence
297
ICMP Data [1100 bytes]
Large size ICMP packet
Data Size
1100
OK
Cancel


Visual Packet Builder
File
Packet Type:
Ethernet II [00:23:18:50:E9:8A - B0:C6:9A:33:39:89]
Source MAC
00:23:18:50:E9:8A
Destination MAC
B0:C6:9A:33:39:89
Protocol
0x0800 : IP
IP [192.168.1.133 - 192.168.2.4]
Version
4 : IP
Hdr. Length (x4 bytes)
5
Source Address (IP)
192.168.1.133
Destination Address (IP)
192.168.2.4
Total Length
21
Identification
0x4132
Differentiated Services
Code Point
0 : Default (DE)
ECN-ECT
ECN-CE
Fragmentation
DF
0 : May Fragment
MF
1 : More Fragments
Offset (x8 bytes)
0
TTL
128
Checksum
0x0000
Protocol
0x8A
Unknown protocol
(0x8A = 138)
OK
Cancel

5.6.3.3 Шаг 5: Просмотр результатов в файле журнала устройства Juniper Networks

Содержимое журнала событий в устройстве Juniper Networks после обнаружения трех вышеупомянутых ненормальных пакетов показано на следующем снимке экрана.



5.7 Краткое содержание главы

В DoS-атаке злоумышленник пытается запретить законным пользователям доступ к информации или услугам. Ориентируясь на компьютеры и сети, злоумышленники не позволяют законным пользователям получать доступ к электронной почте, веб-сайтам, сетевым учетным записям (банковским операциям) или другим службам, которые зависят от уязвимых компьютеров и сетей. В этой главе представлены практические упражнения для четырех известных DoS-атак на базе IP, а именно: Land-атака, атака SYN Flood, атака Teardrop и UDP Flood атака. Кроме того, обсуждалось упражнение об аномальных IP-пакетах, которые могут содержать скрытые угрозы или DoS-трафик. Цель практических занятий в этой главе - научить студентов генерировать и обнаруживать четыре хорошо известные DoS-атаки, а также три типа ненормальных IP-пакетов. Есть много доступных готовых к использованию инструментов атаки. Однако, учитывая образовательный контекст этой книги, мы продемонстрировали пользователям, как практически создавать и тестировать собственный трафик атаки.

Глава 6

Разведывательный трафик

6.1 Введение

Каждый злоумышленник изучает целевую среду до эксплойта. Атакующий собирает некоторую предварительную информацию, такую как количество систем, конфигурации систем и используемых операционных систем (ОС). Вся собранная информация дает четкое представление об окружающей среде, которая является целевой. Поэтому, ретроспективно, для организации чрезвычайно важно знать, какую информацию злоумышленник может получить о себе, и защитить ее, чтобы свести к минимуму потенциальную потерю этой важной информации.

Злоумышленники используют различные инструменты для получения информации о целевой среде; некоторые перечислены здесь:

1. Социальная информация о доменных именах, сведениях о владельце домена и контактной информации, такой как имена, номера телефонов, почтовые адреса и адреса электронной почты. Инструменты Whois и Nslookup позволяют собирать такую информацию.
2. Инструменты для пинга активных хостов позволяют идентифицировать их.

3. Инструменты сканирования портов, такие как Nmap, Nessus и NetScanTools Pro, позволяют идентифицировать открытые порты на целевых хостах.
4. Сканеры Nmap, NetScanTools Pro, Xprobe2 и GFI LANguard являются одними из инструментов, позволяющих идентифицировать удаленные ОС.
5. Команда Traceroute и инструмент VisualRoute являются примерами инструментов, которые позволяют отображать целевые сети.

В этой главе мы рассмотрим некоторые из вышеперечисленных инструментов и рассмотрим, как системы и сети могут быть защищены от разведывательного трафика. В практических упражнениях обсуждаются четыре распространенных действия по разведке, а именно: поиск IP-адреса, сканирование порта TCP, идентификация удаленной ОС и трассировка.

В упражнениях используются следующие аппаратные устройства и программные средства:

* Беспроводное устройство Juniper Networks SSG20 *: устройство обнаружения вторжений
* CommView Tool †: инструмент для мониторинга и анализа сети (сниффер)
* Advanced Port Scanner‡: инструмент сканирования портов
* Advanced IP Scanner§: IP-сканер
* NetScanTools Pro¶: инструмент для исследования сети и сканер безопасности
* Nmap**: инструмент для исследования сети и сканер безопасности.
* VisualRoute††: Инструмент трассировки

*http://www.juniper.net
† http://www.tamos.com
‡ http://www.radmin.com §
http://www.radmin.com
¶ http://www.netscantools.com
*http://www.nmap.org
†http://www.visualroute.com

6.2 Лабораторная работа 6.1: поиск IP-адресов

6.2.1 Результат

Цель этого упражнения состоит в том, чтобы учащиеся научились выполнять и обнаруживать сканирование IP-адресов.

6.2.2 Описание

Сканирование IP-адресов состоит из сканирования диапазона IP-адресов с помощью пинг-пакетов ICMP в поисках активных устройств. То есть каждому целевому IP-адресу отправляются эхо-запросы ICMP-эхо-запросов. Пакеты эхо-ответа ICMP позволяют обнаруживать активные устройства и собирать информацию о них. Обычно он используется в сочетании со сканированием портов для полного учета каждого IP-адреса.

6.2.3 Experiment

Чтобы определить, как генерировать и обнаруживать атаку с развертыванием IP-адреса, проводится эксперимент с использованием устройства Juniper Networks, как примера устройства обнаружения, и Advanced Port Scanner как инструмента для генерации атак с разверткой IP-адреса. Ниже приведено описание и этапы эксперимента. В этом эксперименте используется та же сетевая архитектура, которая описана в практическом упражнении по Land-атаке в главе 5 (лабораторная работа 5.1).

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от очистки IP-адреса.
Шаг 4: Выполните поиск IP-адреса.
Шаг 5: Сниффинг сгенерированного трафика.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте практического упражнения по Land-атаке в главе 5 (лабораторная работа 5.1).

6.2.3.1 Шаг 3. Включите защиту от очистки IP-адресов

Чтобы включить защиту от сканирования IP-адреса на устройстве Juniper Networks, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите Screening и установите следующие параметры, как показано на следующем снимке экрана.

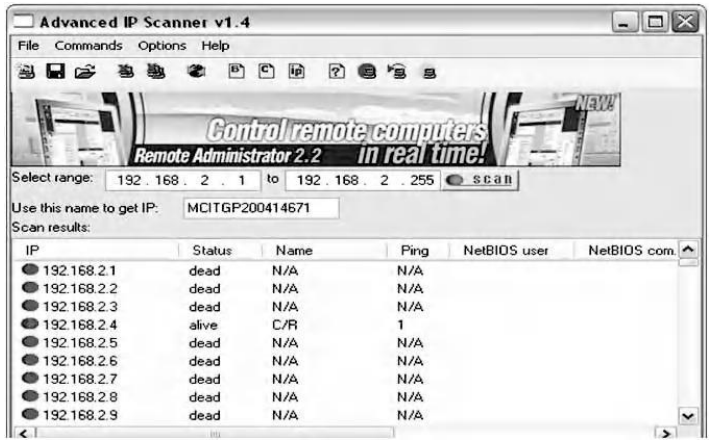
* Установите Zone в Untrust, потому что трафик IP-адреса будет генерироваться из ненадежной зоны.
  — Выберите параметр защиты IP-адреса.
  — Установите пороговые значения: в устройстве Juniper происходит сканирование IP-адреса, когда один IP-адрес источника отправляет десять пакетов ICMP различным хостам в течение определенного интервала. Устройство безопасности внутренне регистрирует количество ICMP-пакетов по разным адресам из одного удаленного источника. Если удаленный хост отправляет трафик ICMP на десять адресов с использованием настроек по умолчанию, то через 0,005 секунды (5000 микросекунд)

устройство безопасности помечает это как атаку развертки адреса и отклоняет все последующие запросы эхо-запроса ICMP от этого хоста на оставшуюся часть указанного порогового периода времени. Пользователь должен выбрать пороговое значение, чтобы обеспечить быстрое обнаружение IP-адреса.

* Затем нажмите “Apply.”

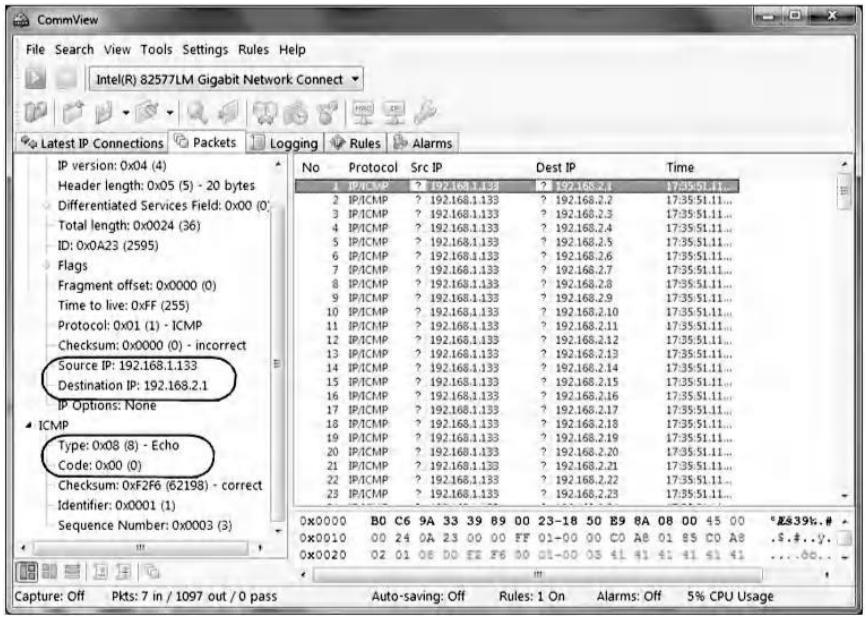
6.2.3.2 Шаг 4. Выполните очистку IP-адреса

На хосте злоумышленника для сканирования IP-адресов используется инструмент Advanced IP Scanner. Например, на следующем снимке экрана показаны живые и мертвые хосты.



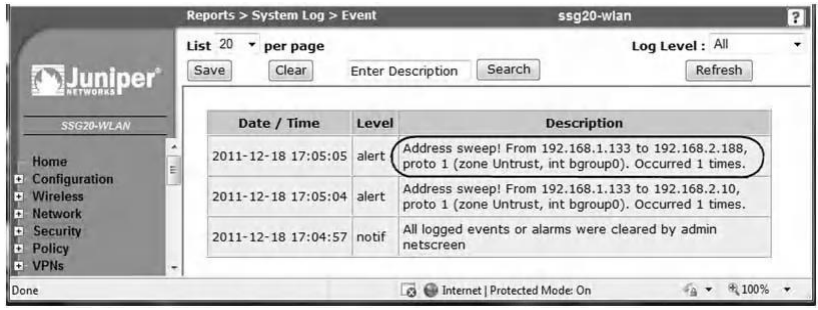
6.2.3.3 Шаг 5: Сниффинг сгенерированного трафика

На хосте злоумышленника можно использовать сниффер для захвата генерируемого трафика. Используя сниффер CommView, на следующем снимке экрана показано, что хост злоумышленника (192.168.1.133) выполняет сканирование IP-адресов, отправляя пакеты эхо-запроса ICMP на диапазон IP-адресов (192.168.2.1–192.168.2.254).



6.2.3.4 Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks

На следующем снимке экрана показано содержимое журнала событий на устройстве Juniper Networks после обнаружения трафика IP-адреса.



6.3 Лабораторная работа 6.2: сканирование портов TCP

6.3.1 Результат

Цель этого практического упражнения - научить студентов выполнять и обнаруживать сканирование портов TCP.

6.3.2 Описание

Сканирование TCP-порта - это популярная методика разведки, используемая злоумышленниками для обнаружения служб, которые можно взломать. Все системы, подключенные к сети, запускают службы, которые прослушивают общеизвестные и не очень известные порты. Сканирование портов помогает злоумышленнику определить, какие порты доступны (т.е. какая служба может прослушивать порт). По сути, сканирование портов состоит из отправки сообщения на каждый порт, по одному за раз. Тип полученного ответа указывает, используется ли порт, и поэтому может быть дополнительно исследован на наличие слабых мест.

Существует несколько различных способов выполнения фактического сканирования портов путем установки различных флагов TCP (Transmission Control Protocol) или отправки различных типов пакетов TCP. Сканирование портов в основном обнаруживает открытые порты. Например, сканирование SYN сообщит сканерам портов, какие порты прослушивают, а какие нет, в зависимости от типа генерируемого ответа. Сканирование FIN будет генерировать ответ от закрытых портов, но открытые и прослушивающие порты не будут отправлять ответ, поэтому сканер портов сможет определить, какие порты открыты, а какие нет.

Программное обеспечение для сканирования портов в своем наиболее простом состоянии просто отправляет запрос на последовательное подключение к целевому компьютеру на каждом порту и записывает, какие порты отреагировали или кажутся открытыми для более глубокого исследования.

Если сканирование порта выполняется злонамеренно, злоумышленник, как правило, предпочитает остаться незамеченным. Приложения сетевой безопасности могут быть настроены на оповещение администраторов, если запросы на соединение обнаруживаются в широком диапазоне портов с одного хоста. Чтобы обойти это, злоумышленник может выполнить сканирование портов в стробоскопическом или скрытом режиме. Стробирование ограничивает порты меньшим целевым набором, а не общим сканированием всех 65 536 портов. Скрытое сканирование использует методы, чтобы замедлить сканирование. Сканируя порты в течение гораздо более длительного периода времени, злоумышленник снижает вероятность того, что цель вызовет предупреждение.

6.3.3 Эксперимент

Чтобы поэкспериментировать с тем, как выполнить и обнаружить атаку сканирования портов, проводится эксперимент с использованием расширенного сканера портов в качестве сканера портов и устройства Juniper Networks в качестве устройства обнаружения. В этом эксперименте используется та же архитектура сети, которая описана в практическом упражнении по наземной атаке в главе 5 (лабораторная работа 5.1).

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от сканирования портов TCP.
Шаг 4: Выполните сканирование порта TCP.
Шаг 5: нюхать сгенерированный трафик.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте практического упражнения по Land-атаке в главе 5 (лабораторная работа 5.1).

6.3.3.1 Включить защиту от сканирования портов

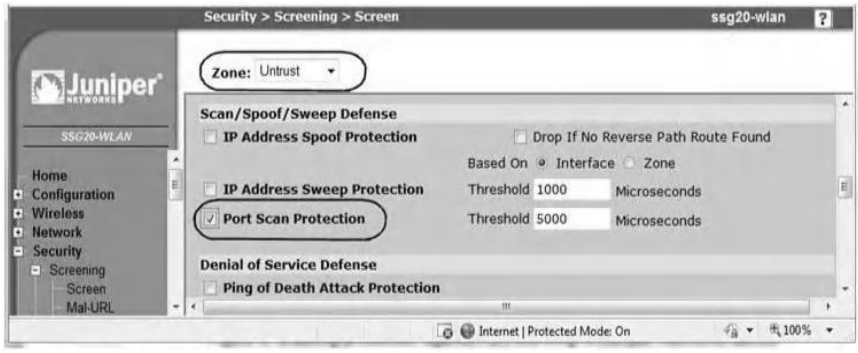
Чтобы включить защиту от сканирования портов в устройстве Juniper Networks, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите «Screening» и установите следующие параметры, как показано на следующем скриншоте:
  — Установите для зоны значение «Недоверять», поскольку трафик сканирования портов будет генерироваться из ненадежной зоны.

–– Выберите «Защита от сканирования портов».

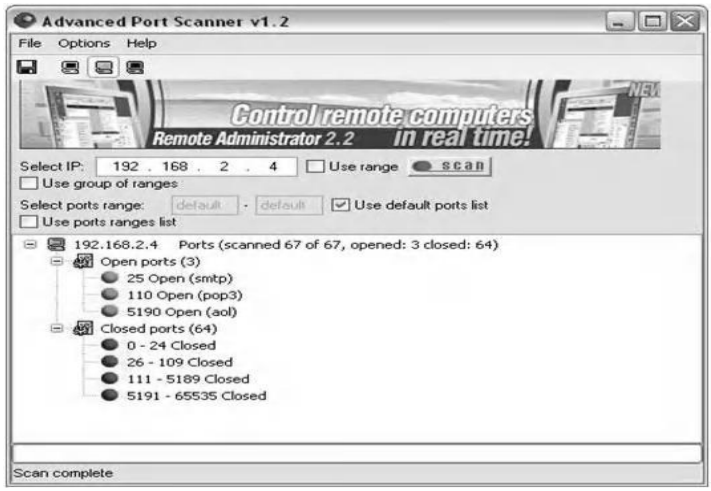
–– Установите значение Threshold: в устройстве Juniper Networks сканирование портов происходит, когда один IP-адрес источника отправляет IP-пакеты, содержащие сегменты TCP SYN, на десять различных портов с одним и тем же IP-адресом назначения в течение определенного интервала. Если удаленный хост отправляет трафик ICMP на десять адресов, используя настройки по умолчанию, за 0,005 секунды (5000 микросекунд), то устройство помечает это как атаку сканирования портов и отклоняет все дальнейшие пакеты из удаленного источника на оставшуюся часть указанного периода времени ожидания , Пользователь должен выбрать пороговое значение, чтобы обеспечить быстрое обнаружение трафика сканирования TCP-порта.

* Затем нажмите “Apply.”



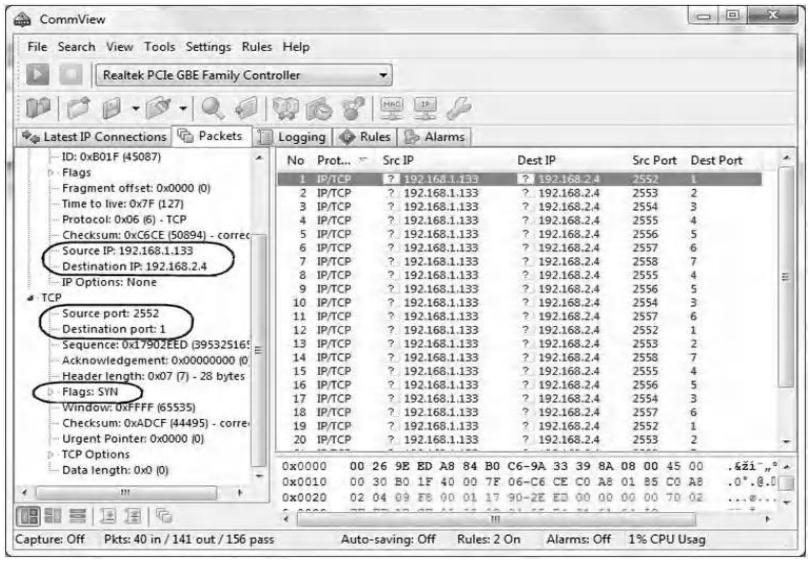
6.3.3.2 Шаг 4. Выполните сканирование портов TCP

На хосте злоумышленника средство Advanced Port Scanner используется для сканирования портов TCP на хосте жертвы (192.168.2.4). На следующем снимке экрана показаны идентифицированные открытые и закрытые порты TCP в целевой системе.



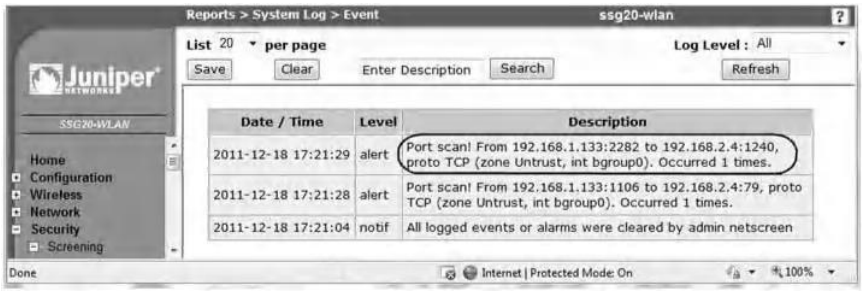
6.3.3.3 Шаг 5: Сниффинг сгенерированного трафика

На хосте злоумышленника можно использовать сниффер для захвата сгенерированного трафика. Например, с помощью сниффера CommView на следующем снимке экрана показано, что хост атаки (192.168.1.133) выполняет сканирование портов TCP на хосте vic-tim (192.168.2.4).



6.3.3.4 Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks

Содержимое журнала событий на устройстве Juniper Networks после обнаружения атаки сканирования порта TCP представлено на следующем снимке экрана.



6.4 Лабораторная работа 6.3: идентификация удаленной операционной системы

6.4.1 Результат

Цель данного практического упражнения состоит в том, чтобы учащиеся узнали, как предотвратить атаки, связанные с идентификацией удаленной операционной системы (ОС).

6.4.2 Описание

Знание операционной системы системы помогает злоумышленнику запустить атаку. Это ценная информация как для тестеров на проникновение, так и для хакеров, поскольку при обнаружении уязвимостей они обычно зависят от версии ОС. Перед запуском эксплойта злоумышленник может попытаться исследовать целевой хост, чтобы узнать его ОС.

Удаленная идентификация ОС выполняется путем активной отправки пакетов на удаленный хост и анализа ответов. Существуют такие инструменты, как NetscanTools Pro, Nmap, Xprobe2 и GFI LANguard сканер, которые могут выполнять удаленную идентификацию ОС. Они принимают ответы и формируют отпечаток, который можно сравнить с базой данных сигнатур известных ОС.

Пакеты, отправляемые на удаленный хост, являются необычными пакетами, поскольку они не указаны в RFC. Каждая ОС обрабатывает их по-разному, и, анализируя выходные данные, злоумышленник может определить, к какому типу устройства обращаются и какая ОС работает. Например, используется один тип пакета с битами SYN и FIN. В обычной работе этот тип пакета не должен возникать, поэтому, когда ОС отвечает на этот пакет, он делает это предсказуемым образом, что позволяет программе определить, какую ОС использует хост. Порядковые номера, используемые в TCP, также имеют различные уровни случайности, в зависимости от того, какая ОС работает. Инструменты также используют эту информацию, чтобы лучше понять, что представляет собой удаленная ОС. В следующем разделе более подробно описываются методы, используемые инструментами NetScanTools Pro и Nmap.

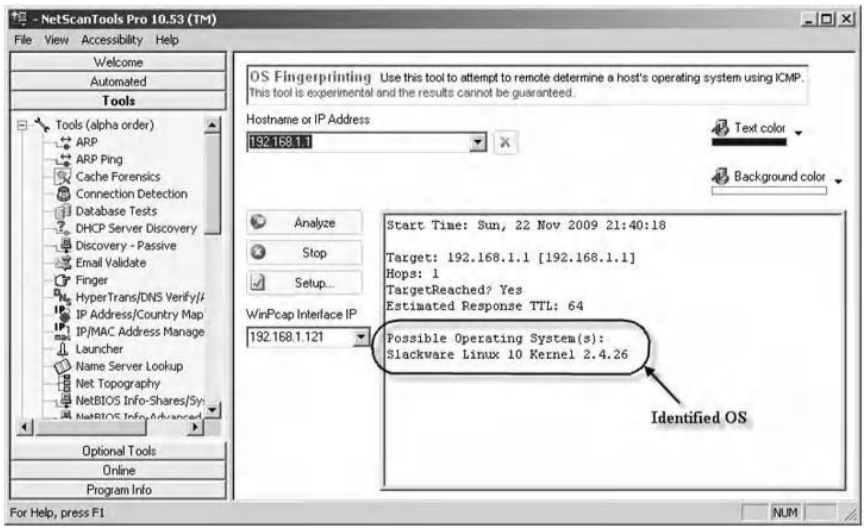
6.4.2.1 NetScanTools Pro

NetScanTools Pro - это интегрированная коллекция утилит сбора информации в Интернете. Чтобы идентифицировать удаленную ОС, этот инструмент полагается на отправку четырем основным типам пакетов ICMP к цели:

1. Стандартные пакеты эхо-запроса ICMP (Ping)
2. Пакеты запроса метки времени ICMP
3. ICMP пакеты информационного запроса
4. Пакеты запроса маски подсети ICMP

Затем инструмент просматривает ответ и отправляет дальнейшие варианты четырех основных типов пакетов. Ответы целевой ОС отмечаются и используются для классификации типа целевой ОС. Важно указать, что если некоторые или все вышеперечисленные четыре входящих ICMP-пакета заблокированы брандмауэром, и поэтому они не могут достичь целевого удаленного хоста, механизм идентификации ОС не сможет работать должным образом, и его выходной результат будет

определенно не точный. На следующем снимке экрана показаны выходные данные, полученные в результате запуска NetScanTools Pro с включенной опцией «Отпечаток пальца».



6.4.2.2 Nmap

Nmap - это инструмент для исследования сети и сканер безопасности. Он предназначен для того, чтобы пользователи могли сканировать сети, чтобы определить, какие хосты работают и какие услуги они предлагают. Nmap также включает такие функции, как идентификация удаленной ОС, параллельное сканирование, обнаружение фильтрации портов и параметры синхронизации.

Определение ОС в Nmap работает путем отправки до 16 зондов TCP, UDP и ICMP на известные открытые и закрытые порты целевой системы. Эти зонды специально разработаны для использования различных неопределенностей в RFC стандартного протокола. Затем Nmap прислушивается к ответам. Десятки атрибутов в этих ответах анализируются и объединяются для создания отпечатка пальца.

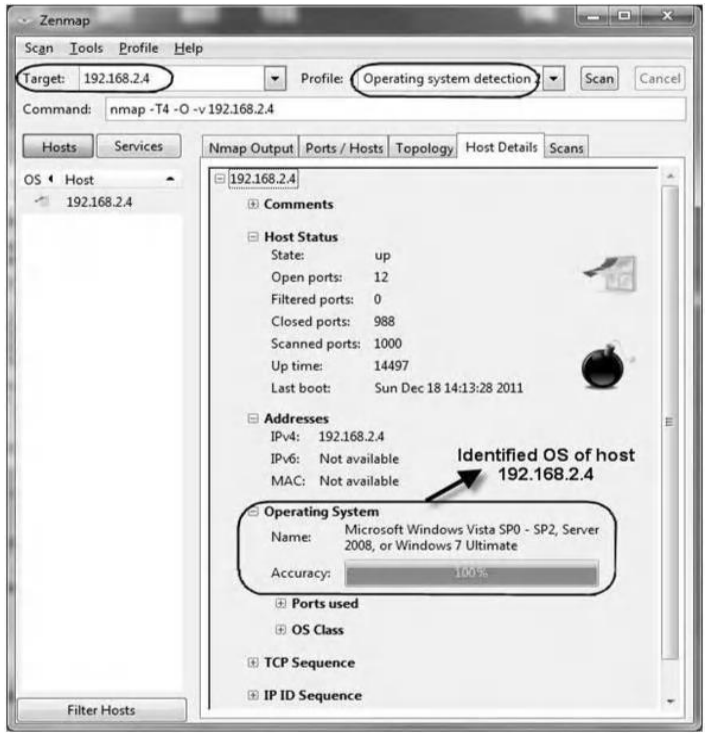
Каждый тестовый пакет отслеживается и повторно отправляется хотя бы один раз, если нет ответа. Все пакеты являются IPv4 со случайным значением IP ID. Зонды к открытому порту TCP пропускаются, если такой порт не был найден. Для закрытых портов TCP или UDP Nmap сначала проверит, найден ли такой порт. Если нет, Nmap просто выберет порт наугад и надеется на лучшее.

Ниже приведены примеры тестовых пакетов TCP, отправленных Nmap на удаленный хост:

* T1: Первый пакет отправляет пакет TCP с включенными флагами SYN и ECN-Echo на открытый порт TCP.
* T2: Второй пакет отправляет нулевой пакет TCP (без установленных флагов) с установленным битом IP DF и полем окна 128 в открытый порт.
* T3: Третий пакет отправляет TCP-пакет с установленными флагами SYN, FIN, URG и PSH и оконным полем 256 в открытый порт. Бит IP DF не установлен.
* T4: Четвертый пакет отправляет пакет TCP ACK с IP DF и полем окна 1024 в открытый порт.
* T5: Пятый пакет отправляет пакет TCP SYN без IP DF и поля окна 31,337 на закрытый порт.
* T6: Шестой пакет отправляет пакет TCP ACK с IP DF и полем окна 32 768 на закрытый порт.
* T7: Седьмой пакет отправляет TCP-пакет с установленными флагами FIN, PSH и URG и полем окна 65 535 в закрытый порт. Бит IP DF не установлен.

Вебсайт <http://nmap.org> подробно описывает все тестовые пакеты TCP / IP, используемые Nmap.

На следующем снимке экрана показаны выходные данные, полученные в результате запуска Nmap с включенной опцией «Отпечаток пальца» ОС с использованием интерфейса Zenmap (официальный интерфейс Nmap GUI).



Некоторые устройства сетевой безопасности, такие как Juniper Networks, способны блокировать некоторые пакеты проверки ОС, так что средство проверки ОС не может определить целевую удаленную ОС, иначе результат идентификации ОС будет неточным.

6.4.3 Эксперимент

Чтобы определить, как запретить инструменту Nmap идентифицировать удаленную ОС, проводится эксперимент с использованием устройства Juniper Networks. Устройство Juniper Networks может заблокировать три TCP-пакета, а именно:

1. *Пакет TCP без флагов (T2):* обычный заголовок пакета TCP имеет по крайней мере один набор управления флагами. Пакет TCP без установленных контрольных флагов является аномальным событием.

Поскольку разные ОС по-разному реагируют на такие аномалии, ответ (или отсутствие ответа) от целевого устройства может дать представление о типе ОС, на которой оно работает.

2. *Пакет TCP с установленными флагами SYN и FIN (T3):* Флаги управления SYN и FIN обычно не устанавливаются в одном и том же заголовке сегмента TCP. Флаг SYN синхронизирует порядковые номера, чтобы инициировать соединение TCP. Флаг FIN указывает на завершение передачи данных для завершения соединения TCP. Их цели взаимоисключающие. Заголовок TCP с установленными флагами SYN и FIN является аномальным поведением TCP, вызывая различные ответы от получателя, в зависимости от ОС.
3. *Пакет TCP с флагом FIN и без ACK (T7):* Обычно TCP-пакеты с установленным флагом FIN также имеют установленный флаг ACK (для подтверждения получения предыдущего пакета). Поскольку заголовок TCP с установленным флагом FIN, но не установленный флаг ACK, является аномальным поведением TCP, предсказуемого ответа на это не существует. ОС может ответить отправкой пакета TCP с установленным флагом RST. Другой может полностью игнорировать это. Ответ жертвы может дать злоумышленнику ключ к пониманию его ОС.

В этом эксперименте используется та же архитектура сети, которая описана в практическом упражнении по Land-атаке в главе 5 (лабораторная работа 5.1).

Эксперимент состоит из следующих этапов:

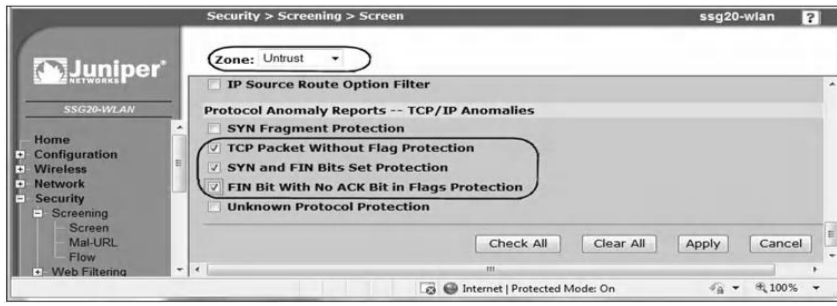
Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Установите политики безопасности (правила фильтрации).
Шаг 3: Включите защиту от трех тестовых пакетов TCP.
Шаг 4: Сгенерируйте три тестовых пакета TCP.
Шаг 5: Сниффинг сгенерированного трафика.
Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks.

Шаги 1 и 2 аналогичны тем, которые описаны в эксперименте практического упражнения по Land-атаке в главе 5 (лабораторная работа 5.1).

6.4.3.1 Шаг 3. Включите защиту от трех пакетов TCP

Чтобы включить защиту от трех тестовых пакетов TCP на устройстве Juniper Networks, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите «Screening» и установите следующие параметры, как показано на следующем снимке экрана.
  — Установите для зоны значение «Недоверие», поскольку трафик Land-атаки будет генерироваться из недоверенной зоны.
  — Выберите:
    - Пакет TCP без защиты флага
    - Защита набора битов SYN и FIN
    - FIN бит без ACK в защите флагов
* Затем нажмите “Apply.”



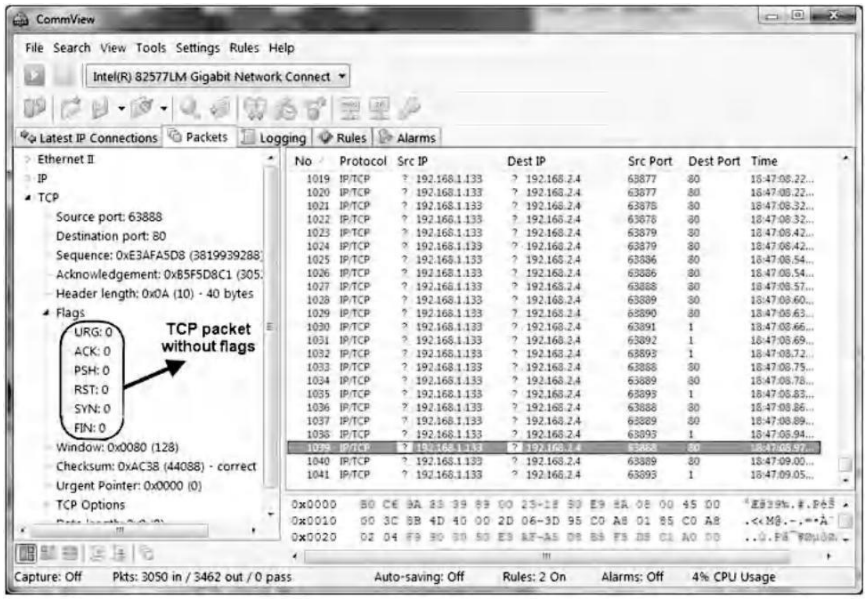
6.4.3.2 Шаг 4. Создайте три пакета пробника TCP

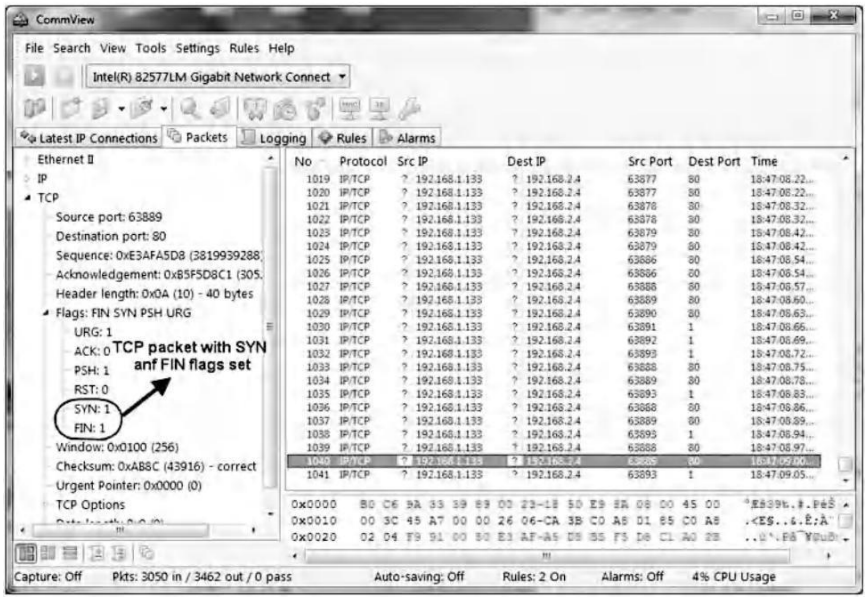
При запуске инструмента Nmap три тестовых TCP-пакета (T2, T3 и T7) отправляются в удаленную ОС.

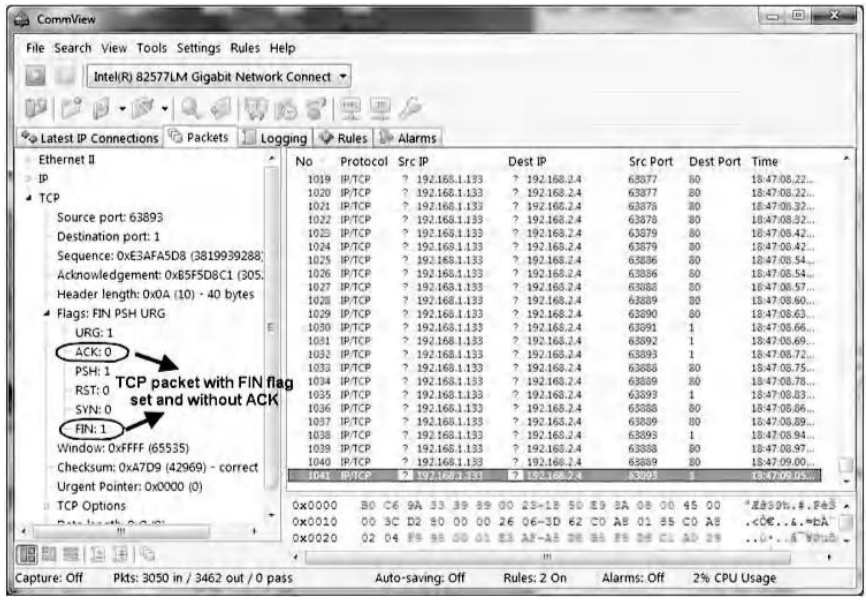
6.4.3.3 Шаг 5: Сниффинг сгенерированного трафика

На хосте злоумышленника, где работает Nmap, для захвата сгенерированного трафика используется анализатор CommView.

На следующих трех снимках экрана показаны пакеты T2 (пакет TCP без флагов), T3 (пакет TCP с установленными флагами SYN и FIN) и пакеты T7 (пакет TCP с флагом FIN и без ACK) соответственно.

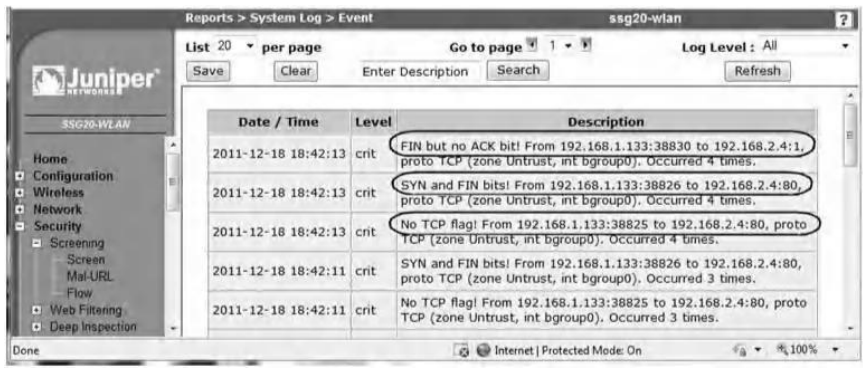






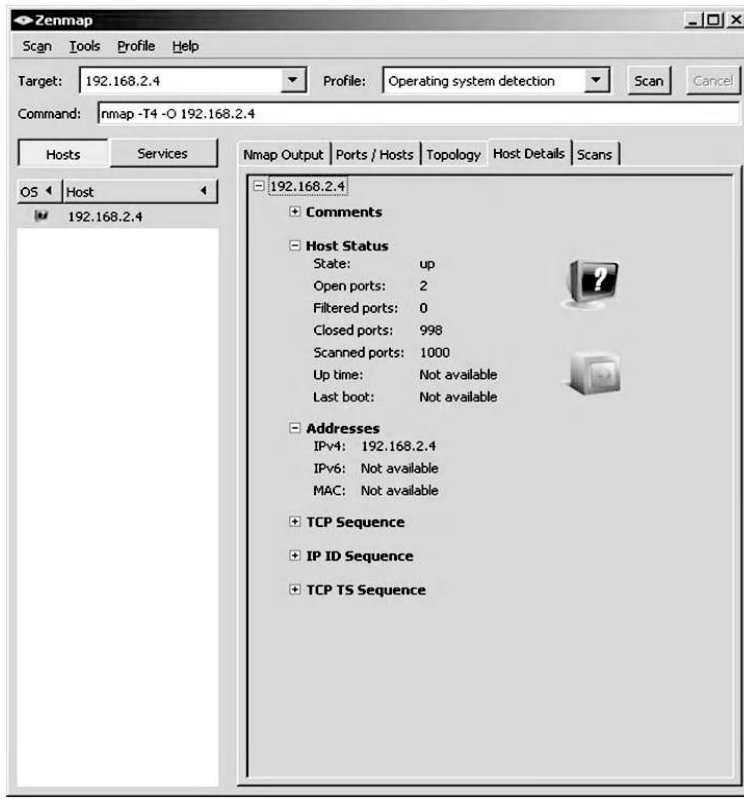
6.4.3.4 Шаг 6: Просмотр результатов в файле журнала устройства Juniper Networks

На следующем снимке экрана показано содержимое журнала событий в устройстве Juniper Networks после обнаружения трех необычных зондирующих TCP-пакетов.



На основании результатов тестов, выполненных инструментом Nmap, не удалось создать сигнатуру ОС, поскольку три тестовых TCP-пакета,

сгенерированных Nmap, были заблокированы устройством Juniper Networks. Поэтому Nmap не может идентифицировать ОС удаленного хоста (192.168.2.4), как показано на следующем снимке экрана.



6.5 Лабораторная работа 6.4: Трассировка

6.5.1 Результат

Цель данного практического упражнения - научить студентов анализировать трафик traceroute и предотвращать сбор информации об удаленных хостах и сетях с использованием traceroute.

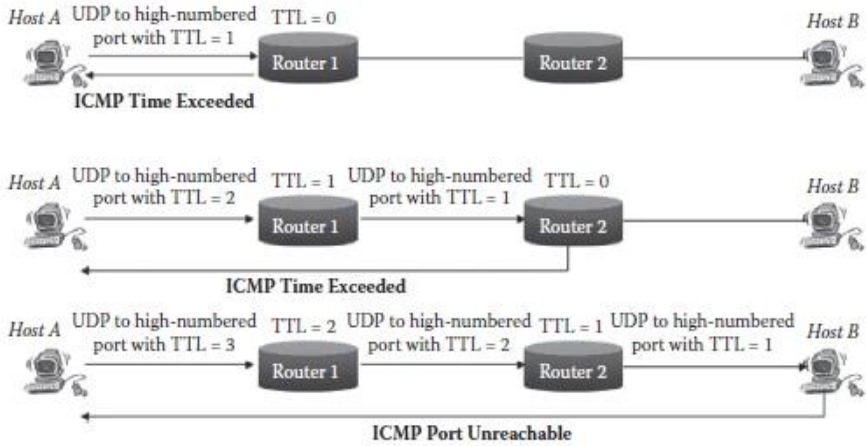
6.5.2 Описание

Traceroute - это программа, которая показывает маршрут по сети между двумя системами, перечисляя все промежуточные маршрутизаторы, через которые должно пройти соединение, чтобы добраться до места назначения. Traceroute - популярная техника разведки.

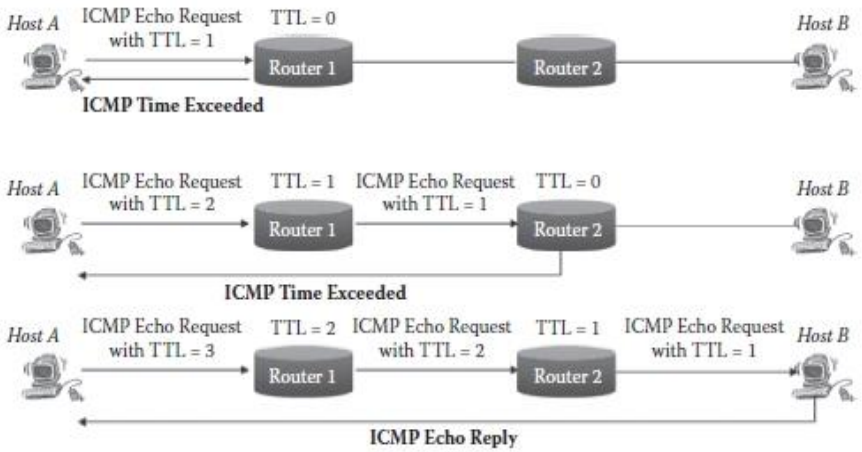
Traceroute работает, заставляя каждый маршрутизатор по сетевому пути возвращать сообщение об ошибке ICMP. Пакет IP содержит значение времени жизни (TTL), которое указывает, как долго он может продолжить поиск пункта назначения, прежде чем его выбросят. Каждый раз, когда пакет проходит через маршрутизатор, его значение TTL уменьшается на единицу; когда он достигает нуля, пакет отбрасывается, и отправителю возвращается сообщение об ошибке ICMP Time-To-Live Exceeded.

Программа Traceroute отправляет свою первую группу пакетов со значением TTL, равным 1. Следовательно, первый маршрутизатор вдоль пути отбрасывает пакет (его TTL уменьшается до 0) и возвращает сообщение об ошибке ICMP TTL Exceeded. Таким образом, первый маршрутизатор на пути найден. Затем пакеты могут быть отправлены с TTL 2, а затем 3 и т. Д., В результате чего каждый маршрутизатор вдоль пути возвращает сообщение об ошибке ICMP TTL, идентифицируя его отправителю. В конечном итоге либо достигается конечный пункт назначения, либо достигается максимальное значение, и маршрут трассировки заканчивается.

В конечном месте возвращается другое сообщение об ошибке ICMP. Большинство версий Traceroute для Linux работают, посылая дейтаграммы UDP на некоторый случайный порт с большим номером, где ничего не будет прослушиваться. Когда эта окончательная система достигнута, поскольку на этом порту ничего не отвечает, возвращается сообщение об ошибке ICMP Port Unreachable, и программа Traceroute завершает работу (см. Следующий рисунок для этапов работы версии Traceroute для Linux).

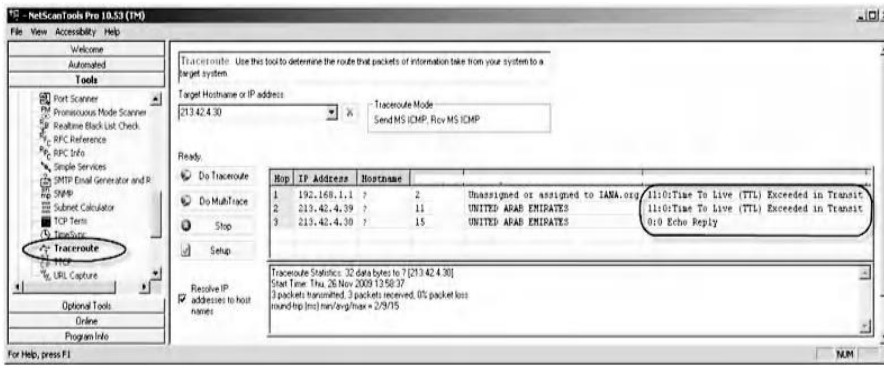


Версия Traceroute для Windows использует пакеты эхо-запроса ICMP (пакеты ping), а не дейтаграммы UDP; обратитесь к следующему рисунку для получения информации о действиях для версии Traceroute для Windows. Несколько версий Traceroute, например, в Solaris, позволяют выбрать любой из методов (эхо-запросы UDP или ICMP с высоким портом).



Для выполнения traceroute обычно онлайн-команды Tracert или Traceroute используются в среде Windows или Linux / Unix, соответственно. Существуют также инструменты трассировки на основе графического интерфейса, такие как NetScanTools Pro и VisualRoute. На следующем снимке экрана показан пример вывода

traceroute с использованием инструмента NetScanTools Pro. Между исходным хостом и хостом назначения существует два прыжка (213.42.4.30), поскольку были получены два пакета ICMP Exceeded и один пакет эхо-ответа ICMP.



6.5.3 Техники предотвращения

Чтобы предотвратить сбор информации при использовании Traceroute, можно использовать два метода:

* Первый метод использует брандмауэр для блокировки исходящих ICMP превышения времени, эхо-ответа ICMP и пакетов ICMP Destination Unreachable-Port. Чтобы заблокировать такой трафик ICMP, на брандмауэрах или маршрутизаторах должны быть реализованы следующие правила фильтрации:

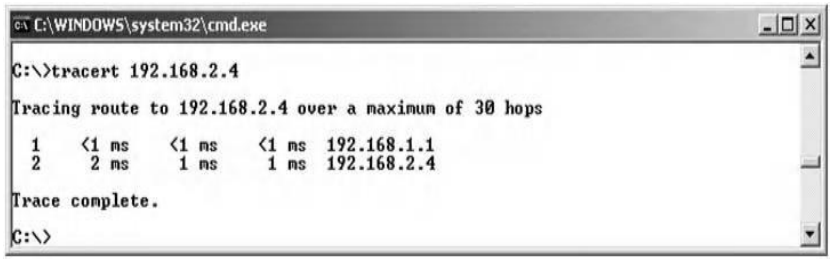
Название правила	направление	Исходный IP	IP-адрес назначения	протокол	тип	Код	Действие
Block_ICMP_Time_Exceeded	Исходящий	Любой	Любой	ICMP	11	0	отказ
Block_ICMP_Echo_Reply	Исходящий	Любой	Любой	ICMP	0	0	отказ
Block_ICMP_Port_Unreachable	Исходящий	Любой	Любой	ICMP	3	3	отказ

* Второй метод использует предопределенное правило фильтрации брандмауэра для блокировки трафика трассировки маршрута. Большинство брандмауэров включают в себя предопределенное правило фильтрации для запрета трафика Traceroute.

Следующие два раздела описывают два эксперимента. Первый показывает, как захватывать и анализировать пакеты, сгенерированные командой Tracert. Второй показывает, как предотвратить трассировку, используя предопределенное правило фильтрации в устройстве Juniper Networks.

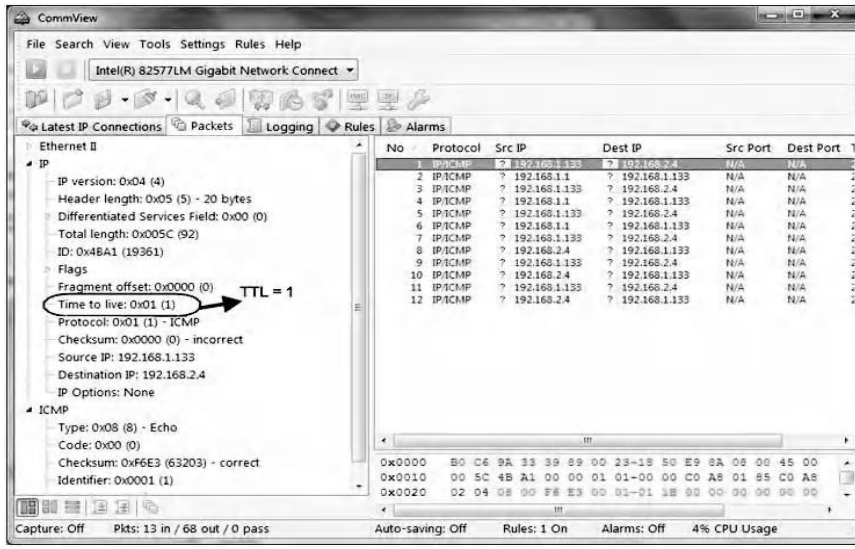
6.5.3.1 Эксперимент 6.4.1. Анализ трафика, генерируемого командой Tracert

Целью этого эксперимента является анализ трафика команд Tracert. На следующем снимке экрана показан результат (вывод) выполнения команды Tracert. Он показывает, что между исходным хостом и целевым хостом существует только один переход (192.168.1.1) (192.168.2.4).

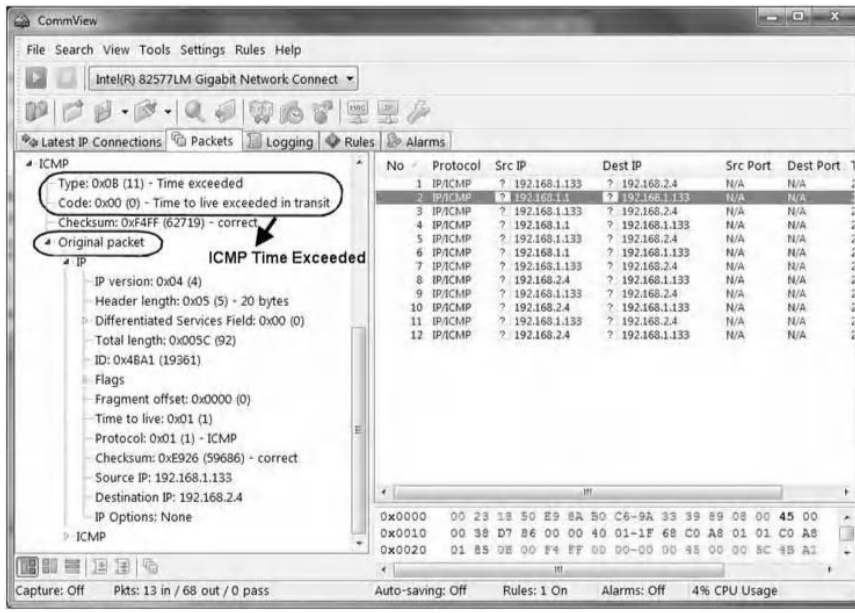


Анализатор CommView используется для захвата сгенерированного трафика. На следующих четырех снимках экрана показаны четыре ICMP-пакета, которыми обмениваются хост-узел атакующего (исходный хост) и целевой хост:

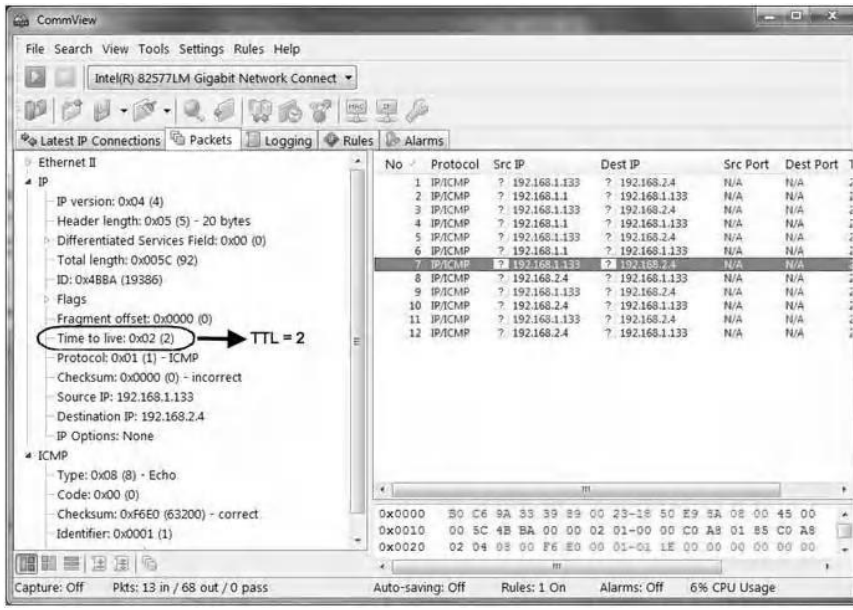
1. Первый пакет эхо-запроса ICMP с TTL = 1, отправленный исходным хостом на целевой хост:



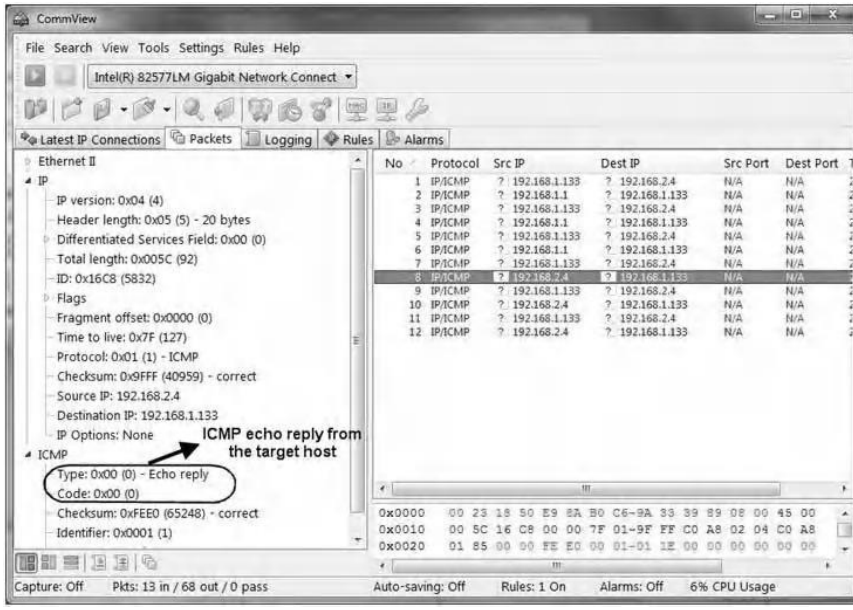
2. После получения этого пакета первый маршрутизатор отправляет пакет ICMP Time Exceeded исходному хосту. Пакет на этом снимке экрана также показывает заголовки IP и ICMP исходного пакета на предыдущем снимке экрана.



3. Второй пакет эхо-запроса ICMP с TTL = 2, отправленный исходным хостом на целевой хост:



4. Эхо-ответ ICMP, отправленный целевым хостом на исходный хост:



6.5.3.2 Эксперимент 6.4.2. Запретить трассировку трафика

6.5.3.2.1 Архитектура сети

В этом эксперименте используется та же архитектура сети, которая описана в практическом упражнении по наземной атаке в главе 5 (лабораторная работа 5.1).

6.5.3.2.2 Шаги эксперимента:

Шаги в эксперименте следующие:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2. Создайте правило фильтрации, чтобы запретить трассировку трафика.
Шаг 3: Выполнить команду Tracert.
Шаг 4: Просмотрите результаты в файле журнала устройства Juniper Networks.

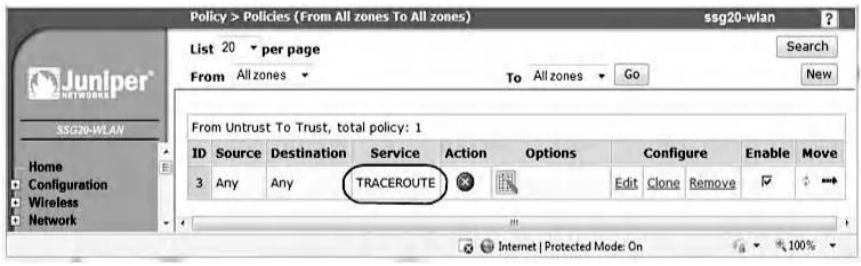
6.5.3.2.2.1 Шаг 1: Настройте сетевые интерфейсы в устройстве Juniper Networks

Шаг 1 аналогичен описанному в эксперименте практической лаборатории по Land-атаке главы 5 (лабораторная работа 5.1).

6.5.3.2.2.2 Шаг 2. Создайте правило фильтрации для запрета трассировки трафика.

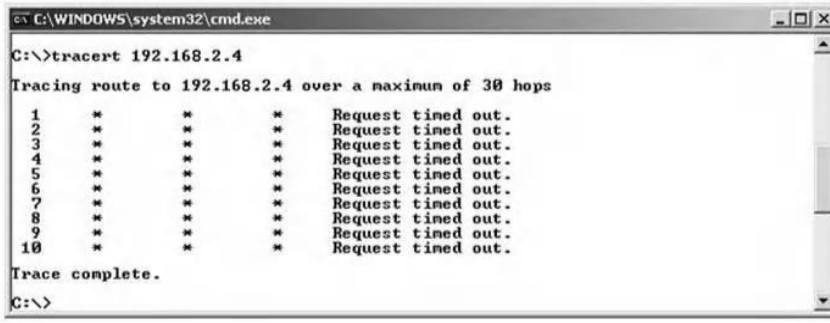
В устройстве Juniper Networks, чтобы создать правило фильтрации, позволяющее запретить трассировку, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите «Policies», затем создайте правило фильтрации, как показано ниже.



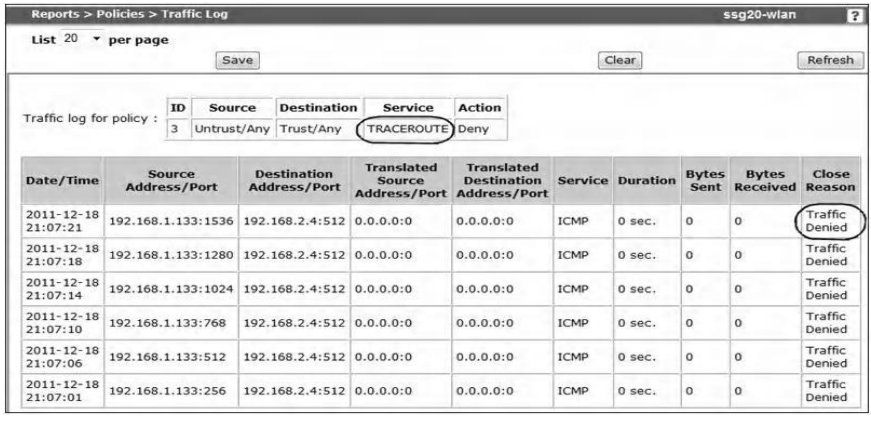
6.5.3.2.2.3 Шаг 3: Выполнить команду Tracert

В случаях, когда трассировка либо не достигает своего места назначения, либо не возвращаются сообщения ICMP Time Exceeded, в выходных данных отображается звездочка в каждом из трех столбцов времени, где обычно отображается время кругового обхода, и «истекло время ожидания запроса». На приведенном ниже снимке экрана показано, что команда Tracert не может определить список прыжков между исходным хостом и хостом назначения. Это связано с тем, что трафик traceroute был отфильтрован по правилу фильтрации предыдущего снимка экрана.



6.5.3.2.2.4 Шаг 4: Просмотр результатов в файле журнала устройства Juniper Networks

Содержимое журнала событий в устройстве Juniper Networks после обнаружения и блокировки трафика traceroute показано ниже.



6.6 Краткое содержание главы

Злоумышленникам необходимо собрать информацию о целевых системах и сетях перед выполнением своих эксплойтов. Существует множество доступных, простых в использовании методов и инструментов для сбора информации о целевой среде. Оглядываясь назад, для организации чрезвычайно важно знать, какую информацию злоумышленник может получить о себе, чтобы обезопасить и минимизировать потенциальную потерю важной информации. В этой главе обсуждались некоторые методы разведки и описывалось, как практически системы и сети могут быть защищены от разведывательного трафика. В практических упражнениях обсуждались четыре общих метода разведки, а именно: поиск IP-адреса, сканирование порта TCP, идентификация удаленной ОС и Traceroute.

Глава 7

Фильтрация и проверка пакетов

7.1 Введение

Большинство организаций контролируют трафик, который пересекает их сети и выходит из них, чтобы предотвратить атаки на их компьютерные системы и соответствовать различным вариантам политики.

Фильтрация и проверка сетевых пакетов являются средствами контроля доступа к сетям и системам. Концепция заключается в определении, разрешено ли пакету входить или выходить из сети, путем сравнения данных полезной нагрузки пакета и / или значения некоторых полей, расположенных в заголовке пакета, с предварительно определенными значениями. Технология фильтрации и проверки пакетов используется в операционных системах, межсетевых экранах, системах обнаружения и предотвращения вторжений, а также в качестве функции безопасности большинства маршрутизаторов и некоторых современных коммутаторов.

Брандмауэры контролируют доступ в и из сети на основе набора правил фильтрации, которые отражают и обеспечивают соблюдение политик безопасности организации. Внутри сети брандмауэр, как правило, является первым фильтрующим устройством, которое обнаруживает пакеты, пытающиеся проникнуть в сеть организации извне, и обычно является последним устройством, которое видит выходящие пакеты. Задача брандмауэра - принимать решения по фильтрации для каждого пакета, который пересекает его: либо пропустить его, либо отбросить.

В этой главе обсуждается серия практических упражнений по фильтрации и проверке общего сетевого трафика и стандартных/нестандартных служб с использованием правил фильтрации брандмауэра. Глава включает упражнение о согласованности и эффективности проверки правил фильтрации брандмауэра. В упражнениях используются следующие аппаратные устройства и программные средства:

* Беспроводное устройство Juniper Networks SSG20 * (устройство Juniper Networks): в качестве устройства брандмауэра
* Устройство адаптивной защиты Cisco ASA 5520 †: в качестве устройства межсетевого экрана
* CommView Tool ‡: сетевой монитор и анализатор (сниффер)
* CommView Visual Packet Builder§: генератор пакетов на основе графического интерфейса пользователя (GUI)
* LiteServe¶: программное обеспечение для Интернета, FTP, электронной почты и серверов Telnet
* FirePAC **: автономный программный инструмент для проверки несоответствия и неэффективности набора правил фильтрации

7.2 Лабораторная работа 7.1: базовая фильтрация пакетов

7.2.1 Результат

Цель данного практического упражнения - научить студентов внедрять правила фильтрации брандмауэра для основных политик безопасности.

*http://www.juniper.net
† http://www.cisco.com
‡ http://www.tamos.com §
http://www.tamos.com
¶http://www.cmfperception.com
*http://www.athenasecurity.com

7.2.2 Базовая фильтрация пакетов

Базовая фильтрация пакетов - это выборочная передача или блокировка пакетов при их прохождении через сетевой интерфейс. Критерии, которые использует фильтрация пакетов при проверке пакетов, основаны на заголовках Уровня 3 (IPv4 и IPv6) и Уровня 4 [TCP (Протокол управления передачей), UDP (Протокол пользовательских дейтаграмм), ICMP (Протокол управляющих сообщений Интернета) и ICMPv6]. модели OSI (Взаимодействие открытых систем). Наиболее часто используемыми критериями являются IP-адреса источника и назначения, порты TCP / UDP источника и назначения, биты флага TCP, поля типа и кода в заголовке ICMP и поле протокола заголовка уровня 4.

Правила фильтрации брандмауэра определяют критерии, которым должен соответствовать пакет, и результирующее действие. Действие может быть «Пропустить» (пропустить пакет), «Заблокировать» (не пересылать пакет) или «Отклонить» (аналогично «Отбросу», за исключением того, что отправителю отправляется специальный ICMP-пакет, сообщающий ему, что пакет был отфильтрован) , Правила фильтрации оцениваются в последовательном порядке, от начала до конца. В конце набора правил фильтрации есть неявное «Пропустить все» или «Запретить все», что означает, что если пакет не соответствует ни одному правилу фильтрации, результатом будет передача или отклонение. Рекомендуемая практика при реализации правил фильтрации заключается в применении подхода «запрет по умолчанию». То есть запретить все, а затем выборочно разрешить определенный трафик через брандмауэр. Этот подход рекомендуется, потому что он ошибается, а также облегчает написание набора правил

Например, чтобы отфильтровать весь трафик Ping, поступающий в сеть, заблокируйте все входящие пакеты эхо-запроса ICMP (Тип = 8 и Код = 0). Чтобы отфильтровать все входящие запросы на доступ к внутренним FTP-серверам, заблокируйте весь входящий трафик, который направляется на TCP-порт 21. Для этих двух политик безопасности правила фильтрации должны быть определены и реализованы в выбранной технологии фильтрации пакетов (межсетевой экран, маршрутизатор, коммутатор, операционная система и т. д.). Следующие два правила фильтрации (R1 и R2) отражают две вышеупомянутые политики безопасности:

правило	направление	IP-адрес источника	IP-адрес получателя	протокол	тип	код	действие
R1	входящий	любой	любой	ICMP	8	0	отказ

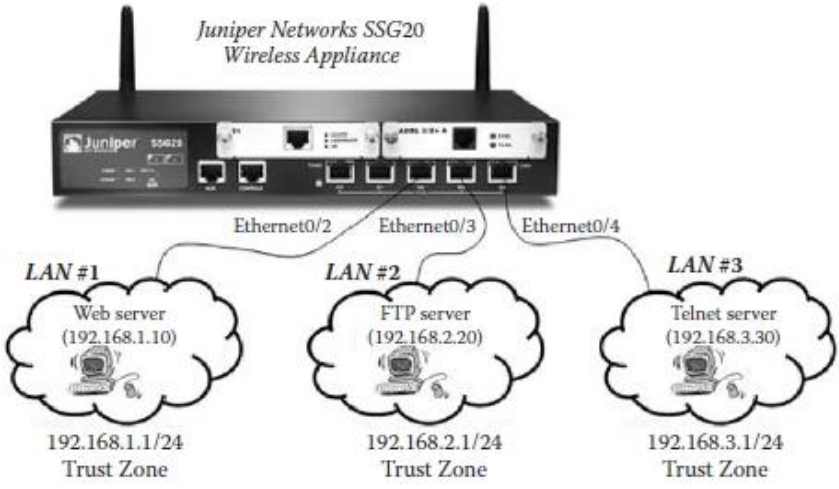
правило	направление	IP-адрес источника	IP-адрес получателя	протокол	Порт источника	Порт получателя	действие
R1	входящий	любой	любой	TCP	любой	21	отказ

7.2.3 Эксперимент

Этот эксперимент состоит из реализации правил фильтрации в устройстве Juniper Networks для различных политик безопасности. Политики безопасности позволяют применять правила фильтрации к сетевому трафику, которым обмениваются клиентские хосты и серверы.

7.2.4 Архитектура сети

На следующем рисунке показана сетевая архитектура, использованная в эксперименте. Трафик, которым обмениваются три сети, проходит через устройство Juniper Networks, где он фильтруется и проверяется набором правил фильтрации.



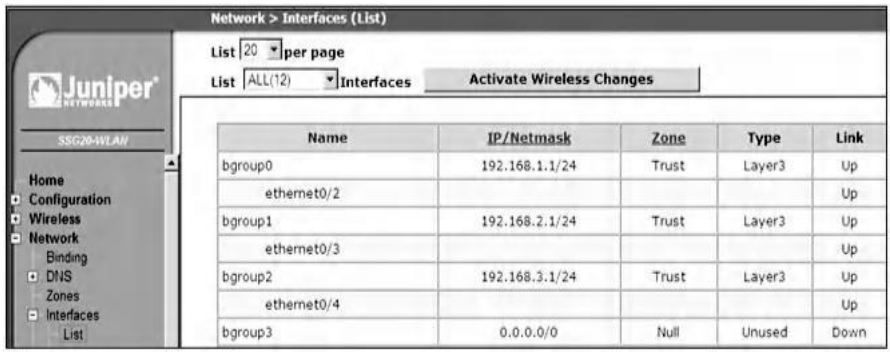
7.2.5 Шаги эксперимента

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Настройте серверы Web, FTP и Telnet.
Шаг 3. Реализация правил фильтрации для политик безопасности.
Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks

7.2.5.1 Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks

Используя интерфейс WebUI устройства Juniper Networks, настройте интерфейсы *ethernet0/2, ethernet0/3* и *ethernet0/4*, как показано на следующем снимке экрана. LAN № 1 (192.168.1.1/24), LAN № 2 (192.168.2.1/24) и LAN № 3 (192.168.3.1/24) подключены к сетевым интерфейсам *ethernet0/2, ethernet0/3* и *ethernet0/4* соответственно.



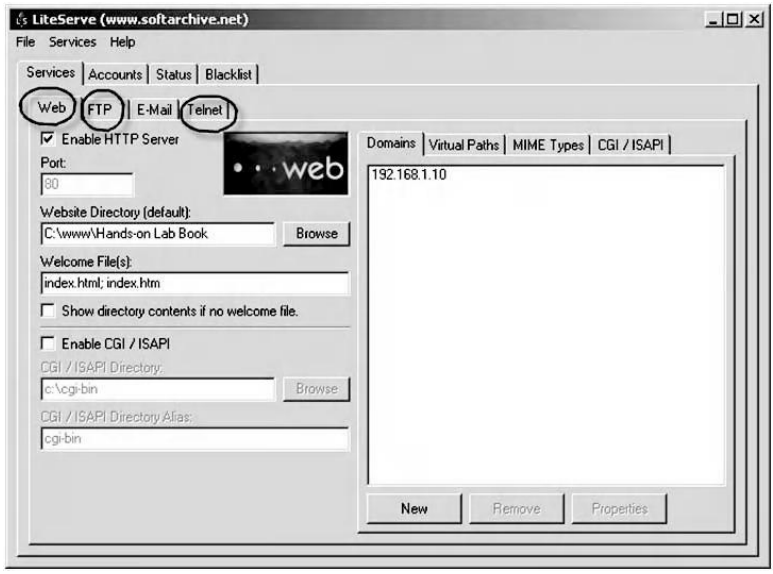
7.2.5.2 Шаг 2. Настройка серверов Web, FTP и Telnet

В Интернете имеется множество доступных серверных программ, которые можно загрузить и использовать для настройки серверов Web, FTP и Telnet. Например, если вы используете компьютер под управлением Windows, вы можете использовать встроенные службы IIS. Это набор интернет-сервисов для серверов, созданных

Microsoft для использования с Microsoft Windows. В настоящее время предоставляются следующие услуги: FTP (протокол передачи файлов), FTPS (безопасный протокол передачи файлов), SMTP (простой протокол передачи почты), NNTP (сетевой протокол передачи новостей) и HTTP / HTTPS (протокол передачи гипертекста / безопасный протокол передачи гипертекста).

В этой практической работе инструмент LiteServe используется для настройки серверов Web, FTP и Telnet (см. Следующий снимок экрана). Серверы настроены следующим образом:

* В LAN # 1 на хосте с IP-адресом 192.168.1.10 размещен веб-сервер.
* В LAN # 2 на хосте с IP-адресом 192.168.2.20 размещен FTP-сервер.
* В LAN #3, на хосте с IP-адресом 192.168.3.30 размещен Telnet-сервер.



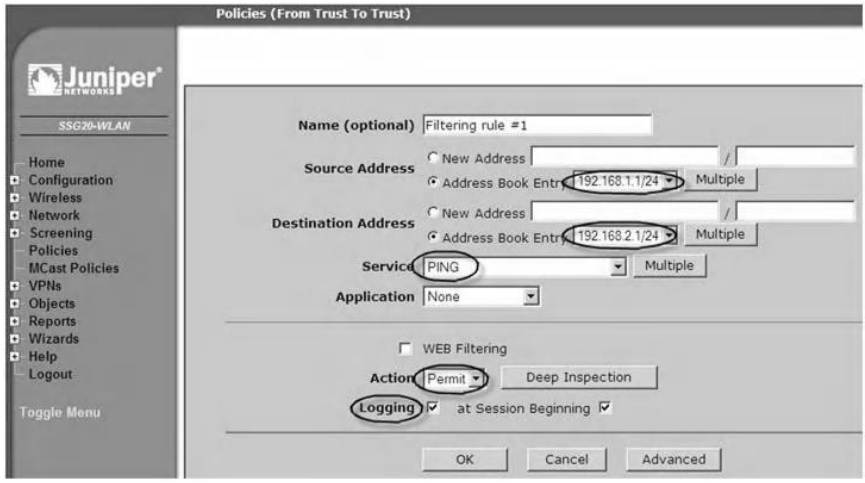
7.2.5.3 Шаг 3. Реализация правил фильтрации для политик безопасности

В устройстве Juniper Networks для реализации правила фильтрации для политики безопасности выполните следующие действия:

* Войдите в интерфейс WebUI устройства.

* Выберите «Policy»; затем укажите зоны сетей, участвующих в правиле фильтрации, как показано ниже:

* Нажмите на кнопку «New» и установите значения полей правила фильтрации. Например, следующий снимок экрана с правилом фильтрации показывает, что всем хостам в LAN # 1 (192.168.1.1/24) разрешено пропинговать все хосты в LAN # 2 (192.168.2.1/24). Кроме того, трафик, которым обмениваются между хостами, будет зарегистрирован.



Ниже приведены примеры политик безопасности и соответствующих им правил фильтрации:

1. *Security Policy#1 (Политика безопасности) (SP#1):* узлам LAN#1 разрешается пинговать узлы LAN#2 и LAN#3. Однако узлы LAN#2 и LAN#3 не могут подключаться к узлам LAN#1.

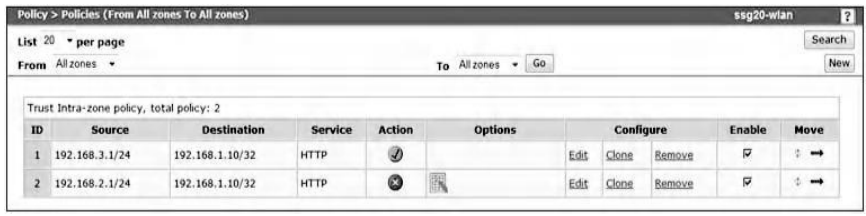
   Политика безопасности по умолчанию - “Deny all”(Запретить все). На следующем снимке экрана показаны правила фильтрации, реализованные в устройстве Juniper Networks и соответствующие политике безопасности SP # 1:

   — Правило с идентификатором 1 позволяет узлам LAN#1 (192.168.1.1/24) проверять связь с узлами LAN#2 (192.168.2.1/24) и узлами LAN#3 (192.168.3.1/24).

   — Правило с идентификатором 2 не разрешает узлам LAN#2 и узлам LAN#3 пинговать узлы LAN#1.

   — Правило с ID 3 является безопасностью по умолчанию.

2. *Security Policy#2 (SP#2):* Узлам LAN#3 разрешен доступ к веб-сайту (192.168.1.10/32) в LAN#1. Однако узлам LAN#2 не разрешен доступ к веб-сайту. На следующем снимке экрана показаны правила фильтрации, реализованные на устройстве Juniper Networks и соответствующие политике безопасности SP # 2:

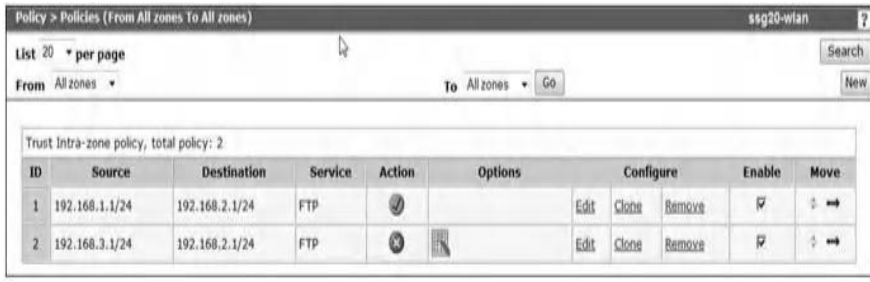


–– Правило с ID 1 позволяет узлам LAN#3 (192.168.3.1/24) получать доступ к веб-сайту (192.168.1.10/32) в LAN#1.
–– Правило с ID 2 не позволяет узлам LAN#2 (192.168.2.1/24) получать доступ к веб-сайту (192.168.1.10/32) в LAN#1.

3. *Security Policy #3 (SP#3):* Единственный хост в LAN#1, которому разрешено подключаться к сети (192.168.3.30) в LAN#3, - это хост (192.168.1.10). На следующем снимке экрана показаны правила фильтрации, реализованные в устройстве Juniper Networks и соответствующие политике безопасности SP # 3:

–– Правило с ID 1 позволяет узлу (192.168.1.10/32) в LAN#1 обращаться к серверу Telnet (192.168.3.30/32) в LAN#3.
–– Правило с ID 2 не позволяет узлам LAN#1 (192.168.1.1/24) получать доступ к серверу Telnet (192.168.3.30/32) в LAN#3.

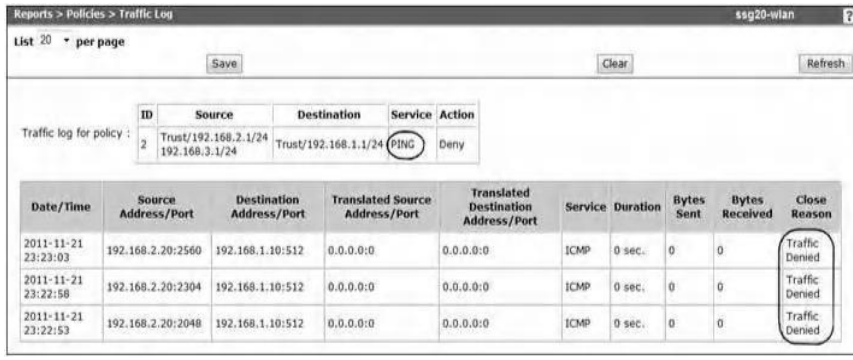
4. *Security Policy #4 (SP #4):* Узлам LAN#1 разрешен доступ к любому FTP-серверу в LAN#2. Однако узлам LAN#3 не разрешен доступ к любому FTP-серверу в LAN#2. На следующем снимке экрана показаны правила фильтрации, реализованные на устройстве Juniper Networks и соответствующие политике безопасности SP # 4:



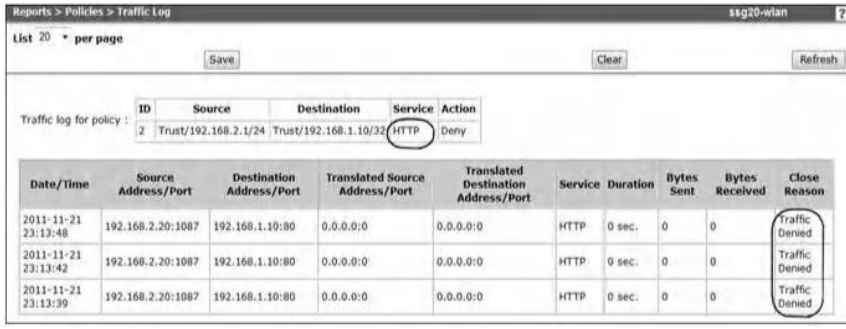
— Правило с ID 1 позволяет узлам LAN#1 (192.168.1.1/24) получать доступ к любому FTP-серверу в LAN#2 (192.168.2.1/24).
— Правило с ID 2 не позволяет узлам LAN#3 (192.168.3.1/24) получать доступ к любому FTP-серверу в LAN#2 (192.168.2.1/24).

7.2.5.4 Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks

Каждую политику безопасности легко протестировать, создав соответствующий трафик и проверив содержимое события журнала на устройстве Juniper Networks. Например, чтобы протестировать правила фильтрации, соответствующие политике безопасности SP # 1, мы предполагаем, что хост в LAN#2 пытается пропинговать хост в LAN#1. Однако журнал событий устройства Juniper Networks (следующий снимок экрана) показывает, что трафик Ping отклонен правилом фильтрации с ID 2.



Чтобы проверить правила фильтрации, соответствующие политике безопасности SP # 2, мы предполагаем, что хост в LAN#2 пытается получить доступ к веб-сайту (192.168.1.10) в LAN # 1. Однако журнал событий устройства Juniper Networks (следующий снимок экрана) показывает, что веб-трафик (HTTP) был отклонен правилом фильтрации с ID 2.



7.3 Лабораторная работа 7.2: Фильтрация нестандартных сервисов

7.3.1 Результат

Цель данного практического упражнения - научить студентов внедрять правила фильтрации брандмауэра для служб, работающих на нестандартных портах TCP и UDP.

7.3.2 Нестандартная фильтрация сервисов

Стандартные службы обычно работают на стандартных портах. Например, стандартные порты для служб HTTP и FTP - 80 и 21 соответственно. Клиентские программы, такие как веб-браузеры, обычно не требуют от пользователя указывать порты, на которых работают стандартные службы. Им требуется только IP-адрес (или доменное имя) целевого сервера, на котором размещается служба. Однако по определенной причине, например, по соображениям безопасности или недоступности стандартных портов, стандартные службы могут быть запущены на альтернативных портах. В таком случае клиентские программы требуют, чтобы пользователь предоставил альтернативный номер порта целевой службы. В противном случае клиентская программа не сможет подключиться к службе, поскольку она работает на неизвестном порту. Например, чтобы получить доступ к веб-серверу, работающему на порту 3000 и расположенном на хосте с IP-адресом 192.168.1.1, пользователю необходимо ввести URL-адрес http://192.168.1.1:3000 в веб-браузере.

Следовательно, правила фильтрации, которые фильтруют сервисы, работающие на стандартных портах, бесполезны для фильтрации сервисов, работающих на нестандартных портах. Например, если вы хотите запретить внешним хостам доступ к любому внутреннему нестандартному веб-серверу, работающему на порте 3000, то следующее правило фильтрации не будет работать для этой политики безопасности:

Правило	Направление	IP-адрес источника	IP-адрес получателя	Протокол	Порт источника	Порт назначения	Действие
R1	входящий	любой	любой	TCP	любой	80	отказ

Однако работает следующее правило фильтрации, поскольку оно запрещает хостам доступ к любому внутреннему нестандартному веб-серверу, работающему на порте 3000:

Правило	Направление	IP-адрес источника	IP-адрес получателя	Протокол	Порт источника	Порт назначения	Действие
R1	входящий	любой	любой	TCP	любой	3000	отказ

Брандмауэры обычно включают в себя предопределенные правила для фильтрации стандартных служб и не могут фильтровать нестандартные службы, если пользователь не предоставляет брандмауэр с портами TCP или UDP нестандартных служб. На практике это достигается созданием нового профиля службы для нестандартной службы и указанием соответствующего номера порта TCP или UDP.

7.3.3 Эксперимент

Этот эксперимент состоит из создания нестандартного сервиса и последующей реализации соответствующего правила фильтрации для фильтрации трафика, нацеленного на сервис, с использованием устройства Juniper Networks.

7.3.4 Архитектура сети

В этом эксперименте используется та же сетевая архитектура, которая описана в предыдущем практическом упражнении (лабораторная работа 7.1).

7.3.5 Шаги эксперимента

Эксперимент состоит из следующих этапов:

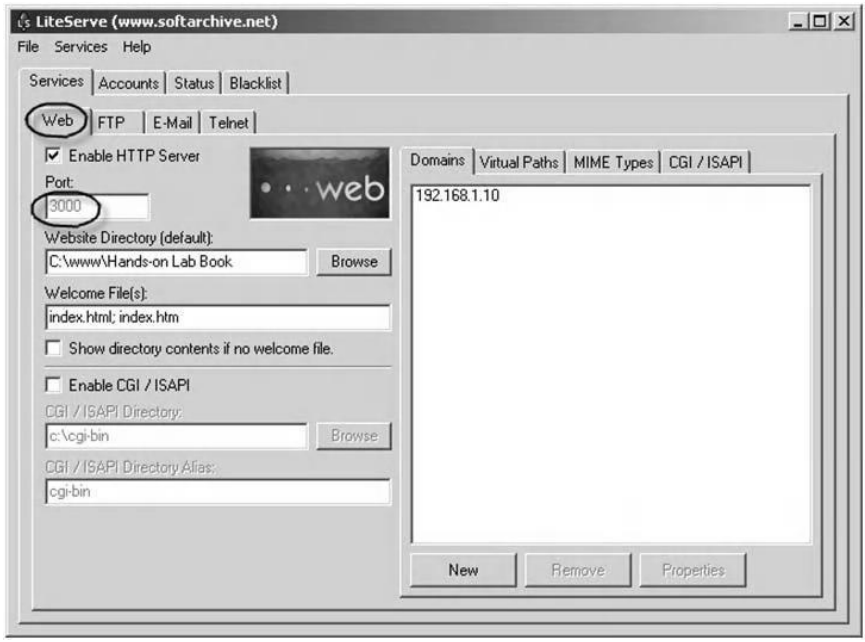
Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Настройте нестандартный веб-сервер, работающий на порте 3000.
Шаг 3: Создайте нестандартный сервисный профиль в устройстве Juniper Networks.
Шаг 4: Внедрить правила фильтрации для фильтрации трафика с нестандартной службой.
Шаг 5: Проверьте правила фильтрации и просмотрите результаты в журнале событий устройства Juniper Networks.

7.3.5.1 Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks

Шаг 1 аналогичен предыдущему практическому лабораторному заданию (Лаб 7.1) Шаг 1.

7.3.5.2 Шаг 2. Настройка нестандартного веб-сервера, работающего на порте 3000

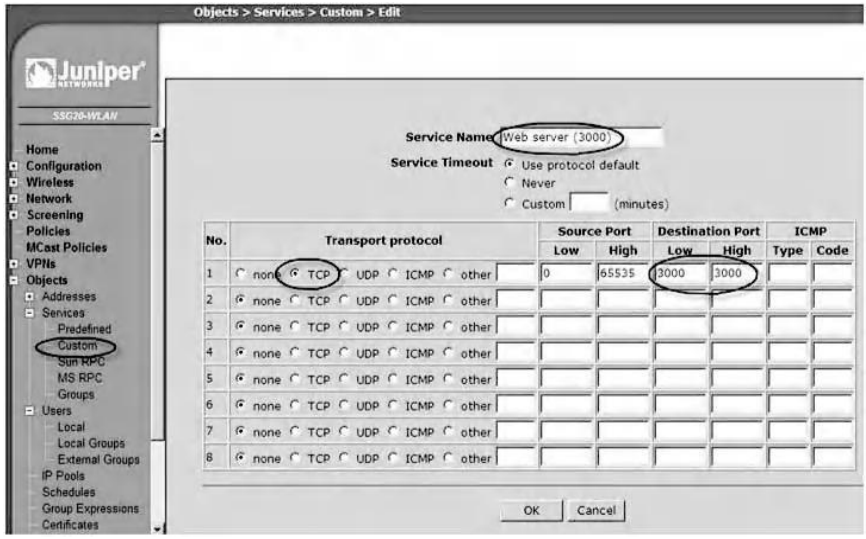
Инструмент LiterServe используется для настройки нестандартного веб-сервера. На следующем снимке экрана показано, что веб-сервер настроен на работу с нестандартным портом 3000.



7.3.5.3 Шаг 3. Создайте нестандартный сервисный профиль в устройстве Juniper Networks

В устройстве Juniper Networks, чтобы создать новый профиль для нестандартной службы, выполните следующие действия:

* Войдите в интерфейс WebUI устройства Juniper Networks.
* Выберите «Objects» => «Services» => «Custom», как показано на следующем снимке экрана.
* Выберите имя для нестандартной службы (например, Web server (3000)).
* Выберите «TCP» для транспортного протокола уровня 4.
* Поскольку нестандартная служба будет работать на порте 3000, установите значение порта назначения на 3000.
* Нажмите на кнопку «OK».



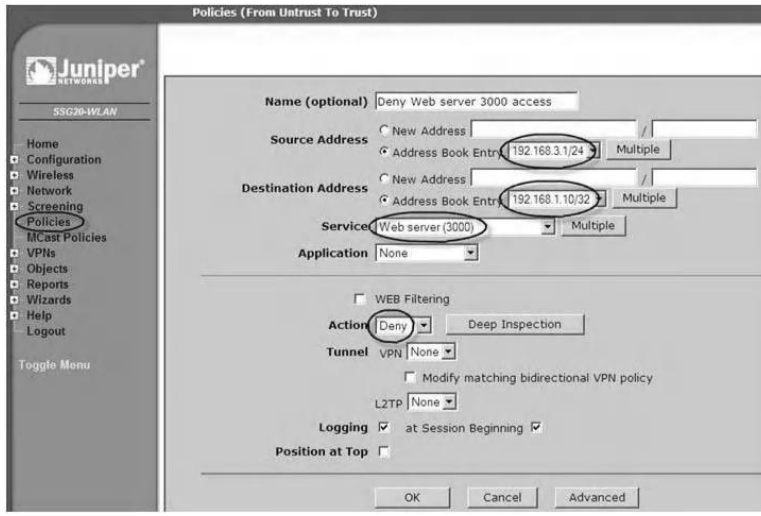
7.3.5.4 Шаг 4. Внедрение правил фильтрации для фильтрации трафика с нестандартной службой

As an example, we assume that we want to create a filtering rule for the following security policy:

* Узлам LAN#3 (192.168.3.1/24) не разрешен доступ к нестандартному веб-серверу (192.168.1.10) в LAN#1.

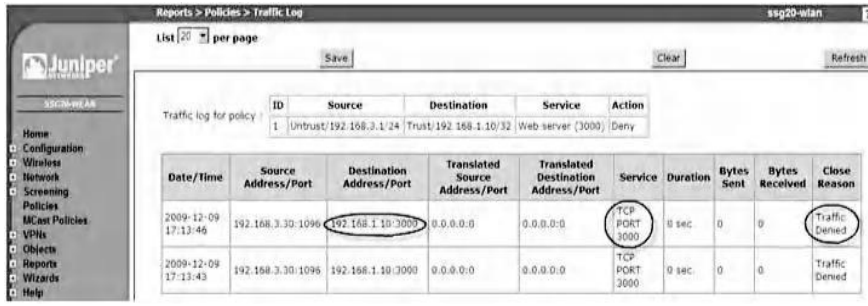
Следующие шаги и снимок экрана показывают, как создать правило фильтрации для вышеуказанной политики безопасности на устройстве Juniper Networks:

* Войдите в интерфейс WebUI устройства.
* Выберите «Policies»; затем укажите зоны сетей, связанные с политикой безопасности.
* Установите *Source address* (адрес источника) на 192.168.3.1/24.
* Установите *Destination address* (адрес назначения) на 192.168.1.10/32.
* Установите *Service* как “Web server (3000)”.
* Установите *Action* как *Deny* (запрещено).
* Выберите *Logging.*



7.3.5.5 Шаг 5. Протестируйте правила фильтрации и просмотрите результаты в журнале событий устройства Juniper Networks

Чтобы проверить указанное выше правило фильтрации, откройте веб-браузер на хосте в локальной сети № 3 и введите следующий URL-адрес: «http://192.168.1.10:3000». Затем откройте журнал событий, соответствующий приведенному выше правилу фильтрации, в устройстве Juniper Networks. На следующем снимке экрана показано, что устройство Juniper Networks отклонило трафик, поступающий с хоста 192.168.3.30 и направленный на порт 3000 на хосте 192.168.1.10.



7.4 Lab 7.3: Consistency and Efficiency Verification of Firewall Filtering Rules

7.4.1 Результат

Цель данного практического упражнения состоит в том, чтобы учащиеся узнали, как проверить последовательность и эффективность правил фильтрации противопожарных перегородок.

7.4.2 Согласованность и эффективность правил фильтрации

Межсетевые экраны играют важную роль в обеспечении политики контроля доступа в современных сетях. Политика безопасности периметра сети обычно описывается реализованными правилами фильтрации в брандмауэре. Создание таких правил считается сложной задачей из-за сложности сети (многие сегменты сети), разнообразия сетевого оборудования (персональный компьютер, серверы, маршрутизаторы и т. Д.) И большого количества уязвимостей в таких сетях. оборудование.

Однако брандмауэры эффективны только в том случае, если они правильно настроены, так что их правила фильтрации являются согласованными и реализуются в соответствии с намеченными политиками безопасности. К сожалению, из-за потенциально большого количества правил и их сложных взаимосвязей задача настройки брандмауэра, как известно, подвержена ошибкам. На практике брандмауэры часто неправильно конфигурируются, оставляя дыры в безопасности в системе защиты. Кроме того, поскольку большинство брандмауэров являются устройствами с индивидуальной настройкой, ручная генерация правил фильтрации брандмауэра, которая подвержена человеческим ошибкам, может привести к сбоям, которые могут быть преобразованы в аномалии, которые изменяют нормальную работу процесса фильтрации. Таким образом, слабые или плохо определенные правила фильтрации могут изменять ожидаемые и требуемые ответы брандмауэра и, как следствие, могут увеличивать возможность брандмауэра, позволяющего нежелательным пакетам входить или выходить из сети. Ошибки неправильной конфигурации приводят к

несоответствиям в брандмауэре. Пример критической несогласованности - это когда все пакеты, которые должны быть отклонены данным правилом фильтрации, принимаются некоторыми правилами предварительной передачи. Следовательно, предполагаемый эффект правила Deny отменяется предыдущими правилами Accept.

Последовательность и эффективность брандмауэра в значительной степени зависят от способности администратора разрабатывать четко определенные и согласованные правила фильтрации, а также от способности постоянно очищать и проверять правильность этих правил. Важно отметить, что в тех случаях, когда существуют десятки или сотни правил фильтрации, несоответствующие и неэффективные правила фильтрации с аномалиями могут быть непросто обнаружить.

Мы рассматриваем три типа несоответствий - *shadowing* (теневое копирование), *generalization* (обобщение) и *correlation* (корреляция) - и один недостаток - *redundancy* (избыточность). Ниже приведены определения этих несоответствий и неэффективности:

* *Shadowing:* Правило затеняется предшествующим правилом, если оно является подмножеством предыдущего правила, и эти два правила определяют разные действия. Таким образом, верхнее правило затеняет нижнее правило, когда верхнее правило соответствует всем пакетам, которые также соответствуют нижнему правилу, так что нижнее правило никогда не будет достигнуто межсетевым экраном. Брандмауэр выполняет поиск правил, начиная с верхней части списка правил фильтрации. Когда он находит соответствие для полученного трафика, он останавливает поиск правил в списке правил фильтрации. Затенение является критической ошибкой в политике безопасности, поскольку нижнее правило фильтрации никогда не вступает в силу. Верхнее правило называется правилом теневого копирования. Нижнее правило называется затененным правилом. Следующая таблица показывает пример правил теневого копирования. Чтобы исправить эту ситуацию, просто удалите одно из правил фильтрации или измените порядок двух правил фильтрации, поместив сначала более конкретное правило (затененное правило).

Правило	Направление	IP-адрес источника	IP-адрес получателя	Протокол	Порт источника	Порт получателя	Действие
R1	входящий	любой	любой	TCP	любой	80	разрешено
R2	входящий	192.168.3.30	любой	TCP	любой	80	запрещено

Shadowing - это критическое несоответствие, поскольку вполне вероятно, что правило с действием отказа запрещает некоторый известный вредоносный трафик. Однако из-за затенения этот трафик фактически не останавливается брандмауэром. Такие несоответствия могут легко возникнуть, когда межсетевой экран имеет распределенную реализацию и / или когда он управляется несколькими администраторами, что часто встречается в крупных организациях.

Generalization: Правило является обобщением предшествующего правила, если оно является надмножеством предыдущего правила, и эти два правила определяют разные действия. Следующая таблица показывает пример правил обобщения. Обобщение часто используется администраторами брандмауэра, чтобы сделать набор правил компактным. Тем не менее может случиться так, что некоторые обобщения не являются преднамеренными, и в этом случае полезно их обнаружить и позволить администратору решить, являются ли они вредными.

Rule	*Direction*	*Source IP address*	*Destination IP address*	*Protocol*	*Source Port*	*Destination Port*	*Action*
R1	Incoming	192.168.3.30	Any	TCP	Any	25	**Deny**
R2	Incoming	Any	Any	TCP	Any	25	**Allow**

Rule — Правило; Direction — Направление; Source IP address — адрес источника; Destination IP address — адрес получателя; Protocol — Протокол; Source Port — порт источника; Destination Port — порт получателя; Action — действие; Deny - запретить; Allow — разрешить; Incoming — входящий; Any -любой/

Correlation: Два правила коррелируют, если их пересечение не является пустым, они не связаны отношениями надмножества или подмножества, и они определяют различные действия. Пакеты, которые соответствуют пересечению, примут действие

предыдущего правила. Следующая таблица является примером правил корреляции.

Rule	Direction	Source IP address	Destination IP address	Protocol	Source Port	Destination Port	Action
R1	Incoming	192.168.3.30	Any	TCP	Any	Any	**Deny**
R2	Incoming	Any	Any	TCP	Any	25	**Allow**

Redundancy: Избыточное правило выполняет те же действия с теми же пакетами, что и другое правило, так что его удаление не повлияет на работу брандмауэра. Избыточное правило может не способствовать принятию решения о фильтрации, но оно увеличивает размер списка правил фильтрации и может увеличить время поиска и требования к пространству. Существует два типа избыточности: замаскированная избыточность и частично замаскированная избыточность. В случае замаскированной избыточности правило преемника не требуется. Однако в случае частично замаскированной избыточности предыдущее правило не требуется. В следующих двух таблицах приведены примеры замаскированной избыточности и частично замаскированной избыточности соответственно.

Rule	Direction	Source IP address	Destination IP address	Protocol	Source Port	Destination Port	Action
R1	Incoming	Any	Any	TCP	Any	80	**Deny**
R2	Incoming	192.168.3.30	Any	TCP	Any	80	**Deny**

Rule	Direction	Source IP address	Destination IP address	Protocol	Source Port	Destination Port	Action
R1	Incoming	Any	Any	TCP	Any	25	**Allow**
R2	Incoming	Any	Any	TCP	Any	Any	**Allow**

Обратите внимание, что не все эти несоответствия и избыточности одинаково важны. Обычно только теневое копирование считается ошибкой конфигурации, в то время как обобщение и корреляция,

на самом деле, часто используются администраторами брандмауэра, чтобы сделать набор правил компактным. Тем не менее может случиться так, что некоторые обобщения и корреляции не являются преднамеренными, и в этом случае полезно их обнаружить и позволить администратору решить, являются ли они вредными или нет. Избыточность также не считается серьезной ошибкой конфигурации, но избыточные правила явно бесполезны; следовательно, стоит их идентифицировать и удалить, а также повысить эффективность фильтрации.

7.4.3 Важность порядка правил фильтрации

Порядок правил фильтрации является решающим и важным фактором в процессе фильтрации. Фактически, любая реорганизация правил фильтрации может полностью изменить результаты процесса фильтрации. Пример, проиллюстрированный в следующих трех таблицах, ясно показывает, как переупорядочение правил фильтрации может изменить все ожидаемые результаты фильтрации для некоторых пакетов.

Первая таблица показывает два правила фильтрации и их порядок (AB). Брандмауэр использует два правила для фильтрации всех входящих и исходящих пакетов. Во второй таблице показаны результаты процесса фильтрации двух пакетов (Packet 1 и Packet 2). При фильтрации двух пакетов процесс фильтрации сохраняет порядок, указанный в первой таблице, которая называется «AB». Вторая таблица четко показывает, что результаты процесса фильтрации (*Real action*) аналогичны ожидаемым результатам (*Desired action*).). Однако третья таблица показывает, что когда порядок правил фильтрации меняется на «BA», процесс фильтрации генерирует реальное действие (*Deny*), которое не похоже на действие *Desired* (*Allow*).

Rules	*Source IP*	*Destination IP*	*Action*
A	10.*.*.*	172.16.6.*	ALLOW
B	10.1.99.*	172.16.*.*	DENY

Packet	*Source IP*	*Target IP*	*Desired action*	*Real action*
1	10.1.99.1	172.16.1.1	DENY	DENY(B)
2	10.1.99.1	172.16.6.1	ALLOW	ALLOW(A)

Packet	*Source IP*	*Target IP*	*Desired action*	*Real action*
1	10.1.99.1	172.16.1.1	DENY	DENY (B)
2	10.1.99.1	172.16.6.1	ALLOW	DENY (B)

Проверка большого брандмауэра (т.е. сотен правил фильтрации) на предмет несоответствий и неэффективности затруднена и подвержена ошибкам, когда это делается вручную и специальным образом.

Таким образом, для выполнения такой задачи требуются автоматизированные инструменты. Однако очень немногие межсетевые экраны объединяют возможности проверки несоответствия и неэффективности набора правил фильтрации. Например, устройство Juniper Networks предоставляет простую онлайн-команду, которая идентифицирует избыточные и скрытые правила. Существует также очень мало автономных программных инструментов, таких как FirePAC и Firesec *, которые могут проверить несоответствие и неэффективность установленных правил фильтрации. Средство FirePAC анализирует файлы конфигурации брандмауэра на наличие угроз безопасности, выявляет проблемные правила в конфигурации, определяет избыточные и неиспользуемые правила и суммирует сервисы, разрешенные правилами фильтрации. FirePAC также предоставляет администратору межсетевого экрана рекомендации по исправлению ситуации. Изменение порядка некоторых правил фильтрации или удаление некоторых из них являются примерами рекомендаций.

В этом случае ответственность за исправление ситуации лежит на администраторе. Firesec - это решение для анализа правил фильтрации брандмауэров. Он решает проблемы, присущие большим наборам правил, и помогает очищать и обновлять базу правил в соответствии с требованиями сети. Firesec анализирует базу правил, чтобы рассмотреть экземпляры двух или более правил, которые соответствуют одному и

* http://www.niiconsulting.com

тому же трафику и выполняют одно и то же действие, или два или более правил, которые соответствуют одному и тому же трафику, но выполняют противоположные действия, или правила, которые можно объединить путем создания групп объектов. Firesec предоставляет несколько функций, таких как удаление избыточных правил, группировка похожих правил и поиск уязвимых шаблонов правил.

В следующих двух экспериментах показаны шаги, используемые для проверки согласованности и эффективности правил фильтрации брандмауэра с использованием устройства Juniper Networks и инструмента FirePAC соответственно.

7.4.4 Эксперимент: устройство Juniper Networks

Этот эксперимент состоит из использования устройства Juniper Networks для проверки согласованности и эффективности набора правил фильтрации брандмауэра.

7.4.5 Архитектура сети

В этом эксперименте используется та же сетевая архитектура, которая описана в лаборатории фильтрации пакетов (лабораторная работа 7.1).

7.4.6 Шаги эксперимента

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Реализация противоречивых и неэффективных правил фильтрации.
Шаг 3: Проверьте последовательность и эффективность правил фильтрации.

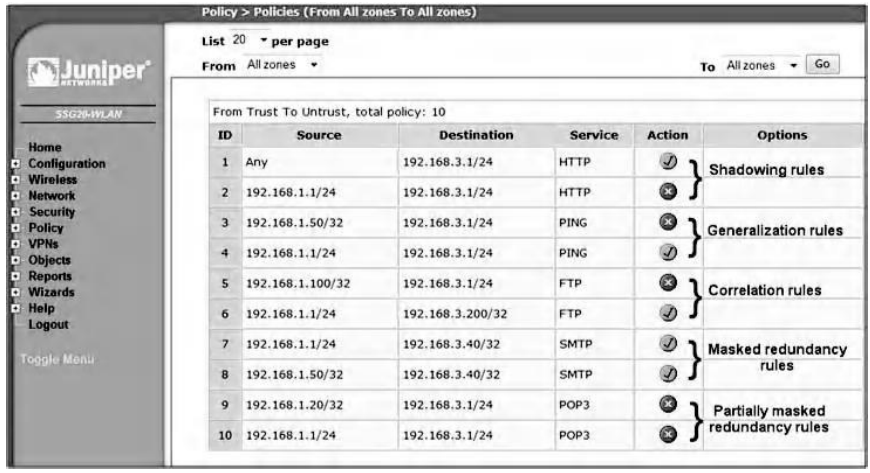
7.4.6.1 Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks

Шаг 1 аналогичен эксперименту лаборатории фильтрации пакетов (лаборатория 7.1).

7.4.6.2 Шаг 2. Внедрение непоследовательных и неэффективных правил фильтрации

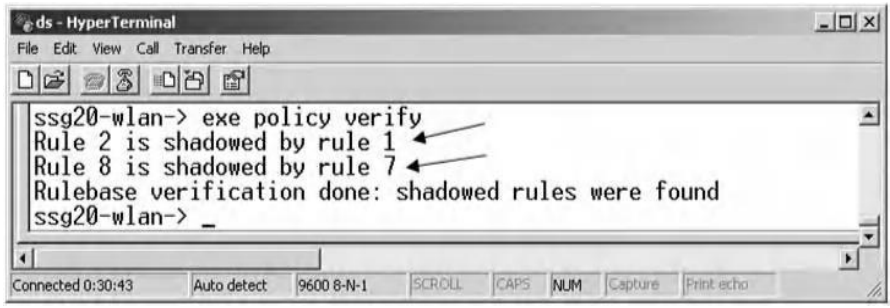
Войдите в интерфейс WebUI устройства Juniper Networks, выберите «Policy», а затем примените следующие непоследовательные и неэффективные правила фильтрации (см. Следующий снимок экрана):

Правила R1 и R2 являются правилами Shadowing.
Правила R3 и R4 являются правилами Generalization (обобщения).
Правила R5 и R6 являются правилами Correlation (корреляции).
Правила R7 и R8 являются правилами Masked redundancy (замаскированные правила избыточности).
Правила R9 и R10 являются правилами Partially masked redundancy (частично замаскированные правила избыточности).



7.4.6.3 Шаг 3. Проверка согласованности и эффективности правил фильтрации.

Устройство Juniper Networks предоставляет онлайн-команду, которая позволяет проверять согласованность и эффективность правил фильтрации. Для выполнения этой задачи подключите хост к устройству Juniper Networks с помощью консольного кабеля и Microsoft Hyper Terminal; затем введите онлайн команду «exec policy verify». На приведенном ниже снимке экрана показаны результаты выполнения этой онлайн-команды.



Устройство Juniper Networks смогло определить, что правило 2 затенено правилом 1, а правило 8 затенено правилом 7. Следовательно, устройство Juniper Networks классифицирует правила маскированной избыточности как скрытые правила. Однако устройству Juniper Networks не удалось обнаружить наличие правил обобщения (R3 и R4), правил корреляции (R5 и R6) и частично замаскированных правил избыточности (R9 и R10) среди списка правил фильтрации. Понятно, что в устройстве Juniper Networks отсутствует мощный механизм проверки согласованности и эффективности правил фильтрации.

7.4.7 Эксперимент: инструмент FirePAC

Этот эксперимент состоит из использования инструмента FirePAC для проверки согласованности и эффективности одного и того же набора правил фильтрации брандмауэра (раздел 7.4.6.2). Средство FirePAC требует в качестве входных данных файл конфигурации брандмауэра, который включает в себя набор правил фильтрации.

7.4.8 Шаги эксперимента

Эксперимент состоит из следующих этапов:

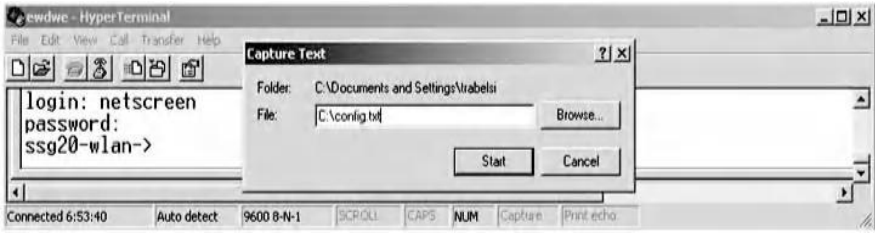
Шаг 1: Получите файл конфигурации брандмауэра.
Шаг 2: Проверьте последовательность и эффективность правил фильтрации.
Шаг 3: Анализ результатов инструмента FirePAC.

7.4.8.1 Шаг 1: Получить файл конфигурации брандмауэра

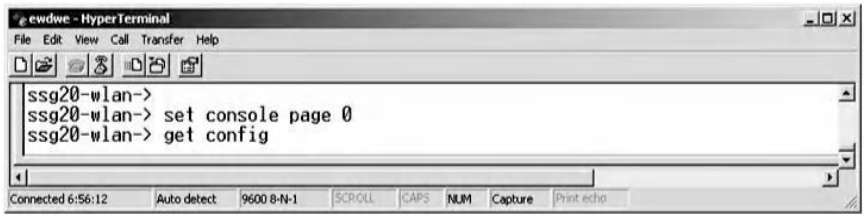
Ниже приведены шаги для сбора файла конфигурации устройства Juniper Networks:

* Подключитесь к устройству Juniper Networks с помощью консольного кабеля и инструмента Microsoft Hyper Terminal.
* В меню панели инструмента Microsoft Hyper Terminal выберите «Transfer», затем «Capture Text…» (снимок экрана ниже).

* Выберите папку и имя для файла конфигурации брандмауэра (скриншот ниже).



* Введите команду «set console page 0», затем команду «get config» (скриншот ниже).



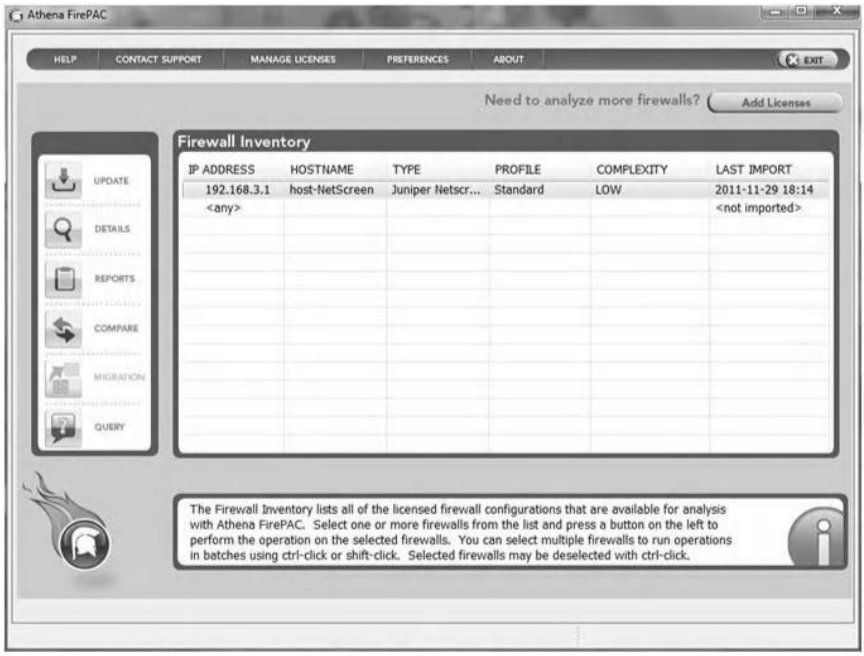
7.4.8.2 Шаг 2. Проверка согласованности и эффективности правил фильтрации.

Ниже приведены шаги, используемые для проверки согласованности и эффективности правил фильтрации, показанных в разделе 7.4.6.2, но с использованием инструмента FirePAC:

* Запустите инструмент FirePAC.

* Выберите «UPDATE» в графическом интерфейсе инструмента FirePAC (скриншот ниже) и следуйте инструкциям.

* Выберите «REPORT» в графическом интерфейсе инструмента FirePAC, чтобы сгенерировать отчет, показывающий любое непостоянство и / или неэффективность среди правил фильтрации (скриншот ниже).

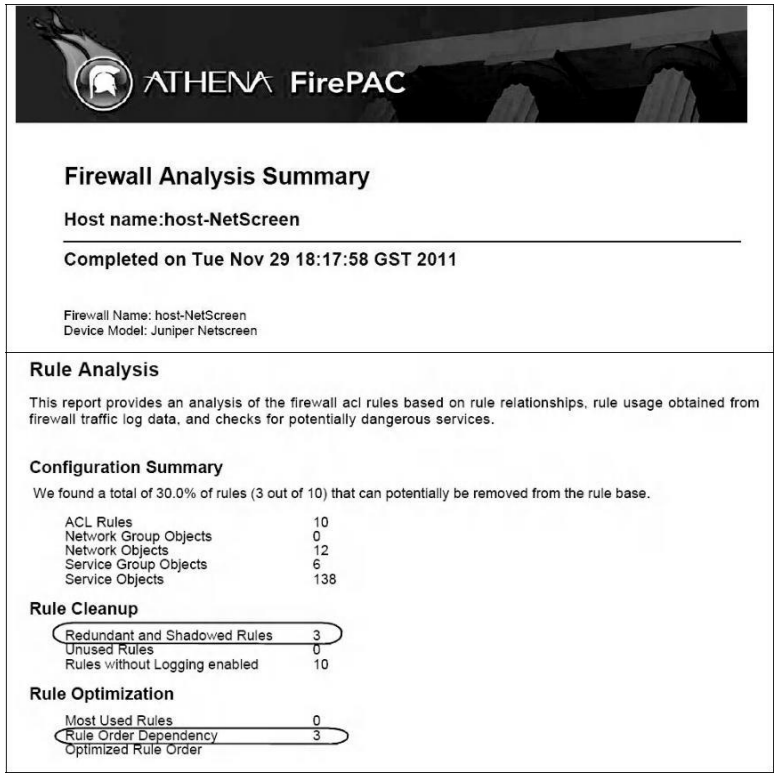


7.4.8.3 Шаг 3: Анализ результатов FirePAC Tool

Инструмент FirePAC создает отчеты, касающиеся результатов анализа набора правил фильтрации входных данных. На следующем экране

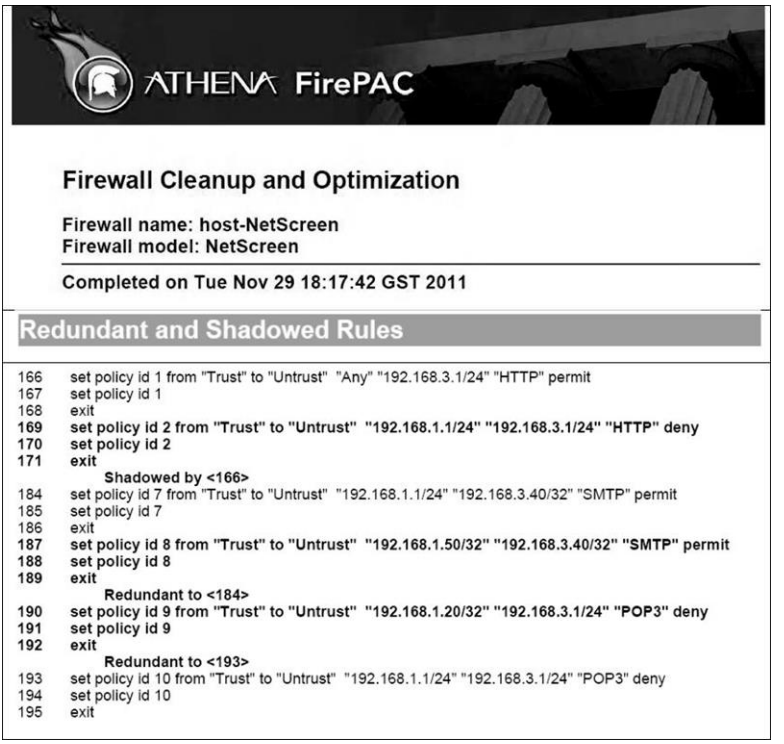
показана часть отчета, относящаяся к выявленным несоответствиям и недостаткам в правилах фильтрации ввода. Отчет показывает в основном, что:

* Были определены три избыточных и скрытых правила.
* Были определены три правила зависимости порядка.



На следующем экране представлен более подробный отчет об обнаружении инструмента FirePAC, то есть

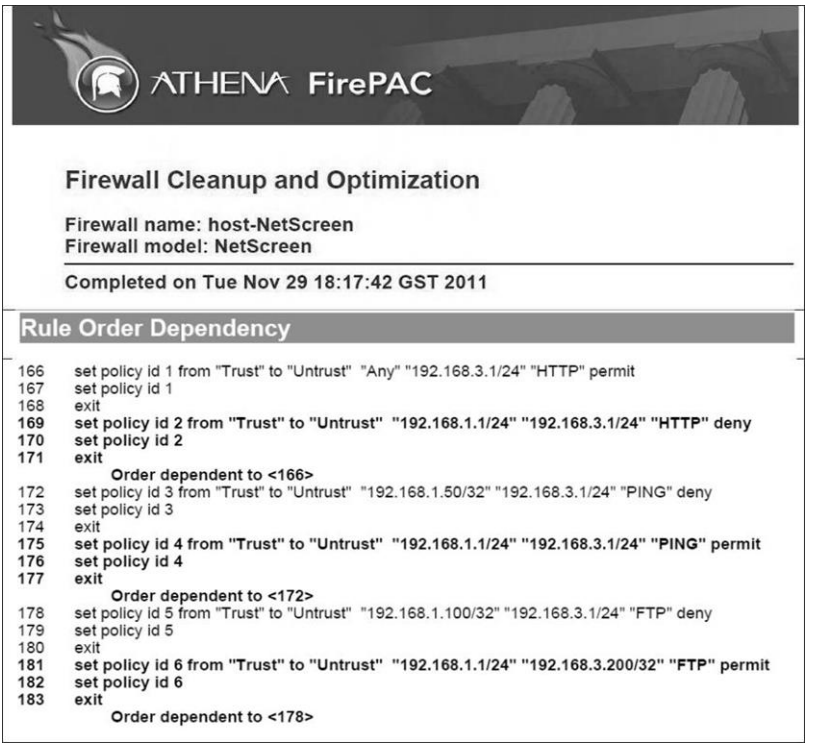
* Правило 2 (строка 169) затенено правилом 1 (строка 166).
* Правило 8 (строка 187) избыточно правилу 7 (строка 184).
* Правило 9 (строка 190) затенено правилом 10 (строка 193).



Среди списка правил, показанного на предыдущем экране, следующий экран показывает правила, зависящие от порядка:

Правило 2 (строка 169) зависит от порядка 1 (строка 166).
Правило 4 (строка 175) зависит от порядка 3 (строка 172).
Правило 6 (строка 181) зависит от порядка по правилу 5 (строка 178).

Правило, зависящее от порядка другого правила (эти правила, выделенные жирным шрифтом на следующем экране), имеет перекрывающиеся диапазоны соответствия с другим правилом и, следовательно, не может быть перемещено над источником зависимости без изменения поведения брандмауэра. Аналогично, правило, являющееся источником зависимости, не может быть перемещено ниже зависимого правила. Таким образом, зависимость порядка правил ограничивает движение правила.



Инструмент FirePAC обеспечивает более подробный анализ набора правил фильтрации и генерирует более подробные отчеты, чем устройство Juniper Networks. Например, устройство Juniper Networks не делало различий между избыточными и теневыми правилами и не могло идентифицировать частично замаскированные правила избыточности (правила 9 и 10). Кроме того, он не определил правила, зависящие от порядка, такие как правила 3 и 4. Кроме того, инструмент FirePAC предоставляет рекомендации по очистке и оптимизации входного набора правил фильтрации.

7.5 Лабораторная работа 7.4: фильтрация содержимого пакетов

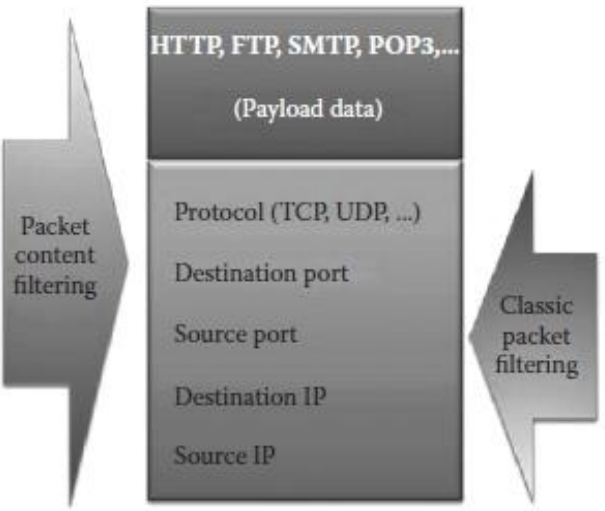
7.5.1 Результат

Цель этого практического упражнения - научить студентов выполнять фильтрацию содержимого пакетов.

7.5.2 Фильтрация содержимого пакета

Фильтрация содержимого пакета, также известная как Deep Packet Inspection (DPI), является формой фильтрации сетевых пакетов, которая проверяет часть данных (данные полезной нагрузки) и, возможно, также заголовки пакета, когда он проходит точку проверки, такую как межсетевой экран. Обычно при фильтрации содержимого пакета выполняется поиск несоответствия протокола, вирусов, спама, вторжений или предварительно определенных критериев, чтобы определить, может ли пакет пройти, или его нужно направить в другое место назначения, или для сбора статистической информации. Фильтрация содержимого пакетов обеспечивает расширенные функции управления сетью и обеспечения безопасности, а также позволяет осуществлять анализ данных в Интернете, прослушивание и цензуру.

В классической фильтрации пакетов проверяются поля протокола, порта назначения, исходного порта, IP-адреса назначения и исходного IP-адреса. Однако в процессе фильтрации содержимого пакета проверяются все поля пакета, в основном данные полезной нагрузки, чтобы определить, содержат ли они вредоносные подписи (обычно вредоносные строки); см. следующий рисунок. Процесс фильтрации содержимого пакета использует набор подписей, обычно создаваемых администратором брандмауэра. Например, вы можете запретить пользователям вашей сети получать электронные письма с определенного адреса электронной почты. Вы также можете заблокировать доступ к любой веб-странице, содержащей слово «Bomb» или URL-адрес, содержащий слово «sex».



Прикладной уровень в модели TCP / UDP содержит поля и данные полезной нагрузки сервисов. Примерами общих служб TCP являются Web (HTTP), электронная почта (SMTP / POP3) и FTP. Например, в электронном письме телу (тексту содержимого) всегда предшествуют строки заголовка, которые идентифицируют конкретную информацию о маршруте сообщения, включая отправителя, получателя, дату и тему. Некоторые заголовки являются обязательными, например заголовки FROM, TO и DATE. Другие являются необязательными, но очень часто используются, такие как SUBJECT и CC. Другие заголовки включают метки времени отправки и метки времени приема всех агентов пересылки почты, которые получили и отправили сообщение. Другими словами, каждый раз, когда сообщение передается от одного пользователя другому (т. Е. Когда оно отправляется или пересылается), сообщение / метка даты / времени отправляются почтовым агентом (MTA), компьютерной программой или программным агентом, который Тейт передачи сообщений электронной почты с одного компьютера на другой. Эта метка даты / времени, как FROM, TO и SUBJECT, становится одним из многих заголовков, которые предшествуют телу электронной почты.

На рисунке ниже показан пример полного заголовка электронной почты.

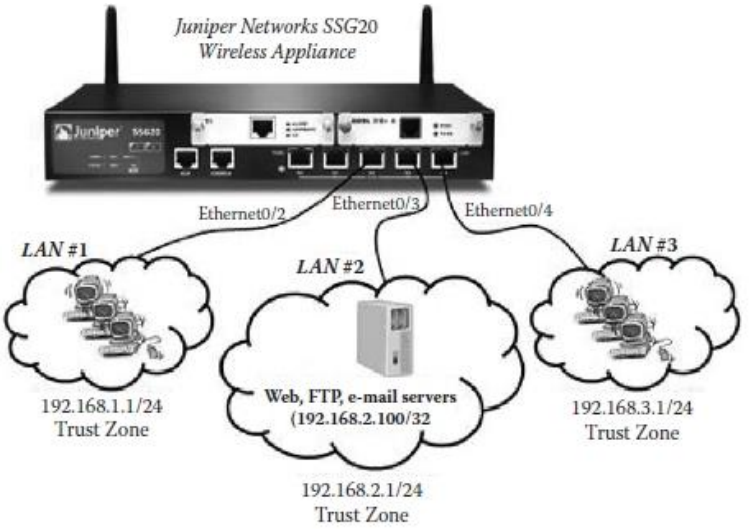
```
Return-Path: <naoufel.kraiem@topnet.tn>
Received: from topnetmail20.outgw.tn (topnetmail20.outgw.tn
[196.203.220.20])
        by fmc.antispam.uaeu.ac.ae id pAGFshNZ001352-
pAGFshNa001352; Wed, 16 Nov 2011 19:54:44 +0400
Received: from smtp23.topnet.tn (unknown [41.226.21.40])
        by topnetmail20.outgw.tn (Postfix) with SMTP id
3C0182570001
        for <trabelsi@uaeu.ac.ae>; Wed, 16 Nov 2011 16:54:43 +0100
(CET)
Received: (qmail 21172 invoked by uid 89); 16 Nov 2011 16:37:49 -0000
Received: from unknown (HELO smtp13.topnet.tn) (41.226.22.47)
 by smtp23.topnet.tn with SMTP; 16 Nov 2011 16:37:49 -0000
Received: (qmail 18962 invoked by uid 89); 16 Nov 2011 15:19:50 -0000
Received: from unknown (HELO as21.topnet.tn) (41.226.21.42)
 by smtp13.topnet.tn with SMTP; 16 Nov 2011 15:19:50 -0000
Received: from (unknown [41.226.21.46]) by as21.topnet.tn with smtp
        id 0766_51df_3b68a1f4_1069_11e1_b80d_00219b8e91e0;
        Wed, 16 Nov 2011 16:39:54 +0100
Received: (qmail 19194 invoked by uid 89); 16 Nov 2011 16:37:45 -0000
Received: from unknown (HELO ?192.168.1.2?) (197.0.49.239)
 by smtp22.topnet.tn with SMTP; 16 Nov 2011 16:37:47 -0000
Subject: Information
From: "Naoufel.kraiem" <naoufel.kraiem@topnet.tn>
Content-Type: text/plain; charset=utf-8
Message-Id: <03849B41-2BA5-4F81-B7D0-D96406885BC1@topnet.tn>
Date: Wed, 16 Nov 2011 11:27:53 +0100
To: "trabelsi@uaeu.ac.ae" <trabelsi@uaeu.ac.ae>
Content-Transfer-Encoding: quoted-printable
Mime-Version: 1.0 (iPad Mail 8J2)
X-Mailer: iPad Mail (8J2)
X-FEAS-DNSBL: zen.spamhaus.org / 197.0.49.239
X-FE-ORIG-ENV-FROM: naoufel.kraiem@topnet.tn
```

7.5.3 Эксперимент

Этот эксперимент состоит из использования устройства Juniper Networks для реализации фильтрации содержимого пакетов для различных политик безопасности.

7.5.4 Архитектура сети

На следующем рисунке показана сетевая архитектура, использованная в эксперименте. Три сети (LAN#1, LAN#2 и LAN#3) подключены к устройству Juniper Networks. Трафик, которым обмениваются три сети, проходит через устройство Juniper Networks, где он фильтруется набором правил фильтрации.



7.5.5 Шаги эксперимента

Эксперимент состоит из следующих этапов:

Шаг 1: Настройте сетевые интерфейсы на устройстве Juniper Networks.
Шаг 2: Настройте веб-серверы, FTP-серверы и почтовые серверы.
Шаг 3. Реализация правил фильтрации для политик безопасности.
Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks

7. 5.5.1 Шаг 1. Настройте сетевые интерфейсы на устройстве Juniper Networks

Шаг 1 аналогичен эксперименту фильтрации пакетов (лаборатория 7.1).

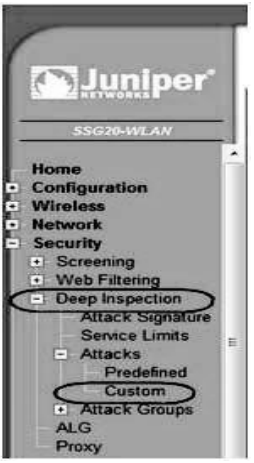
7.5.5.2 Шаг 2. Настройка веб-серверов, FTP-серверов и почтовых серверов

Инструмент LiterServe используется для настройки веб-серверов, FTP-серверов и почтовых серверов. Три сервера установлены на хосте с IP-адресом 192.168.2.100 в LAN#2, как показано выше.

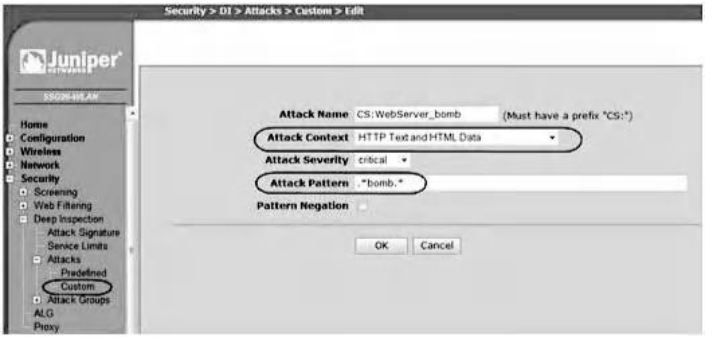
7. 5.5.3 Шаг 3. Реализация правил фильтрации для политик безопасности

Ниже приведены примеры политик безопасности и соответствующих им правил фильтрации, реализованных с использованием интерфейса WebUI устройства Juniper Networks. Политики безопасности занимаются проверкой данных полезной нагрузки в обмененном трафике Интернета, FTP и электронной почты. Соответствующие правила фильтрации реализуются с помощью возможности проверки содержимого пакетов (Deep Inspection) устройства Juniper Networks.

1. ***Security Policy #1 (SP#1):*** Узлам LAN#1 не разрешен доступ к любому веб-серверу в LAN#2 с веб-страницами, содержащими слово «бомба». Эта политика безопасности связана с проверкой полезных данных веб-трафика. В устройстве Juniper Networks для реализации соответствующих правил фильтрации для этой политики безопасности с использованием Deep Inspection сначала необходимо создать сигнатуру атаки следующим образом:
   — Войдите в интерфейс WebUI устройства.
   — Выберите «Security» -> «Deep Inspection» -> «Attacks» -> «custom», как показано на скриншоте ниже.

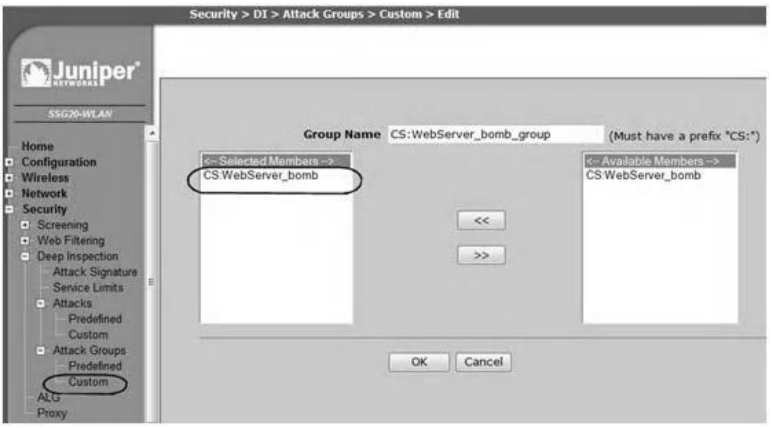


— Затем создайте подпись атаки, как показано на следующем снимке экрана. Подпись атаки указывает на часть данных полезной нагрузки, к которой будет применен Deep Inspection. Для политики безопасности (SP # 1) в сигнатуре атаки указано, что данные полезной нагрузки веб-трафика (HTTP) проверяются на предмет наличия в них слова «бомба». Контекст атаки (который является частью данных полезной нагрузки) это будет проверено) - это «HTTP Text и HTML Data», а паттерн атаки (. * bomb. *) - любая строка, содержащая слово «bomb».



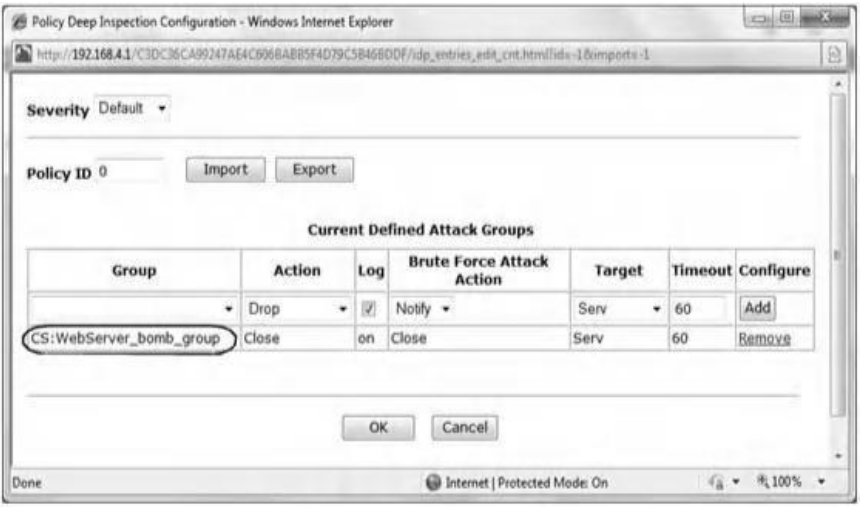
— Затем создайте группу атаки, как показано на снимке экрана ниже. Группа атак включает в себя все сигнатуры атак, которые процесс Deep Inspection будет использовать в данном правиле

фильтрации. Следовательно, группа атак может включать более одной сигнатуры атаки. В случае вышеуказанной политики безопасности (SP # 1) используется только одна сигнатура атаки.

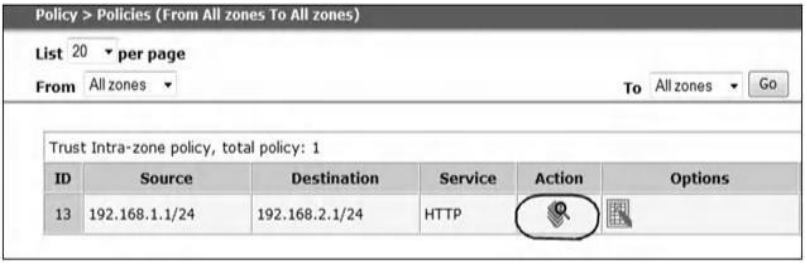


— Выберите «Policy» и затем определите хосты LAN#1 в качестве исходных хостов, а хосты LAN#2 в качестве хостов назначения.
— Нажмите «Deep Inspection», чтобы выбрать подходящую группу атак для этой политики безопасности, как показано на скриншоте ниже.

— Выберите соответствующую “Attack group” (группу атак), как показано ниже. .



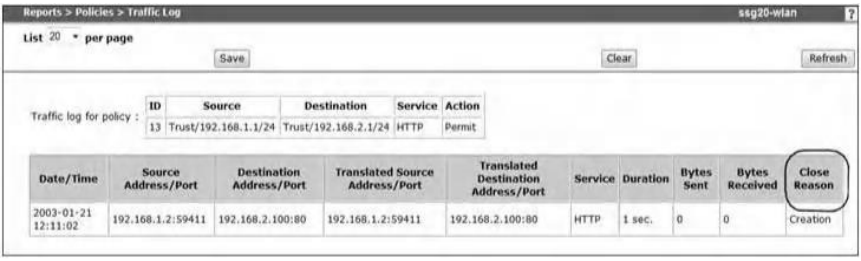
— На следующем снимке экрана показано правило фильтрации, реализованное на устройстве Juniper Networks для политики безопасности (SP # 1). Столбец “Action”(Действие) указывает, что правило использует Deep Inspection.



7. 5.5.4 Шаг 4. Протестируйте правила фильтрации и просмотрите результаты в файле журнала устройства Juniper Networks

Мы предполагаем, что веб-страницы веб-сервера, работающего на хосте (192.168.2.100), содержат слово “bomb”(бомба), как показано на следующем снимке экрана.

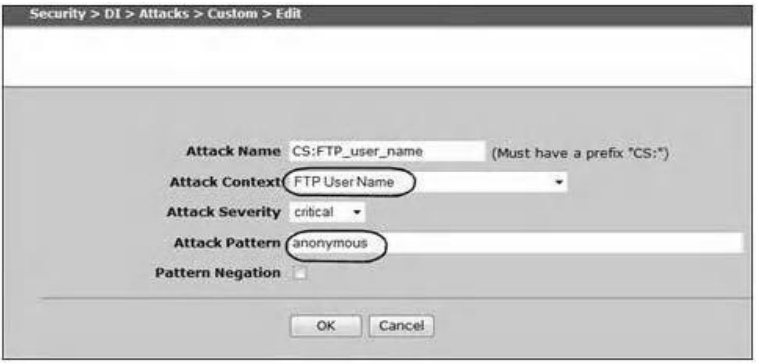
Мы также предполагаем, что хост (192.168.1.2) в LAN # 1 пытается получить доступ к веб-страницам веб-сервера (192.168.2.100). На следующем снимке экрана показан журнал событий для предыдущего правила фильтрации. На следующем снимке экрана показано, что хосту (192.168.1.2) было отказано в доступе к веб-серверу (192.168.2.100). Это связано с тем, что правило фильтрации использует Deep Inspection для запрета доступа к веб-страницам, содержащим слово «бомба».



2. ***Security Policy #2 (SP#2):*** Узлам LAN#3 не разрешен доступ к любому FTP-серверу в LAN#2, используя «anon-ymous» в качестве имени пользователя или «12345678» в качестве пароля. Эта политика безопасности связана с проверкой полезных данных трафика FTP.

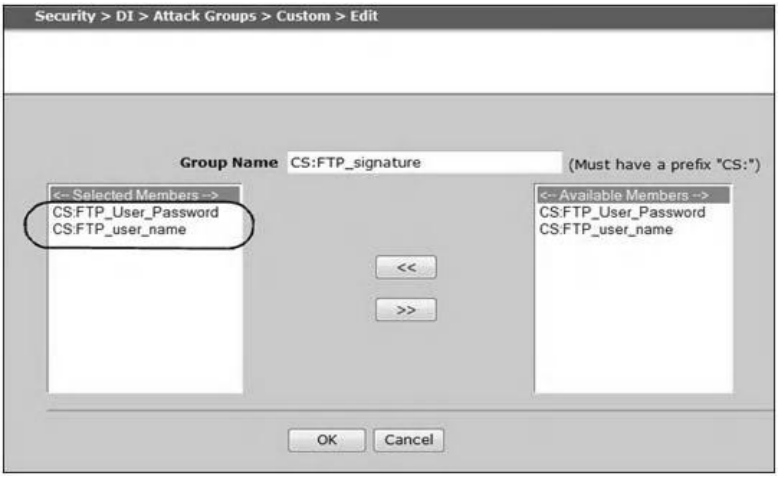
   — Для этой политики безопасности (SP # 2) требуются две сигнатуры атаки. Первая сигнатура атаки гласит, что данные

полезной нагрузки трафика FTP проверяются, чтобы проверить, содержит ли имя пользователя FTP слово «анонимный». Следовательно, контекст атаки - «Имя пользователя FTP», а шаблон атаки - «анонимный» (см. скриншот ниже).

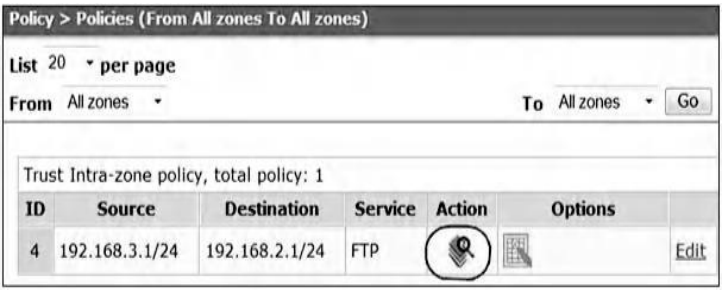


— Вторая сигнатура атаки гласит, что данные полезной нагрузки трафика FTP проверяются для проверки того, является ли пароль пользователя FTP «12345678.» Следовательно, контекст атаки - «FTP User Password», а шаблон атаки - «12345678» (снимок экрана ниже).

— Затем создается группа атак, включающая две сигнатуры атаки, как показано ниже.

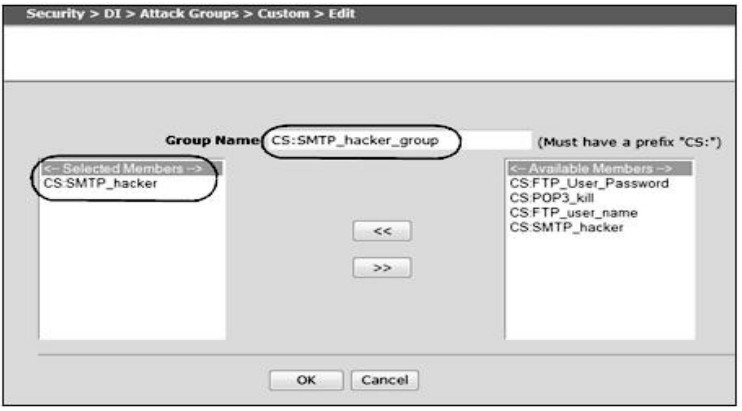


— На следующем снимке экрана показано правило фильтрации, реализованное в устройстве Juniper Networks для политики безопасности (SP # 2). Столбец “Action” указывает, что правило использует Deep Inspection:

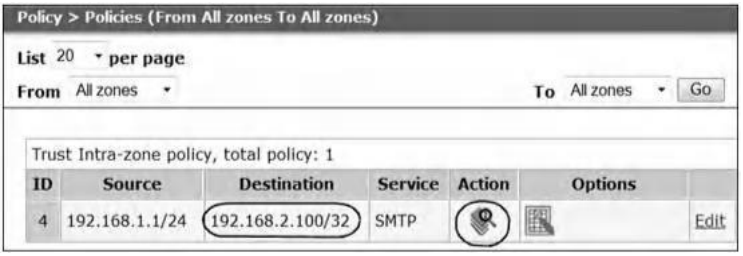


3. ***Security Policy #3 (SP#3):*** Хостам LAN#1 не разрешено отправлять электронные письма, содержащие строку «хакер» в любой строке заголовка электронного письма. Эта политика безопасности связана с проверкой данных полезной нагрузки трафика электронной почты (SMTP).
   — Для этой политики безопасности (SP # 3) требуется одна подпись атаки. В сигнатуре атаки указывается, что данные полезной нагрузки SMTP-трафика проверяются для проверки того, содержат ли строки заголовка электронной почты строку «хакер». Следовательно, контекст атаки - «SMTP Any Header Line», а шаблон атаки - “.*hacker.*” (Скриншот ниже)

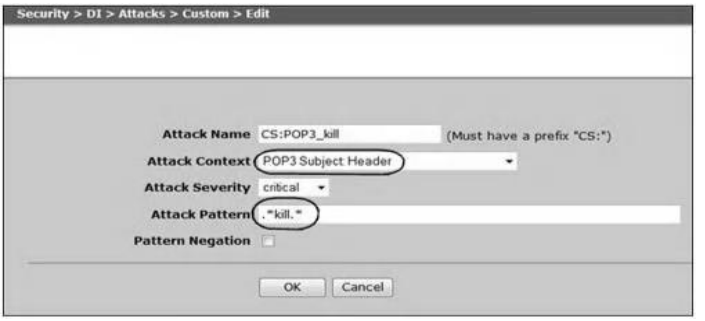
— Затем создается группа атак, включающая вышеуказанную сигнатуру атаки, как показано ниже.



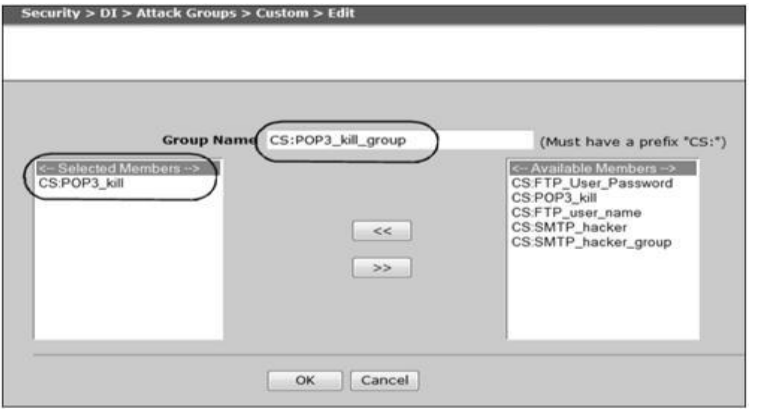
На следующем снимке экрана показано правило фильтрации, реализованное на устройстве Juniper Networks для политики безопасности (SP # 3). Столбец «Action» указывает, что правило использует Deep Inspection.



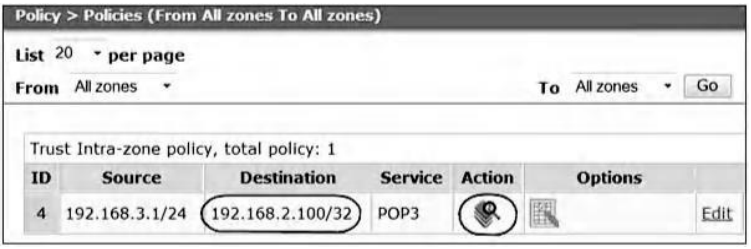
4. ***Security Policy #4 (SP #4):*** Хостам LAN#3 не разрешено получать электронные письма, содержащие строку «kill» в строке заголовка темы. Эта политика безопасности связана с проверкой данных полезной нагрузки трафика электронной почты (POP3).
   — Для этой политики безопасности (SP # 4) требуется одна подпись атаки. В сигнатуре атаки указано, что данные полезной нагрузки трафика POP3 проверяются, чтобы проверить, содержит ли строка заголовка темы электронной почты строку «kill». Следовательно, контекст атаки - “PO3 Subject Header”, а шаблон атаки - “.*kill.*” (Скриншот ниже).



   — Затем создается группа атак, включающая вышеуказанную сигнатуру атаки, как показано ниже.



   — На следующем снимке экрана показано правило фильтрации, реализованное в устройстве Juniper Networks для политики безопасности (SP#4). Столбец «Action» указывает, что правило использует Deep Inspection.



7.6 Лабораторная работа 7.5: фильтрация пакетов без сохранения состояния и против состояния

7.6.1 Результат

Цель данного практического упражнения состоит в том, чтобы студенты лучше анатомировали концепцию фильтрации пакетов без сохранения состояния и состояния с помощью примеров и экспериментов.

7.6.2 Проблемы безопасности с фильтрацией пакетов без сохранения состояния

Интернет-сервисы, основанные на технологии клиент / сервер (например, Интернет, FTP и электронная почта), являются двунаправленными. Очевидно, что правила фильтрации, относящиеся к двунаправленной услуге, должны позволять обоим направлениям трафика пересекать межсетевой экран. Комбинации пакетов, проходящих в обоих направлениях в службах TCP и UDP, называются сеансами TCP и UDP соответственно. У сеанса TCP или UDP есть клиент, который является компьютером, который инициирует сеанс и сервер, который является компьютером, на котором размещается служба. Например, следующее единственное правило фильтрации должно разрешать двунаправленный трафик между веб-клиентами с IP-адресами 192.168.1.1/24 и веб-серверами с IP-адресами 192.168.2.1/24 для прохождения через межсетевой экран:

Rule	*Direction*	*Source IP*	*Destination IP*	*Protocol*	*Source Port*	*Destination Port*	*Action*
R1	Client-to-Server	*192.168.1.1/24*	*192.168.2.1/24*	TCP	Any	HTTP (80)	Allow

Сеанс TCP или UDP характеризуется четырьмя атрибутами, а именно: IP-адрес клиента, IP-адрес сервера, порт клиента (известный как порт источника) и порт сервера (известный как порт назначения). Как правило, номер порта сервера позволяет определить характер предлагаемой услуги. Например, веб-сеанс и сеанс Telnet почти всегда находятся на портах TCP 80 и 23 соответственно. Однако клиентский порт обычно выбирается динамически во время выполнения операционной системой клиентского хоста, и он больше 1023. Следовательно, номер клиентского порта по существу непредсказуем. Важно отметить, что, поскольку порт клиента непредсказуем, брандмауэр должен позволять любому потоку сеанса с любым портом источника пересекать брандмауэр. Следовательно, при базовой фильтрации пакетов это привело бы к очень серьезной уязвимости в системе безопасности, которая позволяет вредоносным хостам заполнять целевые серверы нежелательным трафиком, который может вызвать атаку DoS (отказ в обслуживании). Чтобы лучше анатомировать эту проблему безопасности, мы предполагаем следующие две политики безопасности:

* Политика безопасности (SP # 1): Мы хотим, чтобы наши внутренние хосты с IP-адресами 192.168.1.1/24 имели доступ к любому внешнему веб-серверу (прослушивающему порт TCP 80) с IP-адресами 192.168.2.1/24.
* Политика безопасности (SP # 2): Кроме того, мы хотим запретить любому внешнему хосту (192.168.2.1/24) устанавливать соединения TCP с нашими внутренними хостами (192.168.1.1/24).

Первая политика безопасности (SP # 1) позволяет внутренним хостам устанавливать веб-соединения с любым внешним сервером. Однако вторая политика безопасности (SP # 2) не позволяет внешним хостам устанавливать TCP-соединения на внутренних серверах и, следовательно, защищает внутренние серверы от атак TCP SYN flood. Кроме того, в случае, если внутренние узлы заражены вирусами на основе программ с дистанционным управлением, такими как троянские кони, вторая политика безопасности предотвращает удаленное подключение злоумышленников к зараженному внутреннему узлу. Вирусы на основе программ с дистанционным управлением представляют собой очень серьезную угрозу, поскольку они позволяют злонамеренным пользователям полностью контролировать удаленные хосты-жертвы.

Пакеты, которыми обмениваются веб-клиенты и серверы, будут выглядеть так:

Клиент-серверные пакеты:

Source IP = 192.168.1.1/24, Destination IP = 192.168.2.1/24, Source port = Y, Destination port = 80,

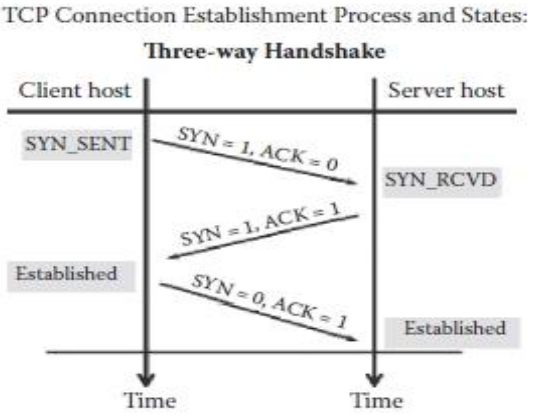
где 192.168.1.1/24 - возможные IP-адреса веб-клиентов, 192.168.2.1/24 - возможные IP-адреса веб-серверов, а Y - произвольный номер порта, выбранный веб-клиентом.

С другой стороны, возврат трафика с веб-серверов на веб-клиенты (сервер-клиент) меняет местами IP-адреса и номера портов и выглядит следующим образом:

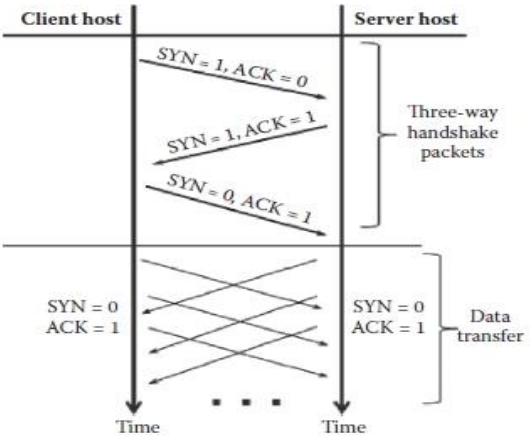
Source IP = 192.168.2.1/24, Destination IP = 192.168.1.1/24, Source port = 80, Destination port = Y.

Прежде чем писать соответствующие правила фильтрации для двух вышеуказанных политик безопасности, важно понять трехсторонний механизм квитирования, используемый для установления сеанса TCP. Фактически процесс установления TCP-соединения включает в себя следующие шаги (см. Следующий рисунок):

* Клиент отправляет сообщение SYN и переходит в состояние SYN_ SENT.
* Сервер отправляет сообщение, которое объединяет ACK для SYN клиента, содержит SYN сервера и переходит в состояние SYN_RCVD.
* Клиент отправляет ACK для SYN сервера и переходит в состояние ESTABLISHED.
* После получения сообщения ACK сервер переходит в состояние ESTABLISHED.



После установления TCP-соединения все обмениваемые пакеты будут иметь установленный флаг ACK и неустановленный флаг SYN (рисунок ниже).



Поэтому, если мы рассмотрим только флаги SYN и ACK, в TCP-соединении будут передаваться только четыре типа пакетов TCP:

* Пакет клиент-сервер: TCP-пакет с установленным флагом SYN и не установленным флагом ACK.
* Пакет сервер-клиент: TCP-пакет с установленными флагами SYN и ACK.

* Пакет клиент-сервер: TCP-пакет с установленным флагом SYN и установленным ACK.
* Пакет сервер-клиент: TCP-пакет с установленным флагом SYN и установленным флагом ACK.

Следовательно, в соединении TCP, чтобы разрешить двунаправленный трафик обслуживания через межсетевой экран, межсетевой экран должен разрешать прохождение вышеупомянутых четырех типов пакетов TCP.

Например, правила фильтрации для двух вышеуказанных политик безопасности SP#1 и SP#2, соответственно

Rule	Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
R1	Client-to-Server	192.168.1.1/24	192.168.2.1/24	TCP	Y	80	1	0	Allow
R2	Server-to-Client	192.168.2.1/24	192.168.1.1/24	TCP	80	Y	1	1	Allow
R3	Client-to-Server	192.168.1.1/24	192.168.2.1/24	TCP	Y	80	0	1	Allow
R4	Server-to-Client	192.168.2.1/24	192.168.1.1/24	TCP	80	Y	0	1	Allow

Rule	Direction	Source IP	Destination IP	Protocol	Source port	Destination port	SYN	ACK	Action
R5	Client-to-Server	192.168.2.1/24	192.168.1.1/24	TCP	Y	Z	1	0	Deny

К сожалению, злоумышленник может использовать правила 2 и 4 для проведения DoS-атак, поскольку эти два правила соответствуют пакетам на основе их исходных портов. Помните, что порт источника находится под контролем отправителя пакета. Злоумышленник на любом хосте с поддельным IP-адресом 192.168.2.1/24 может создать поддельные пакеты с портом источника 80, назначить любой хост с IP-адресом 192.168.1.1/24 и порт назначения по своему выбору. Поддельные пакеты, созданные таким образом, будут проходить через брандмауэр, потому что они соответствуют либо правилу 2, если установлены их флаги SYN и ACK, либо правилу 4, если их флаг SYN не установлен и их флаг ACK установлен. Например, ниже показан пример пакета TCP, который

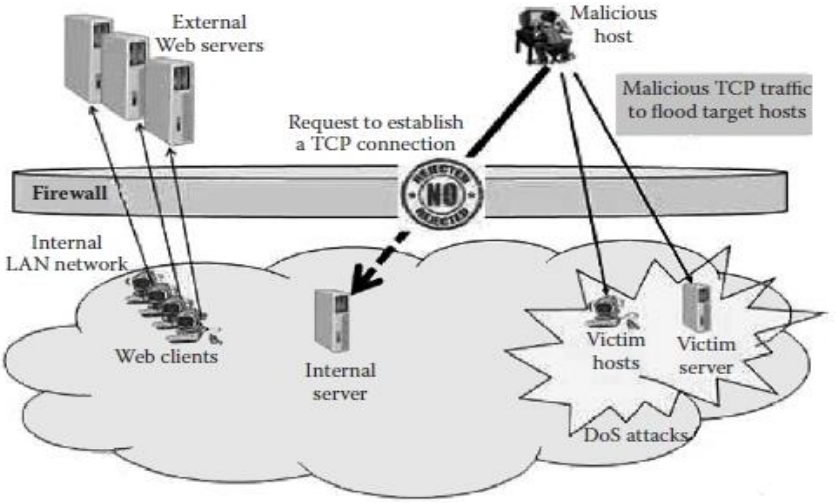
отклоняется брандмауэром, так как пакет пытается установить веб-соединение с внутренним хостом. Пакет отклоняется по правилу 5 приведенного выше списка правил фильтрации (предыдущий снимок экрана).

Packet	*Source IP*	*Destination IP*	*Protocol*	*Source port*	*Destination port*	*SYN*	*ACK*
Packet #1	*192.168.2.20*	*192.168.1.10*	TCP	6000	80	1	0

Однако ниже приведен пример вредоносного TCP-пакета, который разрешен брандмауэром для прохождения. Вредоносный пакет TCP делает вид, что соединение TCP с исходным портом 9000 уже установлено, поскольку его флаг SYN не установлен и установлен флаг ACK.

Packet	*Source IP*	*Destination IP*	*Protocol*	*Source port*	*Destination port*	*SYN*	*ACK*
Packet #2	192.168.2.20	192.168.1.10	TCP	80	9000	0	1

На основании приведенного выше списка правил фильтрации брандмауэр разрешит прохождение вредоносного пакета. Следовательно, заполнение целевого внутреннего хоста такими вредоносными TCP-пакетами может создать ситуацию атаки DoS на целевом хосте (см. рисунок ниже).



Таким образом, этот простой пример демонстрирует ограничения базовой фильтрации пакетов, хотя правила фильтрации для политики безопасности SP#1 и SP#2, приведенные выше, позволяют внутренним хостам устанавливать TCP-соединения с внешними веб-серверами и не позволяют внешним хостам устанавливать TCP соединения с внутренними серверами. Однако основной недостаток правил фильтрации заключается в том, что они позволяют злонамеренным пользователям наводнять внутренние хосты вредоносными TCP-пакетами, что может создать ситуацию атаки DoS на внутренних хостах, как показано на предыдущем рисунке.

В базовой фильтрации пакетов эта атака DoS может происходить легко, потому что брандмауэры не используют механизмы, которые позволяют решить, принадлежит ли данный пакет TCP к уже установленному сеансу. Фактически, брандмауэры не отслеживают состояние текущих сеансов TCP-соединений и не запоминают, какой номер порта источника выбран клиентами сеансов.

7.6.3 Контроль состояния фильтрации пакетов TCP

Чтобы устранить вышеуказанную проблему безопасности при базовой фильтрации пакетов, межсетевые экраны отслеживают установленные соединения TCP. На практике межсетевые экраны сохраняют запись в кеше для каждого открытого TCP-соединения.

Запись TCP-соединения включает в себя IP-адреса клиента и сервера, а также номера портов клиента и сервера. Информация о номере порта клиента не была полностью известна, когда администратор брандмауэра написал правила. Однако при настройке соединения оба номера портов известны, так как они перечислены в заголовке TCP пакета. Все пакеты, которые принадлежат существующему TCP-соединению, в обоих направлениях разрешено пересекать межсетевой экран. Этот тип межсетевого экрана называется межсетевым экраном с контролем состояния.

Записи в кэше состояний установленных TCP-соединений создаются с использованием простого механизма. То есть, когда первый пакет (пакет SYN) нового TCP-соединения достигает брандмауэра, он сопоставляет его с набором правил фильтрации. Если существует правило фильтрации, разрешающее передачу пакета, брандмауэр вставляет новую запись в кеш

а состояние соединения TCP устанавливается в состояние SYN_RCVD. Как только два других оставшихся пакета процесса трехстороннего рукопожатия получены, состояние соединения TCP переходит в состояние ESTABLISHED. Поэтому первый пакет (пакет SYN) TCP-соединения эффективно открывает дыру в брандмауэре, а механизм кэширования позволяет обратному трафику проходить через эту дыру.

После установления TCP-соединения решение о том, разрешать или нет последующие TCP-пакеты, основывается на содержимом кэша состояний. То есть, когда последующий пакет TCP с установленным флагом SYN и установленным флагом ACK достигает межсетевого экрана, межсетевой экран проверяет, существует ли запись для соединения TCP, к которому он принадлежит, уже существует в кэше. Если соединение указано в кеше, пакет сразу пропускается. Если такого соединения не существует, пакет отклоняется. Ниже приведен пример пакета SYN нового соединения TCP:

Packet	*Source IP*	*Destination IP*	*Protocol*	*Source port*	*Destination port*	*SYN*	*ACK*
Packet #1	192.168.1.5	192.168.2.10	TCP	1200	80	1	0

Когда вышеупомянутый первый пакет (Пакет#1) виден межсетевым экраном, межсетевой экран сопоставляет его с набором правил фильтрации. Поскольку правило 1 (как показано на скриншоте выше для правил фильтрации брандмауэра для политики безопасности SP # 1) разрешает передачу пакета через брандмауэр, брандмауэр вставляет новую запись в кэш состояния, а состояние соединения TCP - SYN_RCVD (см. ниже).

TCP connection	*Client IP*	*Server IP*	*Client port*	*Server port*	*Connection State*
Connection #1	192.168.1.5	192.168.2.10	1200	80	SYN_RCVD

После завершения процесса трехстороннего рукопожатия состояние соединения TCP переходит в состояние ESTABLISHED (как показано ниже).

TCP connection	Client IP	Server IP	Client port	Server port	Connection State
Connection #1	192.168.1.5	192.168.2.10	1200	80	ESTABLISHED

Когда соединение TCP прерывается, брандмауэр удаляет запись в кэше, тем самым блокируя соединение. Как правило, брандмауэр также имеет значение времени ожидания; если соединение TCP становится неактивным слишком долго, брандмауэр удаляет запись из кэша и блокирует соединение.

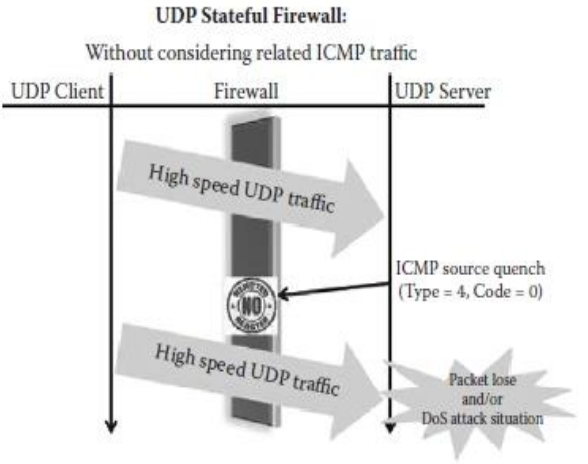
7.6.4 Контроль состояния фильтрации пакетов UDP

Отслеживание состояния сеанса UDP является сложным процессом, поскольку UDP является транспортным протоколом без установления соединения и, в отличие от TCP, не имеет порядковых номеров или флагов (таких как шесть флагов TCP: SYN, ACK, FIN, PSH, URG и FIN). Единственный элемент, который может использовать процесс отслеживания, - это IP-адреса и номера портов клиента и сервера, участвующих в сеансе UDP.

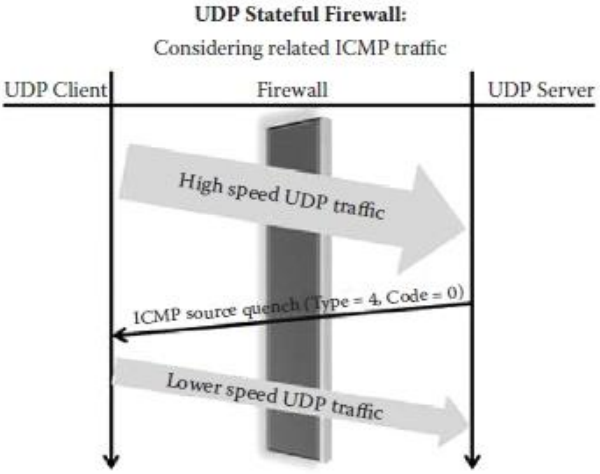
Кроме того, UDP не имеет механизма, который объявляет конец сессии. Следовательно, записи таблицы состояний сеанса UDP должны быть очищены после достижения предопределенного значения времени ожидания. В противном случае злонамеренный пользователь может использовать это ограничение в протоколе UDP для заполнения таблицы состояний сеанса UDP поддельными сеансами, что приводит к ситуации атаки DoS.

С другой стороны, UDP полностью полагается на ICMP в качестве обработчика ошибок. Следовательно, ICMP является важной частью сеанса UDP, который необходимо учитывать при отслеживании его общего состояния. Например, в сеансе UDP клиент или серверный хост может не иметь достаточно места в буфере для обработки принимаемых пакетов. Следовательно, хост может не справиться со скоростью, с которой он принимает пакеты. В такой ситуации принимающий хост может отправить сообщение об отказе источника ICMP (Тип = 4, Код = 0), которое запрашивает, чтобы хост-отправитель уменьшил скорость отправляемых пакетов. Однако, если брандмауэр блокирует исходное

сообщение ICMP об отказе, поскольку оно не является частью обычного сеанса UDP, узел, который отправляет пакеты слишком быстро, не знает, что возникла проблема, и продолжает отправлять с той же скоростью, что приводит к потере пакетов или DoS-атаке на принимающем хосте (следующий рисунок).



Поэтому межсетевой экран с отслеживанием состояния, который отслеживает состояние сеанса UDP, должен учитывать такой связанный трафик ICMP при принятии решения о том, какой трафик следует возвращать защищенным хостам (см. Рисунок ниже).



7.6.5 Контроль состояния фильтрации пакетов ICMP

ICMP - это протокол сообщений об ошибках и диагностики, который считается обязательной частью любой реализации IP. Существует два типа ICMP-пакетов: отчеты об ошибках и пакеты управления. Пакеты сообщений об ошибках ICMP используются для возврата сообщений об ошибках и включают одностороннюю связь. Они всегда сообщаются на исходный IP-адрес исходного пакета. Однако управляющие пакеты ICMP используются хостами для отправки сообщений запроса и получения соответствующих ответных сообщений. Следовательно, сообщения об ошибках ICMP включают двустороннюю связь или сообщения типа запрос / ответ. ICMP, как и UDP, не является протоколом с отслеживанием состояния. Однако, как и UDP, он также имеет атрибуты, которые позволяют отслеживать его соединения. Атрибутами ICMP обычно являются поля Тип, Код, Идентификатор и Порядковый номер в заголовке ICMP.

Примерами сообщений об ошибках ICMP являются сообщение об ошибке источника ICMP (описанное в предыдущем разделе) и сообщение об превышении времени ICMP. В сообщении, превышающем время ICMP, в поле Тип должно быть установлено значение 11. Поле Код, в котором указана причина сообщения о превышении времени, включает в себя следующее:

Код	Описание
0	Время жизни превышено в пути
1	Превышено время сборки фрагмента

Шлюзом генерируется сообщение об превышении времени ICMP с неустановленным полем кода, которое информирует источник отброшенного пакета о том, что поле времени жизни достигло нуля. То есть каждая машина (например, промежуточный маршрутизатор), которая пересылает IP-дейтаграмму, должна уменьшать поле времени жизни (TTL) заголовка IP на единицу. Если TTL достигает 0, в источник в источник графика данных отправляется ICMP-сообщение о

превышении времени жизни. Сообщение ICMP о превышении времени с установленным полем Код отправляется хостом, если ему не удается повторно собрать фрагментированную грамму данных в течение своего ограничения по времени.

Примером приложения, основанного на сообщениях типа запрос / ответ ICMP, является Ping. Он был создан для проверки того, существует ли конкретный компьютер в сети или в Интернете и подключен ли он. Ping - это программа, которая отправляет серию ICMP-эхо-запросов (Тип = 8, Код = 0) по сети или Интернету на конкретный компьютер для генерации эхо-ответов ICMP (Тип = 0, Код = 0) с этого компьютера.

Отслеживание ICMP-трафика, который включает одностороннюю коммуникацию, является сложным, поскольку сообщения об ошибках ICMP ускоряются запросами других протоколов (TCP, UDP). Из-за этой многопротокольной проблемы преобразование сообщений ICMP в состояние существующего сеанса UDP или TCP может привести к путанице и затруднить управление.

Однако сеансы ICMP, которые включают двустороннюю связь, менее сложно отслеживать, поскольку для каждого ответного сообщения ICMP должно быть сообщение запроса ICMP, которое было отправлено ранее. То есть сеанс ICMP отслеживается на основе адресов источника / назначения, типа, кода, идентификатора и порядкового номера сообщений запроса и ответа. В сеансе ICMP поля «Идентификатор», «Номер последовательности» и «Данные» должны быть возвращены отправителю без изменений. Идентификатор и порядковый номер могут использоваться отправителем эхо-запроса, чтобы помочь в сопоставлении ответов с эхо-запросами. Идентификатор может использоваться как порт в TCP или UDP для идентификации сеанса, а номер последовательности может увеличиваться при каждом отправленном эхо-запросе. Эхо-узел возвращает эти же значения в эхо-ответ.

Этот метод отслеживания является единственным способом, которым ICMP может войти в таблицу состояний.

Например, после получения пакета эхо-запроса ICMP, показанного ниже,

Packet	*Source IP*	*Destination IP*	*Type*	*Code*	*Identifier*	*Sequence number*
Packet #1	192.168.1.5	192.168.2.10	8	0	200	1

межсетевой экран с сохранением состояния создает новую запись в кеше своего сеанса ICMP, как показано ниже.

ICMP session	*Source IP*	*Destination IP*	*Type*	*Code*	*Identifier*	*Sequence number*	*Session State*
Session #1	192.168.1.5	192.168.2.10	1200	80	**200**	**1**	**Request**

Поэтому последующий пакет эхо-ответа ICMP будет принят межсетевым экраном с сохранением состояния, поскольку он включает в себя те же значения атрибутов, что и пакет эхо-запроса ICMP.

Packet	*Source IP*	*Destination IP*	*Type*	*Code*	*Identifier*	*Sequence number*
Packet #2	192.168.2.10	192.168.1.5	0	0	**200**	**1**

Однако следующий поддельный пакет эхо-ответа ICMP отклоняется, так как не было никакого сообщения запроса эхо-запроса ICMP, включающего те же значения атрибута.

Packet	*Source IP*	*Destination IP*	*Type*	*Code*	*Identifier*	*Sequence number*
Packet #3	192.168.2.10	192.168.1.5	0	0	**300**	**1**

Другая проблема с ICMP заключается в том, что, как и UDP, он не требует соединения; следовательно, он должен основывать сохранение записи таблицы состояний на заранее определенном тайм-ауте, поскольку ICMP также не имеет специального механизма для завершения своих сеансов связи.

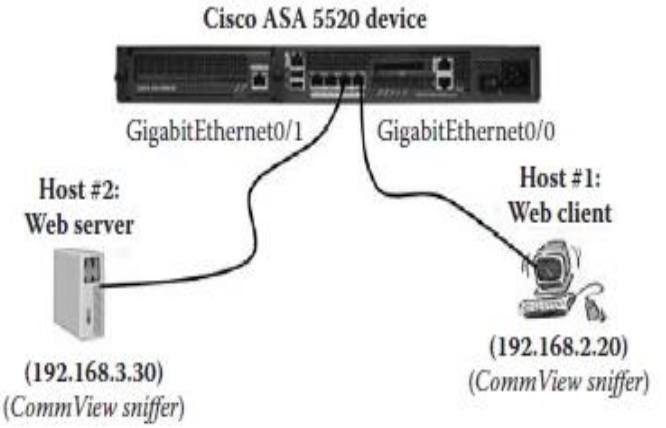
7.6.6 Эксперимент

Этот эксперимент состоит из описания ряда шагов, позволяющих пользователям проверить, предлагает ли устройство адаптивной защиты Cisco ASA 5520 (брандмауэр) фильтрацию пакетов TCP и ICMP с сохранением состояния или без учета состояния. Те же шаги можно использовать для проверки любого другого брандмауэра.

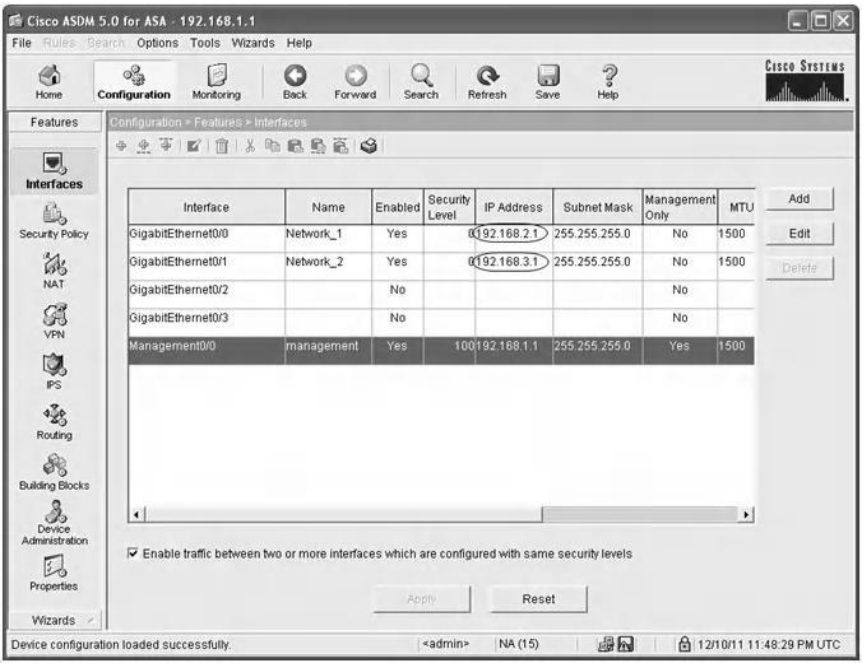
7.6.7 Архитектура сети

На следующем рисунке показана сетевая архитектура, использованная в эксперименте. Мы предполагаем, что хост (хост#1) с IP-адресом 192.168.2.20 и хост (хост#2) с IP-адресом 192.168.3.30 подключены к интерфейсам GigabitEthernet0/0 и GigabitEthernet0/1 Cisco ASA 5520, соответственно. Мы также предполагаем, что

* Host #1 - это хост веб-клиента.
* Host #2 является хостом веб-сервера (LiteServer - это программное обеспечение веб-сервера).
* Оба хоста используют анализатор CommView для захвата обмениваемого сетевого трафика.



На следующем снимке экрана показана конфигурация интерфейсов GigabitEthernet0 / 0 (192.168.2.1/24) и GigabitEthernet0/1 (192.168.3.1/24) Cisco ASA 5520.



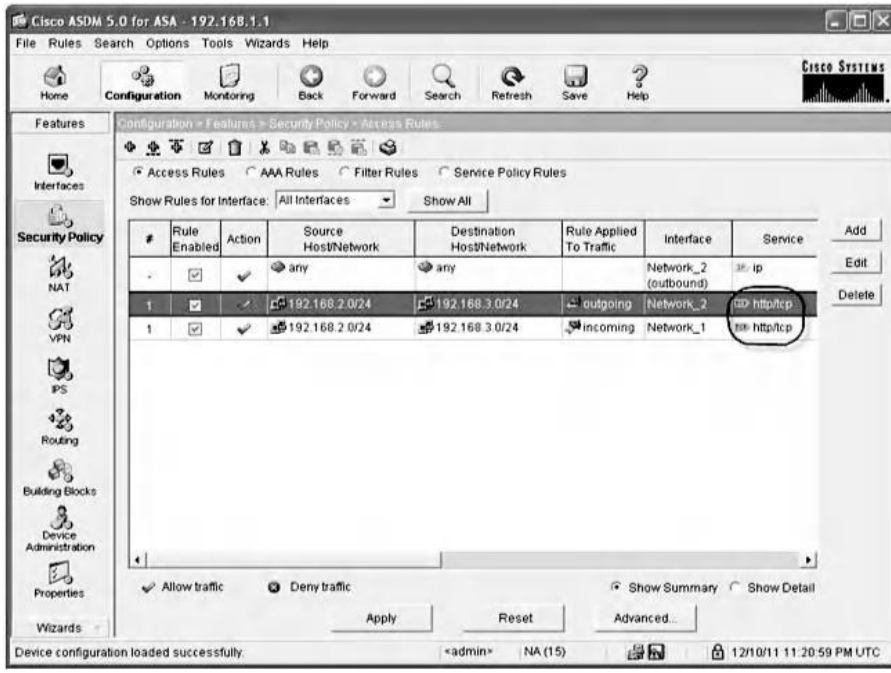
7.6.8 Шаги эксперимента

Эксперимент состоит из двух частей, чтобы проверить, предлагает ли Cisco ASA 5520 фильтрацию пакетов с отслеживанием состояния для трафика TCP и трафика ICMP соответственно.

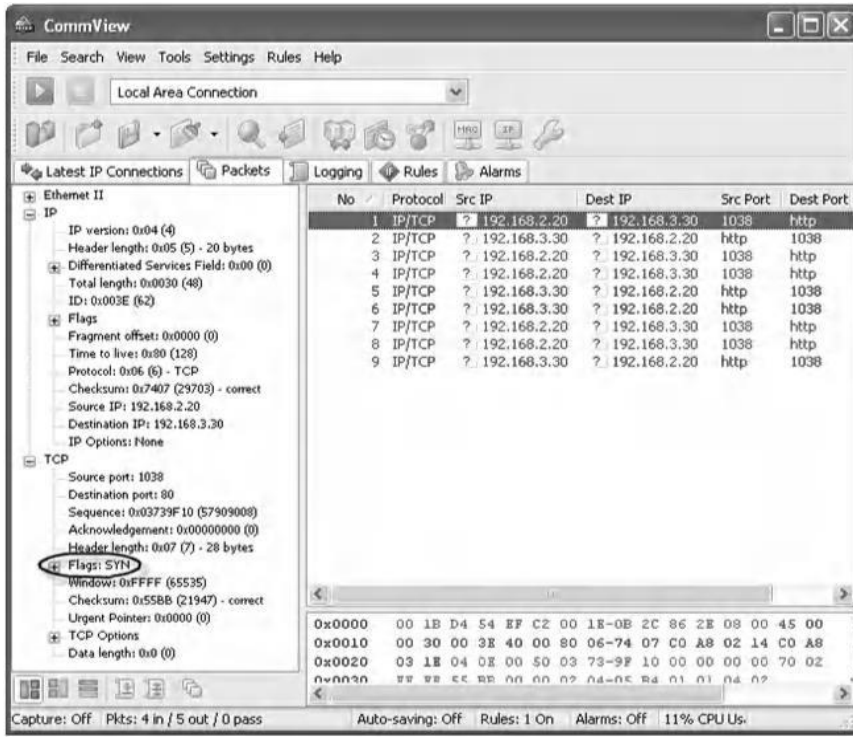
7.6.8.1 Часть 1. Полноценное тестирование TCP пакетов.

Этот эксперимент состоит из проверки, предлагает ли Cisco ASA 5520 возможность фильтрации TCP-пакетов с отслеживанием состояния. Ниже приведены этапы эксперимента:

1. Во-первых, чтобы разрешить стандартный веб-трафик (TCP / 80) между хостом веб-клиента (Host#1) и хостом веб-сервера (Host#2), два правила фильтрации реализованы с использованием интерфейса графического интерфейса Cisco ASA 5520, как показано ниже.



2. Затем с хоста № 1 (Host#1) веб-браузер используется для подключения к веб-серверу на хосте № 2 (Host#2).
3. На хосте № 1 (Host#1) сниффер CommView используется для захвата TCP-пакетов трехстороннего рукопожатия веб-сеанса, как показано ниже.



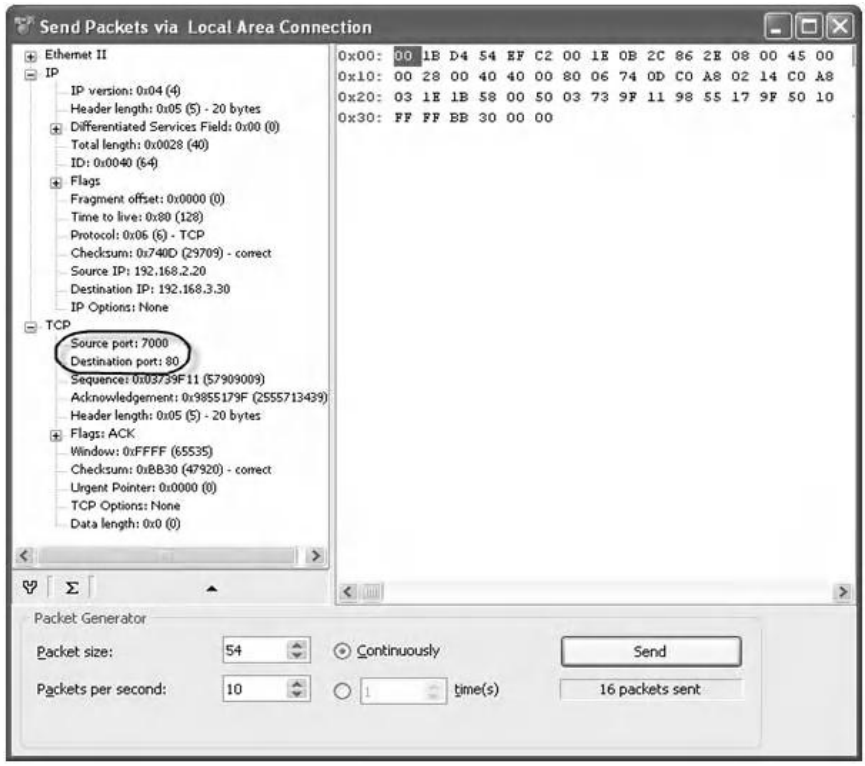
4. Значения основных полей пакетов трехстороннего рукопожатия, характеризующих веб-сеанс,

Packet number as displayed in CommView sniffer	*Source IP*	*Destination IP*	*Source port*	*Destination port*	*SYN*	*ACK*
1	192.168.2.20	192.168.3.30	1038	80	0	1
2	192.168.3.30	192.168.2.20	80	1038	1	1
3	192.168.2.20	192.168.3.30	1038	80	0	1

5. Затем CommView Visual Packet Builder используется для отправки с хоста № 1 на хост № 2 поддельного TCP-пакета, притворяющегося, что TCP-соединение на порте 80 уже установлено (SYN = 0 и ACK = 1). Поддельный TCP-пакет включает в себя одинаковые IP-адреса источника и назначения, но включает в себя порт источника, отличный от порта источника текущего активного веб-сеанса, как показано ниже.

Source IP	Destination IP	Source port	Destination port	SYN	ACK
192.168.2.20	192.168.3.30	**7000**	80	0	**1**

6. На следующем снимке экрана показаны поля вышеуказанного поддельного TCP-пакета, созданного с помощью CommView Visual Packet Builder.

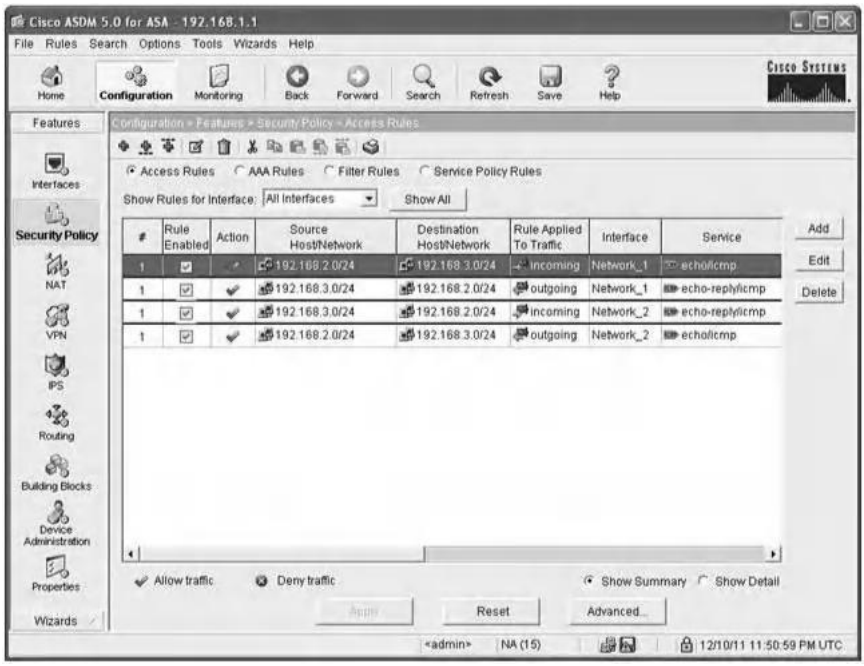


После отправки поддельного TCP-пакета сниффер CommView не перехватил отправленный поддельный TCP-пакет на узле №2. Это связано с тем, что поддельный пакет TCP был заблокирован Cisco ASA 5520. Следовательно, Cisco ASA 5520 является межсетевым экраном с отслеживанием состояния для трафика, связанного с TCP, поскольку он запрещает пакеты TCP, которые не принадлежат установленным сеансам TCP. Важно указать, что если бы анализатор CommView смог перехватить поддельный пакет TCP на хосте веб-сервера (хост № 2), то Cisco ASA 5520 был бы межсетевым экраном без сохранения состояния.

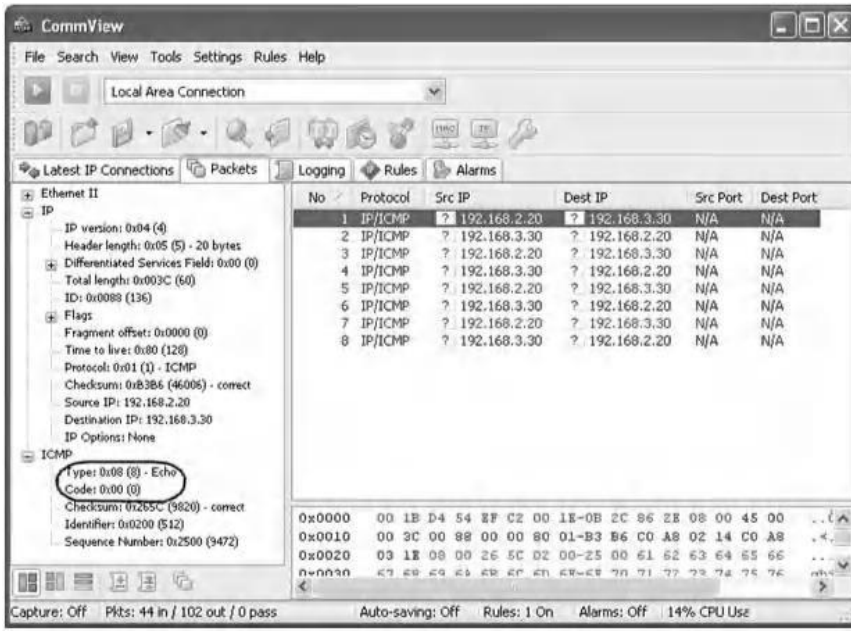
7.6.9 Часть 2: Тестирование фильтрации пакетов ICMP с учетом состояния

Этот эксперимент состоит из проверки, предлагает ли Cisco ASA 5520 возможность фильтрации пакетов с сохранением состояния ICMP. Ниже приведены этапы эксперимента:

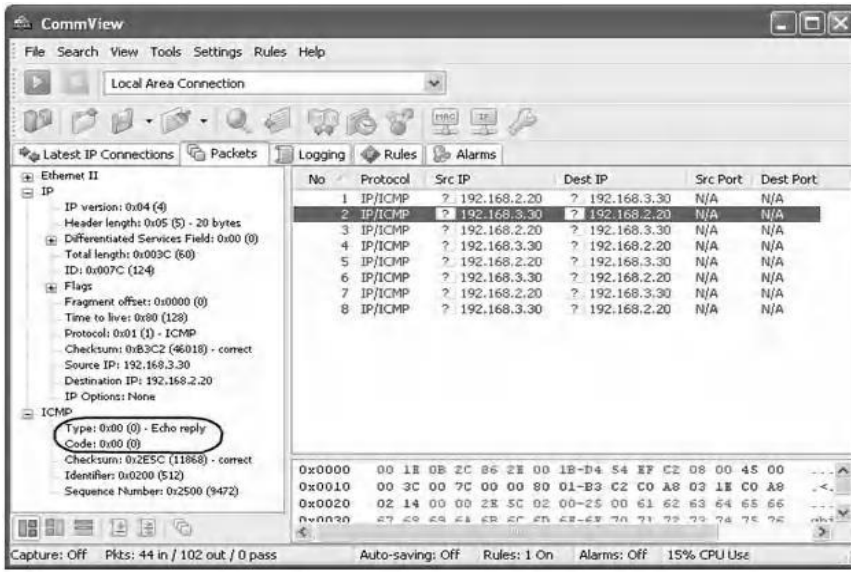
1. Во-первых, чтобы разрешить узлу № 1 проверять связь с узлом № 2, реализуются два правила фильтрации с использованием интерфейса графического интерфейса Cisco ASA 5520, как показано ниже.



2. Затем Хост № 1 пингует Хост № 2.
3. На хосте № 1 сниффер CommView используется для захвата обмениваемых пакетов ICMP. На следующем снимке экрана показан пакет эхо-запроса ICMP, отправленный с хоста № 1 на хост № 2



На следующем снимке экрана показан пакет эхо-ответа ICMP, отправленный с хоста № 2 на хост № 1.



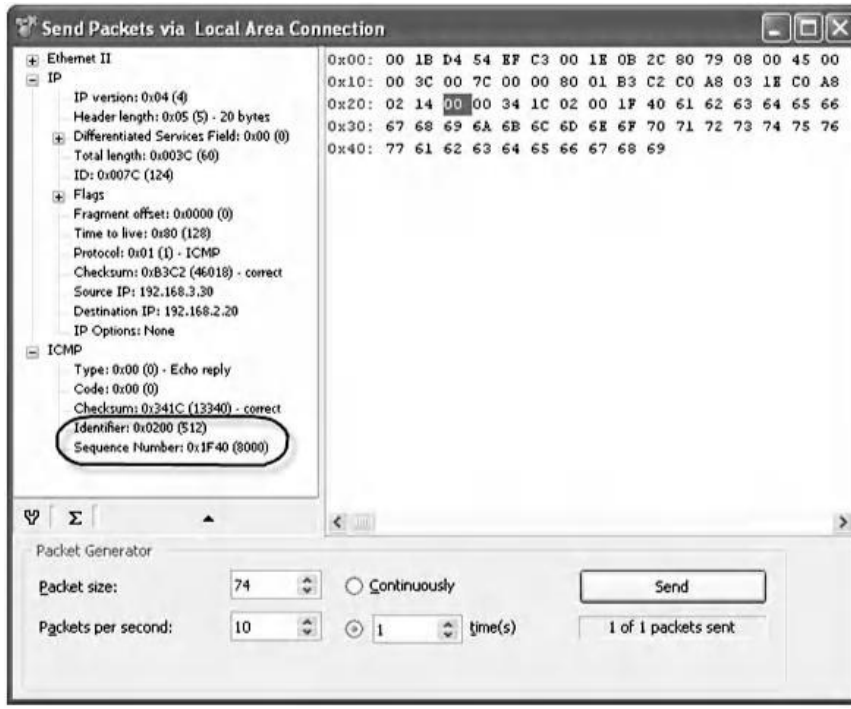
4. Значения основных полей двух пакетов ICMP, характеризующих трафик Ping:

Packet number as displayed in CommView	Source IP	Destination IP	Type	Code	Identifier	Sequence Number
1	192.168.2.20	192.168.3.30	8	0	512	9472
2	192.168.3.30	192.168.2.20	0	0	512	9472

5. Затем CommView Visual Packet Builder используется для отправки с хоста № 2 на хост № 1 поддельного пакета эхо-ответа ICMP, делая вид, что пакет эхо-запроса ICMP был получен ранее от хоста № 1. Поддельный пакет эхо-ответа ICMP включает в себя одинаковые IP-адреса источника и назначения, но включает в себя разные идентификатор и порядковый номер, как показано ниже.

Source IP	Destination IP	Type	Code	Identifier	Sequence Number
192.168.3.30	192.168.2.20	0	0	512	8000

6. Ниже приведен снимок экрана с полями поддельного пакета эхо-ответа ICMP, созданного с помощью CommView Visual Packet Builder.



После отправки поддельного ICMP-пакета с эхо-ответом, сниффер CommView успешно захватил поддельный пакет. Следовательно, Cisco ASA 5520 является межсетевым экраном без сохранения состояния для трафика, связанного с ICMP, так как он не запрещал поддельный пакет эхо-ответа ICMP. Важно указать, что если бы анализатор CommView не перехватил поддельный пакет эхо-ответа ICMP на хосте № 1, то Cisco ASA 5520 был бы межсетевым экраном с отслеживанием состояния для трафика, связанного с ICMP.

7.7 Лабораторная работа 7.6: активные и пассивные режимы FTP

7.7.1 Результат

Цель данного практического лабораторного занятия - научить студентов лучше анатомировать концепцию активных и пассивных режимов FTP с помощью примеров и экспериментов.

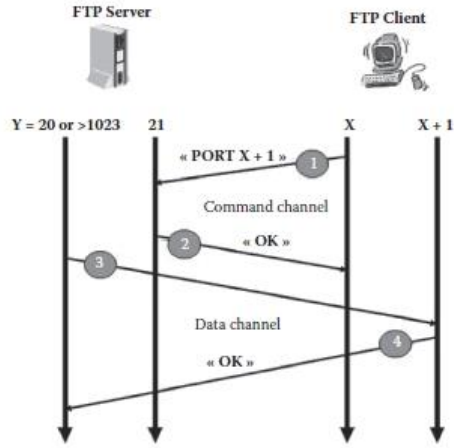
7.7.2 Активные и пассивные режимы FTP

FTP - это сервис, основанный на архитектуре TCP клиент / сервер. FTP является необычным сервисом, поскольку он использует два канала связи, называемых Командный канал (также известный как Канал управления) и Канал данных. FTP использует два порта на стороне сервера: командный порт (21) и порт данных (обычно 20 или 1024-65535). Кроме того, FTP предлагает два режима подключения, а именно: режим активного FTP (также известный как режим обычного FTP) и режим пассивного FTP. В следующих подразделах описываются два режима.

7.7.2.1 Активный режим FTP

В активном режиме FTP клиент FTP подключается от случайного порта (X> 1023) к командному порту FTP-сервера, порт 21. Затем клиент начинает прослушивать порт X + 1 и отправляет команду «PORT X + 1» на сервер. Значение «X + 1» представляет номер порта канала данных на стороне клиента. Затем сервер инициирует канал данных. Таким образом, сервер подключается обратно к указанному клиенту порту данных через его локальный порт данных, который является портом 20 или случайным портом (Y> 1023).

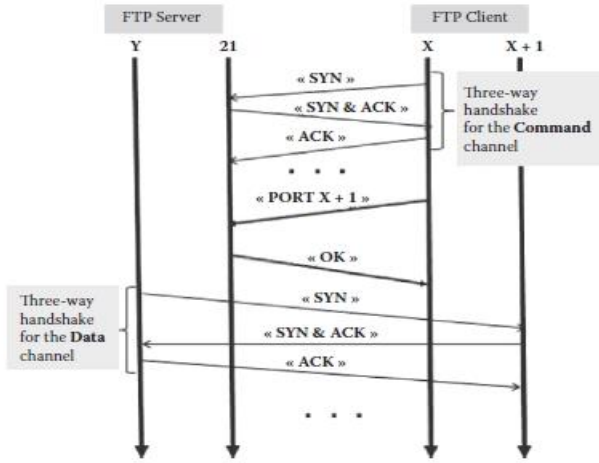
На следующем рисунке показаны два канала TCP активного FTP-соединения. На шаге 1 командный порт клиента FTP (X 1023) связывается с командным портом сервера (21) и отправляет команду PORT (X + 1). На шаге 2 сервер затем отправляет ACK обратно на командный порт клиента. На шаге 3 сервер инициирует соединение через свой локальный порт данных (Y) с портом данных (X + 1), указанным ранее клиентом. Наконец, клиент отправляет ACK обратно, как показано на шаге 4.



7.7.2.2 Активная фильтрация трафика FTP

Чтобы разрешить активному FTP-трафику проходить через брандмауэр, должны быть реализованы правила фильтрации, чтобы разрешить трафик как командного канала, так и канала данных.

На следующем рисунке показаны различные TCP-пакеты, которыми обмениваются в активном сеансе FTP. Сеанс команд инициируется FTP-клиентом, а сеанс данных - FTP-сервером.



Кроме того, поскольку FTP использует каналы на основе TCP, для каждого канала требуются четыре правила фильтрации, позволяющие соответствующему трафику проходить через брандмауэр. Например, если FTP-клиент является внутренним хостом, а FTP-сервер является внешним хостом, то в двух последующих таблицах перечислены все необходимые правила фильтрации для каналов команд и данных соответственно.

Правила фильтрации для командного канала в активном сеансе FTP

Direction	*Source IP*	*Destination IP*	*Protocol*	*Source port*	*Destination port*	*SYN*	*ACK*	*Action*
Outgoing	FTP client	FTP server	TCP	1024–65535	21	1	0	Allow
Incoming	FTP server	FTP client	TCP	21	1024–65535	1	1	Allow
Outgoing	FTP client	FTP server	TCP	1024–65535	21	0	1	Allow
Incoming	FTP server	FTP client	TCP	21	1024–65535	0	1	Allow

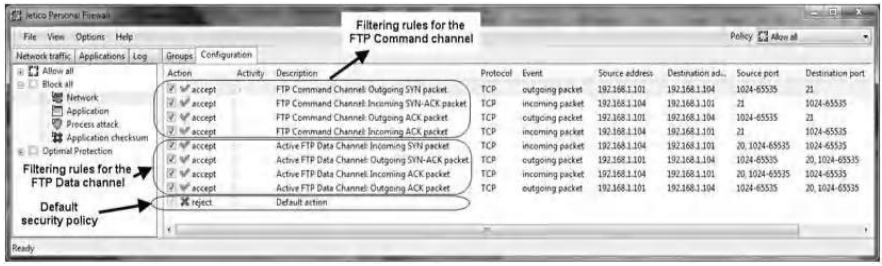
Правила фильтрации для канала данных в активном сеансе FTP

Direction	*Source IP*	*Destination IP*	*Protocol*	*Source port*	*Destination port*	*SYN*	*ACK*	*Action*
Incoming	FTP server	FTP client	TCP	20, 1024–65535	1024–65535	1	0	Allow
Outgoing	FTP client	FTP server	TCP	1024–65535	20, 1024–65535	1	1	Allow
Incoming	FTP server	FTP client	TCP	20, 1024–65535	1024–65535	0	1	Allow
Outgoing	FTP client	FTP server	TCP	1024–65535	20, 1024–65535	0	1	Allow

7.7.2.3 Реализация правил фильтрации для активного FTP-трафика

Большинство брандмауэров содержат предопределенные правила фильтрации, чтобы разрешить и поддерживать активный трафик FTP. Однако для образовательных целей, чтобы вручную реализовать правила фильтрации, показанные в двух таблицах выше в брандмауэре, брандмауэр должен позволять манипулировать значениями флагов TCP при создании правила фильтрации. Например, Jetico Personal Firewall * предлагает такую возможность и

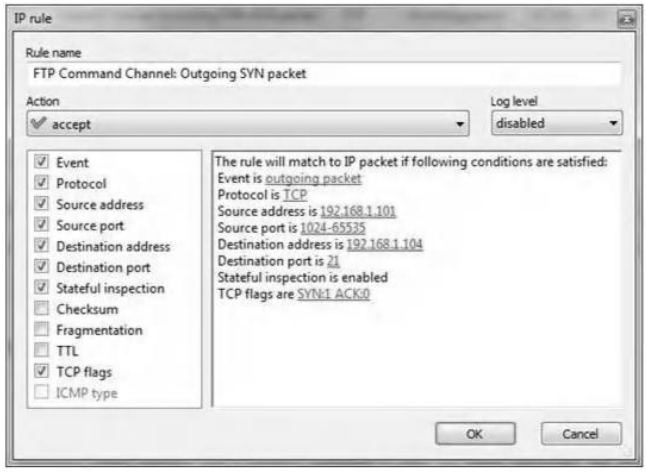
позволяет указывать значения полей правила фильтрации, показанных в двух таблицах выше. С помощью графического интерфейса Jetico Personal Firewall на следующем снимке экрана показана реализация правил фильтрации высоты из приведенных выше таблиц, необходимых для разрешения трафика Active FTP. Мы предполагаем, что IP-адреса внутреннего FTP-клиента и внешнего FTP-сервера равны 192.168.1.101 и 192.168.1.104 соответственно. Политика безопасности по умолчанию - “Deny All” (Запретить все).



На следующих рисунках показано подробное содержание правил фильтрации, показанных на снимке экрана выше.

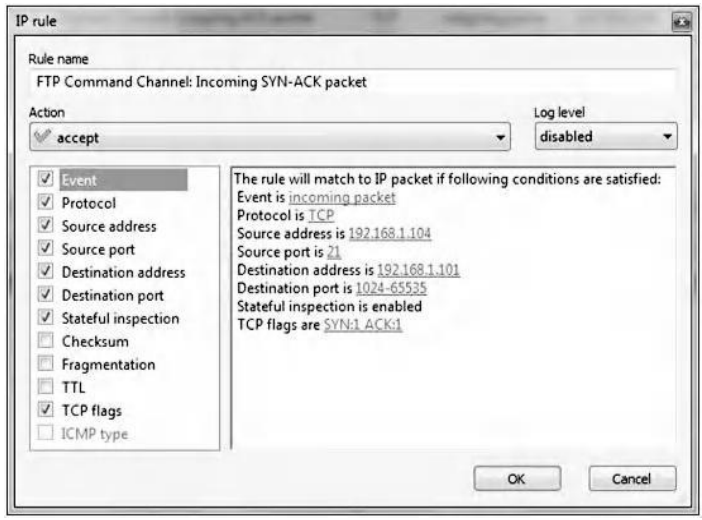
A. Правила фильтрации для канала Command в активном сеансе FTP:

1. Исходящие SYN-пакеты для Командного канала:

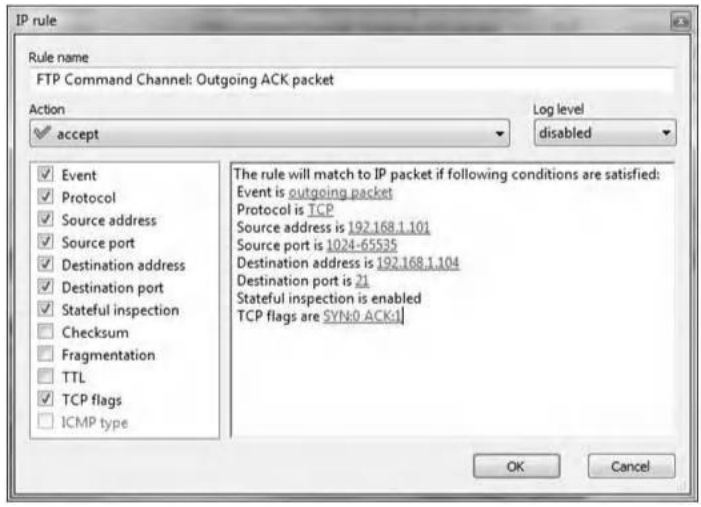


* http://www.jetico.com

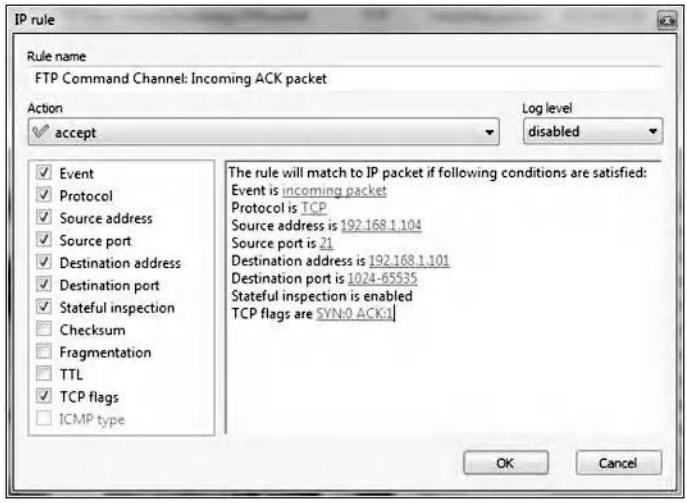
2. Входящие пакеты SYN-ACK для командного канала:



3. Исходящие ACK-пакеты для Командного канала:

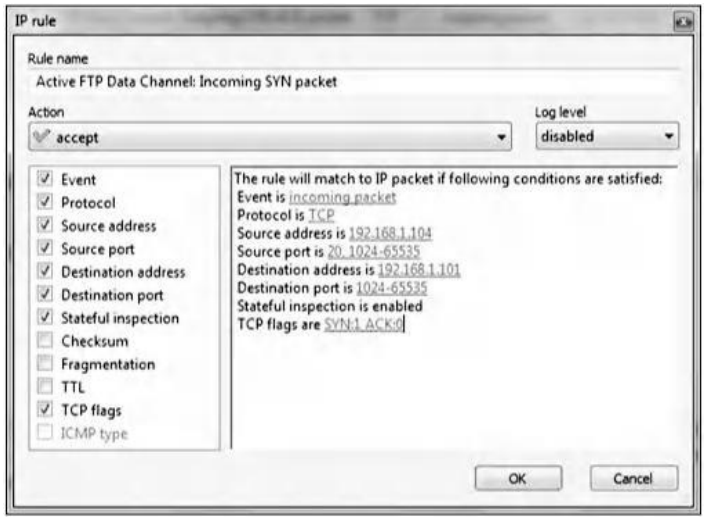


4. Входящие ACK-пакеты для Командного канала:

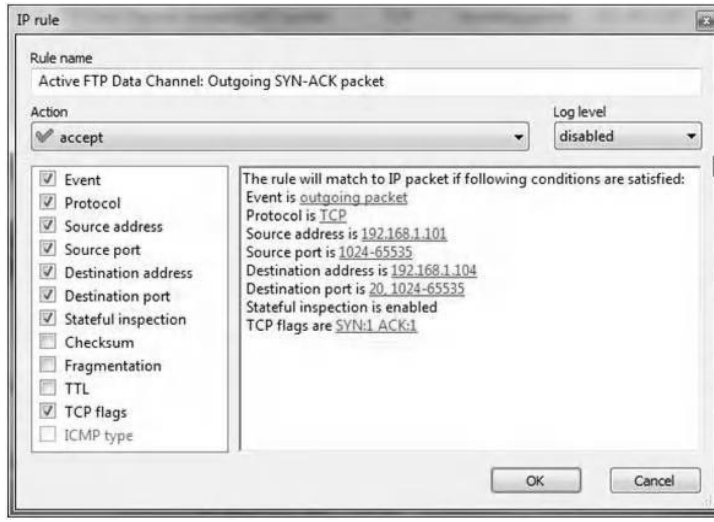


B. Правила фильтрации для канала данных в активном сеансе FTP:

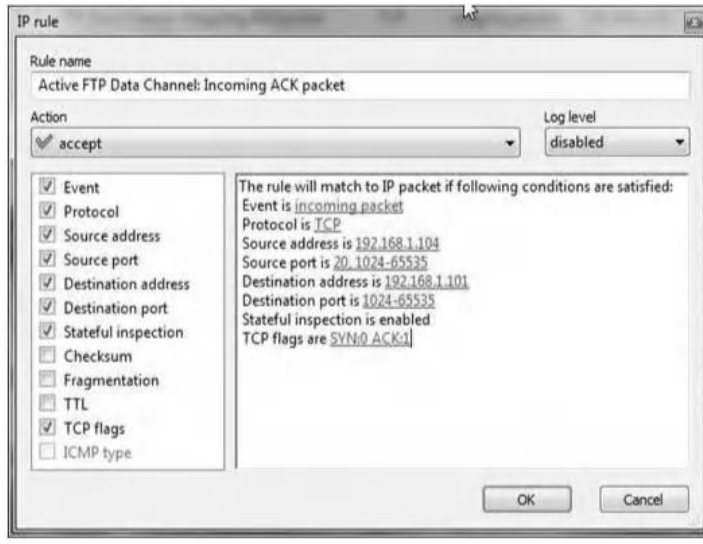
1. Входящие пакеты SYN для канала данных:



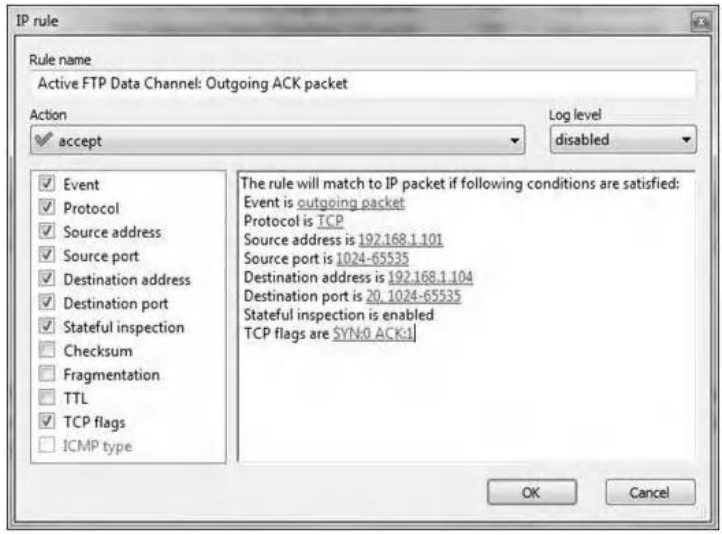
2. Исходящие пакеты SYN-ACK для канала данных:



3. Входящие пакеты ACK для канала данных:



4. Исходящие пакеты ACK для канала данных:



7.7.2.4 Проблема безопасности с активным режимом FTP

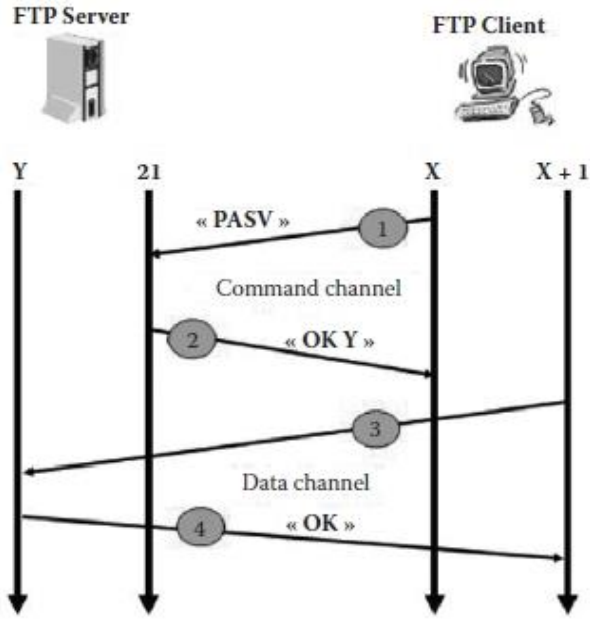
Обычно в сеансе TCP клиент / сервер клиент запускает сеанс. Однако в активном сеансе FTP FTP-клиент инициирует сеанс Command, а FTP-сервер инициирует сеанс Data. Это серьезная проблема безопасности, поскольку для брандмауэра внешним хостам разрешено инициировать сеансы TCP на внутренних хостах. Этот тип соединения обычно блокируется, поскольку он позволяет злонамеренным внешним хостам генерировать атаки на внутренние хосты. То есть в сеансе активного FTP злонамеренный хост может использовать правила фильтрации, соответствующие каналу данных, для установления TCP-соединений с внутренними хостами. Эта уязвимость позволит злонамеренному хосту легко атаковать внутренние хосты. DoS-атаки или атаки на основе программ с дистанционным управлением (например, троянские кони) являются примерами атак, которые злонамеренные хосты могут выполнять против внутренних хостов. Таким образом, активный FTP полезен для администратора сервера FTP, но вреден для администратора на стороне клиента.

7.7.3 Пассивный режим FTP

Чтобы решить проблему безопасности в режиме активного FTP, был разработан другой метод для FTP-соединений. Это называется пассивным режимом FTP. В этом режиме клиент FTP запускает каналы

команд и данных, что позволяет решить проблему безопасности в режиме активного FTP. FTP-клиент использует команду «PASV», чтобы сообщить серверу, что FTP-сессия будет в пассивном режиме.

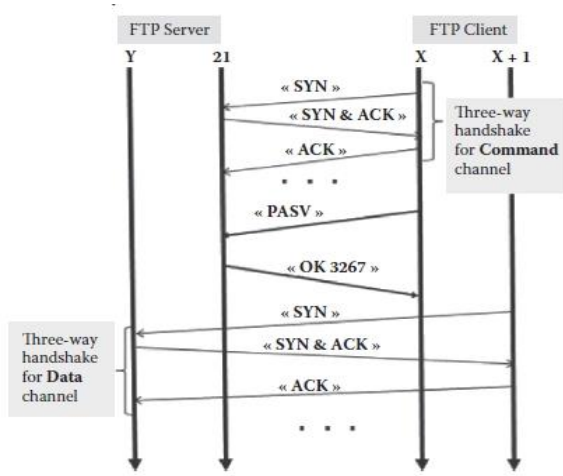
На следующем рисунке показаны два TCP-канала пассивного FTP-соединения. При открытии FTP-соединения клиент открывает два случайных порта локально (X> 1023 и X + 1). Первый порт связывается с сервером через порт 21, затем клиент выдает команду «PASV» (шаг 1). Результатом этого является то, что сервер затем открывает порт Y (20 или случайный порт (Y> 1023)) и отправляет команду «PORT Y» обратно клиенту (Шаг 2). Затем клиент инициирует соединение от порта «X + 1» к порту Y на сервере для передачи данных (шаг 3). Наконец, на шаге 4 сервер отправляет обратно ACK на порт данных клиента.



7.7.3.1 Пассивная фильтрация трафика FTP

Чтобы разрешить пассивному FTP-трафику проходить через брандмауэр, должны быть реализованы правила фильтрации, чтобы разрешить трафик как командного канала, так и канала данных.

На следующем рисунке показаны различные TCP-пакеты, которыми обмениваются в сеансе пассивного FTP. Сеансы команд и данных инициируются клиентом FTP.



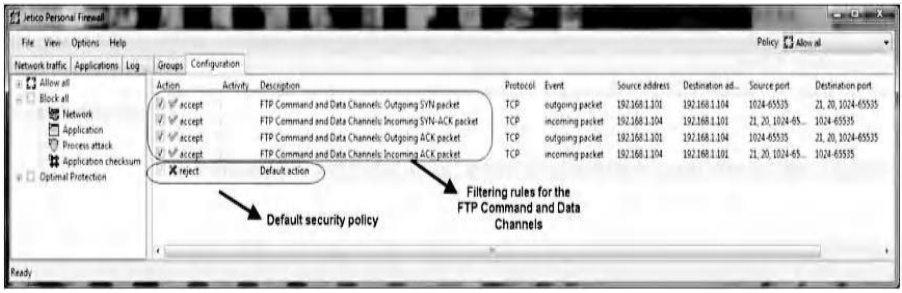
In addition, because FTP uses TCP-based channels, for each channel, four filtering rules are required to allow the cor-responding traffic to pass through the firewall. For example, if the FTP client is an internal host and the FTP server is an external host, then the following table provides all the filtering rules for the Command and Data channels, respectively.

Правила фильтрации для командного канала и канала данных в пассивном сеансе FTP

Direction	*Source IP*	*Destination IP*	*Protocol*	*Source Port*	*Destination Port*	*SYN*	*ACK*	*Action*
Outgoing	FTP client	FTP server	TCP	1024–65535	21, 20, 1024–65535	1	0	Allow
Incoming	FTP server	FTP client	TCP	21, 20, 1024–65535	1024–65535	1	1	Allow
Outgoing	FTP client	FTP server	TCP	1024–65535	21, 20, 1024–65535	0	1	Allow
Incoming	FTP server	FTP client	TCP	21, 20, 1024–65535	1024–65535	0	1	Allow

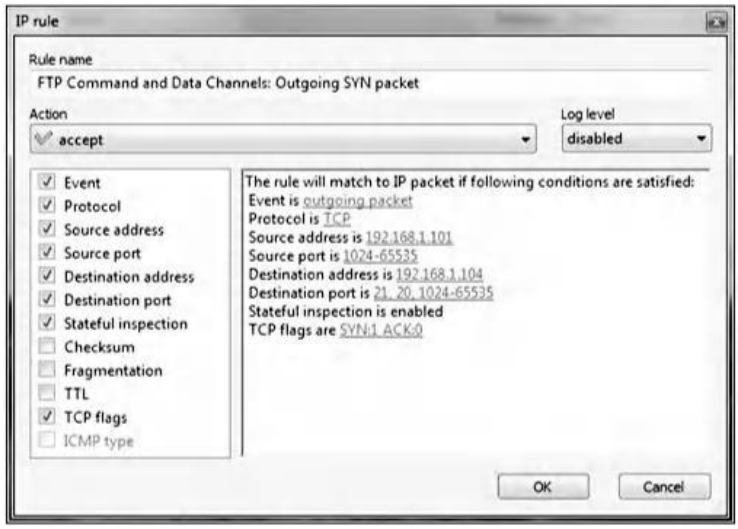
7.7.3.2 Реализация правил фильтрации для пассивного FTP-трафика

На следующем снимке экрана с использованием графического интерфейса Jetico Personal Firewall показана реализация четырех правил фильтрации из приведенной выше таблицы, необходимых для разрешения пассивного трафика FTP.

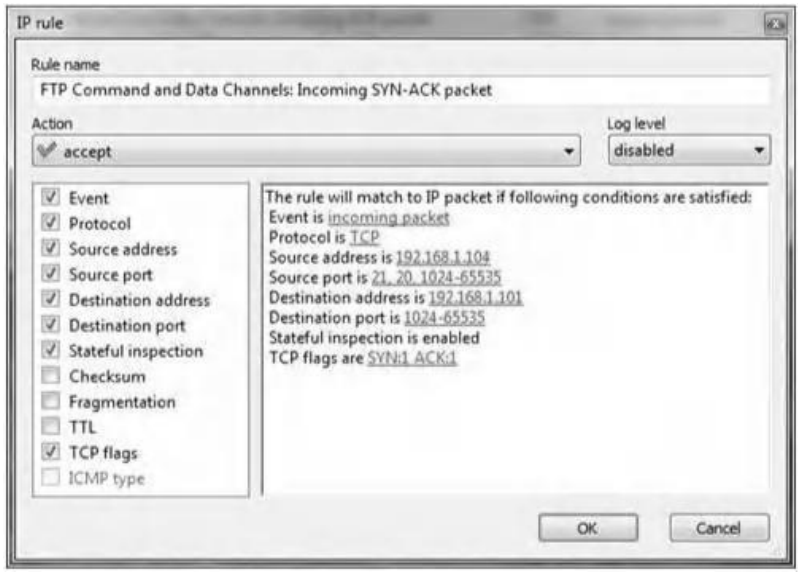


На следующих снимках экрана показано подробное содержание правил фильтрации, показанных на снимке экрана выше.

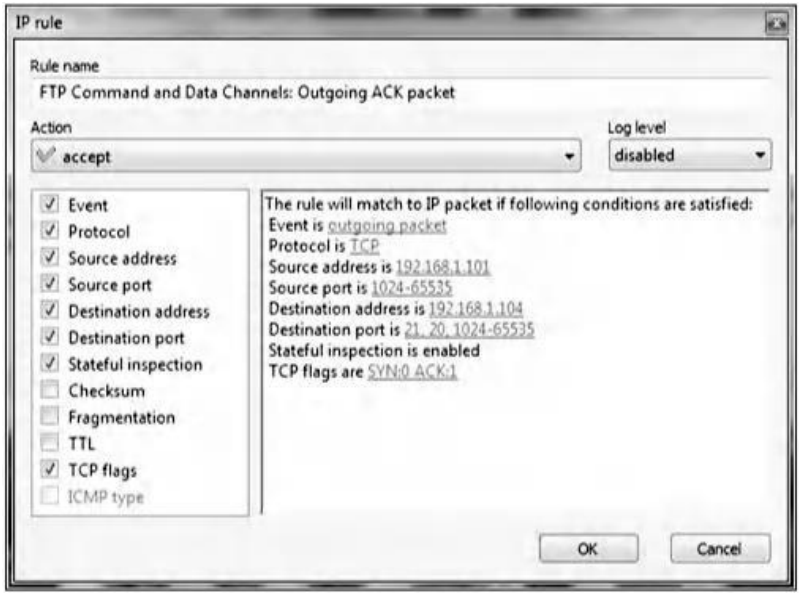
1. Исходящие пакеты SYN для каналов команд и данных:



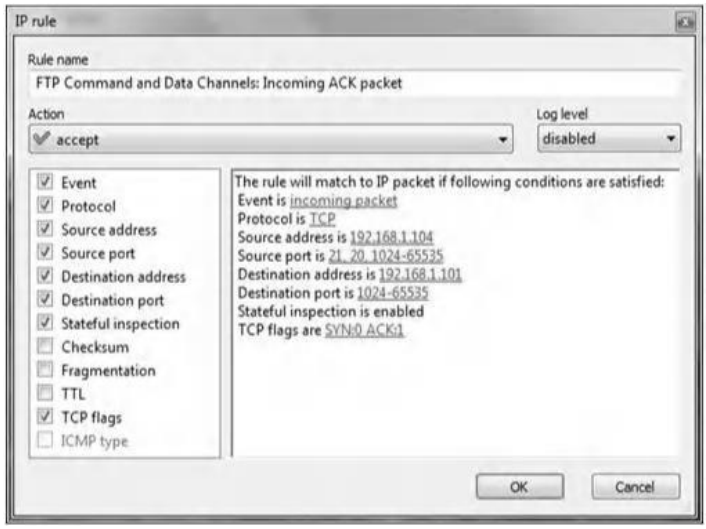
2. Входящие пакеты SYN-ACK для каналов команд и данных:



3. Исходящие пакеты ACK для каналов команд и данных:



4. Входящие пакеты ACK для каналов команд и данных:



7.7.3.3 Проблема безопасности с пассивным режимом FTP

Несомненно, что пассивный режим FTP является более безопасным режимом по сравнению с активным режимом FTP. Однако основная проблема безопасности в режиме пассивного FTP заключается в том, что узлам FTP-клиента разрешено инициировать подключения к портам с большим номером на сервере FTP. Это может открыть целый ряд проблем на стороне FTP-сервера. Однако, поскольку администраторам FTP-серверов необходимо сделать свои серверы доступными для наибольшего числа клиентов, им почти наверняка потребуется поддержка Passive FTP. Проблему безопасности в режиме пассивного FTP можно минимизировать, используя FTP-серверы, которые позволяют администраторам определять ограниченный диапазон портов для использования FTP-серверами. Кроме того, межсетевые экраны будут блокировать любой порт, который не принадлежит этому диапазону. Таким образом, пассивный FTP выгоден для клиента, но вреден для администратора FTP-сервера.

С другой стороны, использование режима пассивного FTP в сети предполагает поддержку и устранение неполадок клиентов, которые поддерживают (или не поддерживают) режим пассивного FTP.

Кроме того, в настоящее время пользователи предпочитают использовать свои веб-браузеры в качестве FTP-клиента. Если брандмауэр настроен на разрешение только пассивного режима FTP, тогда браузеры должны быть настроены на подключение в режиме пассивного FTP. Это требует дополнительной поддержки и устранения неполадок для клиентов. Например, чтобы изменить Internet Explorer 8 для подключения в пассивном режиме FTP, выполните следующие действия:

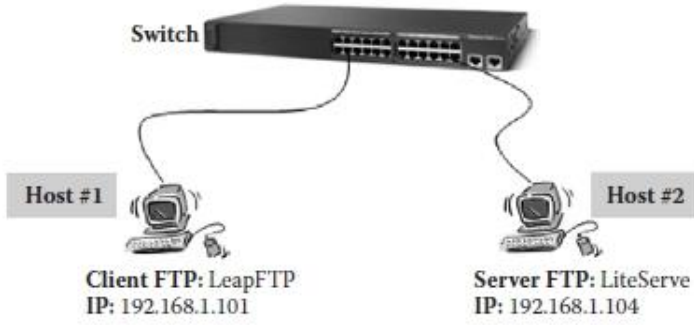
1. Откройте Internet Explorer; нажмите “Tools – Internet Options” (Инструменты - Свойства обозревателя» и выберите вкладку “Advanced” (Дополнительно).
2. В разделе “Browsing” (Просмотр) снимите флажок “Enable folder view for FTP sites” (Включить просмотр папок для FTP-сайтов). Это необходимо, поскольку сохранение этого флажка переопределит пассивную опцию.
3. Установите флажок “Use Passive FTP (for firewall and DSL modem compatibility)” (Использовать пассивный FTP (для совместимости с брандмауэром и модемом DSL)), как показано на следующем снимке экрана.
4. Нажмите “Apply” (Применить), а затем кнопку “OK”.

7.7.4 Эксперимент: активный анализ трафика FTP и анализ

Эксперимент связан с анализом и анализом активного и пассивного FTP-трафика. Эксперимент состоит из двух частей. Первый касается активного FTP-трафика, а второй - пассивного FTP-трафика.

7.7.5 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Два хоста (Host #1 и Host #2) подключены к коммутатору Cisco. На Host #1 запущен инструмент LeapFTP в качестве клиента FTP. На Host #2 запущено программное обеспечение LiteServe в качестве FTP-сервера.



7.7.6 Шаги эксперимента - часть 1: активный сеанс FTP

В следующем эксперименте описывается, как анализировать и анализировать пакеты активного сеанса FTP. Эксперимент состоит из следующих этапов:

Шаг 1. Подключитесь к FTP-серверу, используя режим активного FTP, и прослушайте пакеты сеанса.
Шаг 2. Анализ активных пакетов сеанса FTP.

7.7.6.1 Шаг 1. Подключитесь к FTP-серверу, и используя активный режим FTP, перехватите сессионные пакеты

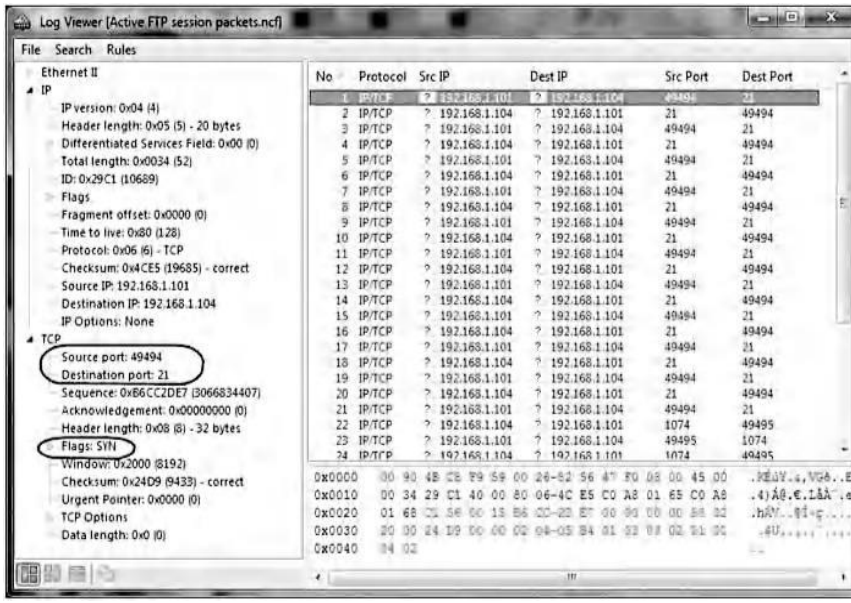
С хоста № 1 и с помощью LeapFTP подключитесь к FTP-серверу хоста № 2. По умолчанию LeapFTP использует режим активного FTP. Затем, используя сниффер CommView на хосте № 1 или хосте № 2, перехватите пакеты сеанса.

7.7.6.2 Шаг 2. Анализ пакетов активного сеанса FTP

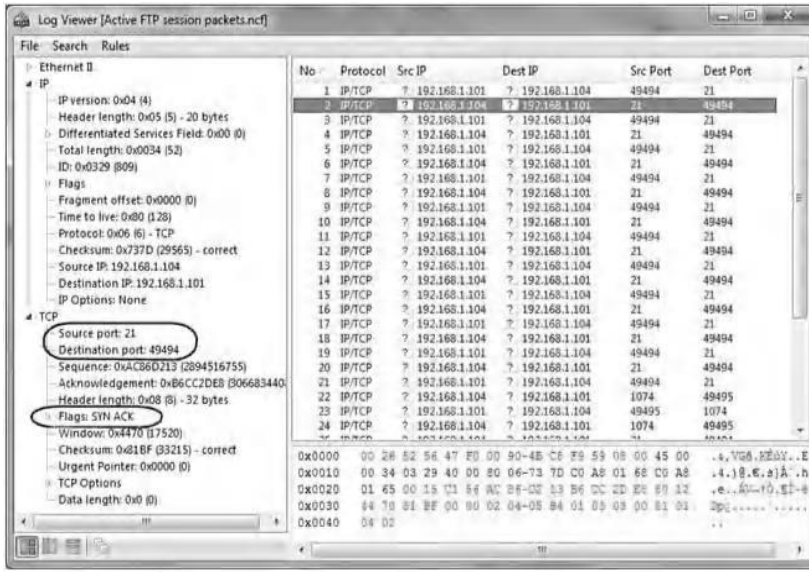
На следующих снимках экрана показано подробное содержимое основных пакетов сеансов Command и Data:

A. Для командного канала в активном сеансе FTP:

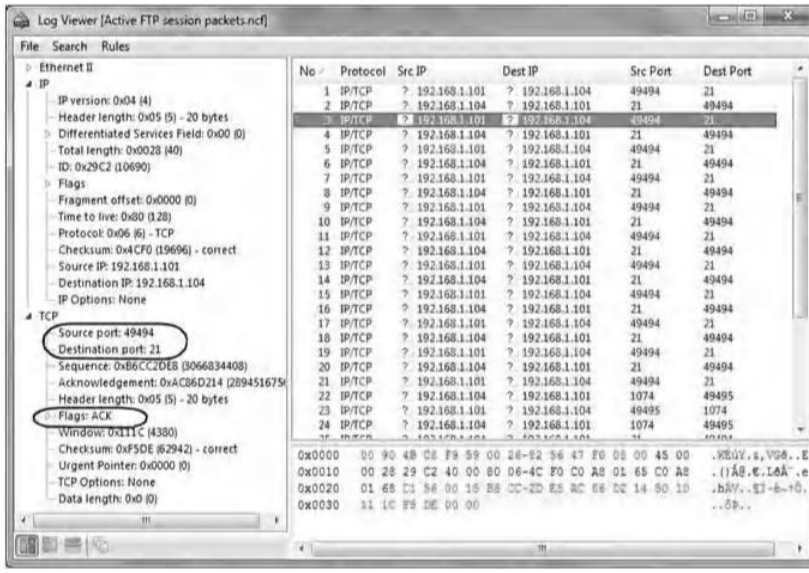
1. Первый пакет (пакет SYN) трехстороннего рукопожатия командного канала в активном сеансе FTP:



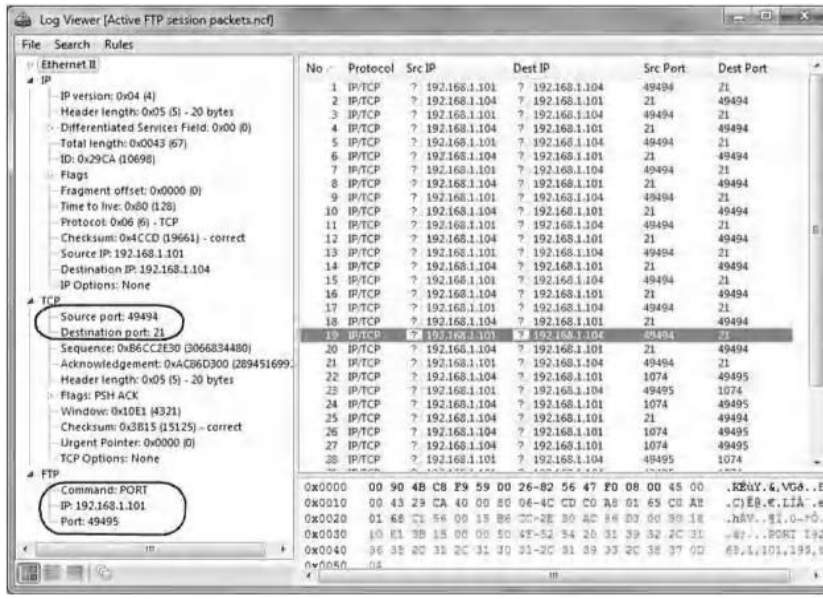
2. Второй пакет (пакет SYN-ACK) трехстороннего рукопожатия командного канала в активном сеансе FTP:



3. Третий пакет (ACK-пакет) трехстороннего рукопожатия Командного канала в активном сеансе FTP:

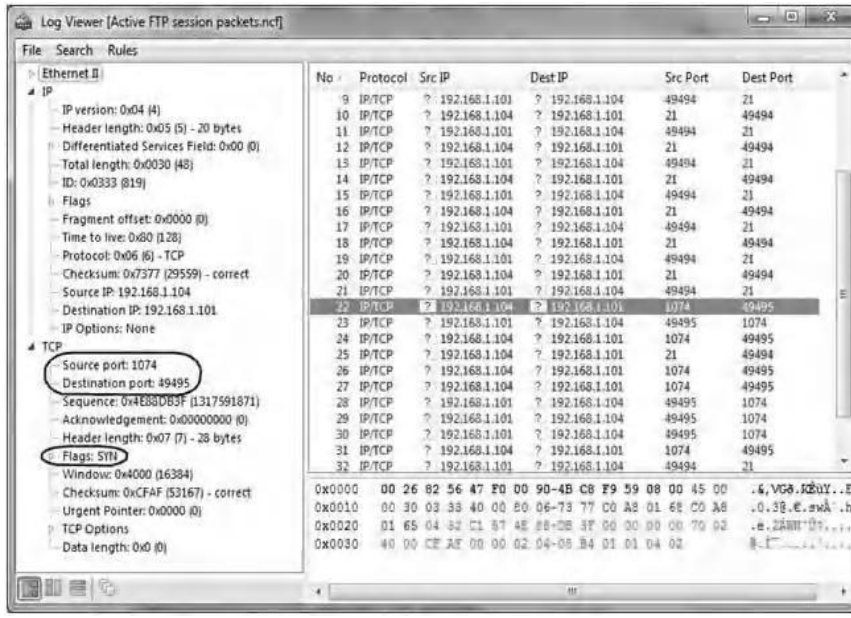


4. Пакет TCP канала Command в сеансе активного FTP, который включает номер порта для канала данных (PORT Y = 49495):

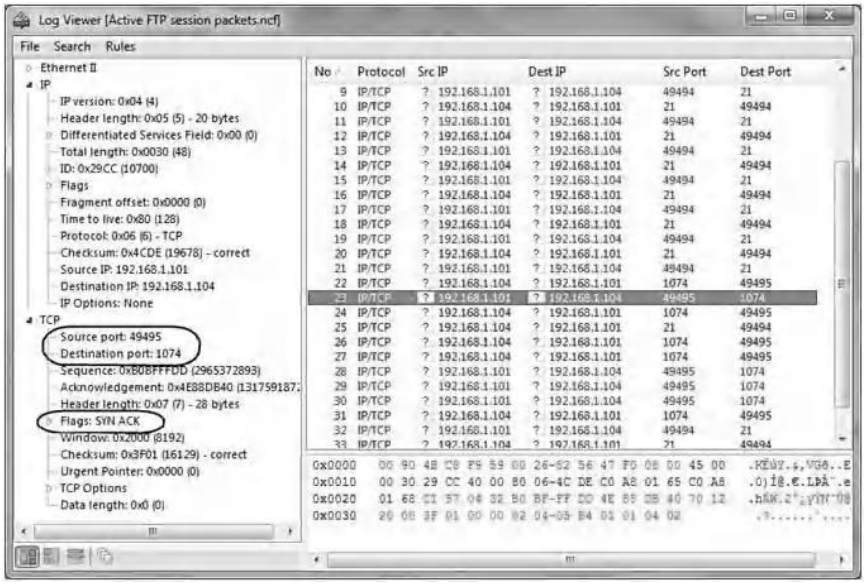


B. Для канала данных в активном сеансе FTP:

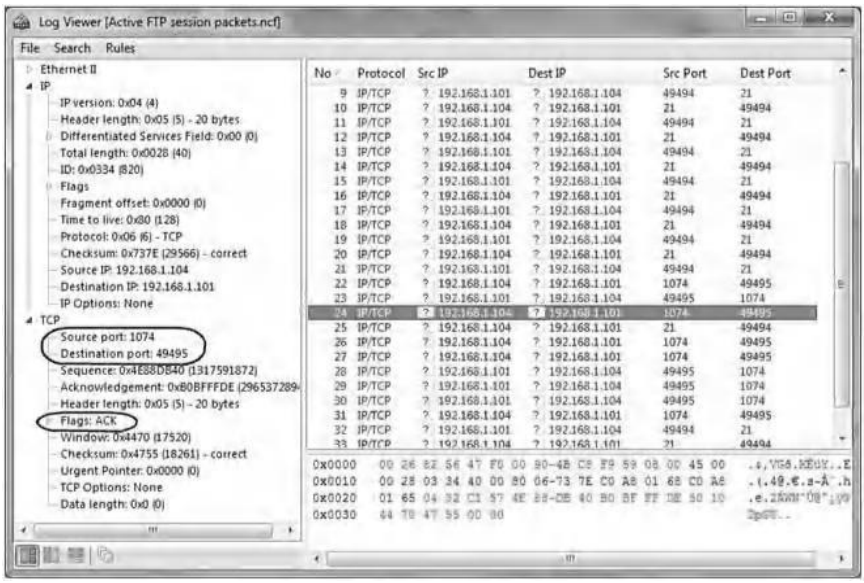
1. Первый пакет (пакет SYN) трехстороннего рукопожатия канала данных в активном сеансе FTP:



2. Второй пакет (пакет SYN-ACK) трехстороннего квитирования канала данных в активном сеансе FTP:



3. Третий пакет (ACK-пакет) трехстороннего рукопожатия канала данных в активном сеансе FTP:



7.7.7 Шаги эксперимента. Часть 2. Пассивный режим FTP

В следующем эксперименте описывается, как анализировать и анализировать пакеты сеанса пассивного FTP. Эксперимент состоит из следующих этапов:

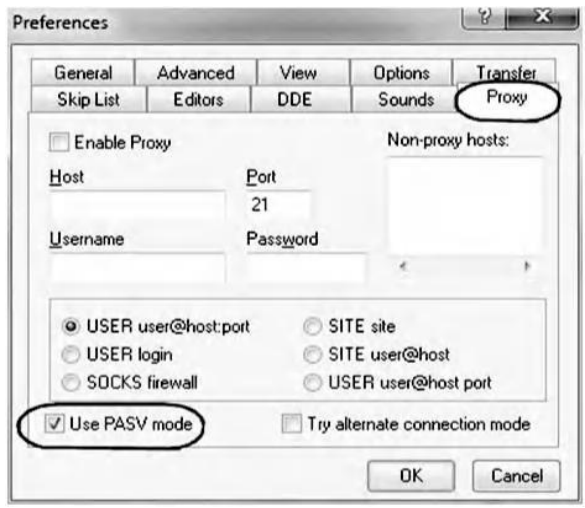
Шаг 1: Настройте LeapFTP в качестве пассивного FTP-клиента.
Шаг 2: Подключитесь к FTP-серверу и прослушайте пакеты сеанса.
Шаг 3: Проанализируйте пассивные пакеты сеанса FTP.

7. *7.7.1 Шаг 1. Настройте LeapFTP в качестве пассивного FTP-клиента*

Чтобы настроить LeapFTP в качестве пассивного FTP-клиента, выполните следующие действия:

Из графического интерфейса LeapFTP, перейдите к:
— Options -> Preferences ->General -> Proxy.

Выберите “Use PASV mode”(Использовать режим PASV); затем нажмите «ОК» (как показано на скриншоте ниже).



7.7.7.2 Шаг 2. Подключитесь к FTP-серверу и прослушайте сессионные пакеты

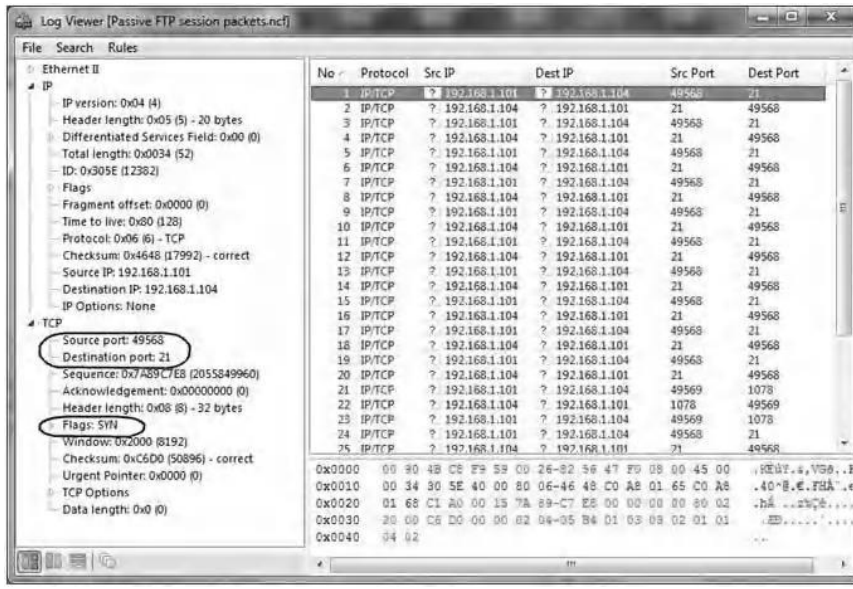
С хоста № 1 и с помощью LeapFTP подключитесь к FTP-серверу, работающему на хосте № 2. Затем, используя сниффер CommView, вынюхивайте пакеты сеанса.

7.7.7.3 Шаг 3. Анализ пассивных пакетов сессий FTP

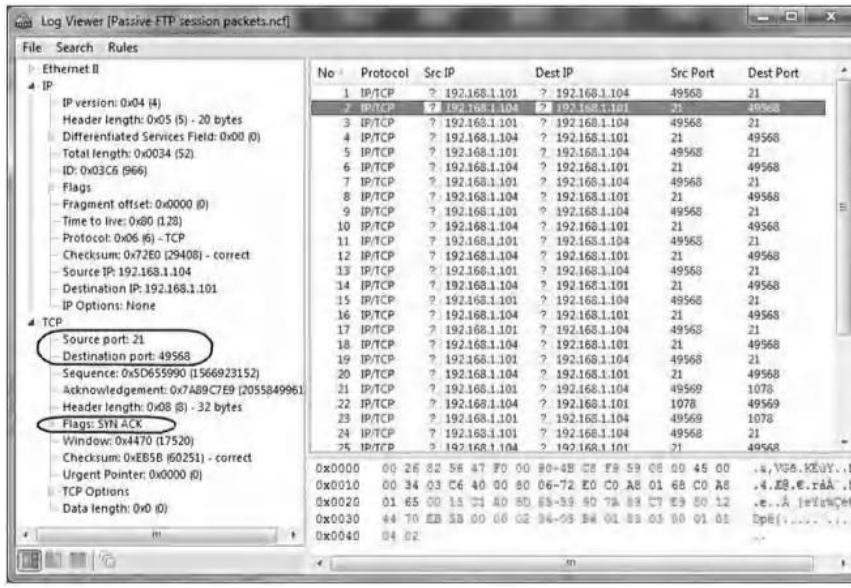
На следующих снимках экрана показано подробное содержимое основных пакетов каналов команд и данных сеанса пассивного FTP:

A. Для канала Command в сеансе пассивного FTP:

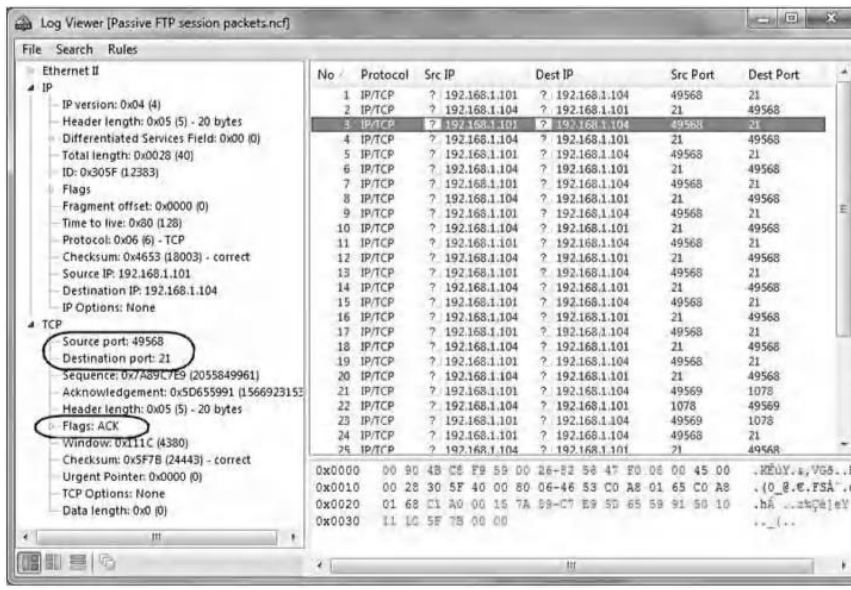
1. Первый пакет (пакет SYN) трехстороннего рукопожатия Командного канала в сеансе пассивного FTP:



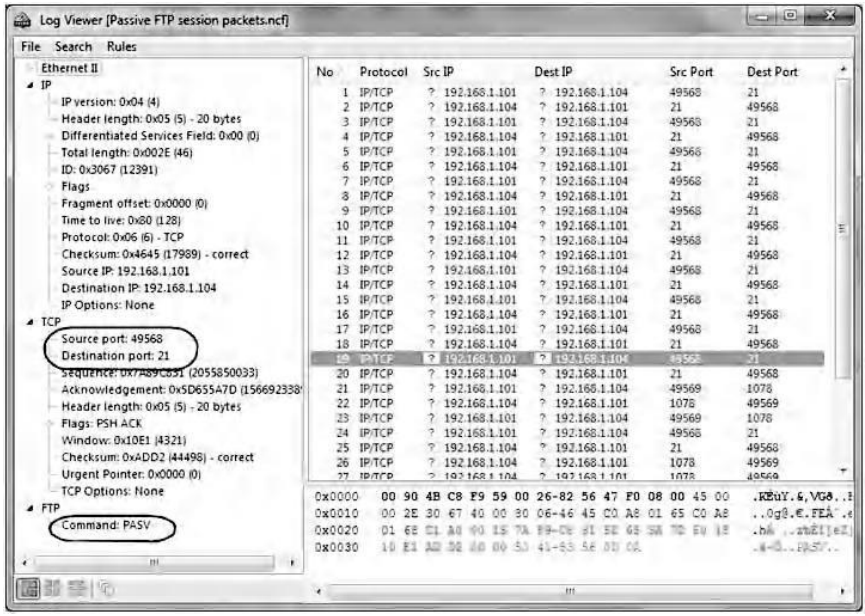
2. Второй пакет (пакет SYN-ACK) трехстороннего рукопожатия Командного канала в сеансе пассивного FTP:



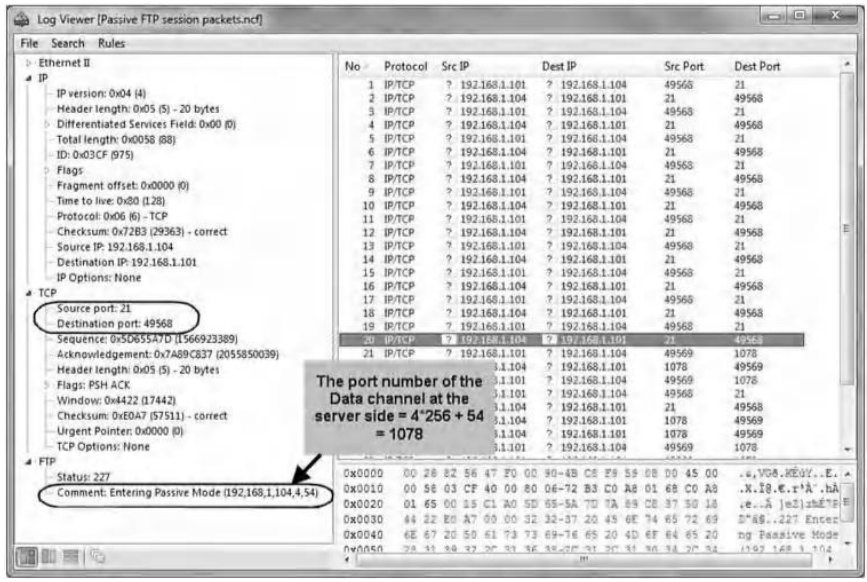
3. Третий пакет (ACK-пакет) трехстороннего рукопожатия Командного канала в сеансе пассивного FTP:



4. Пакет TCP канала Command в сеансе пассивного FTP, который включает запрос «PASV»:

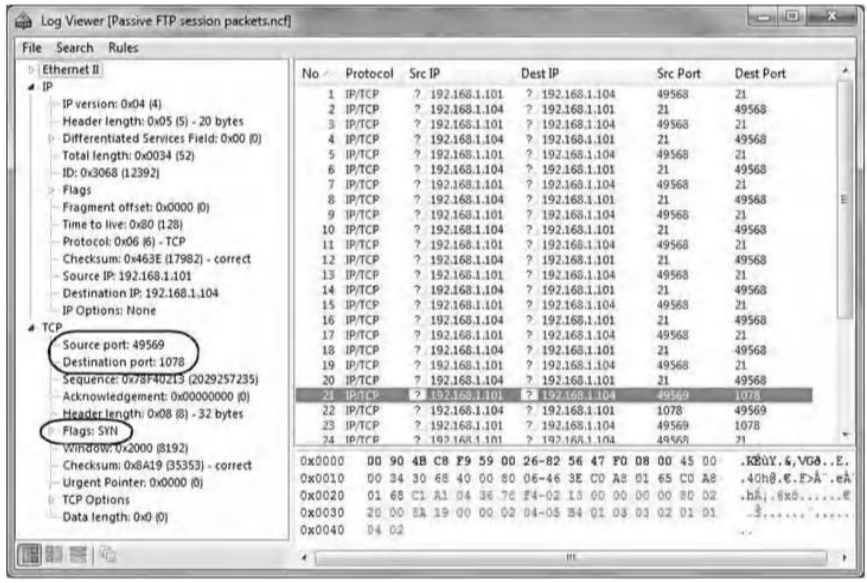


5. Пакет TCP канала Command в сеансе пассивного FTP, который отправляет номер порта канала данных на стороне сервера. Команда PORT отформатирована как последовательность из шести чисел, разделенных запятыми. Первые четыре октета являются IP-адресом сервера FTP, а последние два октета составляют порт, который будет использоваться для подключения к данным. Чтобы найти фактический порт, умножьте пятый октет на 256, а затем добавьте шестой октет к общему. Таким образом, в приведенном ниже примере номер порта ((4 * 256) +54) или 1078.

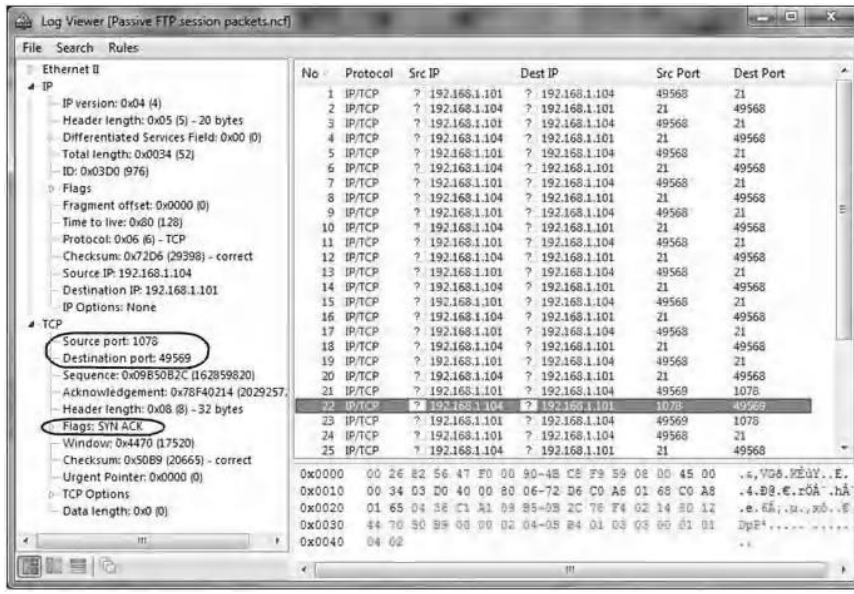


B. Для канала данных в сеансе пассивного FTP:

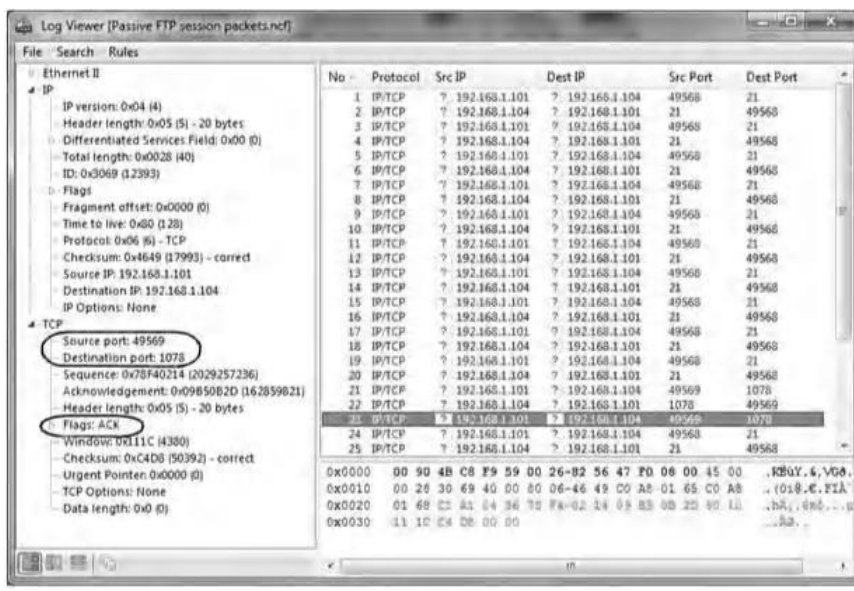
1. Первый пакет (пакет SYN) трехстороннего рукопожатия канала данных в сеансе пассивного FTP:



2. Второй пакет (пакет SYN-ACK) трехстороннего квитирования канала данных в сеансе пассивного FTP:



3. Третий пакет (ACK-пакет) трехстороннего рукопожатия канала данных в сеансе пассивного FTP:



7.8 Краткое содержание главы

Предприятие с интрасетью, которая позволяет его работникам получать доступ к более широкому Интернету, устанавливает брандмауэр, чтобы предотвратить доступ посторонних лиц к своим собственным частным данным и для управления внешними ресурсами, к которым имеют доступ его собственные пользователи. По сути, межсетевой экран проверяет каждый сетевой пакет, чтобы определить, следует ли пересылать его к месту назначения. Поэтому брандмауэры играют важную роль в обеспечении соблюдения политик контроля доступа в современных сетях.

В этой главе обсуждался ряд практических упражнений о реализации правил фильтрации для базовых политик безопасности, фильтрации служб, работающих на нестандартных портах TCP и UDP, проверке согласованности и эффективности правил фильтрации брандмауэров, фильтрации содержимого пакетов, отсутствия состояний. фильтрация пакетов с отслеживанием состояния, а также активный и пассивный режимы FTP.

Глава 8

Безопасность маршрутизатора

8.1 Введение

Важной мерой защиты любой сети является обеспечение безопасного трафика через ее границы. Маршрутизатор - это устройство, которое соединяет одну или несколько сетей вместе и, следовательно, является точкой входа в сеть. Следовательно, маршрутизатор обеспечивает безопасность решений, которые жизненно важны для безопасности любой сети.

В этой главе обсуждается реализация следующих функций безопасности на маршрутизаторе:

* *Модель аутентификации, авторизации и учета (Authentication, Authorization, and Accounting (AAA)):* Модель AAA (тройной A) использует модульный подход и является масштабируемым решением для обеспечения безопасности. Он гибко выполняет политики аутентификации, авторизации и учета. Модель сначала определяет метод службы безопасности, а затем применяет его к различным линиям или консолям. Тем самым он способствует удобству использования, возможности повторного использования и масштабируемости.

* *Безопасность сетевых сервисов (Network services security):* Одной из наиболее важных задач по усилению безопасности маршрутизатора является отключение ненужных сетевых служб и

защита необходимых служб, особенно тех, которые используются для управления устройствами (например, Telnet и HTTP). Атака с использованием анализатора используется для использования уязвимостей сетевых служб открытого текста, а именно Telnet и HTTP. Позже эти уязвимые службы заменяются зашифрованными текстовыми службами SSH (Secure Shell) и HTTPS.

* *Фильтрация пакетов с использованием списков контроля доступа (Packet filtering, using Access Control Lists* (*ACLs*)*):* Стандарт Internet Engineering Task Force (IETF), установленный в Запросах на комментарии (RFC) 1918 и RFC 2827, используется для описания политик фильтрации. RFC 1918 определяет частные адреса, которые не разрешены в Интернете. В RFC 2827 обсуждается фильтрация входа в сеть для предотвращения атак с использованием IP-спуфинга. Кроме того, различные правила фильтрации пакетов настроены так, чтобы разрешать и запрещать различные типы трафика на основе определенной политики.

* *Проверка:* Общие маршрутизаторы поддерживают проверку фильтрации пакетов с отслеживанием состояния. Эта функция позволяет возвращать трафик в защищенную сеть для прохождения через маршрутизатор на основе информации о состоянии, полученной из прошлых сообщений. Это достигается путем открытия динамической дыры в политике безопасности, которая выполняется с использованием механизма, известного как контекстно-зависимый контроль доступа (CBAC) на маршрутизаторах Cisco.

Эта глава включает практические упражнения по реализации модели AAA, безопасным сетевым сервисам и фильтрации пакетов с отслеживанием состояния на пограничном маршрутизаторе. Маршрутизаторы Cisco широко используются в практических реализациях. Следовательно, практические упражнения используют устройства Cisco для реализации обсуждаемых концепций безопасности. Тем не менее, такие концепции безопасности могут быть применены к продуктам других поставщиков, предлагающих те же функциональные возможности. Для выполнения упражнений используются следующие аппаратные устройства и программные средства:

* Cisco router *: сетевой маршрутизатор
* CommView Tool †: инструмент для мониторинга и анализа сети (сниффер)

8.2 Лабораторная работа 8.1: базовая модель AAA

8.2.1 Результат

Цель данного упражнения - научить студентов изучать функции безопасности маршрутизатора Cisco путем настройки базовой модели AAA.

8.2.2 Описание

Управление доступом к ресурсам сетевого устройства имеет первостепенное значение при рассмотрении сетевой безопасности. Более ранние меры для обеспечения доступа включают пароль линии, пароль ENABLE и локальное имя пользователя. Однако они обеспечивают только базовый уровень аутентификации, который идентифицирует пользователей, вошедших в систему на маршрутизаторе или другом сетевом устройстве. С другой стороны, модель AAA - это обобщенная основанная на политике структура, которая удовлетворяет большинству распространенных проблем в управлении доступом к сети. Он обращается к трем основным службам безопасности любой системы контроля доступа, а именно к аутентификации, авторизации и учету, как независимые функции безопасности.

Authentication (Аутентификация) должна предшествовать авторизации и учету и состоит из двух этапов: идентификация и проверка. Во-первых, пользователь идентифицируется путем отправки учетных данных, таких как имя пользователя и пароль, с помощью ряда вызовов и ответов. Затем эти учетные данные проверяются для подтверждения личности пользователя из авторизованной базы данных. База данных может быть локальной базой данных, которая хранится на сетевом устройстве, или

* HTTP://www.cisco.com
† HTTP://www.tamos.com

это может быть сам маршрутизатор. База данных может быть удаленной базой данных, размещенной на выделенном удаленном сервере AAA. Двумя известными протоколами безопасности, используемыми для связи с удаленным сервером AAA, являются Cisco TACAS + (система контроля доступа контроллера терминального доступа Plus) и RADIUS (удаленный пользовательский сервис удаленной аутентификации), указанные в RFC 2865.

Authorization (Авторизация) следует процессу аутентификации, чтобы обеспечить соблюдение определенных политик для сетевых ресурсов. Это обеспечивает более детальный контроль над привилегиями пользователя для доступа к сетевым ресурсам. Основными ресурсами, доступными для управления доступом на маршрутизаторах Cisco, являются команды IOS. В соответствии с политикой авторизации пользователям назначается определенный уровень привилегий от 0 до 15. При уровне привилегий 0 пользователь не может выполнять никакие команды IOS на маршрутизаторе. Уровень привилегий 1 представляет режим «Пользователь EXEC», который по умолчанию назначается пользователю, который подключается к маршрутизатору. Уровень привилегий 15, который является уровнем привилегий по умолчанию для режима «Privileged EXEC» (режим включения) маршрутизатора, дает пользователю возможность выполнять все команды IOS. Следуя принципу наименьших привилегий, который требует, чтобы пользователи имели доступ только к необходимым ресурсам для своих целей и не более, оставшиеся уровни привилегий назначаются разным пользователям в зависимости от спецификаций их работы. Политики авторизации могут быть определены локально на самом маршрутизаторе или удаленно с использованием серверов AAA.

Accounting (Учет) - это процесс сбора и записи информации о действиях пользователя и сетевых событиях, который может использоваться для целей аудита. Учет происходит после завершения аутентификации и авторизации. Бухгалтерская информация может храниться на самом маршрутизаторе или удаленно на серверах AAA. Примерами учетной информации являются события сеанса входа в систему, выданные команды IOS и количество пакетов.

Это практическое упражнение посвящено объяснению методов аутентификации и авторизации модели AAA с использованием маршрутизатора Cisco IOS. В упражнении представлен пошаговый подход к реализации методов аутентификации и авторизации, которые защищают доступ управления к маршрутизатору Cisco. Локальная база

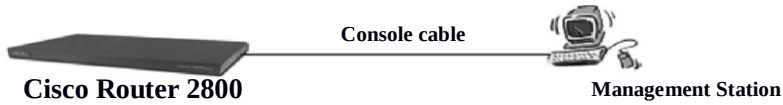
данных политик аутентификации и авторизации была настроена на маршрутизаторе для назначения пользователям необходимого уровня привилегий. Методы, используемые для управления маршрутизатором, - это консольная линия и Telnet, которые были защищены моделью AAA. Кроме того, были реализованы методы учета не AAA, чтобы показать различные уровни ведения журнала, доступные на маршрутизаторе Cisco IOS.

8.2.3 Эксперимент

Шаги в следующем эксперименте выполняются с использованием маршрутизатора Cisco 2800 с ОС 12.4 для настройки методов аутентификации и авторизации.

8.2.4 Архитектура сети

Следующий рисунок иллюстрирует сетевую архитектуру эксперимента. Станция управления подключается к маршрутизатору через консольный кабель для выполнения необходимой конфигурации.



8.2.5 Шаги эксперимента

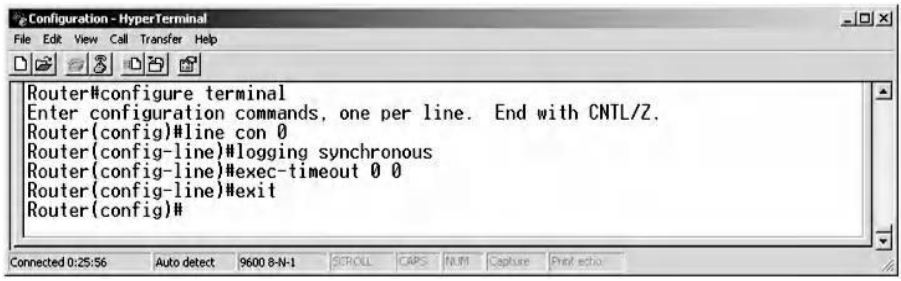
Эксперимент состоит из следующих этапов:

Шаг 1: Основные команды настройки маршрутизатора.
Шаг 2: Настройте интерфейс обратной связи.
Шаг 3: Консоль по умолчанию для аутентификации и авторизации.
Шаг 4: Telnet аутентификация и авторизация по умолчанию.
Шаг 5: Настройте модель AAA: Аутентификация.
Шаг 6: применить аутентификацию к VTY.

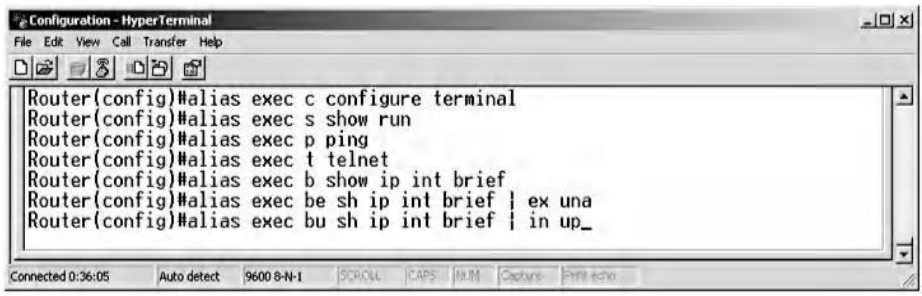
Шаг 7: применить аутентификацию к консоли.
Шаг 8: Проверьте консоль и аутентификацию Telnet.
Шаг 9: Настройте модель AAA: Авторизация.
Шаг 10: применить авторизацию к VTY.
Шаг 11: Примените авторизацию к консоли.
Шаг 12: Проверьте консоль и авторизацию Telnet.
Шаг 13: Настройте ведение журнала консоли.

8.2.5.1 Шаг 1: Основные команды настройки маршрутизатора

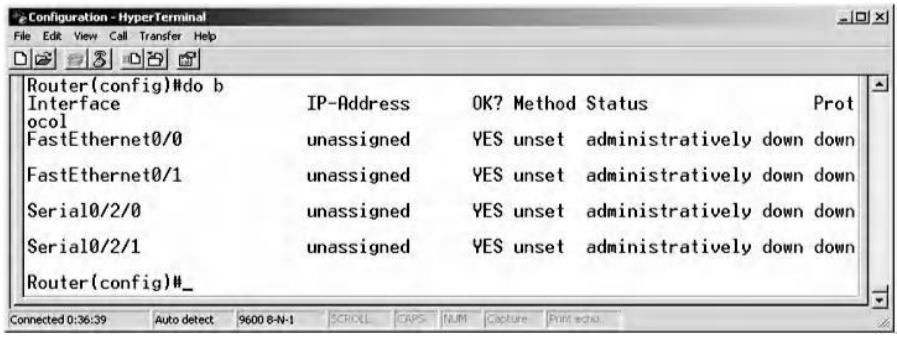
Сначала подключите ноутбук к последовательной консоли маршрутизатора. Введите «enable», чтобы маршрутизатор перешел в режим привилегированного пользователя EXEC. Затем, чтобы отключить поиск DNS, введите «no ip domain lookup» в режиме глобальной конфигурации. Наконец, чтобы синхронизировать сообщения журнала и установить время ожидания консоли в бесконечность, выполните следующие команды:



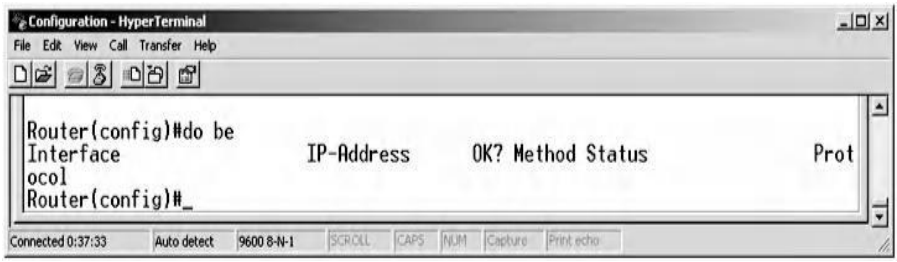
Используйте команду «alias», чтобы упростить настройку, как показано ниже:



Например, введите команду псевдонима «do b» для отображения краткого представления интерфейсов.

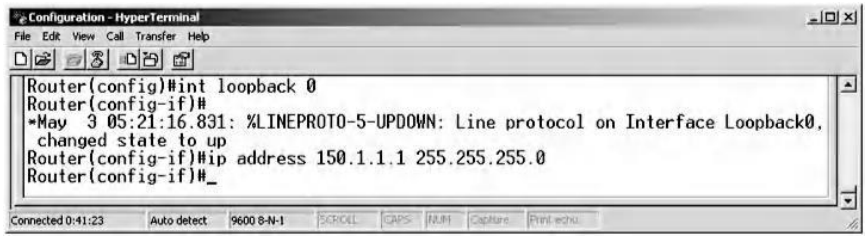


Чтобы исключить неназначенные интерфейсы, введите следующую команду:

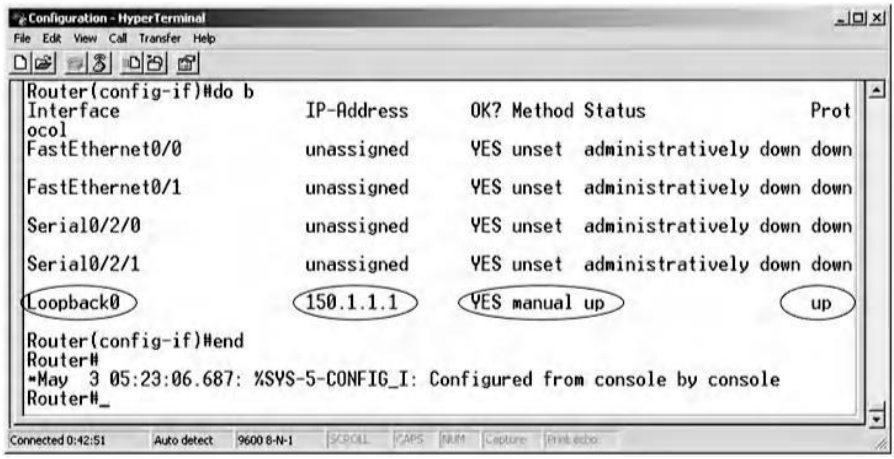


8.2.5.2 Шаг 2: Настройте интерфейс обратной связи

Интерфейс обратной связи используется для тестирования Telnet. Чтобы создать петлевой интерфейс, введите следующие команды:

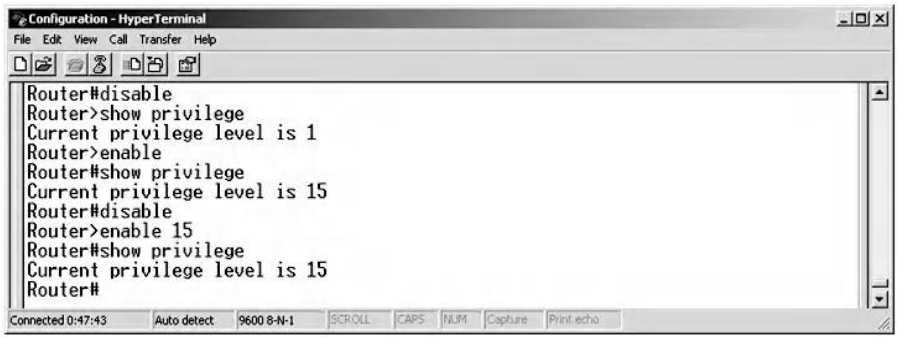


Затем, чтобы отобразить созданный петлевой интерфейс, введите следующие команды:



8. 2.5.3 Шаг 3: Консольная аутентификация и авторизация по умолчанию

Чтобы отобразить уровни привилегий различных пользователей, вошедших в систему, введите команду «show privilege». Обратите внимание, что уровень привилегий по умолчанию для режима ENABLE равен 15.



8. 2.5.4 Шаг 4: VTY (Telnet) аутентификация и авторизация по умолчанию

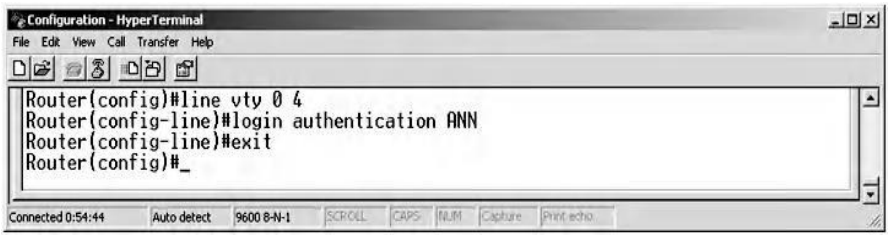
Чтобы проверить аутентификацию и авторизацию линии VTY по умолчанию, используйте следующую команду, которая показывает, что для работы соединения Telnet требуется пароль:

8. 2.5.5 *Шаг 5: Настройте модель AAA: аутентификация*

Конфигурация аутентификации требует имени пользователя, пароля и типа базы данных. В этом примере база данных является локальным экземпляром. Имя метода AAA, используемого для Аутентификации, является ANN.

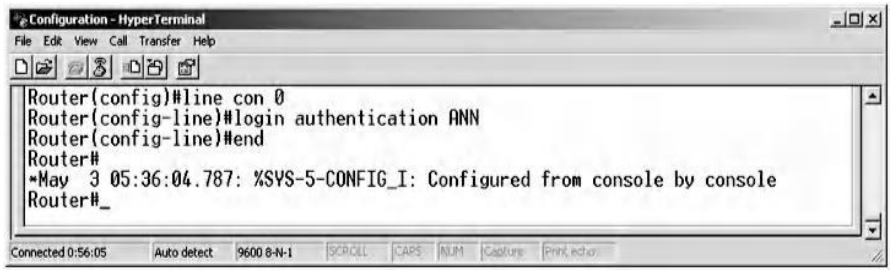
8.2.5.6 Шаг 6: применить аутентификацию к VTY

Чтобы применить метод аутентификации ANN, созданный на шаге 5, к VTY, введите следующую команду:



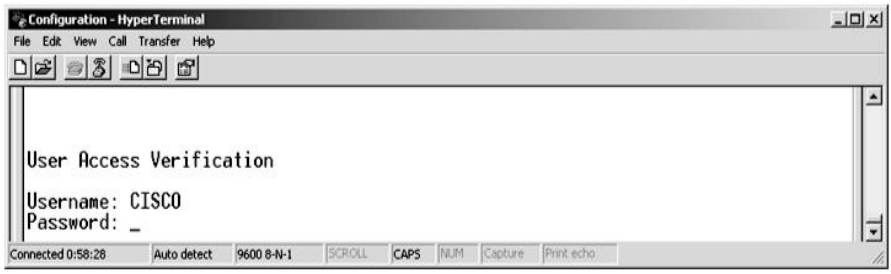
8.2.5.7 Шаг 7: применить аутентификацию к консоли

Следующие команды описывают, как применить конфигурацию аутентификации, созданную на шаге 5, к строке консоли.

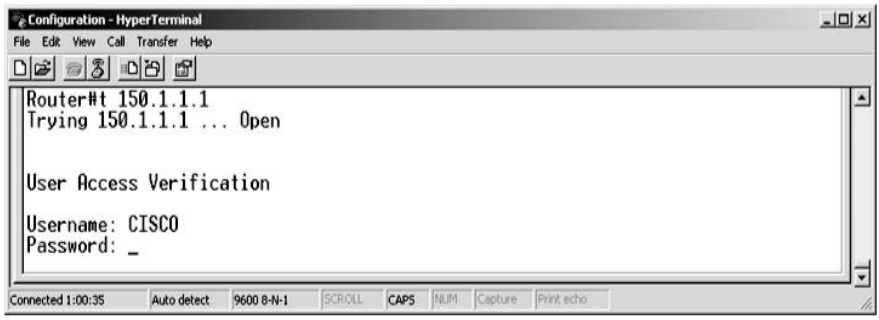


8. 2.5.8 Шаг 8: Проверьте консольную и Telnet аутентификацию

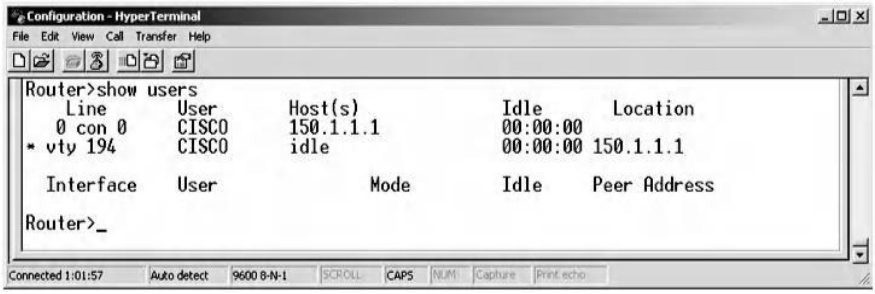
Используя команду «exit», появляется сообщение User Access Verification, потому что аутентификация для консоли настроена. Введите «CISCO» в качестве имени пользователя и пароля, как указано при создании локальной базы данных.



Затем, telnet 150.1.1.1, что приводит к сообщению о подтверждении доступа пользователя, поскольку аутентификация была настроена для Telnet. Затем введите «CISCO» в качестве имени пользователя и пароля.

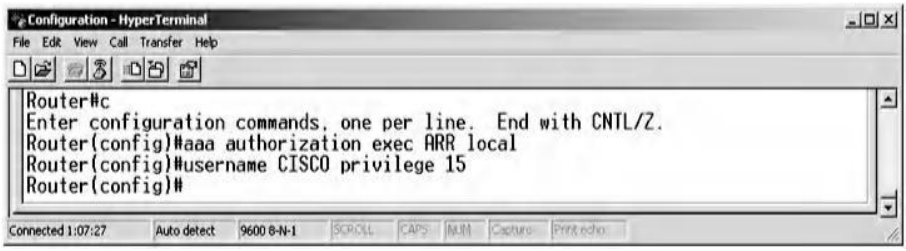


Чтобы отобразить пользователей, которые вошли в маршрутизатор, введите команду «show users». Команда указывает, что два пользователя вошли в систему. Один вошел в систему через консольную линию, а другой является пользователем Telnet.



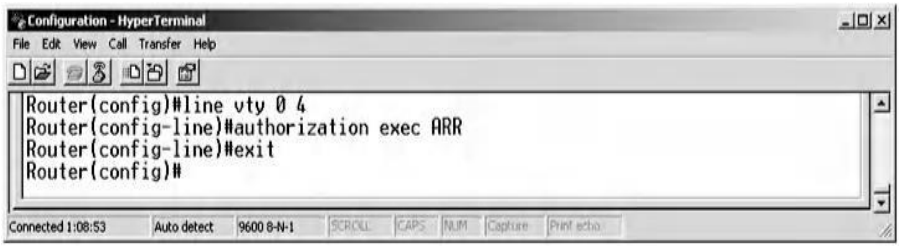
8.2.5.9 Шаг 9: Настройте модель AAA: Авторизация

Конфигурация авторизации требует указания метода, типа базы данных, имени пользователя и уровня привилегий, равного 15, как в следующих командах. Название используемого метода авторизации - ARR.



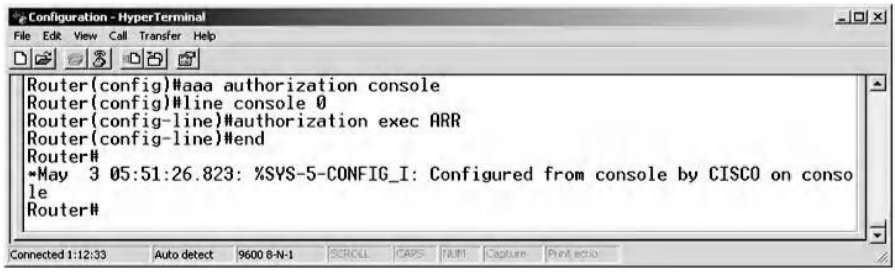
8.2.5.10 Шаг 10: Применить авторизацию к VTY

Следующая команда показывает, как применить метод авторизации (с шага 9) к VTY, который дает пользователю уровень привилегий 15.



8.2.5.11 Шаг 11: Применить авторизацию к консоли

Чтобы применить метод авторизации, начиная с шага 9, к строке консоли, введите следующую команду:



8. 2.5.12 Шаг 12: Проверьте консоль и авторизацию Telnet

Затем выполните команду «exit». Имя пользователя и пароль «CISCO» указаны для подтверждения доступа пользователя. Уровень привилегий по умолчанию 15 назначен пользователю, что означает, что пользователь авторизован для выполнения всех команд Cisco IOS на маршрутизаторе. Чтобы проверить уровень привилегий, используйте следующую команду:

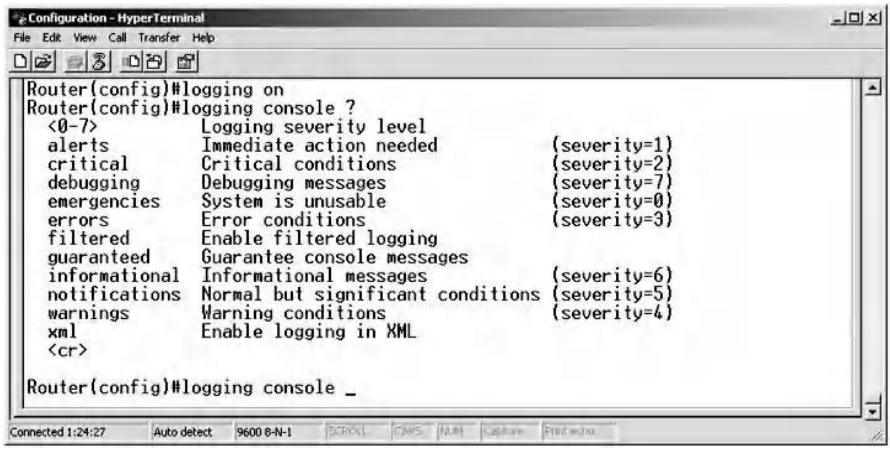
Затем, telnet 150.1.1.1, сообщение проверки доступа, появляется, потому что аутентификация и авторизация для VTY были настроены ранее. Введите «CISCO» в качестве имени пользователя и пароля; уровень привилегий 15 назначается непосредственно пользователю.

Чтобы убедиться, что у пользователя есть привилегия 15, используйте команду «show privilege».

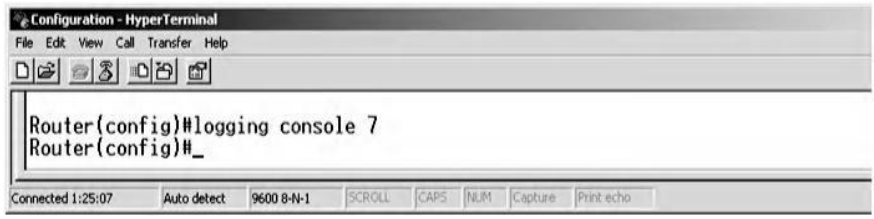
Наконец, отключите сеанс Telnet, введя команду выхода.

8.2.5.13 Шаг 13: Настройте ведение журнала консоли

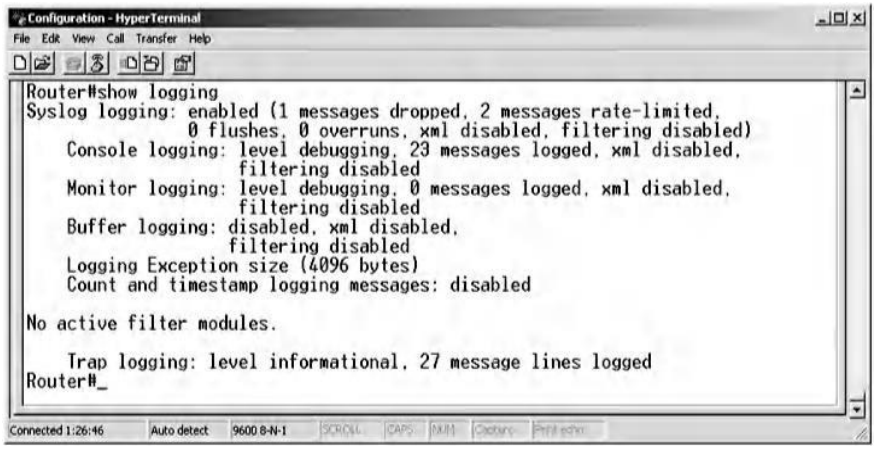
Чтобы перейти в режим настройки, используйте псевдоним «c» команды «configure terminal». Затем включите ведение журнала, введя команду «logging on». Затем используйте «logging console?», Которая отображает справку о доступных уровнях серьезности ведения журнала на маршрутизаторе Cisco IOS. Существует восемь уровней от 0 до 7. Уровень 0 регистрирует только аварийные события, а уровень 7 показывает сообщения отладки, как в следующих командах:



Уровень ведения журнала отладки - это полезный уровень, который показывает подробную информацию, которая полезна при устранении неполадок и обслуживании. Используйте команду «logging console 7», чтобы выбрать уровень серьезности 7 для отображения сообщений отладки на консоли.



Выйдите из режима конфигурации, а затем с помощью команды «show logging» проверьте, работает ли уровень ведения журнала консоли.



8.3 Лабораторная работа 8.2: безопасные сетевые службы

8.3.1 Результат

Целью обучения в этом упражнении является оценка функций безопасности маршрутизатора Cisco путем защиты сетевых служб.

8.3.2 Описание

Метод доступа по умолчанию для управления и настройки маршрутизатора - через консольный порт. Поскольку подключение напрямую связано с консольным портом, это относительно безопасный метод. Тем не менее, сетевые устройства обычно находятся в комнате,

где поддерживается очень низкая температура и довольно шумно, и поэтому администраторы предпочитают удаленный доступ к устройствам. Следовательно, на маршрутизаторах Cisco IOS поддерживаются различные протоколы удаленного интерактивного доступа, такие как Telnet, SSH, HTTP и HTTPS.

Возможно, протокол Telnet, описанный в RFC 854, является наиболее распространенным протоколом, используемым для удаленного подключения к сетевым устройствам. Это протокол клиент / сервер, которому назначен стандартный TCP-порт 23 для обеспечения удаленного входа в систему и доступа к командной строке (CLI) удаленного хоста. Уязвимость безопасности в Telnet заключается в том, что он не шифрует данные, которыми обмениваются его клиент и сервер. Следовательно, злоумышленник может подслушивать трафик и извлекать конфиденциальную информацию, такую как имена пользователей и пароли.

Протокол SSH, описанный в RFC 4253, предназначен для замены Telnet для исправления основного недостатка безопасности, который заключается в отправке данных в виде открытого текста. SSH - это протокол клиент-сервер, которому назначен стандартный TCP-порт 22. Он предлагает безопасный канал для удаленного входа в систему и доступа к сеансам CLI. Он использует криптографию с открытым ключом, обычно криптографический алгоритм RSA, и криптографические алгоритмы с симметричным ключом для обеспечения аутентификации, конфиденциальности данных и обеспечения безопасности целостности данных. Зашифровывая весь свой трафик, он эффективно защищает от нескольких атак, таких как прослушивание, перехват сеансов и атаки «человек посередине» (MiM).

Протокол HTTP (HyperText Transfer Protocol), описанный в RFC 26126, является протоколом прикладного уровня для World Wide Web (WWW). Он принимает архитектуру клиент / сервер и ему назначается стандартный TCP-порт 80. Клиент HTTP, как и веб-браузер, отправляет сообщение запроса на сервер HTTP для запроса ресурсов, таких как файлы HTML. HTTP-сервер возвращает ответное сообщение, предоставляющее запрошенный ресурс. Проблема безопасности с HTTP заключается в том, что весь его трафик является открытым текстом, что делает его уязвимым для перехвата атак.

HTTP secure или HTTP over SSL (HTTPS), описанный в RFC 2818, является безопасной альтернативой для HTTP. Он назначен стандартному TCP-порту 443 и использует архитектуру клиент / сервер. HTTPS использует протокол Secure Socket Layer / Transport Layer (SSL / TLS), описанный в RFC 5246, для создания безопасного канала между клиентами и серверами через общедоступную сеть, такую как Интернет. SSL / TLS имеет два основных уровня: уровень рукопожатия и уровень записи. В Handshake клиент и сервер согласовывают набор шифров, алгоритмы шифрования и хэширования и генерируют сеансовые ключи, используя криптографию с открытым ключом. Клиент аутентифицирует сервер, используя технологию цифровых сертификатов. Затем шифрование и дешифрование данных начинается на уровне записи. В настоящее время HTTPS широко распространен и используется почти повсеместно в Интернете для обеспечения эффективных решений в области безопасности и безопасности, таких как электронные транзакции, обмен почтой и поисковые системы.

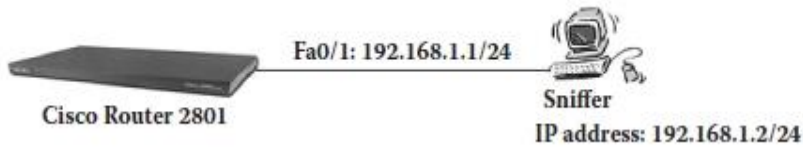
Эта практическая лаборатория устанавливает серверы Telnet, SSH, HTTP и HTTPS на маршрутизаторе Cisco IOS, чтобы продемонстрировать их слабость или силу безопасности. Он следует оскорбительному подходу, запуская атаки перехвата и анализа пакетов на эти сетевые службы для извлечения конфиденциальной информации, такой как имена пользователей и пароли.

8.3.3 Эксперимент

Для защиты сетевых служб на маршрутизаторе Cisco проводится эксперимент с использованием маршрутизатора Cisco 2801 с ОС 12.4. Ниже приводится описание и этапы эксперимента.

8.3.4 Архитектура сети

Архитектура сети, использованная в эксперименте, показана на следующем рисунке. Хост подключен к интерфейсу FastEthernet0/1 (Fa0 /1) маршрутизатора Cisco через прямые кабели. Анализатор CommView используется для анализа пакетов и определения действий по прослушиванию.



8.3.5 Шаги эксперимента

Эксперимент состоит из следующих этапов:

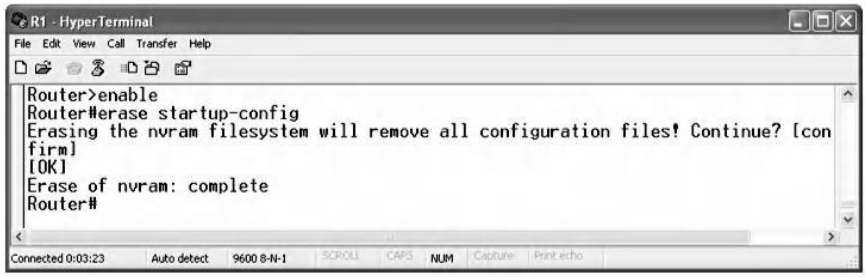
Шаг 1: Инициализация ПК и роутера.
Шаг 2: Сниффинг и анализирование ICMP-трафика.
Шаг 3: Сниффинг и анализирование Telnet-трафика.
Шаг 4: Сниффинг и анализирование SSH-трафика.
Шаг 5: Сниффинг и анализирование HTTP-трафика.
Шаг 6: Сниффинг и анализирование HTTPS-трафика.

8.3.5.1 Шаг 1: Инициализация ПК и маршрутизатора

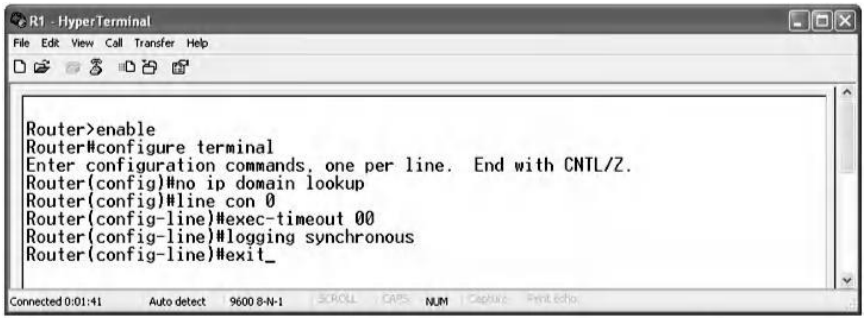
Назначьте ПК следующие параметры сети:

IP address (IP-адрес): 192.168.1.2
Subnet mask (Маска подсети): 255.255.255.0
Default gateway (Шлюз по умолчанию): 192.168.1.1

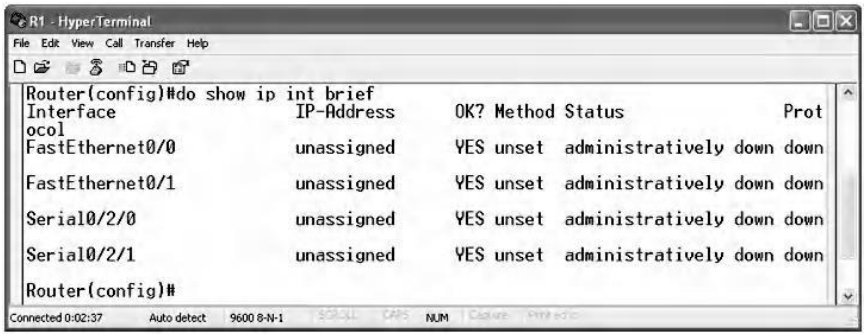
Для инициализации маршрутизатора подключите ПК к интерфейсу Fa0 / 1 маршрутизатора с помощью прямого кабеля. Затем подключите ПК к последовательной консоли маршрутизатора и запустите настройку с помощью Hyper Terminal. Чтобы стереть все предыдущие настройки, используйте следующую команду:



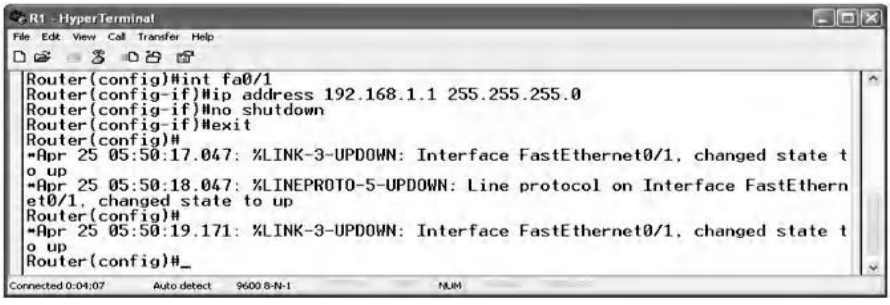
Используйте команду «reload» для перезагрузки системы, а затем отключите поиск DNS и синхронизируйте сообщения журналов, как показано в следующих командах:



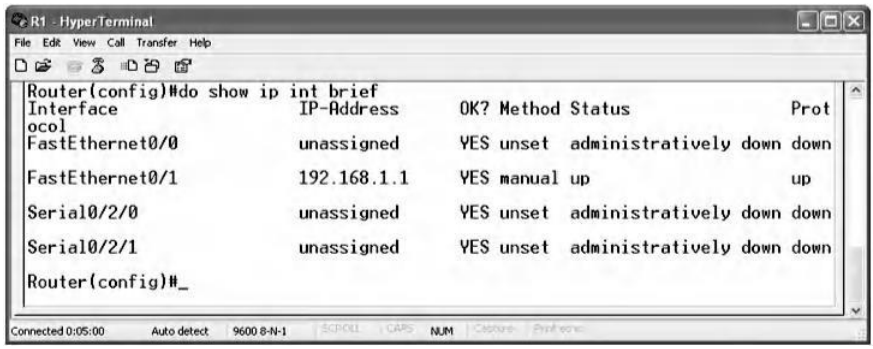
Чтобы просмотреть интерфейсы маршрутизатора, введите следующую команду:



Чтобы назначить IP-адрес 192.168.1.1 интерфейсу Fa0/1, используйте следующую команду:



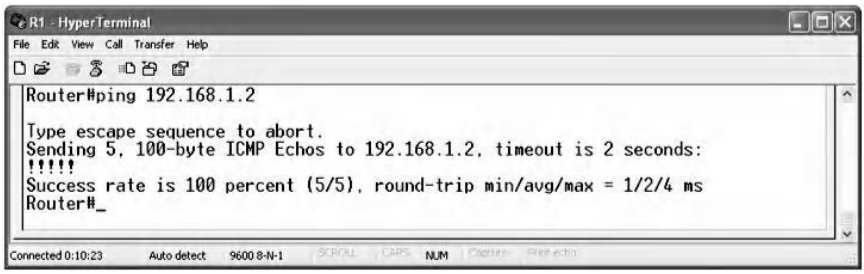
Проверьте назначение IP для интерфейсов маршрутизатора, используя следующую команду:



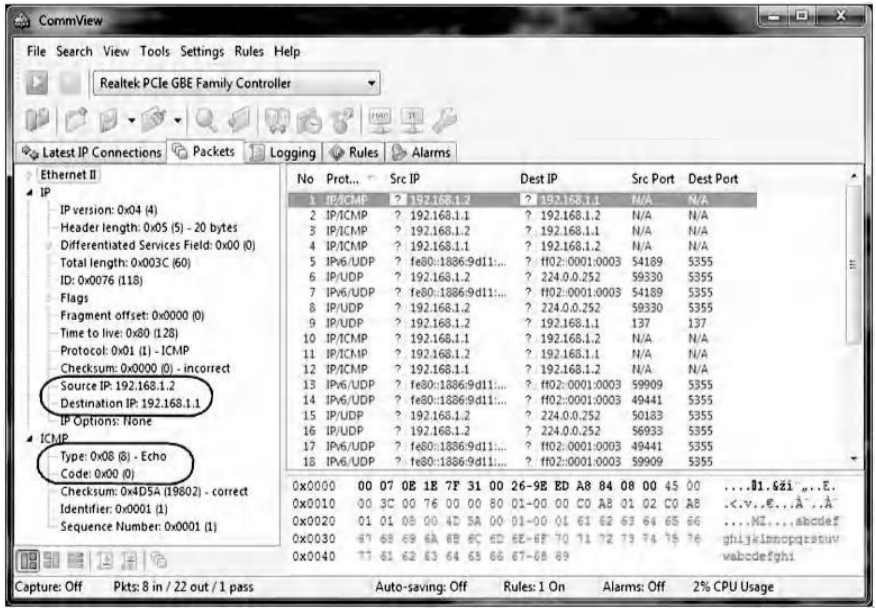
Анализатор CommView используется в этой лаборатории для запуска атаки перехвата на разных изучаемых сетевых протоколах.

8.3.5.2 Шаг 2: Сниффинг ICMP-трафика

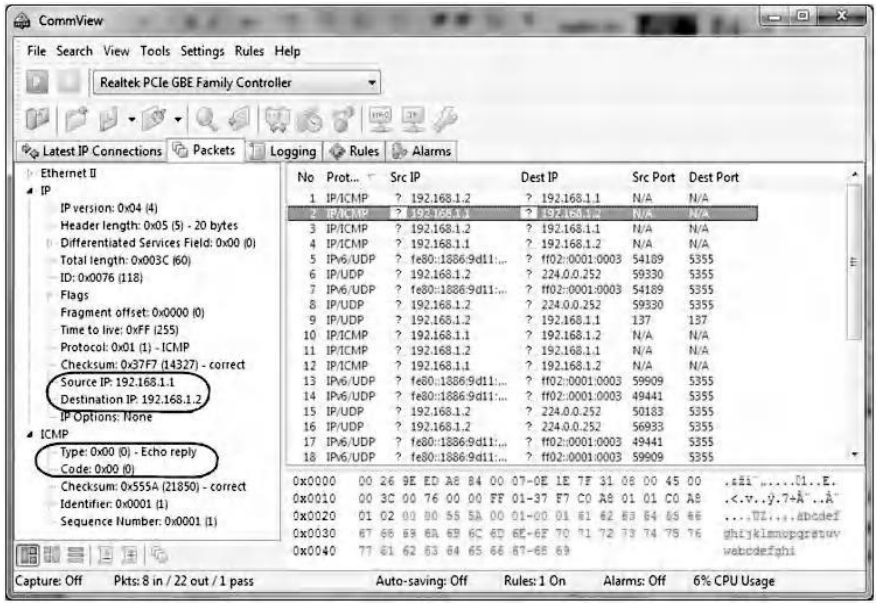
Выполните пинг ПК от маршрутизатора, чтобы обеспечить взаимосвязанность, и прослушать пакеты эхо-ответа ICMP и эхо-ответа.



На следующем снимке экрана показано содержимое эхо-пакета ICMP.

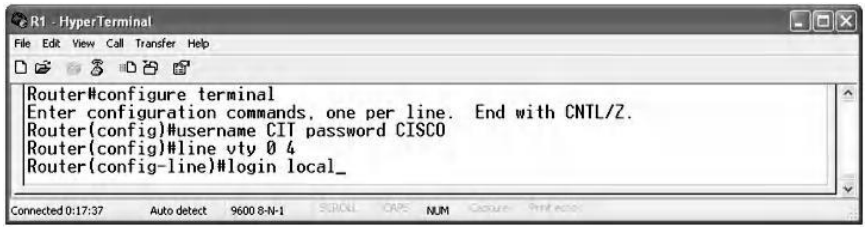


На следующем снимке экрана показано содержимое пакета эхо-ответа ICMP.



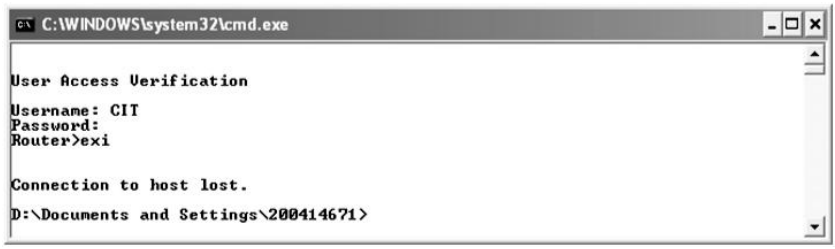
8.3.5.3 Шаг 3: Снифинг Telnet-трафика

Чтобы настроить учетные данные для аутентификации Telnet, создайте локальную базу данных и назначьте ее службе входа в линию VTY (Telnet), введя следующие команды:

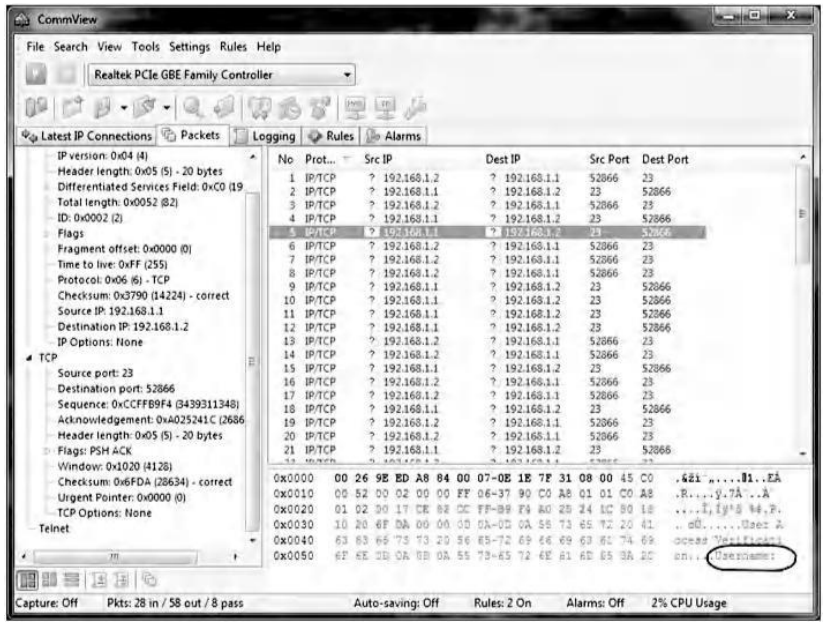


Telnet 192.168.1.1 (маршрутизатор) с ПК для генерации трафика Telnet с использованием встроенного клиента Telnet от Microsoft.

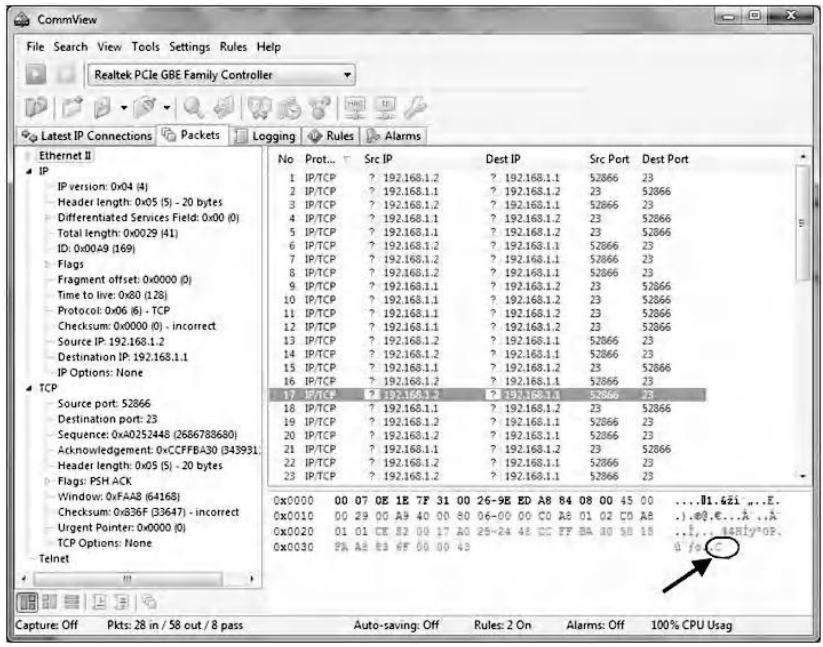
Когда появится окно подтверждения доступа пользователя, введите имя пользователя как «CIT» и пароль как «CISCO», как было настроено ранее.



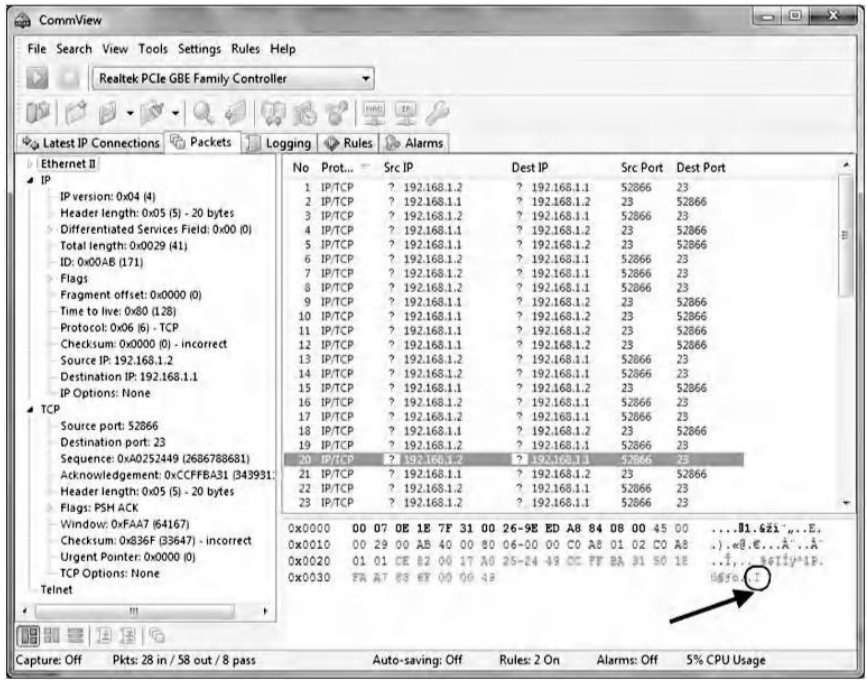
Обнаружение пакетов Telnet на порту 23. Как показано в следующих сериях снимков экрана, трафик Telnet не шифруется. Анализируя трафик, легко получить имя пользователя и пароль Telnet, которые отображаются символ за символом. Пакет TCP № 5, как показано на следующем снимке экрана, содержит подсказку сообщения подтверждения доступа пользователя.



Пакет TCP номер 17, как показано на следующем снимке экрана, содержит первый символ имени пользователя, который является «C».

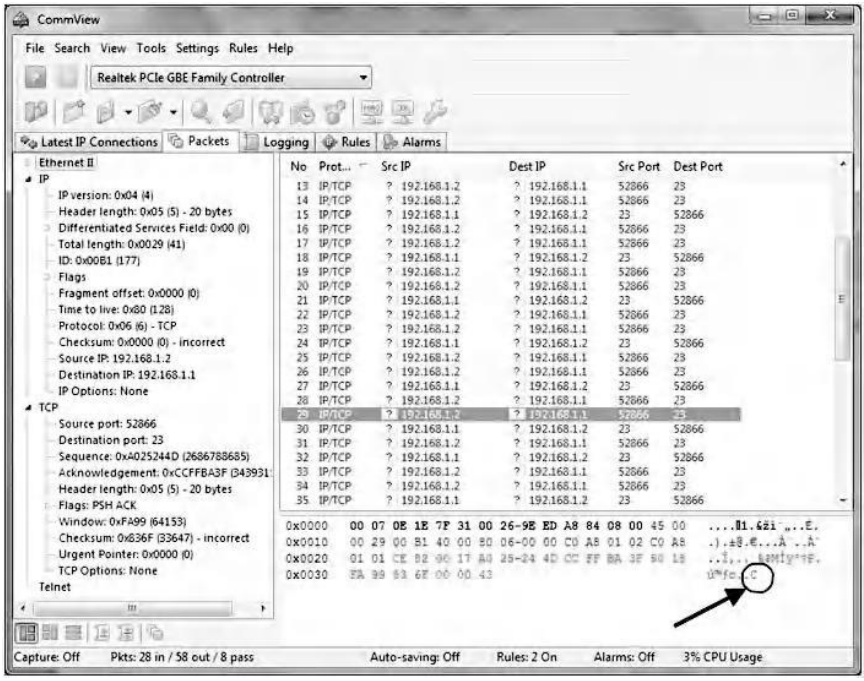


Пакет TCP номер 20, как показано далее, содержит второй символ имени пользователя, который является «I».



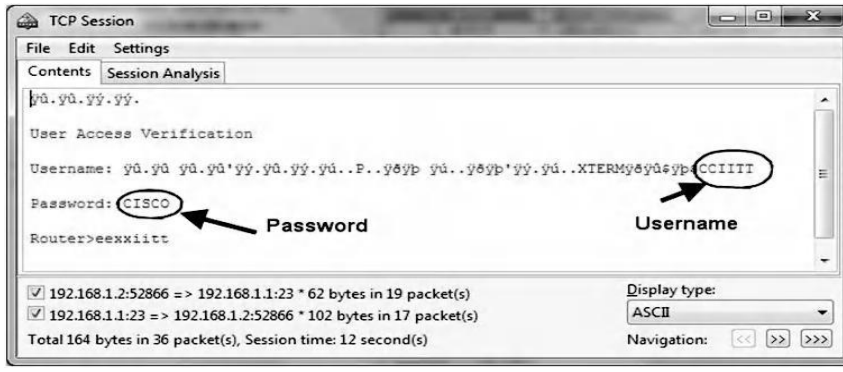
Последовательный TCP-пакет отображает последний символ имени пользователя, который является «T». Следовательно, прослушанное имя пользователя «CIT».

Пакет TCP номер 29, как показано на следующем снимке экрана, содержит первый символ пароля пользователя, который является «C».



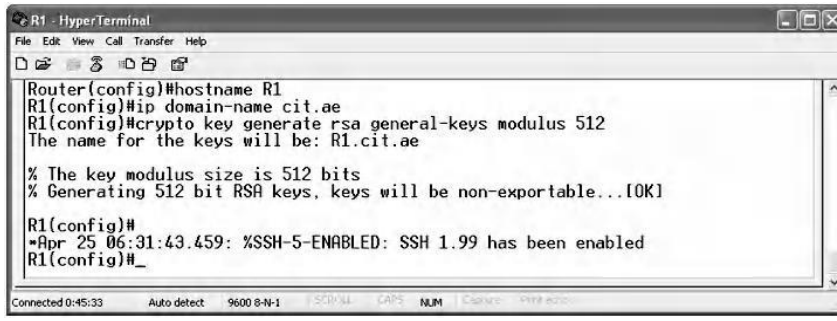
Последующие пакеты содержат оставшиеся символы пароля.

Используя сниффер CommView, сеанс TCP можно легко восстановить, чтобы отобразить имя пользователя и пароль в виде простого текста, как показано на следующем снимке экрана.

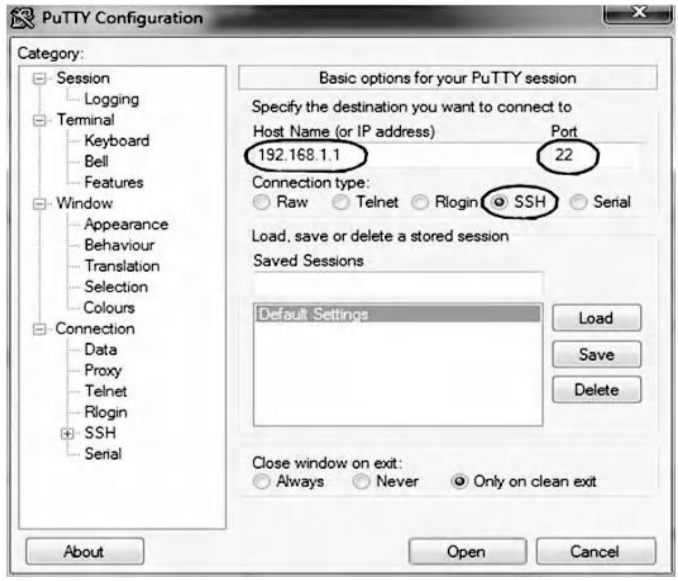


8.3.5.4 Шаг 4: Сниффинг SSH-трафика

Для запуска службы SSH на маршрутизаторе необходимо настроить имя хоста и имя домена, как показано в следующих командах. Кроме того, криптографические ключи RSA должны генерироваться с модульным размером 512 битов, что достаточно для выполнения упражнения, чтобы обеспечить быстрый процесс генерации ключа. Однако он считается слабым для промышленного стандарта, который требует размера модуля 1024 бит или даже 2048 бит.



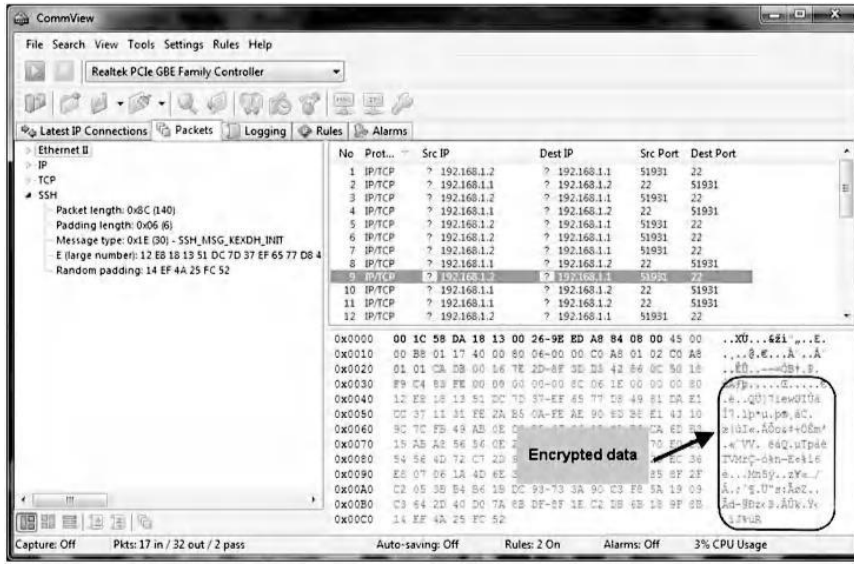
Запустите приложение «Putty» на ПК и введите IP-адрес 192.168.1.1 и TCP-порт 22 для удаленного маршрутизатора, как показано на следующем снимке экрана.



Нажмите на кнопку «Open», и соединение будет установлено. Нажмите «Yes», как показано ниже, чтобы добавить ключ SSH-сервера в кэш PuTTY.

Войдите на сервер SSH, используя те же учетные данные аутентификации сеанса Telnet, как показано ниже.

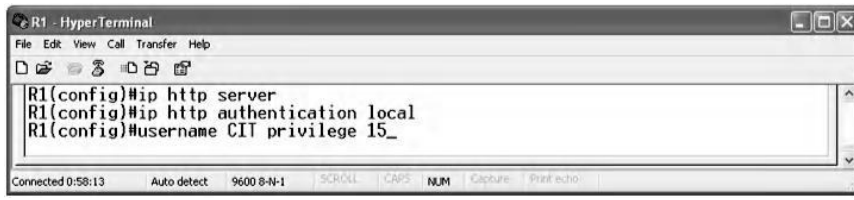
Наблюдайте за SSH-пакетами и перехватывайте их с помощью анализатора CommView. На следующем снимке экрана показано, что сеанс SSH зашифрован, и, следовательно, злоумышленник не может использовать какой-либо захваченный пакет.



Поэтому сетевой администратор должен заменить незащищенную службу Telnet на безопасную службу SSH, чтобы защитить данные проверки подлинности и управления от таких атак, как перехват, перехват сеансов и атаки MiM.

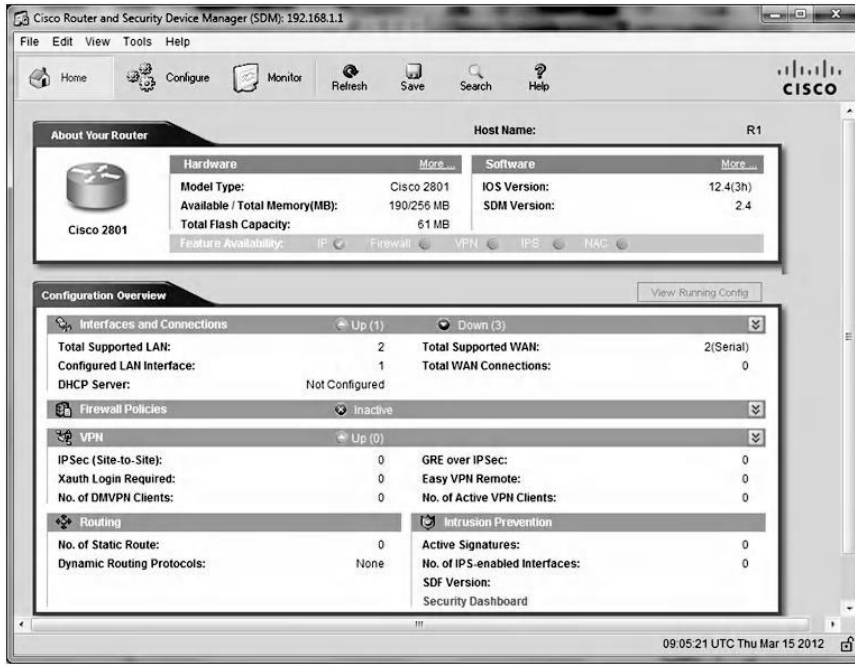
8.3.5.5 Шаг 5: Сниффинг HTTP-трафика

Чтобы запустить службу HTTP на маршрутизаторе, укажите тип базы данных аутентификации, которая является локальной в этом эксперименте. Он обозначает уровень привилегий 15 для пользователя CIT.



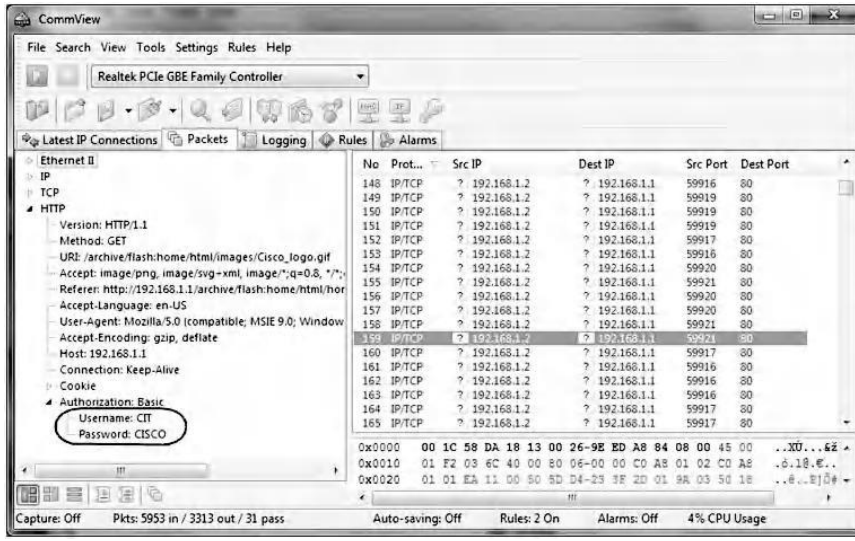
Перейдите по следующему URL-адресу: HTTP://192.168.1.1 на своем ПК и войдите в систему, введя «CIT» в качестве имени пользователя и «CISCO» в качестве пароля, как показано ниже.

Нажмите «ОК», чтобы получить доступ к веб-интерфейсу пользователя маршрутизатора (WebUI), который можно использовать для выполнения большинства задач, которые можно выполнить с помощью интерфейса командной строки, как показано на следующем снимке экрана.



Выполните сниффинг HTTP-пакетов и проанализируйте их, чтобы убедиться, что HTTP-трафик не зашифрован. Выбранный пакет

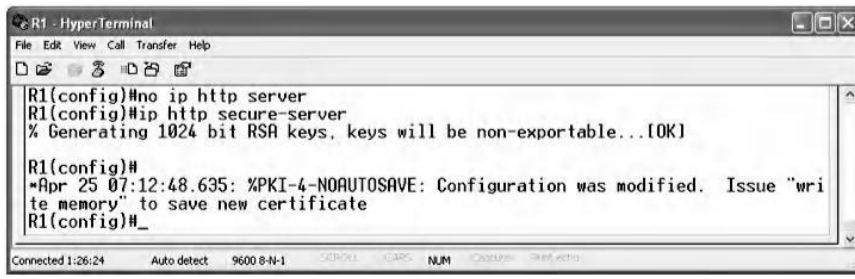
отображает имя пользователя и пароль в явном виде в заголовке HTTP, как показано на левой панели следующего экрана.



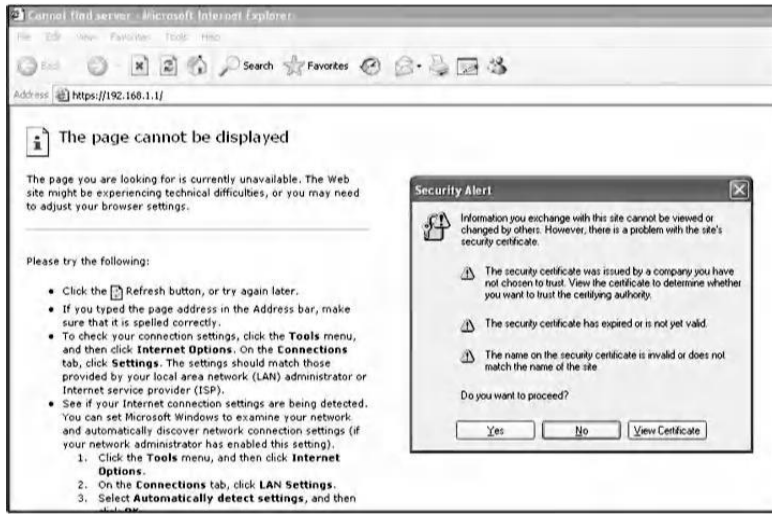
8.3.5.6 Шаг 6: Сниффинг HTTPS-трафика

Для запуска службы HTTPS используются следующие команды, которые сгенерируют

- ❿ Требуемые ключи RSA размером 1024 бита в этом примере
- ❿ Новый SSL-сертификат для аутентификации сервера HTTPS

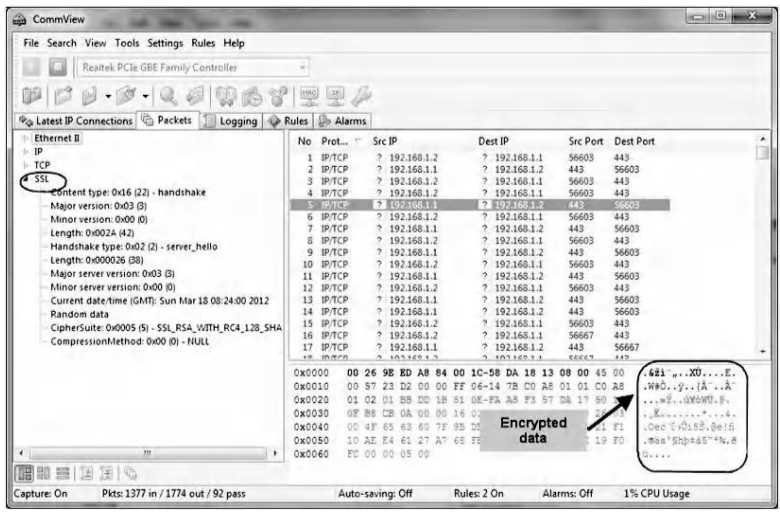


От клиента HTTPS (ПК) перейдите к веб-серверу маршрутизатора, используя URL: HTTPS://192.168.1.1. Важно отметить, что теперь HTTPS используется вместо HTTP, как показано на следующем снимке экрана.



Когда появится предупреждение безопасности SSL-сертификата, нажмите «Yes», чтобы принять сертификат безопасности SSL. Введите имя пользователя и пароль для доступа к веб-странице маршрутизатора с уровнем привилегий 15.

Наблюдайте за HTTPS-пакетами на порту 443 и анализируйте их. Весь трафик HTTPS через TCP-порт 443 зашифрован, как показано на следующем снимке экрана. Следовательно, этот эксперимент ясно демонстрирует, что HTTPS должен заменить HTTP для безопасного доступа к веб-интерфейсу маршрутизатора.



8.4 Лабораторная работа 8.3: фильтрация пакетов на пограничном маршрутизаторе

8.4.1 Результат

Цель данного упражнения - научить студентов настраивать фильтрацию пакетов с отслеживанием состояния на маршрутизаторе Cisco.

8.4.2 Описание

Фильтрация пакетов является важнейшей задачей пограничных маршрутизаторов, поскольку они представляют точки входа в сети и внутренние ресурсы. Поэтому управление трафиком в этих точках входа является первой линией защиты сетевой инфраструктуры. С другой стороны, успешные атаки на пограничные маршрутизаторы приводят к серьезным угрозам безопасности для всей сети.

Основным механизмом, используемым на маршрутизаторе Cisco IOS для реализации фильтрации пакетов, является список контроля доступа (ACL). ACL состоит из трех основных частей, а именно действия, которое может разрешить или запретить пакеты, критериев соответствия и направления, которое входит или выходит. Критерии соответствия определяют, какие поля заголовка пакета будут проверяться для принятия решений о фильтрации пакетов. На основе критериев сопоставления списки ACL подразделяются на два типа: (1) стандартные списки ACL, которые совпадают только по исходному IP-адресу; и (2) Расширенные списки ACL, которые соответствуют IP-адресу источника, IP-адресу назначения, протоколам, порту источника, порту назначения и флагам TCP.

Важно реализовать RFC 1918 и RFC 2827 на пограничном маршрутизаторе. Это помогает защитить от нескольких известных атак DoS (отказ в обслуживании). RFC 1918 определяет диапазоны частных IP-адресов, которые не маршрутизируются ни в одной общедоступной сети, такой как Интернет. Поэтому он зарезервирован для внутреннего использования сети. Эти частные диапазоны адресов следующие:

Class A: 10.0.0.0–10.255.255.255

Class B: 172.16.0.0–172.31.255.255

Class C: 192.168.0.0–192.168.255.255

RFC 2827 рассказывает о различных методах входной фильтрации для защиты от DoS-атак с использованием подмены IP-адресов. RFC сообщает, что политика входной фильтрации пограничных маршрутизаторов должна блокировать эти частные адреса, адреса RFC 1918, на его внешних интерфейсах. Кроме того, одной из основных рекомендаций RFC 2827 является отклонение пакетов с исходными IP-адресами, которые совпадают с IP-адресами вашей сети. Единственная причина этого состоит в том, что злоумышленник подделал ваши собственные IP-адреса, чтобы обойти ваши меры безопасности или запустить DoS-атаки на вашу сеть. Известный пример этого типа DoS-атаки - DoS-атака Smurf.

Всякий раз, когда настраивается правило фильтрации пакетов, пограничный маршрутизатор действует как межсетевой экран, который разделяет сеть на два сегмента: доверенный сегмент, который является защищенной сетью, и ненадежный сегмент, который является внешней сетью, такой как Интернет. , Большинство стандартных протоколов, таких как HTTP, SMTP и FTP, возвращают трафик из ненадежных в доверенные сегменты, которые должны быть разрешены для завершения сеанса TCP. Это может быть достигнуто на маршрутизаторе Cisco IOS путем использования управления доступом на основе контекста (CBAC), который обеспечивает фильтрацию пакетов с отслеживанием состояния. CBAC создает таблицу сеансов для соединений, проходящих через маршрутизатор, от доверенного до ненадежного сегмента. В таблице сеансов хранится такая информация, как IP-адреса источника и назначения, порты источника и назначения, а также количество активных сеансов.

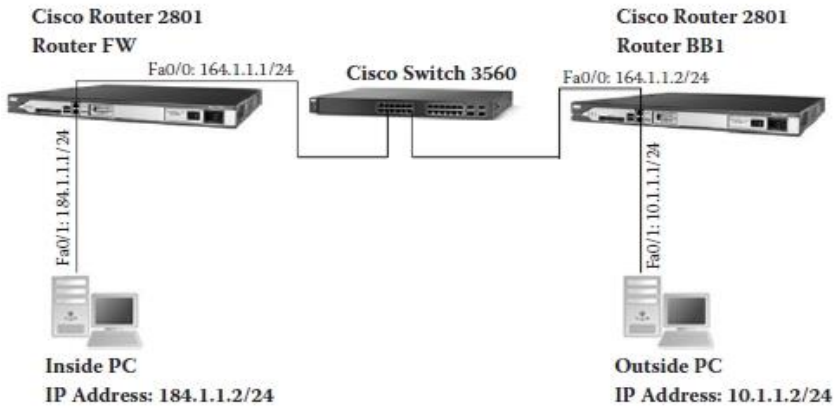
Это практическое лабораторное упражнение демонстрирует, как реализовать фильтрацию пакетов на пограничном маршрутизаторе. Сетевая архитектура имитирует реальную сеть, в которой граничный маршрутизатор подключен к магистральному маршрутизатору поставщика услуг Интернета (ISP). Для простоты защищенная сеть в доверенном сегменте и сеть ISP в ненадежном сегменте моделируются двумя хостами. Все вышеперечисленные меры безопасности настроены и тщательно протестированы.

8.4.3 Эксперимент

Чтобы узнать, как защитить пограничный маршрутизатор и настроить фильтрацию пакетов с отслеживанием состояния, проводится эксперимент с использованием маршрутизатора Cisco 2801 с ОС 12.4 и коммутатором Cisco 3560. Ниже приведено описание и этапы эксперимента.

8.4.4 Архитектура сети

На следующем рисунке показана сетевая архитектура эксперимента. Как показано на рисунке, внутренняя сеть будет состоять из внутреннего ПК с IP-адресом 184.1.1.2/24, подключенного к маршрутизатору FW через интерфейс Fa0 / 1. Внешняя сеть состоит из магистрального маршрутизатора BB1, который должен быть частью ISP, и внешнего ПК с IP-адресом 10.1.1.2/24.



8.4.5 Шаги эксперимента

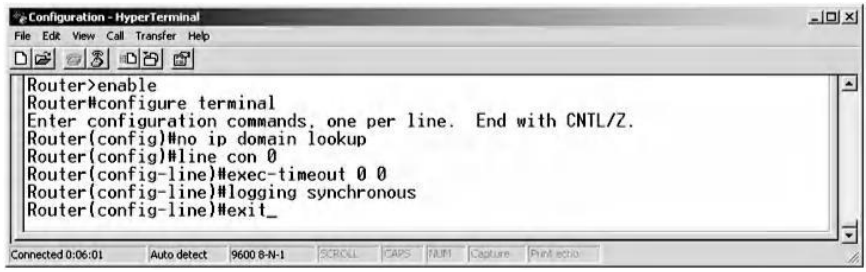
Эксперимент состоит из следующих этапов:

Шаг 1: Основные команды настройки маршрутизатора.
Шаг 2: Включите буферизованное ведение журнала на уровне отладки.
Шаг 3: Инициализируйте маршрутизаторы и ПК: IP-адреса и имена хостов.
Шаг 4: Запустите динамическую маршрутизацию: область OSPF 0 с перераспределением.

Шаг 5: Запустите серверы HTTP и Telnet на обоих маршрутизаторах.
Шаг 6: Реализуйте политики безопасности на пограничном маршрутизаторе.
Шаг 7: Проверьте политики безопасности, созданные на шаге 6.

8.4.5.1 Шаг 1: Основные команды настройки маршрутизатора

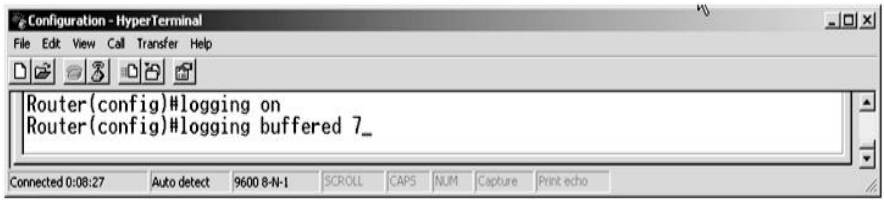
Подключите внутренний компьютер к последовательной консоли маршрутизатора через HyperTerminal, чтобы получить интерфейс командной строки маршрутизатора FW. Используйте команду «enable», чтобы маршрутизатор перешел в привилегированный режим EXEC. Чтобы отключить поиск DNS, используйте команду «no ip domain lookup»; и для синхронизации сообщений журнала введите следующие команды:



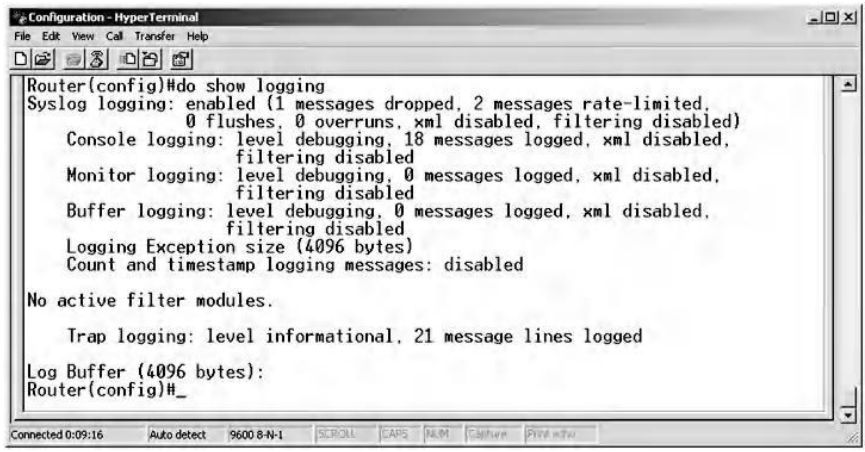
Те же шаги повторяются для маршрутизатора BB1 на внешнем ПК.

8.4.5.2 Шаг 2. Включите буферизованное ведение журнала на уровне отладки.

В режиме конфигурации включите ведение журнала с уровнем серьезности ведения журнала уровня 7. Учетная информация хранится локально в файле на маршрутизаторе, поскольку выбран тип буферизации в буфере, как в следующих командах:



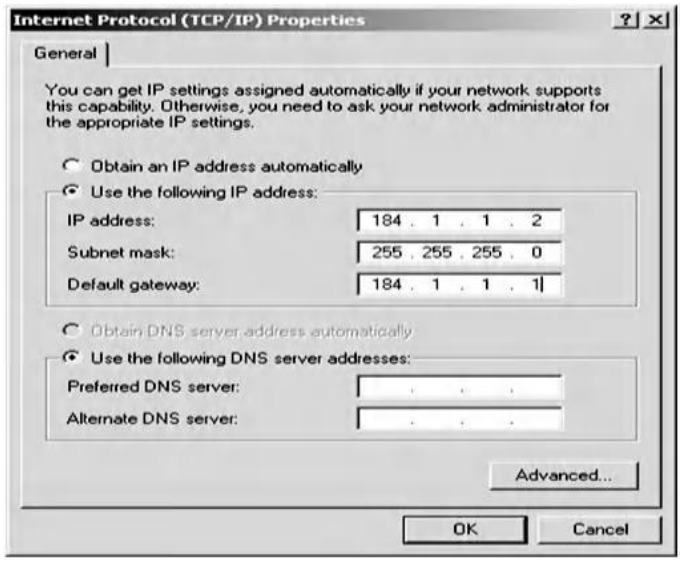
Чтобы убедиться, что ведение журнала работает, используйте команду «do show logging»:



Повторите шаг 2 для маршрутизатора BB1.

8.4.5.3 Шаг 3. Инициализация маршрутизаторов и ПК: IP-адреса и имена хостов

Назначьте следующие параметры сети для ПК внутренней сети:

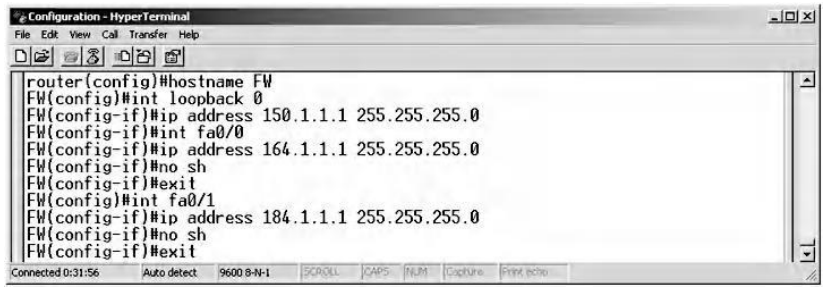


Назначьте следующие параметры сети на ПК внешней сети:

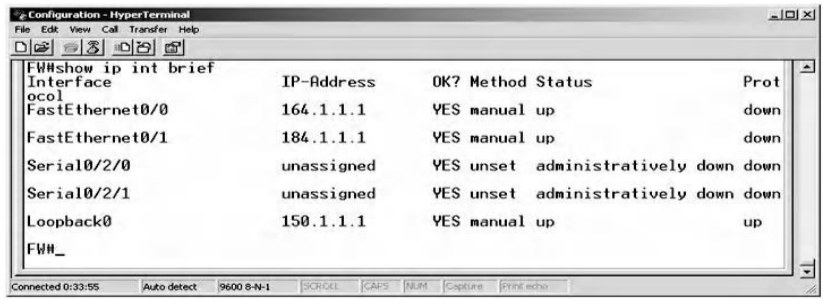
* IP Address: 10.1.1.2
* Subnet mask (Маска подсети): 255.255.255.0
* Default gateways (Шлюз по умолчанию): 10.1.1.1

Шаги конфигурации для маршрутизатора FW:

* Присвойте имя хосту, который является FW в нашем эксперименте.
* Создайте интерфейс Loopback, который будет использоваться в качестве идентификатора для процесса маршрутизации OSPF.
* Назначьте IP-адрес 164.1.1.1 интерфейсу Fa0/0 маршрутизатора FW.
* Назначьте IP-адрес 184.1.1.1 интерфейсу Fa0/1 маршрутизатора FW.

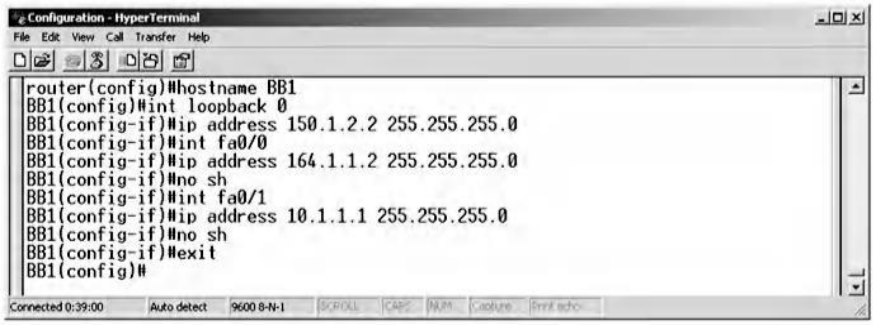


Чтобы проверить настроенные адреса для маршрутизатора FW, введите следующую команду:

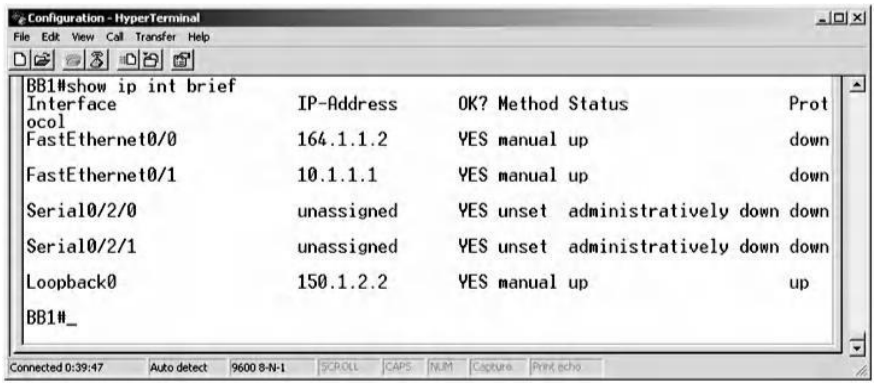


Аналогично, следующие шаги выполняются для маршрутизатора BB1:

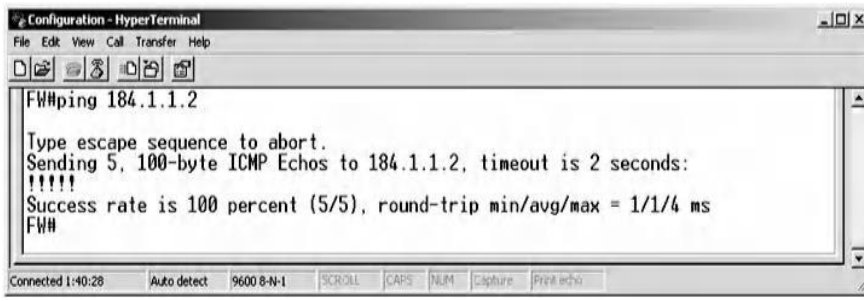
* Присвойте имя хосту - BB1 в нашем эксперименте.
* Создайте интерфейс Loopback, который будет использоваться в качестве идентификатора для процесса маршрутизации OSPF.
* Назначьте IP-адрес 164.1.1.2 интерфейсу Fa0/0 маршрутизатора BB1.
* Назначьте IP-адрес 10.1.1.1 интерфейсу Fa0/1 маршрутизатора BB1.



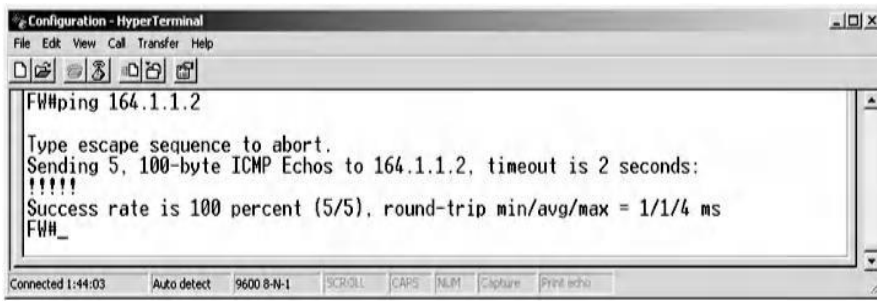
Чтобы отобразить адреса, которые вы только что настроили для интерфейса маршрутизатора BB1, введите следующую команду:



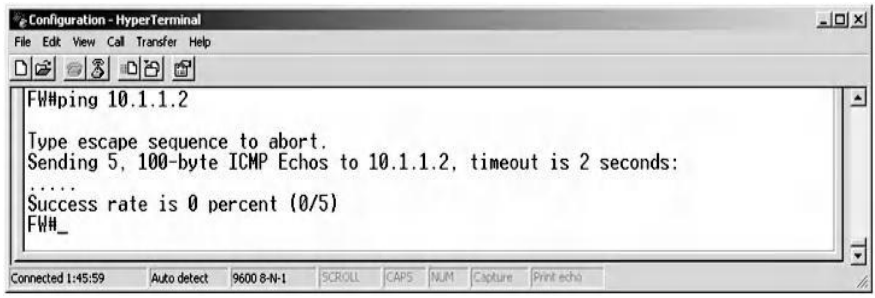
Проверьте подключение к сети, сначала отправив эхо-запрос на внутренний компьютер с маршрутизатора FW.



Затем выполните команду ping для следующего перехода маршрутизатора FW, который является 164.1.1.2, который должен быть успешным, как в следующей команде:



Далее пингуем конец внешней сети. Это не должно быть успешным, потому что не был настроен протокол динамической маршрутизации, такой как OSPF.



Наконец, пинг с внутреннего компьютера на внешний компьютер. Это не должно быть успешным из-за отсутствия протокола динамической маршрутизации, как в следующей команде:

8.4.5.4 Шаг 4: Запустите динамическую маршрутизацию: область OSPF 0 с перераспределением

Маршрутизация - это процесс выбора лучших путей к различным пунктам назначения в сети. Существует два типа маршрутизации: статическая и динамическая. Статическая маршрутизация использует ручную настройку для указания путей к пунктам назначения. В нашем примере он используется на ПК, когда настроен шлюз по умолчанию. С другой стороны, динамическая маршрутизация достигает своей цели, заполняя таблицу маршрутизации маршрутами к напрямую подключенным сетям. Затем он динамически узнает о маршрутах в другие сети из объявлений о маршрутах других маршрутизаторов, использующих тот же протокол динамической маршрутизации, таких как: протокол OSPF, протокол маршрутизации информации (RIP) или протокол промежуточной системы в промежуточную систему (IS-IS). Затем маршрутизатор выбирает лучшие пути к различным пунктам назначения на основе метрики стоимости маршрутизации.

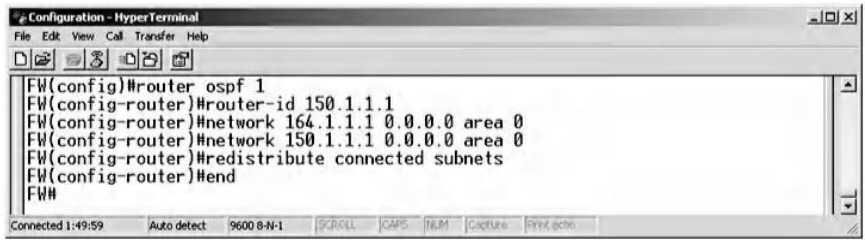
OSPF, описанный в RFC 2328, является широко используемым протоколом маршрутизации для корпоративных сетей. Он собирает информацию о состоянии канала от других маршрутизаторов для создания топологии всей сети, что помогает построить таблицу маршрутизации. Лучшие маршруты выбираются на основе алгоритма кратчайшего пути, известного также как алгоритм Дейкстры. Для облегчения администрирования и оптимизации трафика OSPF разбивает сеть на области, где область 0 считается магистральной областью.

Для запуска динамической маршрутизации на маршрутизаторе FW выполняются следующие шаги.

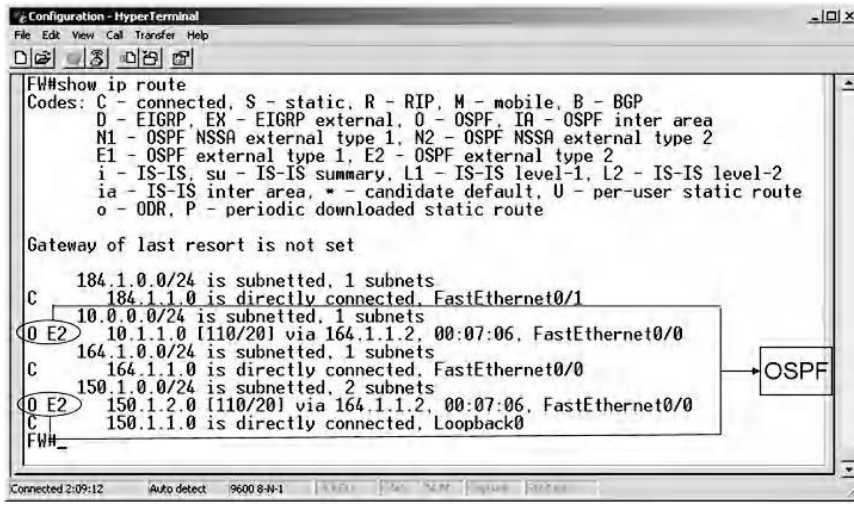
* Установите для идентификатора локального процесса протокола маршрутизации OSPF значение 1.

* Используйте интерфейс Loopback в качестве идентификатора маршрутизатора.

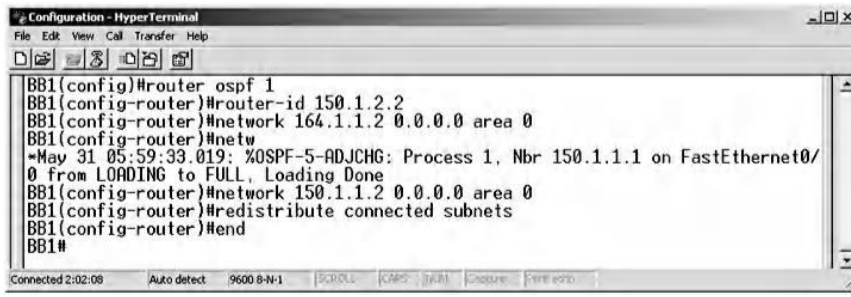
* Присвойте интерфейс маршрутизатора FW области 0 и перераспределите объявление о маршрутизации в напрямую подключенные сети, используя команды ниже:



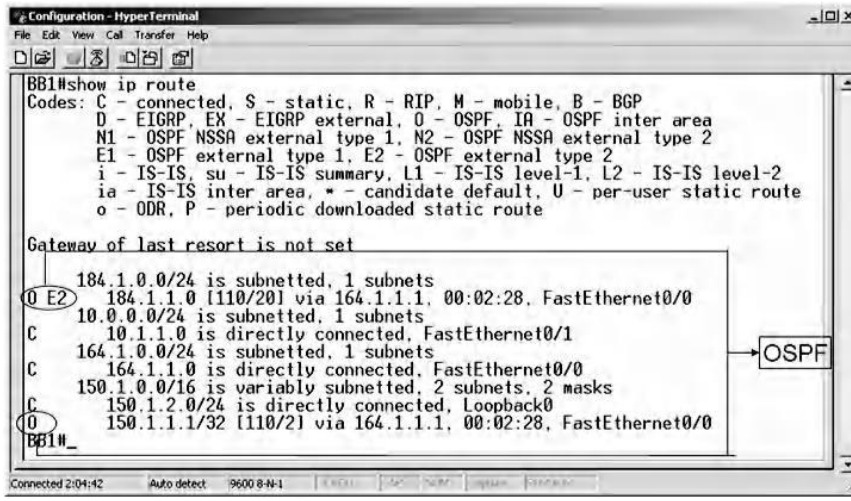
Показать таблицу маршрутизации в маршрутизаторе FW с помощью команды «show ip route». Записи маршрутизации, которые начинаются с «O», представляют OSPF, а «C» обозначает подключенные сети.



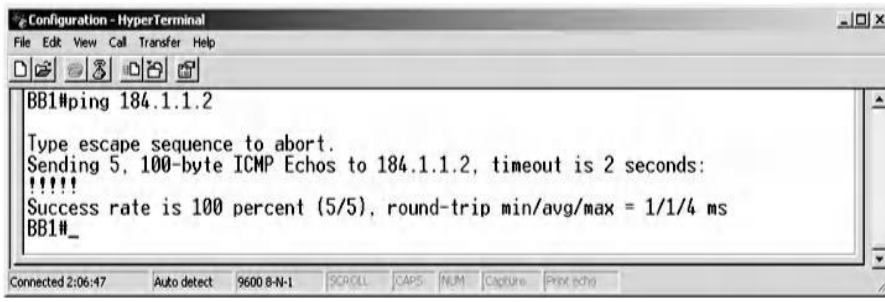
Настройте динамическую маршрутизацию на маршрутизаторе BB1, повторив предыдущий шаг для маршрутизатора FW, но с соответствующими сетевыми IP-адресами, как в следующей команде:



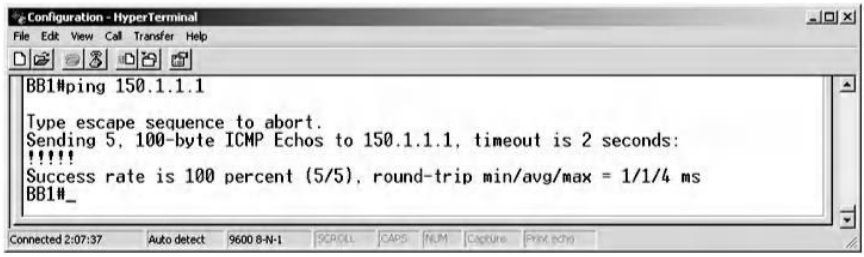
Показать таблицу маршрутизации на маршрутизаторе BB1 с помощью команды «show ip route»:



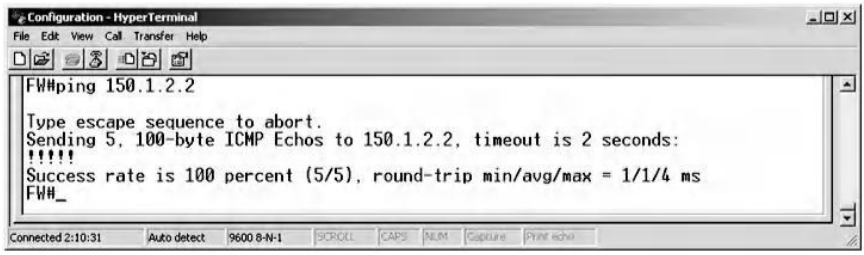
Проверьте подключение к сети, отправив эхо-запрос на внутренний компьютер с маршрутизатора BB1, что успешно, поскольку BB1 узнает о внутренней сети из записей таблицы маршрутизации OSPF.



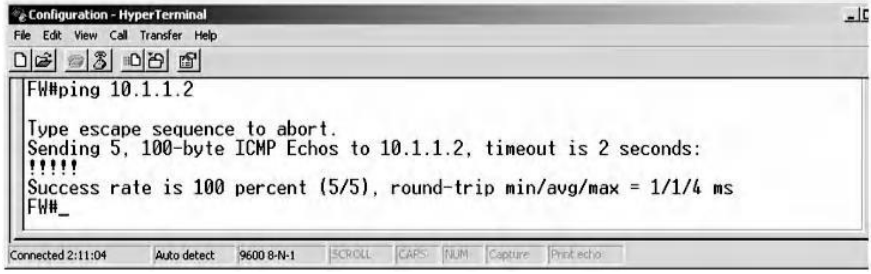
Затем пропингуйте интерфейс обратной связи, который должен быть успешным.



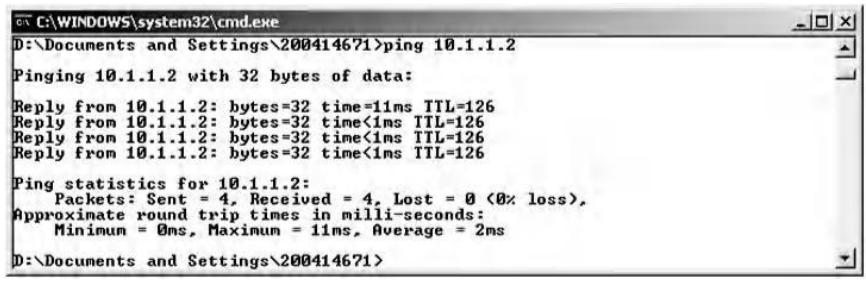
Затем выполните команду ping 150.1.2.2 с маршрутизатора FW, что должно быть успешным.



Далее пингуйте внешний компьютер от роутера FW. Это должно быть успешным, потому что протокол OSPF включен.



Наконец, выполните команду ping с внутреннего компьютера на внешний компьютер, что должно быть успешным, поскольку настроен протокол динамической маршрутизации OSPF.



Это гарантирует, что сквозная связь теперь установлена по всей сети.

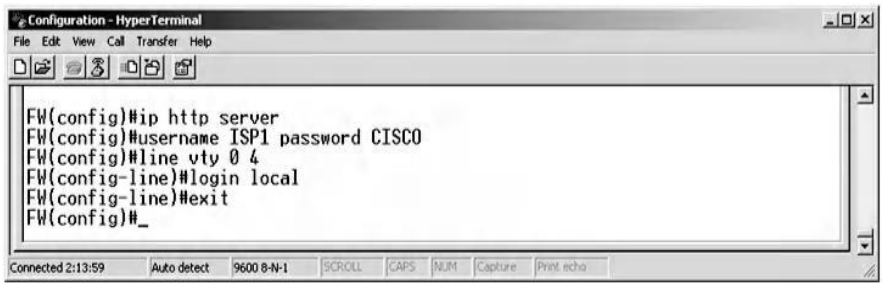
8.4.5.5 Шаг 5: Запустите серверы HTTP и Telnet на обоих маршрутизаторах

Запустите серверы HTTP и Telnet на маршрутизаторе FW, выполнив следующие шаги настройки:

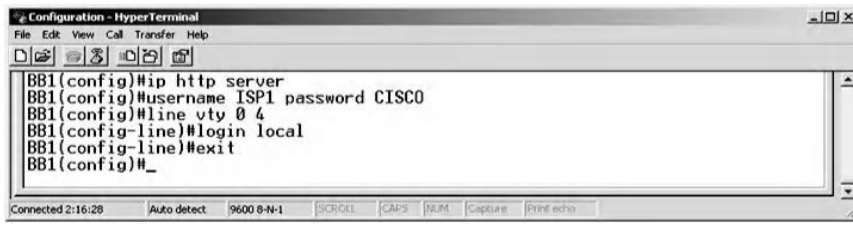
* Включите HTTP-сервер на маршрутизаторе с помощью команды «ip HTTP server».

* Настройте имя пользователя и пароль для целей аутентификации Telnet.

* Включите службу Telnet, чтобы разрешить пользователю подключаться к маршрутизатору через линию VTY.

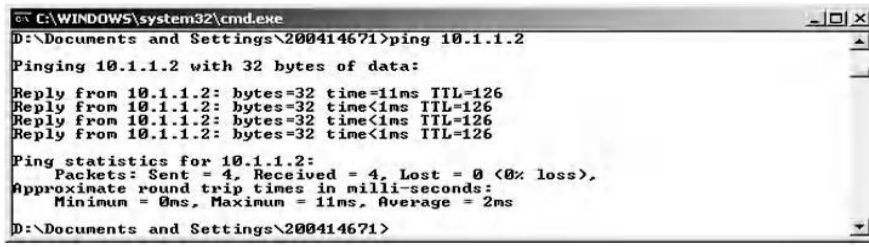


Настройте серверы HTTP и Telnet на маршрутизаторе BB1; повторите шаги для маршрутизатора FW.



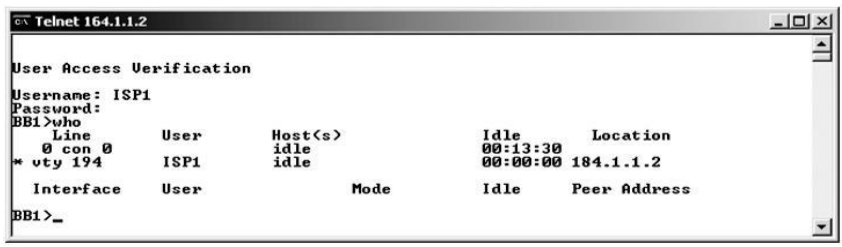
Проверьте конфигурацию шага 5, выполнив следующие шаги:

* Во-первых, проверьте сквозную связь, выполнив эхо-тестирование внешнего компьютера с внутреннего компьютера (Ping 10.1.1.2). Это должно быть успешным.

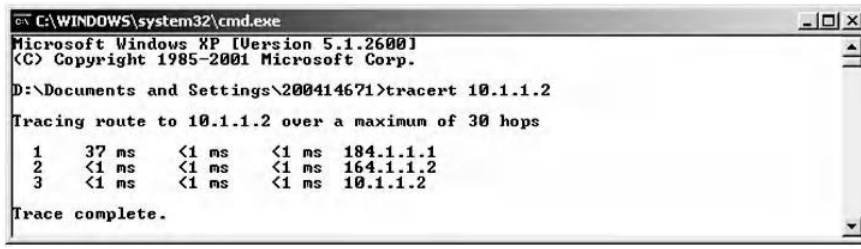


* Пингуйте внутренний компьютер с внешнего компьютера (ping 184.1.1.2), что должно быть успешным. Используйте браузер для навигации к роутеру BB1 (HTTP://164.1.1.2). Аналогичным образом перейдите с внешнего компьютера на маршрутизатор FW(HTTP://164.1.1.1).

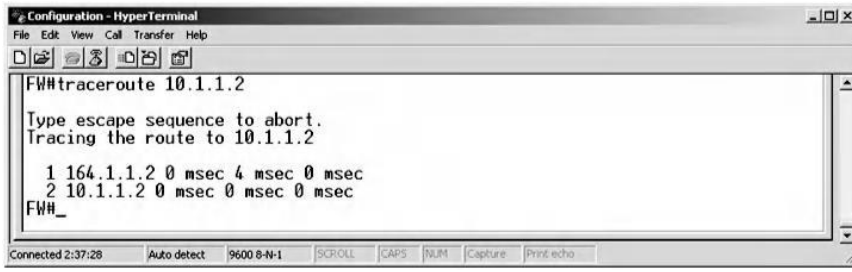
* Telnet от внутреннего компьютера до маршрутизатора BB1 (telnet 164.1.1.2), который должен быть успешным. Запрашивается подтверждение доступа пользователя, для которого используются настроенные имя пользователя и пароль для маршрутизатора BB1.



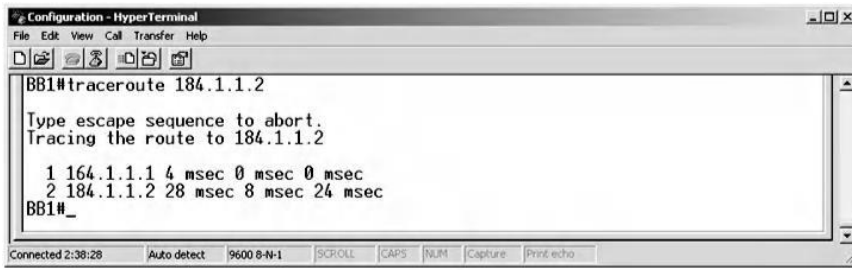
* Используйте Telnet для подключения внешнего компьютера к маршрутизатору FW (telnet 164.1.1.1). Затем с внутреннего ПК проследите маршрут к внешнему ПК («tracert 10.1.1.2»). Traceroute помогает проверить количество прыжков, которые сетевой трафик совершает, чтобы достичь пункта назначения. Обратите внимание, что есть три ряда. В каждой строке есть столбец со значением, которое представляет количество остановок на пути маршрута. Другие три столбца - это время в миллисекундах, которое используется при попытке достичь места назначения. Последний столбец - это IP-адрес хоста, который ответил.



* Затем с внешнего компьютера проследите маршрут к внутреннему компьютеру («tracert 184.1.1.2»). Затем проследите маршрут от маршрутизатора FW до внешнего компьютера («traceroute 10.1.1.2»).



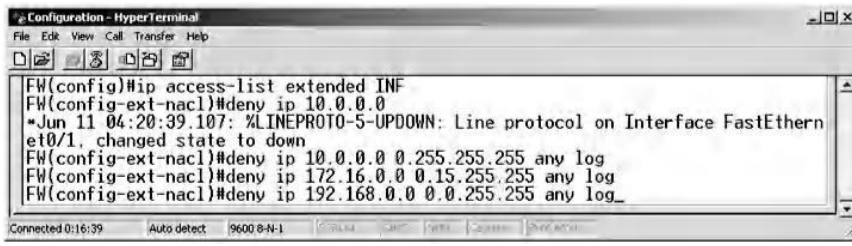
* Наконец, проследите маршрут от маршрутизатора BB1 до внутреннего ПК («traceroute 184.1.1.2»).



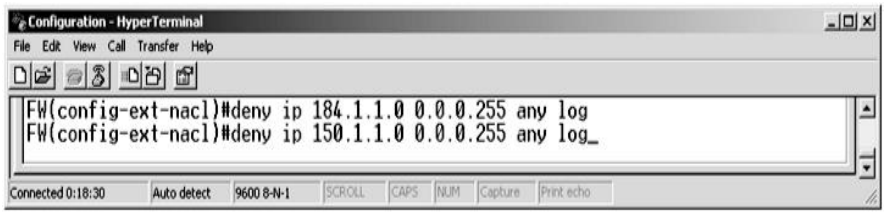
8.4.5.6 *Шаг 6: Реализация политик безопасности на пограничном маршрутизаторе FW*

На маршрутизаторе FW реализованы следующие политики безопасности:

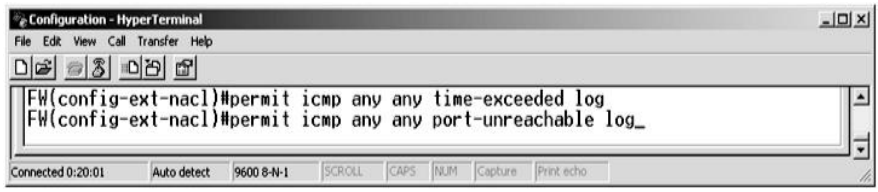
1. *Политика безопасности:* Запретите адреса RFC 1918, полученные из внешних источников и лог. Используйте расширенный список контроля доступа (INF), чтобы сопоставить исходные адреса, которые принадлежат частным адресам, определенным в RFC 1918.



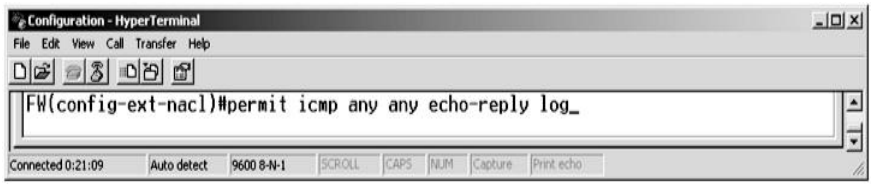
2. *Политика безопасности:* внедрите RFC 2827 и войдите, используя входящую фильтрацию трафика. Чтобы предотвратить DoS-атаку с использованием поддельных IP-адресов источника, необходимо принять меры безопасности, чтобы блокировать пакеты, которые утверждают, что IP-адреса источника аналогичны внутренней сети.



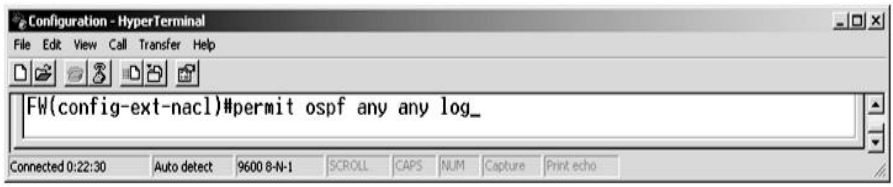
3. *Политика безопасности:* Внутри можно проследить внешний маршрут и войти. Разрешите внутреннему ПК отслеживать маршрут к внешней сети, разрешая ответным сообщениям traceroute проходить через внешний интерфейс FW. Microsoft использует эхо-сообщение ICMP для запроса и эхо-ответ для ответа, в то время как маршрутизаторы Unix и Cisco используют UDP для запроса и превышенного времени и недоступные сообщения ICMP порта для ответа.



4. *Политика безопасности:* Внутри можно пинговать снаружи и войти. Этого можно достичь, принимая сообщения эхо-ответа ICMP на внешнем интерфейсе пограничного маршрутизатора, используя следующую команду:

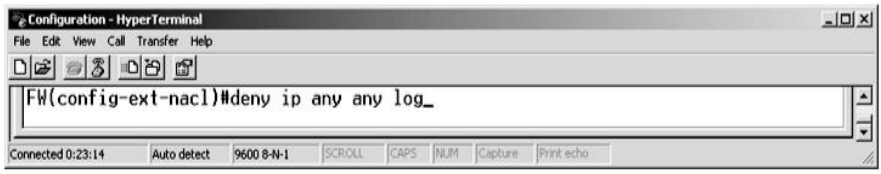


5. Политика безопасности: разрешить необходимые протоколы маршрутизации и журнал. Объявление о маршрутизации OSPF и сообщение об обновлении допускаются на внешнем интерфейсе для заполнения таблицы маршрутизации действительными путями к пунктам назначения с помощью следующей команды:



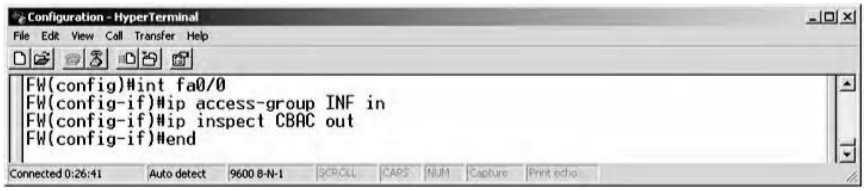
6. Политика безопасности: Запретить весь другой трафик и логи. Отказывая другому трафику, внешнему ПК будет запрещено

инициировать любой трафик, который не указан выше в ACL. Это можно сделать с помощью следующей команды:



7. *Политика безопасности:* Inside может инициировать TCP, UDP и HTTP-соединение с внешним миром. Используя контекстно-зависимый контроль доступа (CBAC), проверяется исходящий трафик TCP и UDP. Это позволяет маршрутизатору действовать как межсетевой экран с отслеживанием состояния, который позволяет обратному трафику проходить через его внешний интерфейс. Обратный трафик связан с открытым исходящим сеансом TCP или UDP. Настройка CBAC выполняется с помощью следующей команды:

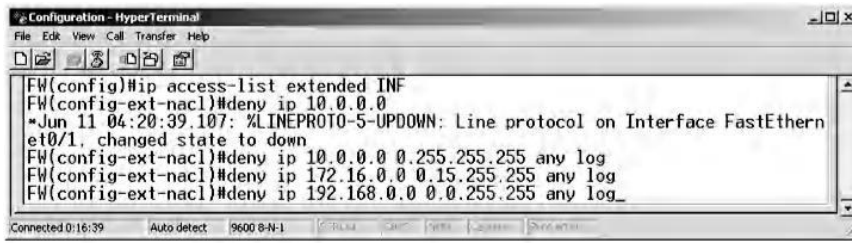
8. Политика безопасности: применить к внешнему интерфейсу. Без применения внешнего внешнего интерфейса ни ACL, ни CBAC работать не будут. Обратите внимание, что направление CBAC отсутствует, а направление ACL - как в следующей команде:



8.4.5.7 Шаг 7. Проверка политик безопасности, созданных на шаге 6

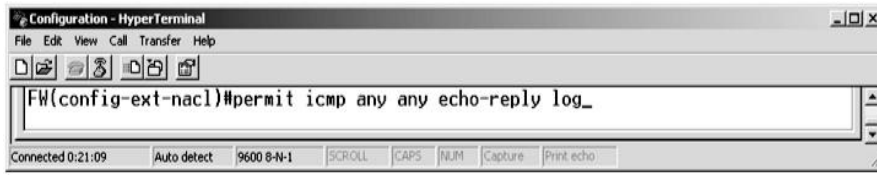
Чтобы проверить ACL и конфигурацию CBAC, проводятся следующие тесты и выделяется причина каждого результата.

Пинг с внутреннего компьютера на внешний компьютер (пинг 10.1.1.2). Это не должно быть успешным, потому что эхо-ответ приходит с внешнего IP-адреса, который является частным адресом. Следующая часть ACL объясняет поведение.

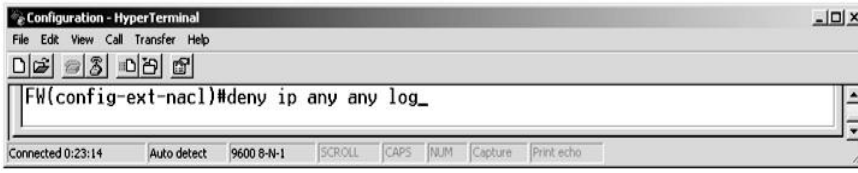


Пинг с внешнего компьютера на внутренний компьютер (Ping 184.1.1.2). Это не будет успешным, потому что эхо исходит от внешнего IP-адреса, который является частным адресом. Причина как описано выше.

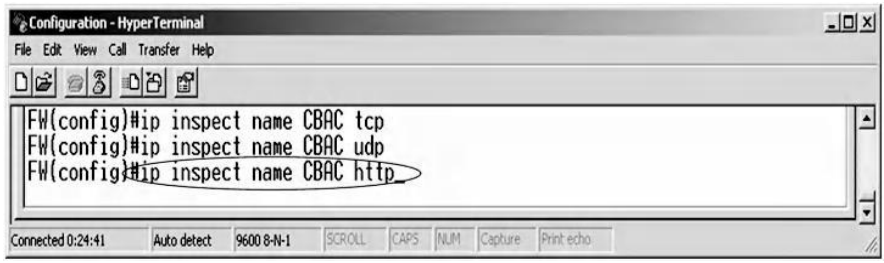
Пинг с внутреннего компьютера на BB1 (Ping 164.1.1.2). Это должно быть успешным, потому что трафик эхо-ответа разрешен, как в следующей записи ACL:



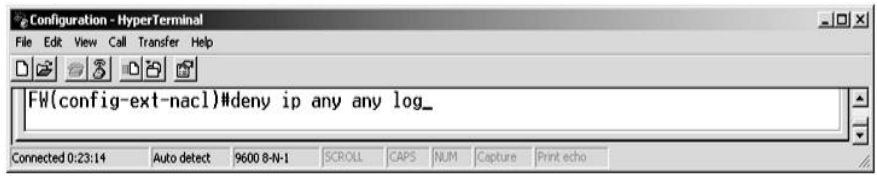
Пинг с BB1 на внутренний компьютер (Ping 184.1.1.2). Это не должно быть успешным, потому что трафик эха не разрешен явно, как в записи ACL ниже:



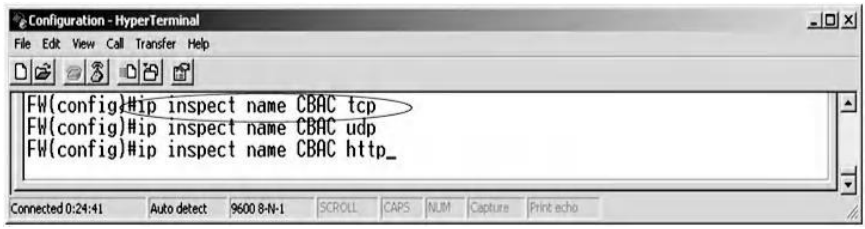
Затем перейдите с внутреннего компьютера на BB1 (HTTP://164.1.1.2). Это будет успешно, потому что HTTP-трафик проверяется по следующему правилу CBAC:



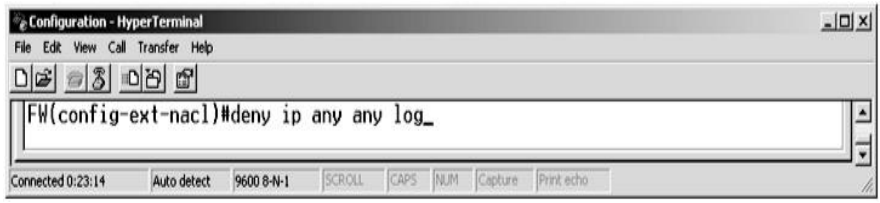
Перейдите с внешнего компьютера на FW (HTTP://164.1.1.2). Это не должно быть успешным, потому что внешний HTTP-трафик явно не разрешен, как в записи ACL ниже:



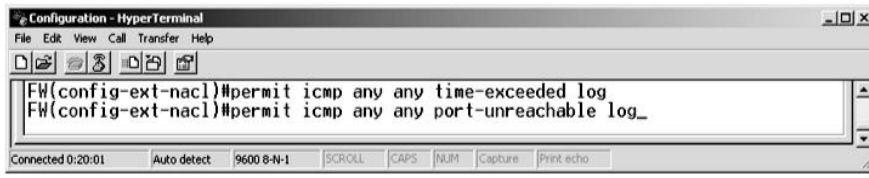
Затем используйте Telnet с внутреннего компьютера на BB1 (telnet 164.1.1.2). Это должно быть успешным, потому что TCP-трафик проверяется в соответствии со следующим правилом CBAC:



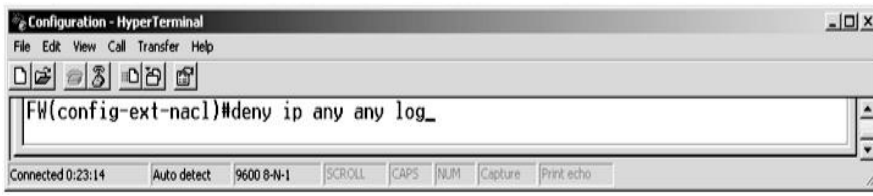
Затем используйте Telnet с внешнего ПК на FW (telnet 164.1.1.1). Это не должно быть успешным, потому что внешний трафик Telnet не разрешен следующей настроенной записью ACL:



Проследите маршрут от внутреннего компьютера до BB1 («tracert 164.1.1.2»). Это должно быть успешным, потому что трафик ответа traceroute (превышено время и порт недоступен) разрешен следующей записью ACL:



Затем проследите маршрут от BB1 до внутреннего ПК (traceroute 184.1.1.2). Это не должно быть разрешено, поскольку внешний трафик UDP запрещен следующей записью ACL:



8.5 Краткое содержание главы

Маршрутизатор на границе сети представляет собой уязвимую точку входа во всю сеть, и, следовательно, его безопасность является значительной. В этой главе обсуждались различные методы защиты маршрутизатора, в том числе модель AAA, защита сетевых служб, фильтрация пакетов и проверка с отслеживанием состояния. Методы аутентификации и авторизации модели AAA выполняются для защиты доступа управления к маршрутизатору от неавторизованного пользователя. Приложение анализатора используется для демонстрации необходимости отключения служб незащищенных сетей, таких как Telnet и HTTP, и замены их службами защищенной сети, такими как SSH и HTTPS. Наконец, на маршрутизаторе реализована фильтрация пакетов для управления потоком трафика на основе IP-адресов, номеров портов и типов сообщений ICMP. Кроме того, в этой главе обсуждалось усовершенствование технологии фильтрации пакетов за счет использования CBAC в качестве механизма проверки состояния.

Глава 9

Реализация VPN-туннеля типа "сеть-сеть" для защиты от подслушивающих атак

9.1 Введение

Обычное требование для любой реализации многосайтовой сети - наличие частных каналов связи между сайтами. Использование выделенной выделенной линии для частного подключения является очевидным выбором. Несмотря на свои преимущества в области безопасности и производительности, это решение имеет тенденцию быть дорогостоящим по сравнению с использованием виртуальной частной сети безопасности протокола Интернета (IPsec VPN). IPsec VPN - это частное соединение, которое обеспечивает безопасное соединение через общедоступную или общую среду, такую как Интернет, между двумя локальными сетями (LAN) или удаленным пользователем и LAN. Криптографические методы и протоколы используются для защиты конфиденциальности трафика, который проходит между конечными точками VPN. Использование IPsec VPN для обеспечения конфиденциальности данных является привлекательным решением, поскольку в нем используется существующая сетевая инфраструктура, обеспечивающая доступ в Интернет.

IPsec VPN является открытым стандартом, который определен Инженерной рабочей группой по Интернету (IETF) для обеспечения конфиденциальности, целостности, аутентификации, защиты от повторов и контроля доступа к сетевому трафику. Важно понимать взаимосвязь между различными технологиями конфиденциальности данных, такими как IPsec VPN и Secure Socket Layer / Transport Layer Security (SSL/TLS). Прежде всего, IPsec VPN - это решение безопасности сетевого уровня, а SSL/TLS - решение безопасности транспортного уровня. Следовательно, SSL/TLS не может скрыть IP-адреса взаимодействующих сторон. Напротив, IPsec VPN имеет возможность скрывать IP-адреса.

С другой стороны, IPsec VPN и SSL/TLS имеют общие черты, такие как сочетание алгоритмов шифрования с асимметричным и симметричным ключами. Криптографические алгоритмы с симметричным ключом быстры и используют маленькие ключи. Однако процесс генерации, распределения, хранения и перемещения ключей является проблематичным. С другой стороны, криптографические алгоритмы с асимметричным ключом решают проблему управления ключами, имея два ключа - открытый ключ и закрытый ключ, но, тем не менее, очень медленные.

Гениальный подход заключается в использовании обоих этих методов, при этом криптографические алгоритмы с асимметричным ключом используются для обмена ключами и аутентификации, а криптографические алгоритмы с симметричным ключом используются для шифрования данных. Следовательно, как IPsec VPN, так и SSL / TLS имеют две основные фазы или уровни. Первый используется для обмена ключами и аутентификации, а второй - для шифрования данных. Эти фазы

* Интернет-ассоциация безопасности и протокол управления ключами (ISAKMP) / Интернет-обмен ключами (IKE) фаза 1 и ISAKMP / IKE фаза 2 для IPsec VPN
* Уровни рукопожатия и записи для SSL / TLS

Представлено краткое описание основных протоколов, фаз, режимов и типов VPN.

9.1.1 Фазы протокола IKE

IKE фаза 1 используется главным образом для обмена сеансовым ключом с помощью групп Диффи-Хеллмана и аутентификации с использованием криптографических алгоритмов с предварительным общим ключом или асимметричным ключом. Другие функции этого этапа - подготовка ключевых материалов для IKE-этапа 2 и защита собственного сообщения с использованием функций шифрования и хэширования. На этом этапе согласовывается сопоставление безопасности (SA), которое называется этапом 1 SA. SA является однонаправленным соглашением между конечными точками IPsec VPN о согласованных параметрах безопасности, которые устанавливают VPN-туннель, включая применимый метод аутентификации, алгоритм шифрования и хэш-функцию. IKE фаза 1 имеет два режима:

* Основной режим - это безопасный режим, который включает в себя защиту идентификатора сверстника и подробные переговоры.
* Агрессивный режим является более быстрым и менее безопасным режимом и не обеспечивает никакой защиты идентификаторов.

На этапе IKE 2 шифрование и дешифрование данных завершаются. Единственный режим, доступный на этом этапе, - это быстрый режим, который устанавливает два однонаправленных SA фазы 2. Каждая однонаправленная SA фазы 2 имеет индекс, называемый индексом параметров безопасности (SPI). Согласованные параметры безопасности SA фазы 2 следующие:

* Протоколы IPsec: инкапсуляция защищенной полезной нагрузки (ESP) или заголовок аутентификации (AH).
* Набор функций шифрования и хэширования.
* Трафик, который должен быть защищен VPN-туннелем.
* Группа Диффи-Хеллмана, если требуется совершенная прямая секретность (PFS). (PFS гарантирует, что будущие ключи не будут получены из предыдущих ключей. Следовательно, компрометация одного ключа повлияет только на данные, защищенные этим ключом.)

9.1.2 Режимы IPsec

Существует два режима IPsec: туннельный режим и транспортный режим. Туннельный режим защищает весь IP-пакет, начиная с уровня 3 модели ISO (т.е. уровня сети) и выше. Этот режим инкапсулирует заголовок IP и полезную нагрузку, и это наиболее часто используемый режим. Транспортный режим защищает уровень 4 модели ISO (т.е. транспортный уровень) и выше, и, следовательно, он не защищает заголовок IP.

9.1.3 Протоколы IPsec

IPsec имеет два протокола: ESP (инкапсуляция полезной нагрузки безопасности) и AH (заголовок аутентификации). ESP использует порт 50 и обеспечивает конфиденциальность, целостность и аутентификацию без защиты заголовка IP в транспортном режиме. Из-за службы безопасности конфиденциальности данных, это наиболее используемый протокол IPsec. AH использует порт 51 и обеспечивает целостность, аутентификацию и защиту IP-заголовка. Тем не менее, он не предоставляет службы безопасности конфиденциальности данных, что делает его подходящим для приложений, требующих в основном аутентификации, таких как аутентификация сообщений IP-маршрутизации.

9.1.4 Типы VPN

В основном существует два типа VPN: VPN типа «сеть-сеть» и VPN с удаленным доступом. VPN типа «сеть-сеть» или VPN-сеть типа «сеть-сеть» обеспечивает конфиденциальность данных для критически важного трафика между сетями на двух сайтах. Эта глава включает в себя две практические работы по реализации VPN типа «сеть-сеть». Первая лаборатория использует два устройства брандмауэра Juniper Networks в качестве шлюзов VPN для соединения двух сайтов, в то время как устройства второй брандмауэра Cisco используются во второй лаборатории. VPN с удаленным доступом позволяет удаленным пользователям получать безопасный доступ к защищенным сетевым ресурсам центрального сайта. Это будет в центре внимания главы 10.

Внедрение IPsec VPN-решений может быть сложной задачей как для новичка, так и даже для инженера промежуточного уровня безопасности. Это требует четкого понимания нескольких технологий безопасности, алгоритмов, протоколов, режимов и концепций. Кроме того, процесс настройки VPN имеет тенденцию быть длительным и включает в себя несколько этапов, процедуры проверки и тестирования. Более того, нет стандартной практики внедрения VPN для разных поставщиков. Ввиду этих опасений ключевой целью этой главы является объяснение реализации VPN двух поставщиков, являющихся лидерами на рынке (Juniper Networks и Cisco Microsystems), используя различные иллюстрации, снимки экрана и этапы настройки. Это поможет читателю сформировать глубокое понимание решений безопасности VPN и процесса внедрения.

В этой главе описываются процедуры для реализации решения VPN для установления защищенной связи между двумя удаленными узлами. Процесс объясняется в лабораторных условиях и использует стандарты и лучшие практики, вплетенные в реальный сценарий, чтобы улучшить понимание читателя.

В практических занятиях используются следующие аппаратные устройства:

* Беспроводное устройство Juniper Networks SSG20 *: шлюз VPN
* Устройство Cisco Microsystems ASA †: шлюз VPN

9.2 Лабораторная работа 9.1: VPN типа «сеть-сеть» - первая реализация

9.2.1 Результат

Целью данной лабораторной работы является научить студентов внедрять туннель VPN (виртуальная частная сеть) между двумя сайтами с использованием шлюза Juniper VPN.

* http://www.juniper.net
† http://www.cisco.com

9.2.2 Описание

Мы представляем это упражнение, используя практический сценарий для обогащения обучения. Головной офис банка находится в Дубае, и необходимо установить безопасную коммуникационную связь с филиалом, расположенным в Аль-Айне, городе, который находится примерно в 160 километрах от Дубая. Подход, принятый для установления этого требования, заключается в создании частного соединения между двумя сайтами с использованием технологии VPN.

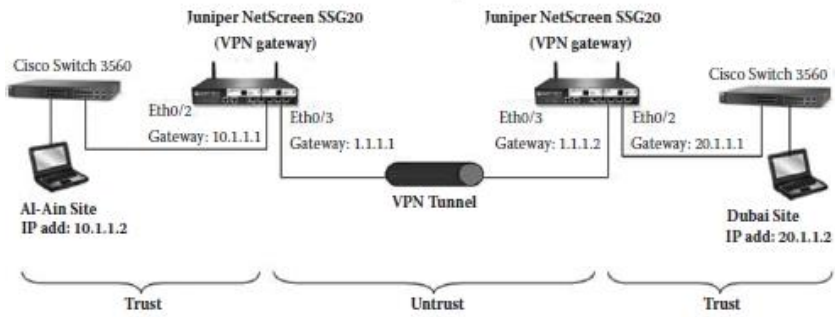
Каждый сайт (головной офис и филиал) имеет локальную сеть (локальную сеть), которая соединяет компьютерные хосты с помощью коммутаторов в пределах ограниченной географической области. Для простоты каждая локальная сеть представлена одним узлом, как показано на следующем рисунке. Реализация в реальном мире для передачи данных между этими двумя сетями потребовала бы технологий глобальной сети (WAN), чтобы охватить обширную область между Аль-Айном и Дубаем. Для нашего упражнения соединение WAN моделируется перекрестным кабелем. В качестве альтернативы, коммутатор и прямые кабели могут служить той же цели.

Чтобы разрешить частное соединение между двумя сайтами, VPN-шлюз должен быть установлен на каждом сайте. Обычно маршрутизаторы и межсетевые экраны используются в качестве шлюзов VPN; в этой реализации устройство межсетевого экрана Juniper Networks используется в качестве шлюза VPN для каждого сайта. Два VPN-шлюза договариваются об ассоциации безопасности IKE фазы 1 для установления VPN-туннеля. Затем они шифруют данные, используя параметры ассоциации безопасности IKE фазы 2.

9.2.3 Эксперимент

На следующем рисунке показана сетевая архитектура эксперимента. Узел 1, представляющий Al-Ain, состоит из хоста, который подключен к коммутатору Cisco 3560 с помощью прямого кабеля. Коммутатор подключается к интерфейсу Ethernet0 / 2 межсетевого экрана Juniper NetScreen с помощью прямого кабеля. Тот же сценарий используется на сайте 2, который представляет Дубай. Два сайта соединены через

интерфейс Ethernet0/3 межсетевого экрана Juniper NetScreen с помощью перекрестного кабеля, в котором будет реализован туннель.



Эксперимент состоит из следующих этапов:

Шаг 1. Сбросьте брандмауэр до значения по умолчанию.
Шаг 2. Назначьте IP-адреса компьютеров и интерфейсы брандмауэра обоих сайтов.
Шаг 3. Назначьте сетевые IP-адреса двух локальных сетей (Аль-Айн и Дубай) обоих сайтов.
Шаг 4: Настройте VPN с сайта Al-Ain на сайт в Дубае и наоборот.
Шаг 5: Маршрут от сайта Аль-Айн до сайта в Дубае и наоборот.
Шаг 6: Установите политики для обоих сайтов.
Шаг 7. Отправьте эхо-запрос из Аль-Айна в Дубаи и наоборот, чтобы проверить установление VPN-туннеля.
Шаг 8: Проверьте установление VPN-туннеля.

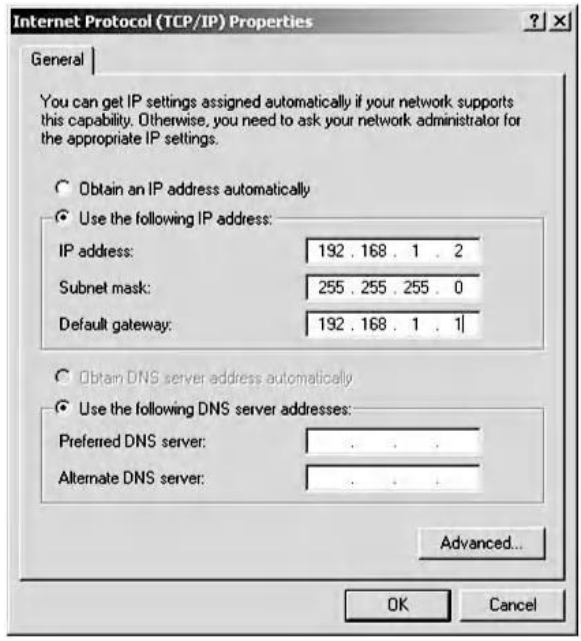
9.2.3.1 Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию

Мы начинаем эксперимент с подключения хоста к последовательной консоли брандмауэра для сайта Al-Ain для доступа к интерфейсу командной строки брандмауэра через гипертерминал. Используйте «netscreen» для логина и пароля. Далее введите «unset all». Наблюдается следующий вывод: “Erase all system config, are you sure [y/n]?” (Удалить все системные настройки, вы уверены [y / n]?) Подтвердите, набрав «y»; затем перезагрузите систему, набрав “reset” (сброс). Появится

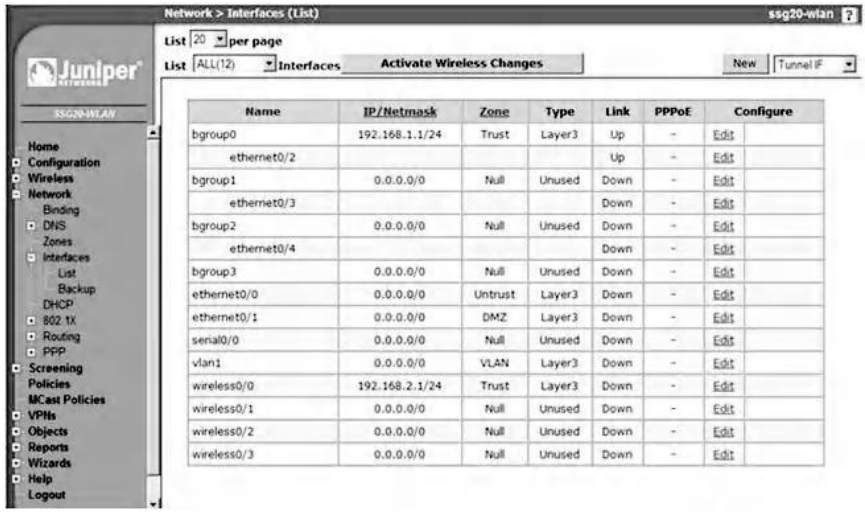
следующий вывод: “Configuration modified, save?” (Конфигурация изменена, сохранить?), Для которой вводится «n». Другой вопрос, “System reset, are you sure?” (Сброс системы, вы уверены?), для которого вводится «y». Затем снова войдите в систему, используя идентификатор входа и пароль по умолчанию, который называется «netscreen». Те же шаги повторяются для брандмауэра для сайта в Дубае.

9. *2.3.2 Шаг 2. Назначьте IP-адреса компьютеров и интерфейсов брандмауэра для обоих сайтов*

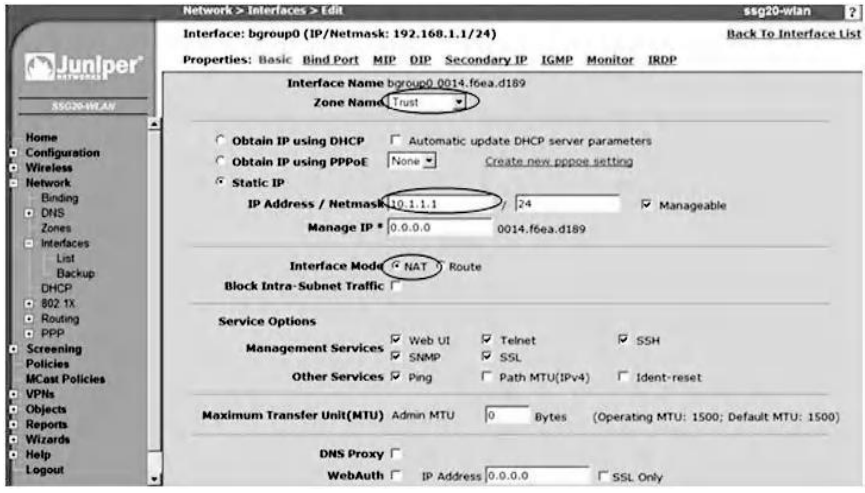
Чтобы назначить IP-адрес устройству и брандмауэру сайта Al-Ain, выберите параметр “Use the following IP address” (Использовать следующий IP-адрес) и заполните записи, как показано на следующем снимке экрана.



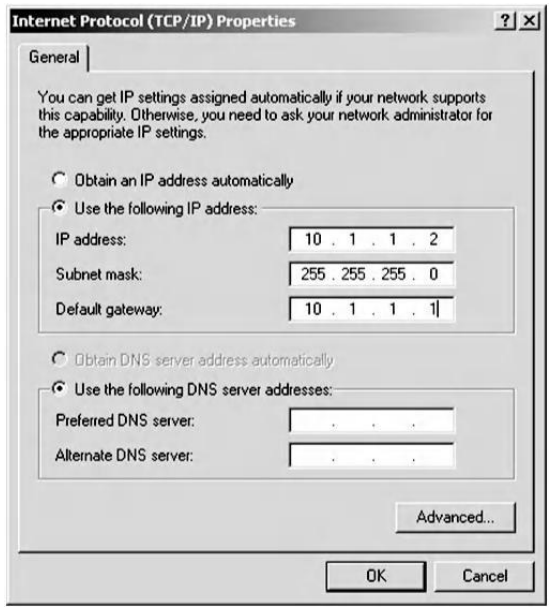
Затем откройте веб-интерфейс пользователя (WebUI) устройства Juniper Network, введя “http://192.168.1.1.” Появится список интерфейсов:



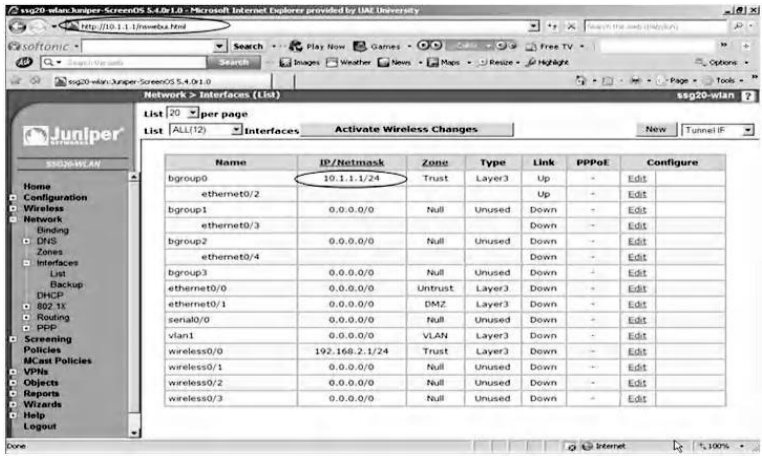
Затем нажмите на ссылку “Edit” (Редактировать) интерфейса bgroup0 и заполните записи, как показано на следующем снимке экрана. Название зоны должно быть “Trust” (Доверие) для сайта Аль-Айн. Режим интерфейса - «NAT», в котором межсетевой экран назначает публичные IP-адреса компьютерам в частной сети. Выберите услуги, которые будут использоваться; например, «Web UI» позволяет пользователю получить доступ к конфигурации брандмауэра через веб-интерфейс пользователя. Нажмите “Apply” (Применить), а затем «OK», чтобы завершить настройку.



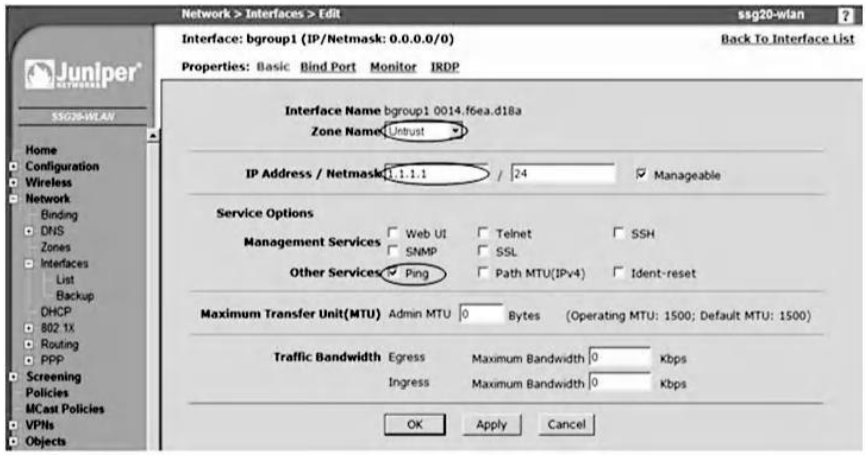
После изменения IP-адреса интерфейса веб-интерфейс Juniper автоматически выходит из системы. Поэтому измените IP-адрес компьютера Al-Ain на 10.1.1.2/24, как показано ниже.



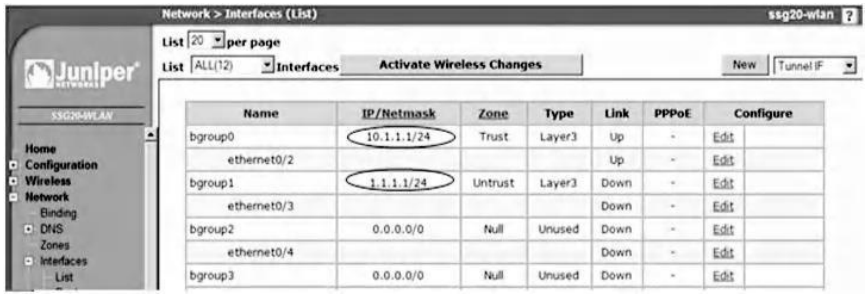
Запустите веб-браузер со следующим URL-адресом - http: //10.1.1.1 - для доступа к веб-интерфейсу пользователя. Затем выберите “Network” (Сеть), затем “Interfaces” (Интерфейсы) и, наконец, “List” (Список), чтобы отобразить экран, как показано далее.



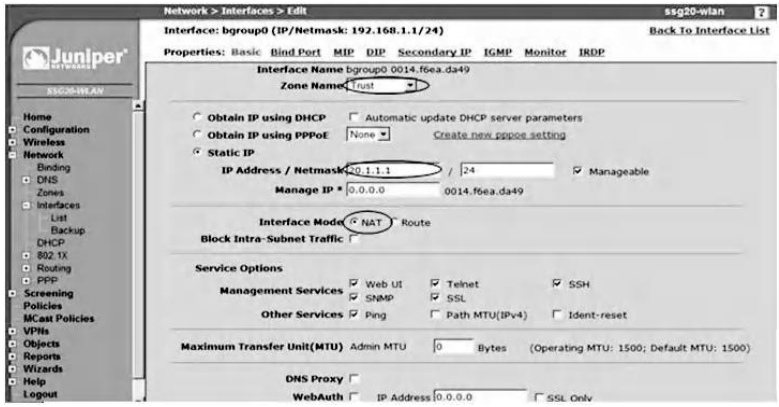
Нажмите на ссылку “Edit” (Редактировать) интерфейса bgroup1 и заполните поля, как показано на следующем снимке экрана. Название зоны будет “Untrust” (Недоверие), в котором VPN-туннель будет создан с сайтом в Дубае. Выберите сервис для использования; например, мы включили службу ping, чтобы разрешить связь между двумя сайтами, что будет безопасно осуществляться через туннель.



Нажмите “Apply” (Применить), а затем «OK». Назначенные IP-адреса для интерфейсов должны выглядеть так, как показано ниже.

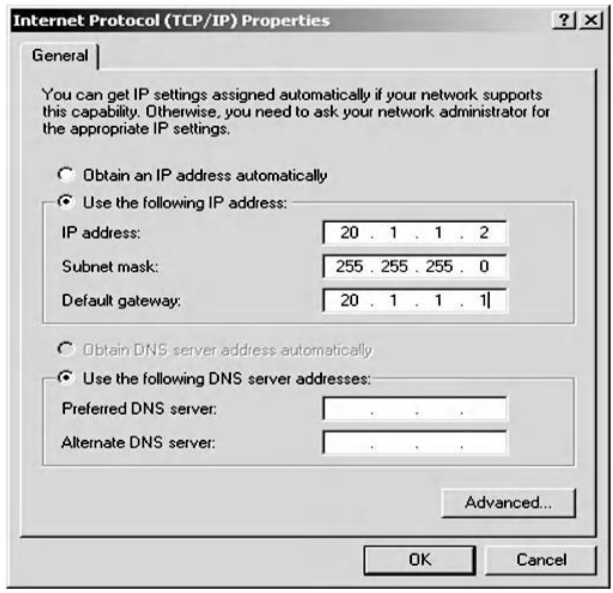


Чтобы назначить IP-адрес устройству и брандмауэру сайта в Дубае, повторите те же действия, что и для сайта Al-Ain. Настройки интерфейса брандмауэра для сайта в Дубае показаны далее.

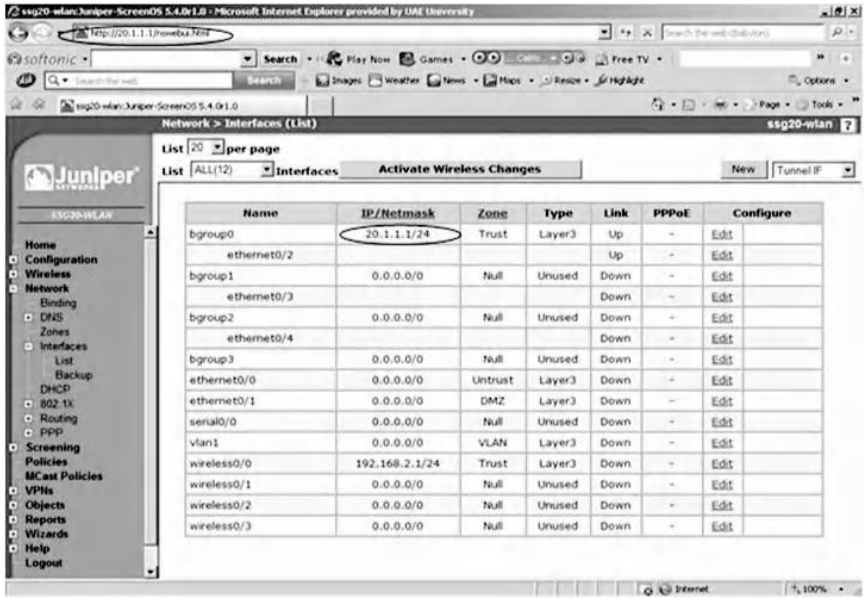


Нажмите на ссылку “Edit” (Редактировать) интерфейса bgroup0 и заполните записи. Название зоны будет “Trust” (Доверие) для сайта в Дубае, а режим интерфейса - «NAT». Включите службы, как это было сделано для сайта в Аль-Айне. Затем нажмите “Apply” (Применить) и «OK».

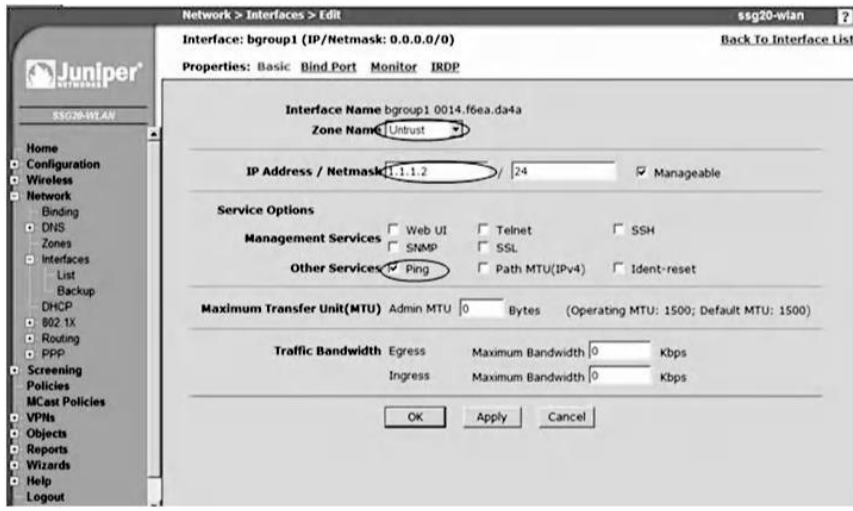
Примечание: После изменения IP-адреса интерфейса веб-интерфейс NetScreen автоматически выйдет из системы. IP-адрес ПК должен быть изменен на 20.1.1.2/24, как показано на следующем снимке экрана.



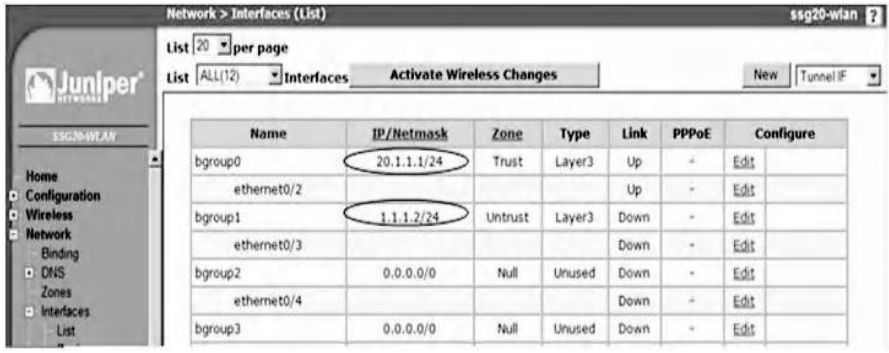
Затем запустите веб-браузер со следующим URL-адресом, http://20.1.1.1, для доступа к веб-интерфейсу пользователя и выберите “Network” (Сеть), затем “Interfaces,” (Интерфейсы) и, наконец, “List,” (Список), как показано на следующем снимке экрана.



Нажмите на ссылку “Edit” (Редактировать) интерфейса bgroup1 и заполните поля, как показано на экране ниже. Имя зоны установлено как “Untrust” (Недоверие), в котором VPN-туннель создается с сайтом Аль-Айн. Выберите сервис для использования; Например, мы включили службу ping, чтобы разрешить безопасную связь между двумя сайтами через туннель. Нажмите “Apply” (Применить), а затем «ОК».

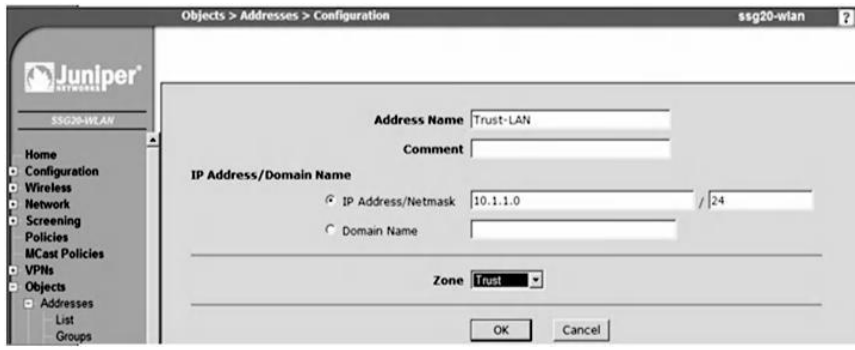


Итоговый список полученного интерфейса брандмауэра Дубая приведен ниже.

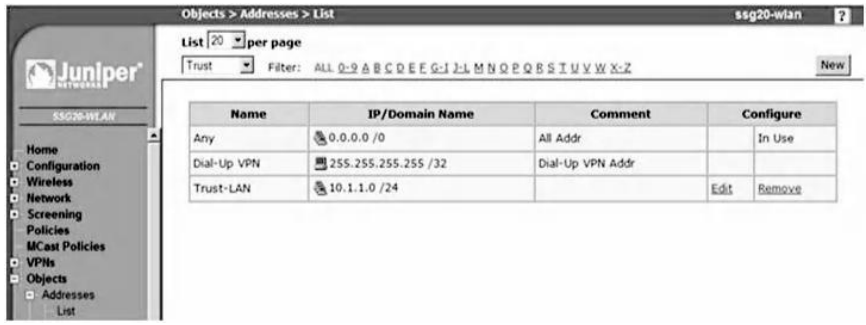


9. *2.3.3 Шаг 3. Назначьте сетевые IP-адреса двух локальных сетей (Аль-Айн и Дубай) для обоих сайтов.*

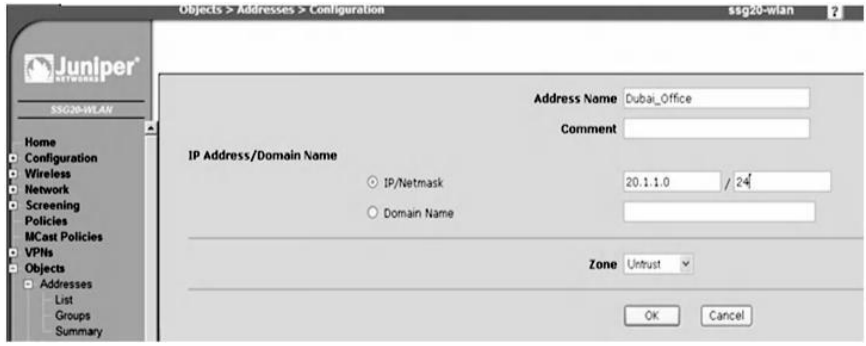
Чтобы назначить сетевые адреса сайта Al-Ain, выберите “Objects” (Объекты), затем “Addresses” (Адреса) и, наконец, “List” (Список). Заполните поля в появившемся окне, как показано ниже.



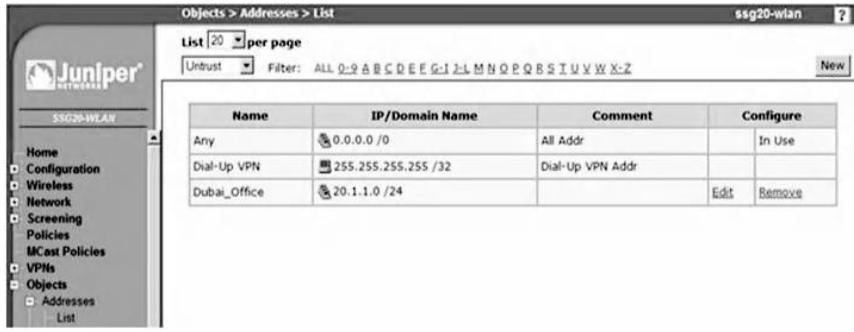
Нажатие на кнопку «ОК» приводит к следующему экрану.



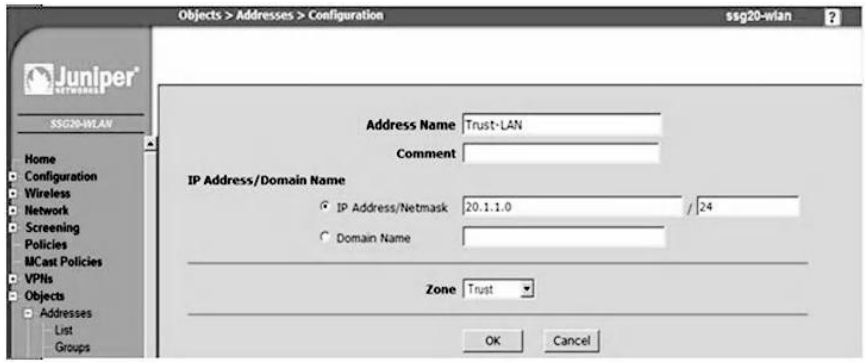
Теперь щелкните в раскрывающемся меню слева и выберите зону “Untrust” (Недоверять), а затем нажмите “New”(Создать). Заполните поля соответствующими значениями, как показано на следующем снимке экрана.



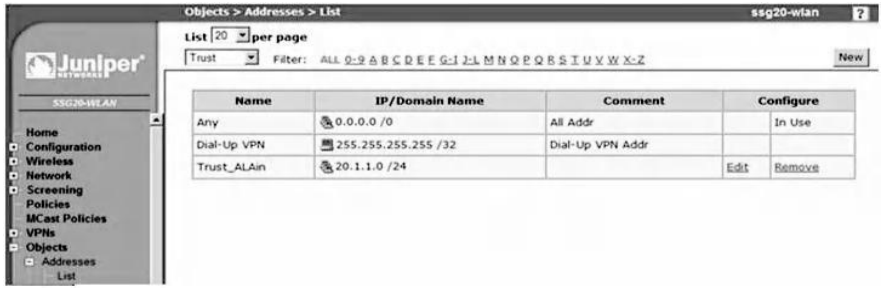
Нажмите на кнопку «ОК»; Сетевой адрес зоны “Untrust” (Недоверие) отображается, как показано на следующем снимке экрана.



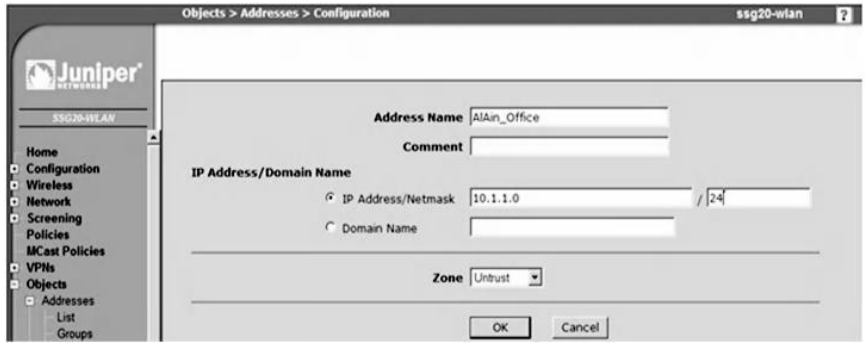
Чтобы назначить сетевые адреса сайта в Дубае, выберите “Objects” (Объекты), затем “Addresses” (Адреса) и, наконец, “List”(Список). Заполните поля соответствующими значениями, как показано ниже.



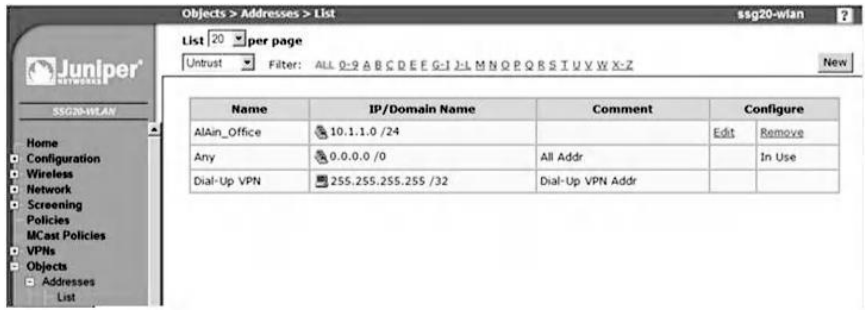
Нажмите на кнопку «ОК», что приведет к скриншоту, показанному ниже.



Нажмите на левое выпадающее меню и выберите зону “Untrust”(Недоверие); затем нажмите “New” (Создать). Заполните значения полей, как показано на следующем снимке экрана.



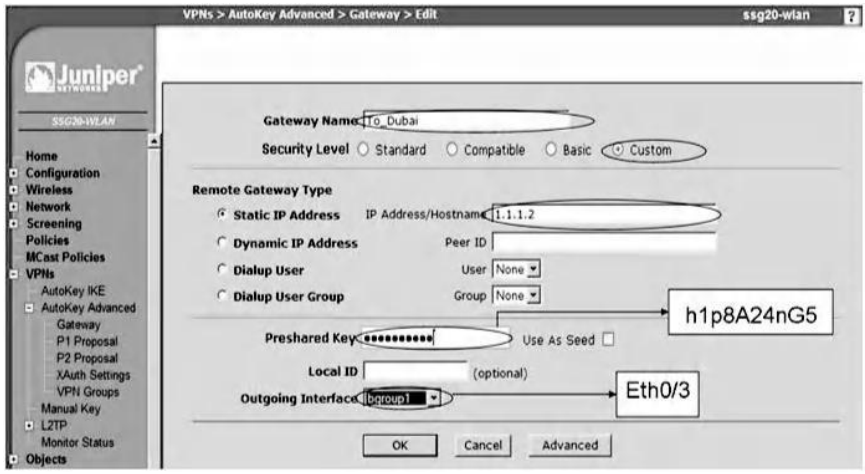
Нажмите «ОК»; сетевой адрес зоны “Untrust” (Недоверчивый) отображается, как показано на снимке экрана ниже.



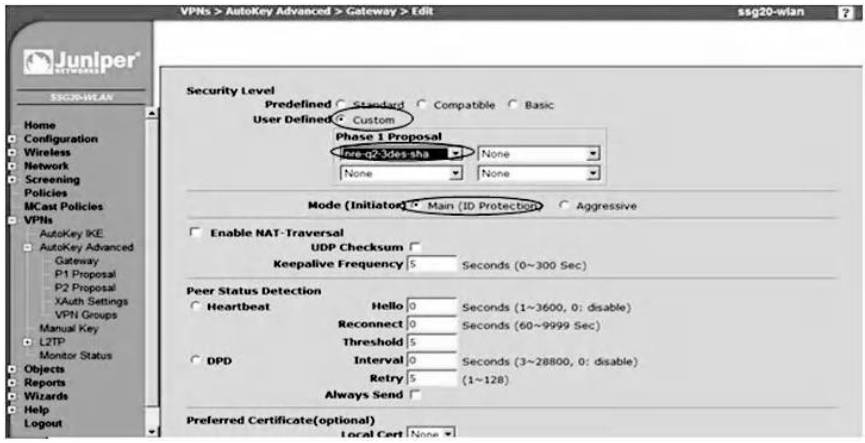
9. *2.3.4 Шаг 4. Настройте VPN с сайта Al-Ain на сайт в Дубае и наоборот*

Чтобы настроить VPN-шлюз с сайта Al-Ain, перейдите к «VPN» и «AutoKey Advanced», затем “Gateway” (Шлюз) и, наконец, «New». Введите значения, как показано на экране ниже. Введите имя шлюза сайта To_Dubai и выберите «Custom» для уровня безопасности. Выберите “Static IP Address” (Статический IP-адрес) для удаленного шлюза и введите IP-адрес шлюза. Введите предварительный общий ключ, который используется для процесса аутентификации между

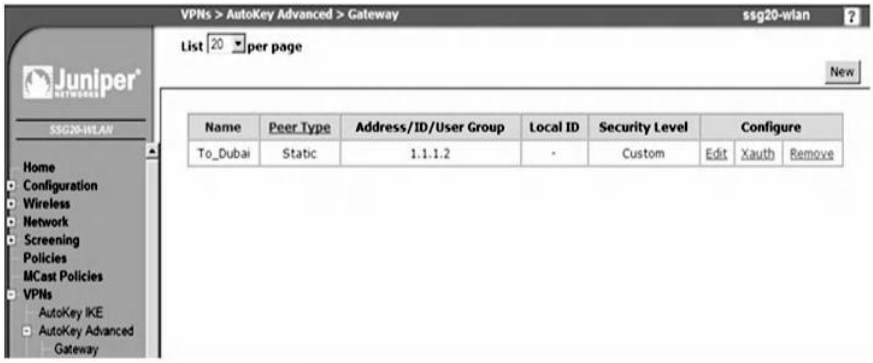
двумя сторонами для идентификации друг друга. Выберите bgroub1 в качестве исходящего интерфейса, где VPN-соединение реализовано между двумя концами.



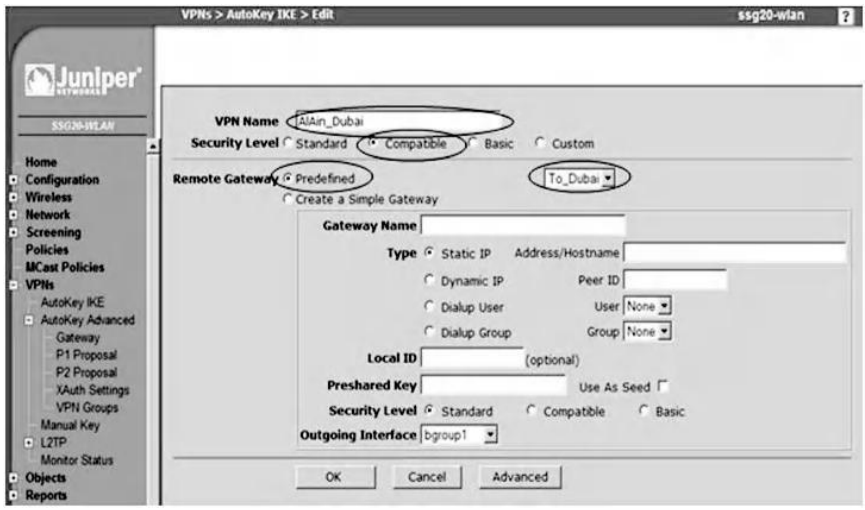
Нажмите на кнопку “Advanced” (Дополнительно), чтобы выбрать предложение фазы 1 для сайта Аль-Айн. Предложение состоит из трех алгоритмов. Diffie–Hellman Group 2 - это метод, позволяющий двум сторонам договориться о секретной ценности; 3DES - это алгоритм шифрования, который используется для целей шифрования, а SHA используется для обеспечения целостности данных. Выберите Main Mode (Основной режим), который обеспечивает защиту идентификатора, как показано на следующем снимке экрана.



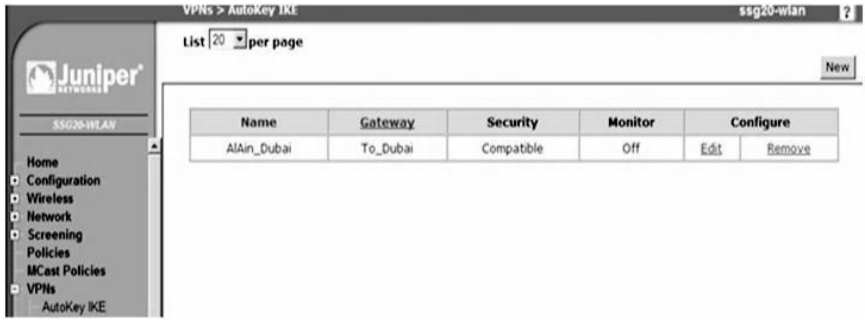
Нажмите кнопку «Return», чтобы вернуться на страницу базовой конфигурации шлюза, а затем нажмите кнопку «OK». Этап 1 создания завершен для сайта Al-Ain, как показано ниже.



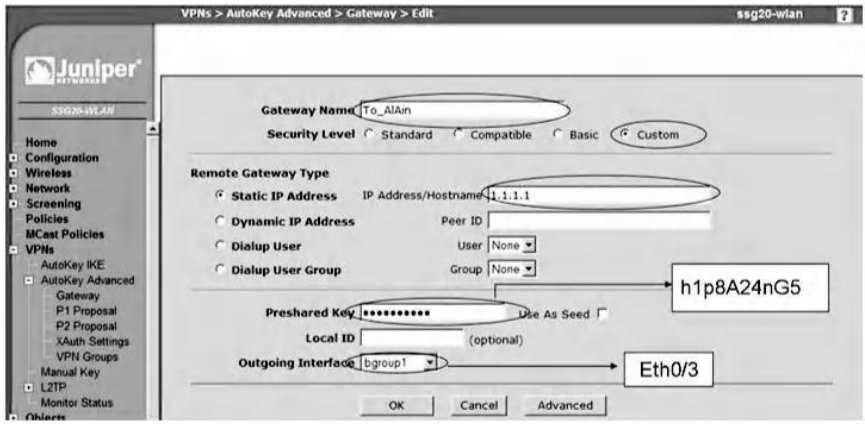
Параметры фазы 2 устанавливаются автоматически, выбирая «VPN», затем «Auto IKE» и, наконец, «New». Введите значения, как показано на следующем экране. Введите имя VPN и выберите совместимый выбор в качестве уровня безопасности. Выберите “Predefined” (Предопределенный) для удаленного шлюза и выберите шлюз To_Dubai.



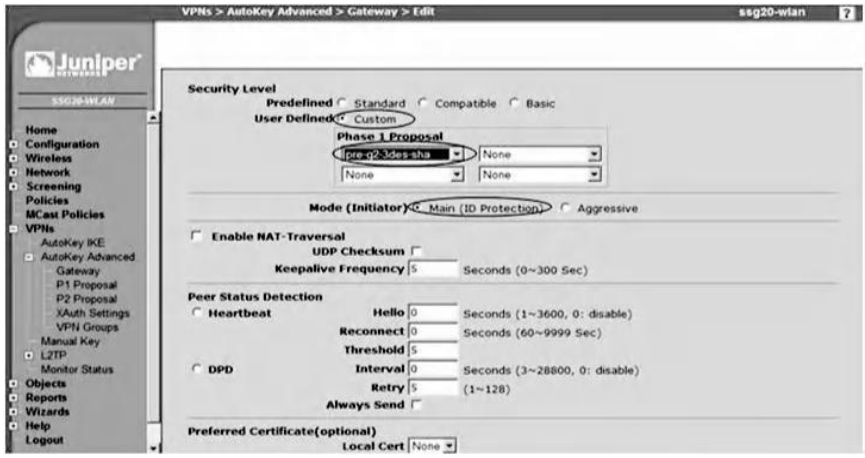
Нажмите кнопку «OK», чтобы отобразить экран, показанный ниже (то есть VPN для сайта «Аль-Айн» завершен).



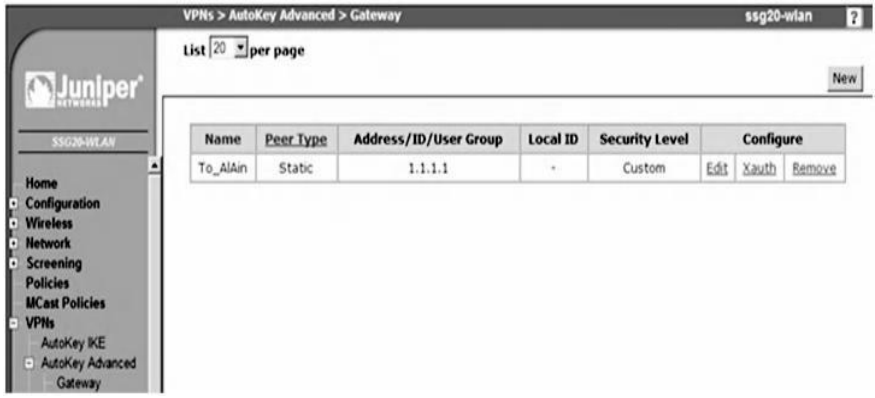
Чтобы настроить VPN с сайта в Дубае, выберите «VPN», затем «AutoKey Advanced», затем “Gateway”(Шлюз) и, наконец, “New” (Новый). Введите следующие данные, как показано на следующем экране: Введите имя шлюза To_Al на сайте и выберите “Custom” (Пользовательский) для уровня безопасности. Выберите “Static IP Address” (Статический IP-адрес) для удаленного шлюза и введите IP-адрес шлюза. Введите тот же предварительный общий ключ, который используется для процесса аутентификации на сайте Al-Ain. Выберите bgroub1 в качестве исходящего интерфейса, где VPN будет реализован между двумя концами.



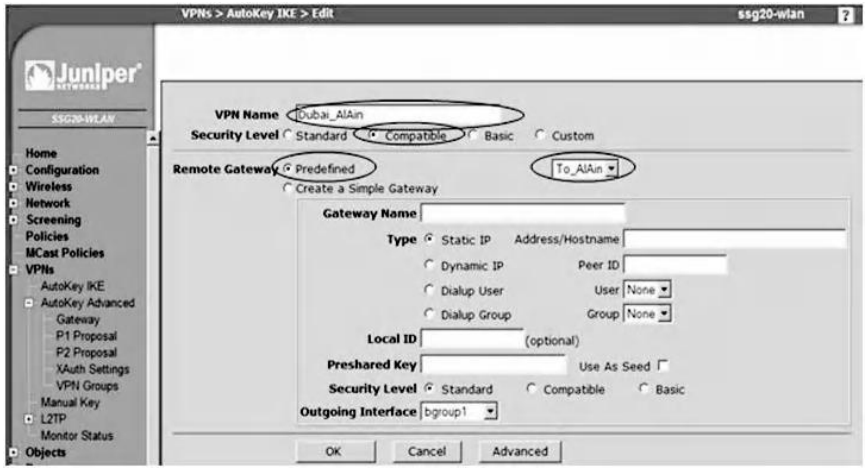
Нажмите кнопку “Advanced” (Дополнительно) и введите значения, как показано на следующем экране. Предложение фазы 1 состоит из трех алгоритмов: группа Диффи-Хеллмана 2, 3DES и SHA. Выберите основной режим для фазы 1.



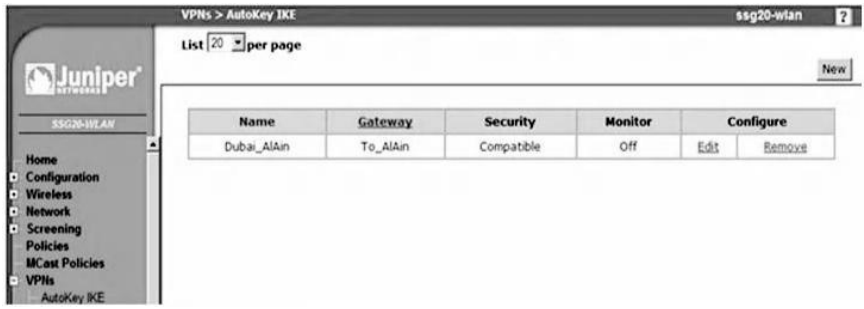
Нажмите кнопку “Return” (Возврат), чтобы вернуться на страницу базовой конфигурации шлюза, затем нажмите «OK», чтобы завершить этап 1, как показано на следующем экране.



Выберите «VPN», затем «Auto IKE» и, наконец, «New». Введите значения, как показано на следующем экране. Введите имя VPN и выберите “compatible choice” (совместимый выбор) в качестве уровня безопасности. Выберите «Predefined» для удаленного шлюза и выберите «To_AlAin gateway», который был ранее настроен.

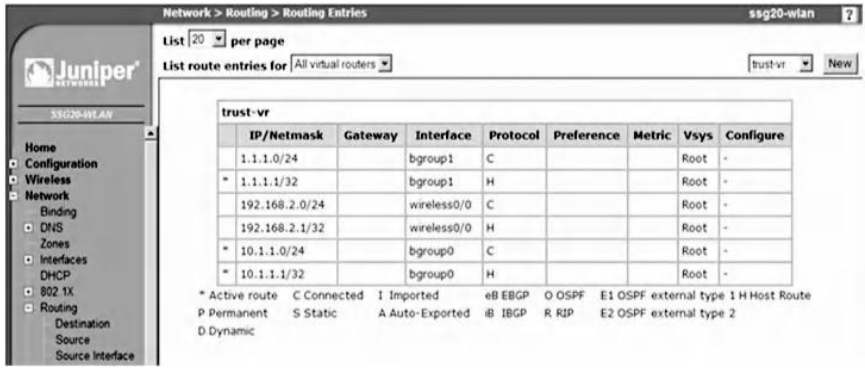


Нажмите «OK», чтобы завершить настройку VPN на сайте в Дубае, как показано на следующем экране.

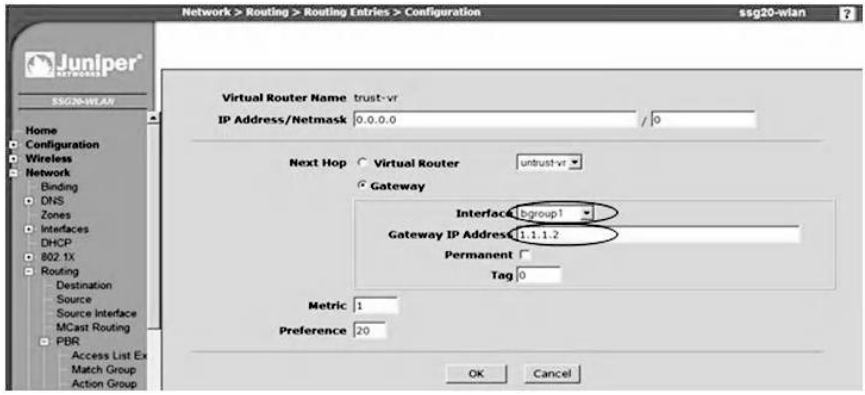


9. 2.3.5 *Шаг 5: Маршрут от площадки в Аль-Айне до шлюза в Дубае и обратно*

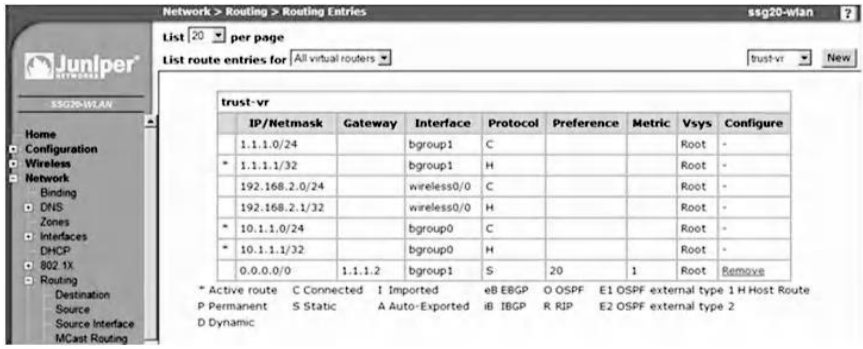
Для маршрутизации с сайта Al-Ain на сайт в Дубае выберите “Network” (Сеть), затем “Routing” (Маршрутизация) и, наконец, “Destination” (Назначение). Страница конфигурации маршрутизации отобразится, как показано ниже.



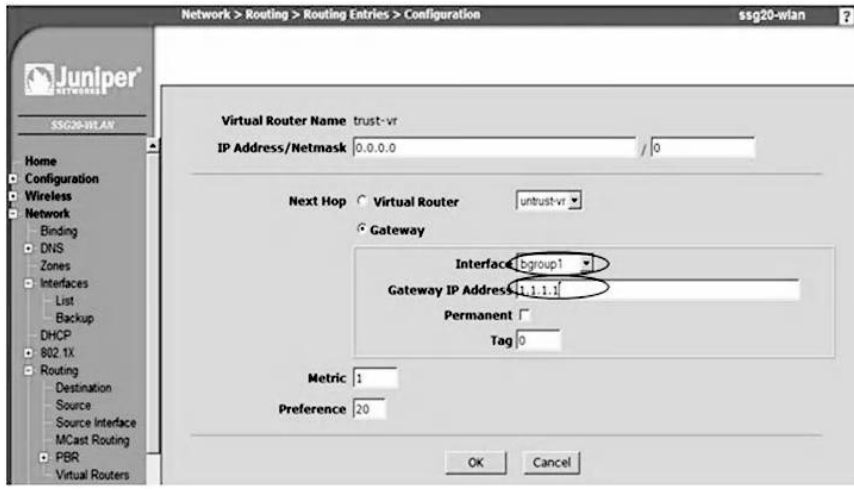
Чтобы создать маршрут по умолчанию к шлюзу Дубая, выберите «trust-vr» в раскрывающемся меню, затем нажмите кнопку «New» и заполните поля, как показано на следующем снимке экрана.



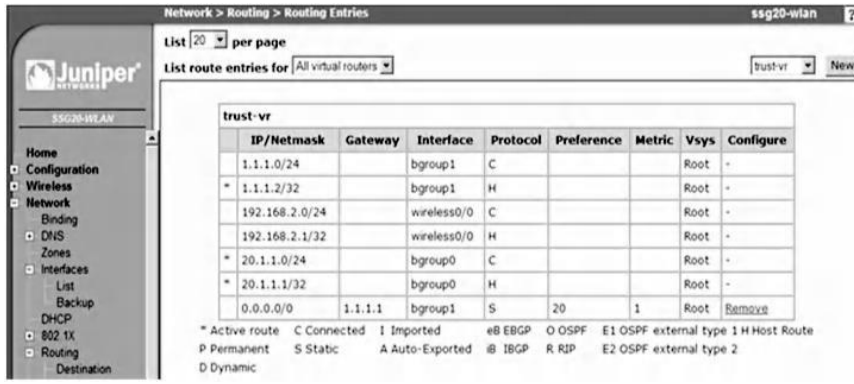
Нажмите на кнопку «ОК»; записи маршрутизации должны выглядеть так, как показано ниже.



Для маршрутизации с сайта в Дубае на сайт в Аль-Айне выберите “Network” (Сеть), затем “Routing” (Маршрутизация) и, наконец, “Destination” (Пункт назначения). Откроется страница конфигурации маршрутизации. Чтобы создать маршрут по умолчанию к шлюзу Аль-Айн, выберите «trust-vr» в раскрывающемся меню; затем нажмите кнопку “New” (Создать) и заполните поля, как показано на следующем снимке экрана.



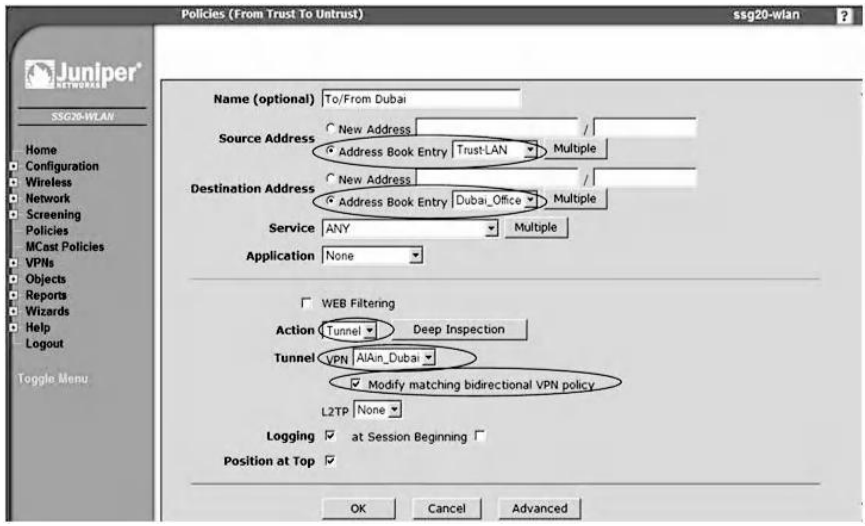
Нажмите на кнопку «ОК»; записи маршрутизации должны выглядеть так, как показано ниже.



9.2.3.6 Шаг 6: Установите политики для обоих сайтов

Чтобы установить политики с сайта Al-Ain, которые позволяют сайту Al-Ain обмениваться данными с сайтом в Дубае через туннель, выберите “Policies” (Политики) и очистите правила по умолчанию; затем

выберите зоны из выпадающего меню из зоны доверия в зону “Untrust” (Недоверять). Нажмите кнопку “New” (Создать) и заполните поля, как показано на следующем экране.

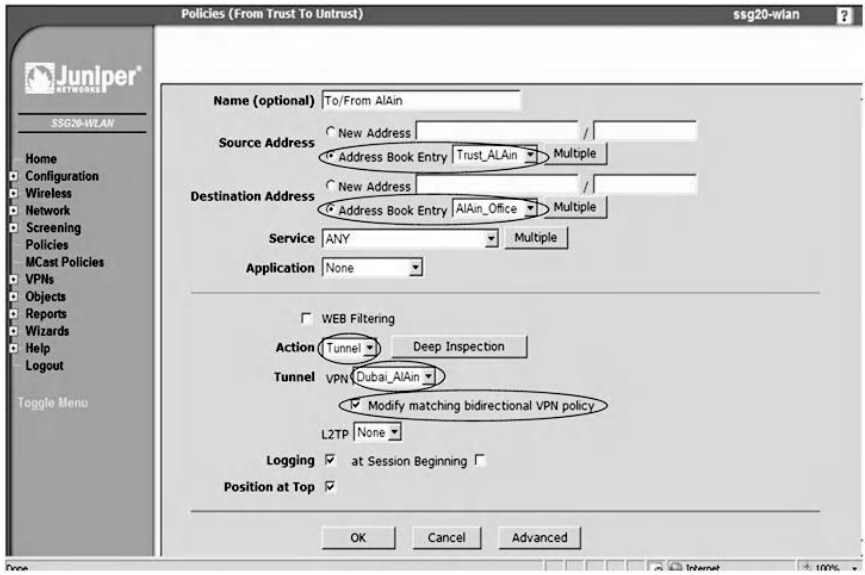


Введите название политики, например, To/From Dubai. Затем укажите источник и предварительно настроенное место назначения для сайта Al-Ain. Выберите “Tunnel” (Туннель) для записи действия. Установите флажок Изменить подходящую двунаправленную политику VPN, которая создаст вторую политику для другого направления: от зоны «Недоверия» до зоны доверия.

Нажмите на кнопку «ОК», чтобы получить две политики, как показано ниже.

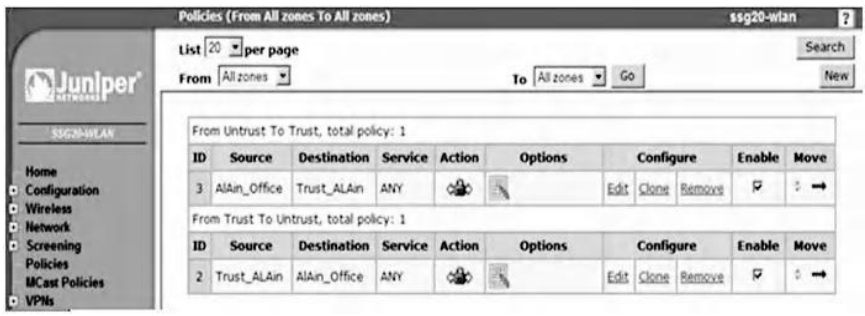
Чтобы установить политики с сайта Дубая, которые позволяют сайту Дубая обмениваться данными с сайтом Аль-Айн через туннель, выберите

“policies” (политики) и очистите правила по умолчанию; затем выберите зоны из выпадающего меню из зоны доверия в зону “Untrust” (Недоверять). Нажмите кнопку “New” (Создать) и заполните поля, как показано на следующем снимке экрана.



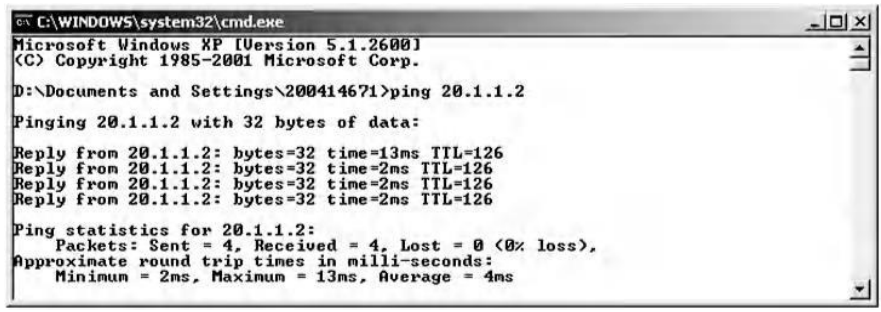
Введите название политики, например, To / From Al-Ain. Затем укажите источник и пункт назначения, которые были предварительно определены для сайта в Дубае. Выберите “Tunnel” (Туннель) для записи действия. Установите флажок Изменить подходящую двунаправленную политику VPN, которая создаст вторую политику для другого направления: от зоны “Untrust”(Недоверия) до зоны доверия.

Нажмите кнопку «ОК», чтобы получить две политики, как показано ниже.



9. *2.3.7 Шаг 7. Отправьте эхо-запрос из Аль-Айна в Дубай и наоборот, чтобы проверить создание VPN-туннеля*

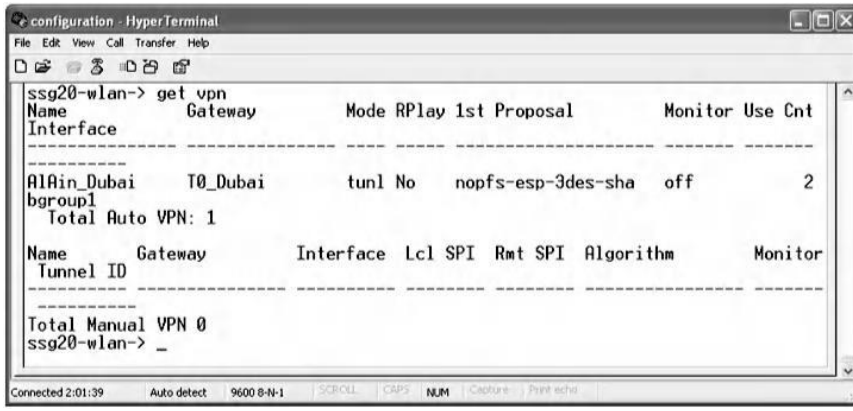
Пинг из Аль-Айна в Дубай, который должен быть успешным, как в следующей команде:



Пинг из Дубая в Аль-Айн, который должен быть успешным. Это подтверждает, что VPN-туннель установлен в обоих направлениях.

9.2.3.8 Шаг 8: Проверьте Установление VPN-туннеля

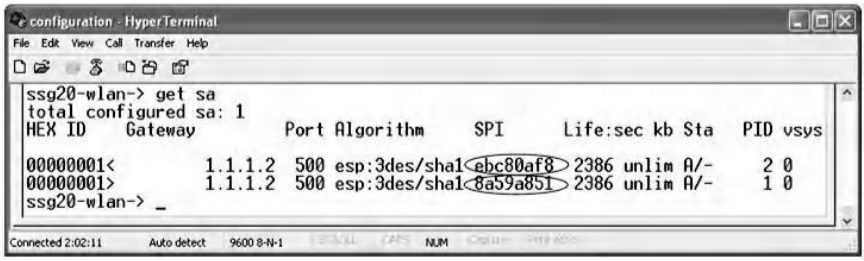
Чтобы проверить установление туннеля между двумя сайтами, проанализируйте ассоциации безопасности, которые создаются после согласования между двумя VPN-шлюзами. Введите следующую команду для сайта Аль-Айн.



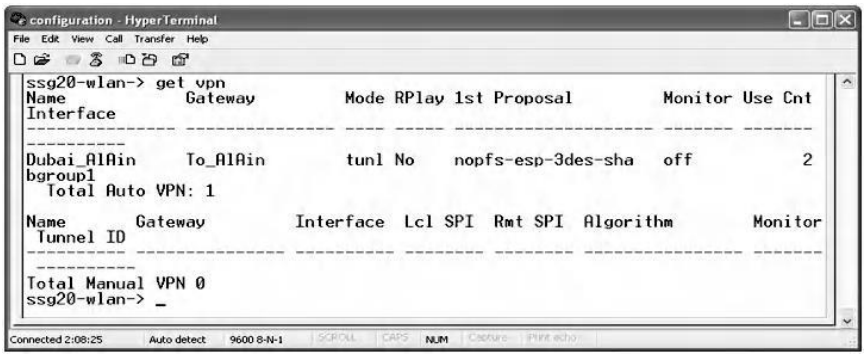
Из приведенного выше вывода ясно, что имя интерфейса - bgroup1 (Al-Ain_Dubai). Имя шлюза - To_Dubai, поскольку оно настроено этим именем для сайта Al-Ain. Режим IPsec - это туннельный режим, который

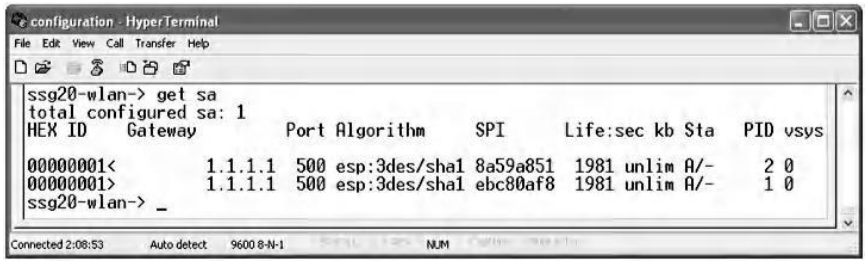
шифрует заголовок IP и полезную нагрузку, так что весь пакет защищен. Первое предложение - это nopfs (без идеальной секретности), что означает, что в будущем не будет никаких изменений в ключевом материале. ESP - это протокол, который обеспечивает безопасные средства для пакета путем шифрования всего IP-пакета и аутентификации его содержимого. 3DES - это алгоритм шифрования, а SHA - используемый алгоритм целостности данных. Количество автоматических VPN равно 1.

Чтобы изучить параметры ассоциации безопасности, используйте команду «get sa», как показано ниже, которая показывает два SA, по одному на направление с IP-адресом шлюза как 1.1.1.2 и портом ISA KMP SHA 1UDP как 500. Алгоритмы - 3DES для шифрования и SHA1 для целостности данных, а SPI - это индекс параметра безопасности, который отличается для каждой ассоциации безопасности.



Чтобы проанализировать установление VPN с сайта в Дубае, повторите предыдущие команды, как показано ниже:





9.3 Лабораторная работа 9.2: VPN типа «сеть-сеть» - вторая реализация

9.3.1 Результат

Цель этого упражнения состоит в том, чтобы учащиеся узнали, как реализовать VPN-туннель между двумя различными сайтами, используя шлюз Cisco VPN.

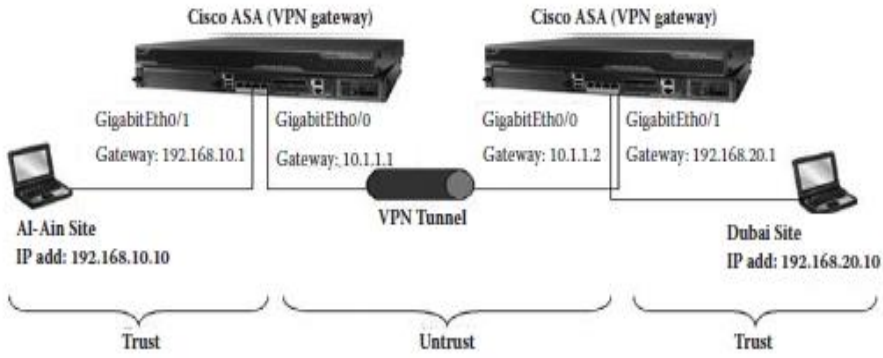
9.3.2 Описание

Этот практический лабораторный сценарий аналогичен предыдущему лабораторному, за исключением того, что он использует шлюз Cisco VPN вместо шлюза Juniper VPN.

9.3.3 Эксперимент

Чтобы узнать, как реализовать VPN-туннель между двумя различными сайтами, проводится эксперимент с использованием Cisco ASA (Adaptive Security Appliance) под управлением ОС 7.0 (7) и коммутатора Cisco 3560.

На следующем рисунке показана сетевая архитектура эксперимента. Сайт 1 представляет Al-Ain и состоит из хоста, который подключен к интерфейсу GigabitEthernet0/1 (Inside) AS-Al-Ain, а сайт 2 представляет Дубай и подключен к интерфейсу Gigabit Ethernet0/1 Дубайской Cisco ASA , Два сайта соединены через интерфейсы Gigabit Ethernet0/0 (снаружи) Cisco ASA, используя перекрестный кабель, где должен быть реализован туннель.



Эксперимент состоит из следующих этапов:

Шаг 1: Сбросьте настройки брандмауэра по умолчанию для обоих сайтов.
Шаг 2. Назначьте IP-адреса компьютеров и интерфейсов брандмауэра на обоих сайтах.
Шаг 3: Определите трафик, который должен быть защищен.
Шаг 4: Создайте статический маршрут от сайта Аль-Айн до сайта в Дубае и наоборот.
Шаг 5: Включите протокол ISAKMP на обоих сайтах.
Шаг 6: Определите параметры фазы 1 IKE.
Шаг 7: Определите предварительный общий ключ, который будет использоваться обоими сайтами.
Шаг 8: Определите параметры IKE фазы 2 протокола IPsec.
Шаг 9: свяжите параметры двух фаз друг с другом.
Шаг 10. Примените криптографическую карту на внешнем интерфейсе (GigabiteEthernet0 / 0).
Шаг 11: Пинг с сайта Al-Ain на сайт в Дубае, и наоборот.
Шаг 12: Изучите параметры, которые установлены в ассоциации безопасности.

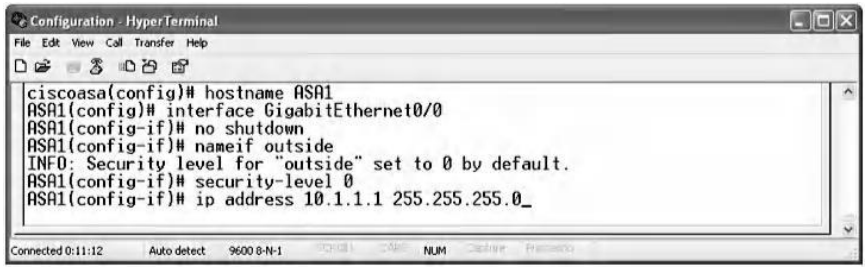
9. *3.3.1 Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию для обоих сайтов*

Подключите ПК к последовательной консоли брандмауэра для сайта Al-Ain через HyperTerminal, чтобы получить интерфейс командной строки брандмауэра. Введите «enable» в приглашении «ciscoasa>».

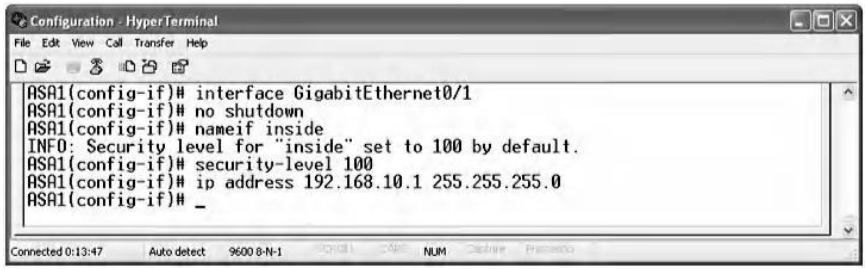
Нажмите клавишу Enter для запроса пароля и затем введите команду терминала «configure». Наконец, введите «configure factory-default», чтобы сбросить систему к настройкам по умолчанию.

9.3.3.2 Шаг 2. Назначьте IP-адреса компьютерам и интерфейсу брандмауэра на обоих сайтах

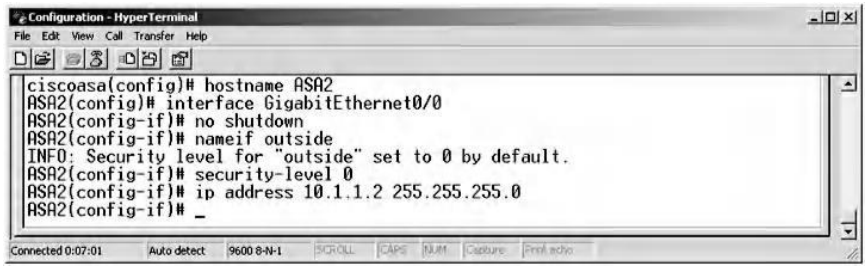
Чтобы переименовать и назначить IP-адреса интерфейсам брандмауэра на сайте Al-Ain, присвойте имя хосту, например ASA1. Назначьте IP-адрес интерфейсу GigabitEthernet0/0 и присвойте имя, например, “outside” (снаружи). Укажите уровень безопасности для интерфейса, как показано на следующем снимке экрана.



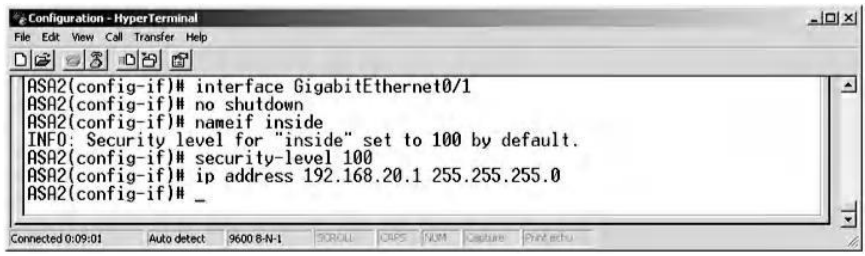
Назначьте IP-адрес интерфейсу GigabitEthernet0/1 и присвойте ему имя, например, “inside” (изнутри). Укажите уровень безопасности 100 для этого интерфейса, как показано на следующем снимке экрана.



Чтобы переименовать и назначить IP-адреса интерфейсу брандмауэра на сайте в Дубае, введите следующие команды:



Назначьте IP-адрес интерфейсу GigabitEthernet0/1 и присвойте ему имя, например, “inside” (внутри).



9. *3.3.3 Шаг 3: Определите трафик, который должен быть защищен*

Чтобы защитить трафик между двумя сайтами, создайте список доступа на сайте ASA в Аль-Айне, введя следующую команду:

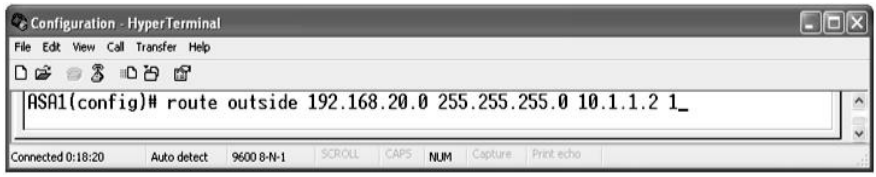
```
ASA1 (config-if)# access-list PROXY_ACL extended
permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

Затем создайте список доступа на сайте ASA в Дубае, введя следующую команду:

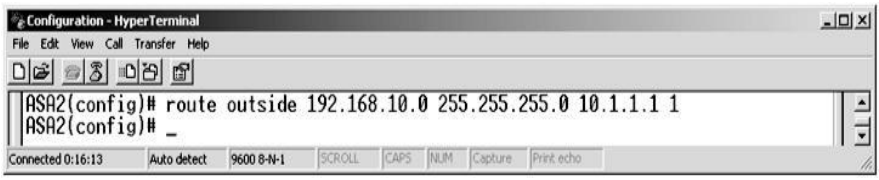
```
ASA2 (config-if)# access-list PROXY_ACL extended
permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

9. *3.3.4 Шаг 4. Создайте статический маршрут от сайта Аль-Айн до сайта в Дубае и наоборот.*

Чтобы сайт Al-Ain мог обмениваться данными с удаленным сайтом, должен быть процесс маршрутизации из-за расстояния между сайтами. Укажите шлюз ASA2 для адреса удаленной сети с помощью следующей команды:

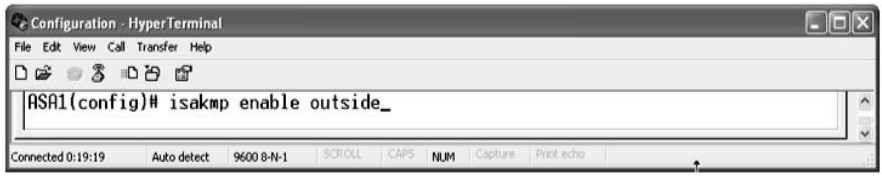


Чтобы сайт Дубая мог обмениваться данными с удаленным сайтом, настройте такой же статический маршрут, как в следующей команде:



9.3.3.5 Шаг 5: Включите протокол IKE на обоих сайтах

Чтобы разрешить согласование между двумя сайтами, включите IKE. Это протокол, который предлагает процедуры аутентификации между связанными узлами, генерации ключей и управления для ассоциации безопасности. Введите следующую команду для сайта Al-Ain:



Аналогично, для сайта в Дубае повторите ту же команду:

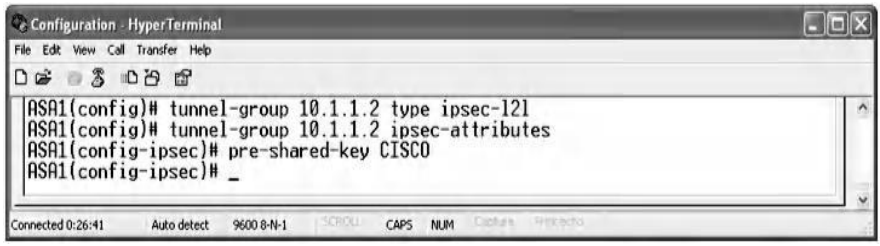
9.3.3.6 Шаг 6: Определите параметры фазы 1 IKE

Чтобы установить параметры IKE сайта Al-Ain, определите методы аутентификации, шифрование, хэш, группу Диффи-Хеллмана и время жизни, как показано ниже:

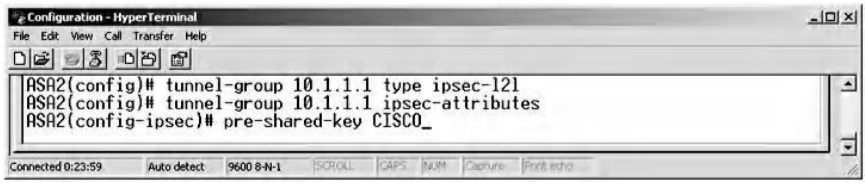
Чтобы установить параметры IKE для сайта в Дубае, повторите приведенные выше команды для сайта в Дубае:

9. 3.3.7 Шаг 7: Определите предварительный общий ключ, который будет использоваться обоими сайтами

Установите предварительный общий ключ, который является секретным значением, которым участники обмениваются заранее, прежде чем произойдет какая-либо связь. Он используется для аутентификации между двумя устройствами. Для этого введите следующие команды:



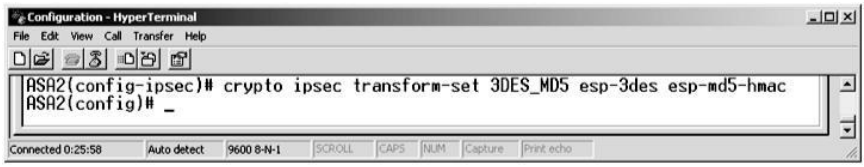
Обязательно используйте тот же предварительный общий ключ для сайта в Дубае, что и в следующих командах:



9. *3.3.8 Шаг 8: Определите параметры фазы IKE 2 протокола IPsec*

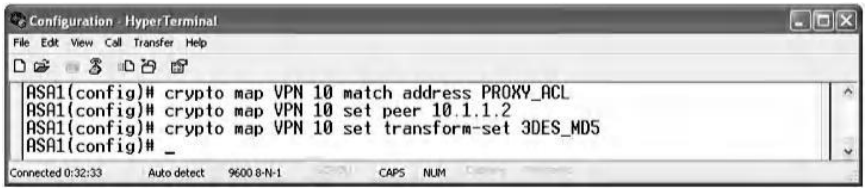
На этом этапе происходит согласование параметров SA и совпадение параметров между узлами. Параметры зашифрованы с использованием 3DES и аутентифицированы с использованием MD5 для Аль-Айна.

Аналогично для сайта в Дубае введите те же команды:

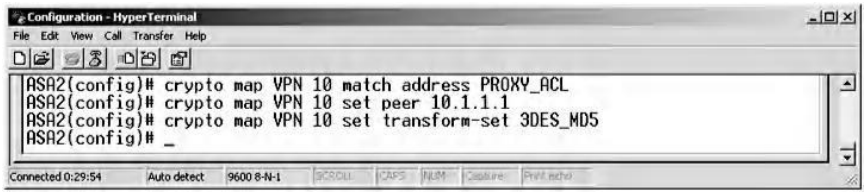


9.3.3.9 Шаг 9: Свяжите параметры двух фаз друг с другом

Используйте команду «crypto map», чтобы связать параметры двух фаз для сайта Аль-Айн. «crypto map» определяет прокси-ACL, который идентифицирует защищенный трафик, равноправный IP-адрес и набор преобразований фаз, как показано в следующих командах:



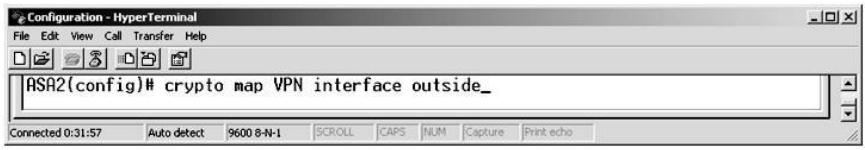
На сайте в Дубае определите другую криптографическую карту:



9. 3.3.10 *Шаг 10. Применение криптокарты на внешнем интерфейсе (GigabitEthernet 0/0)*

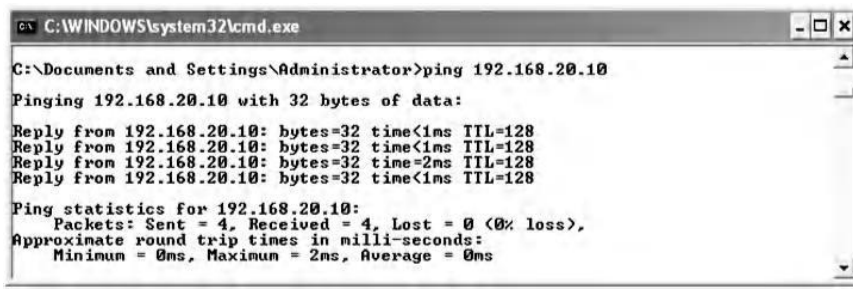
Чтобы криптографическая карта функционировала, ее необходимо применить к внешнему интерфейсу, как показано в следующей команде на сайте Аль-Айн:

Примените криптографическую карту на внешнем интерфейсе ASA2 на сайте в Дубае, как показано ниже:

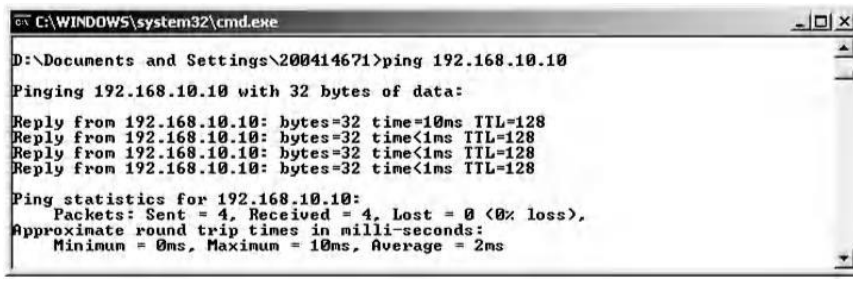


9. 3.3.11 *Шаг 11: Пинг с сайта Al-Ain на сайт в Дубае и наоборот*

Чтобы проверить создание туннеля, выполните команду ping из Аль-Айна в Дубай, как показано ниже:

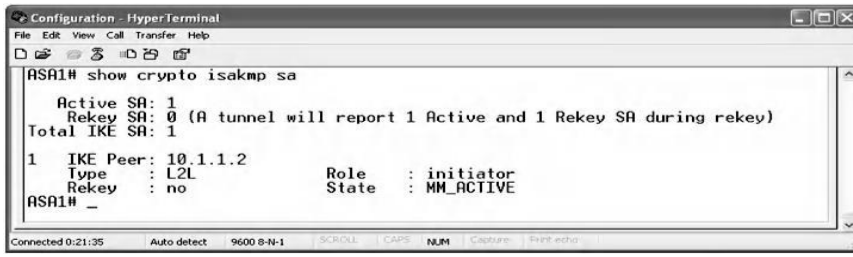


Затем выполните команду ping с сайта в Дубае до сайта Al-Ain, как показано ниже:



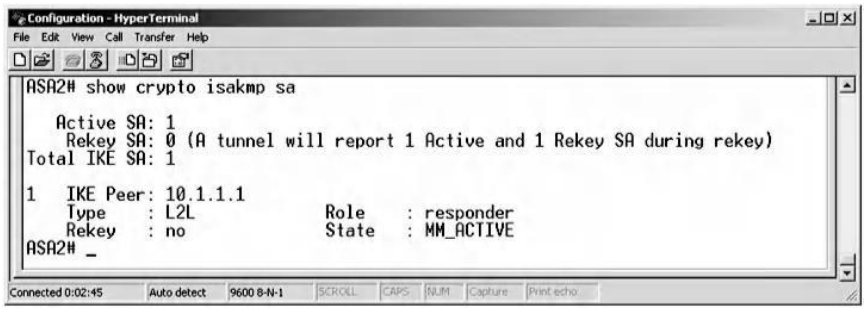
9. 3.3.12 *Шаг 12: Изучите параметры, которые установлены в ассоциации безопасности*

Используйте команду «show crypto isakmp sa» на сайте Al-Ain для отображения согласованных параметров SA IKE фазы 1, как показано ниже:

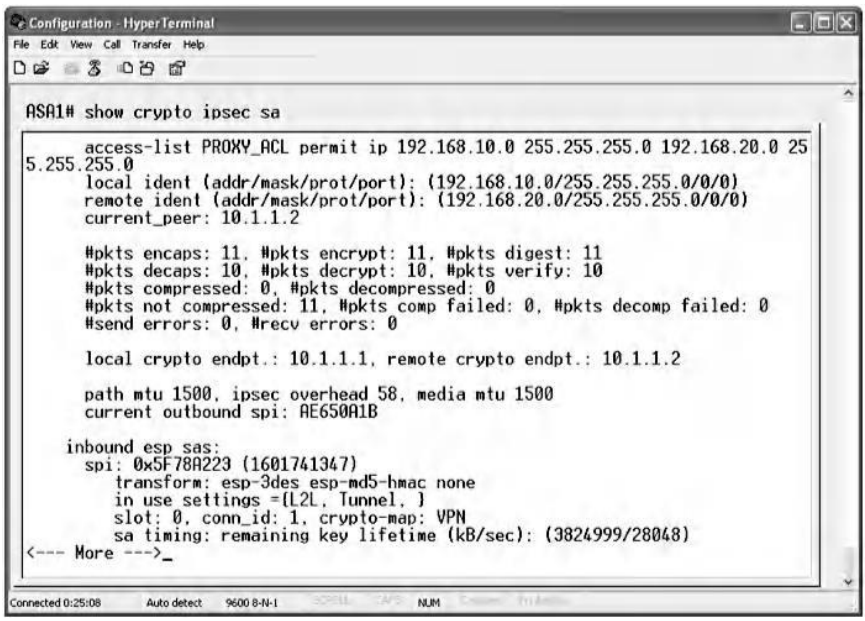


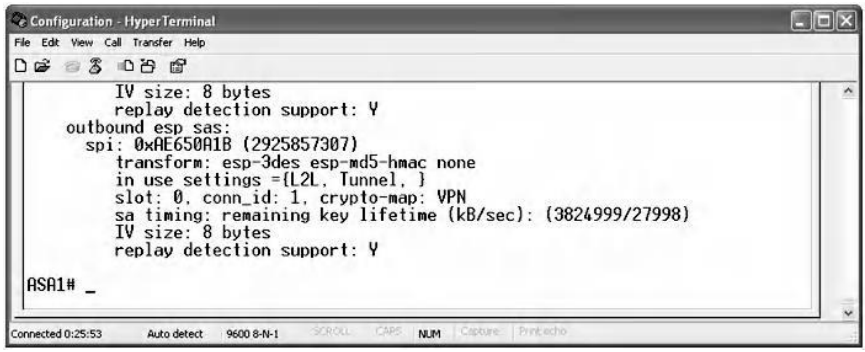
Предыдущая команда указывает, что число активных сопоставлений безопасности равно единице. Узел IKE 10.1.1.2 является шлюзом для удаленного узла (сайт Дубая). Тип соединения - соединение LAN-LAN. Роль устройства Al-Ain - это роль инициатора соединения с удаленным узлом.

Вывод этой же команды на сайте в Дубае следующий:

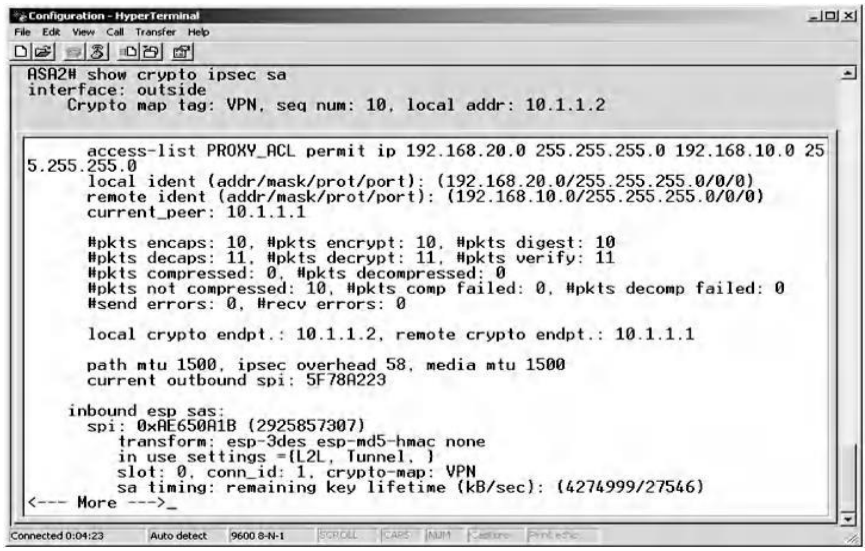


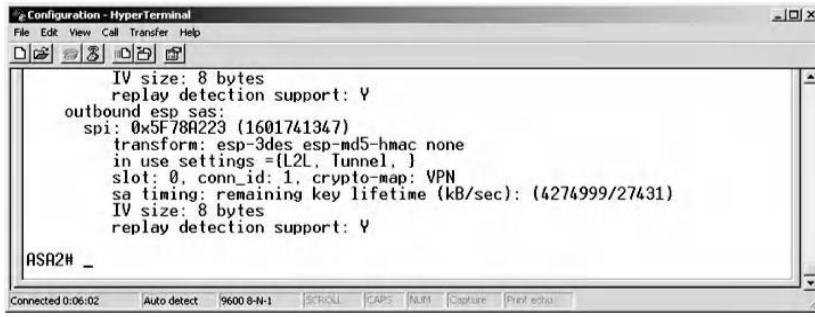
Чтобы отобразить сопоставление безопасности IKE фазы 2, введите следующую команду для сайта Al-Ain: «show crypto ipsec sa».



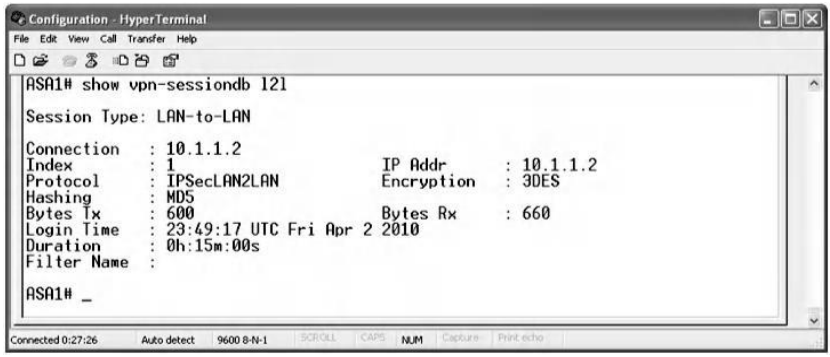


Выходные данные вышеприведенной команды указывают, что количество инкапсулированных, зашифрованных и переваренных пакетов равно 11. Количество декапсулированных, дешифрованных и проверенных пакетов равно 10. Количество сжатых и распакованных пакетов равно 0. IPsec режим туннельный режим. Есть два SA, один входящий и один исходящий. Каждый SA имеет свой собственный SPI. Аналогичный вывод появится для сайта в Дубае, как показано ниже:

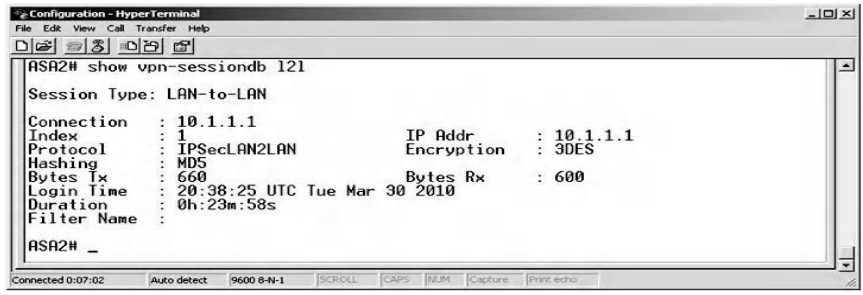




Чтобы просмотреть более подробную информацию о VPN-туннеле, введите следующую команду для обоих сайтов:



Отображается несколько параметров сеанса, который произошел между узлами, например, Тип сеанса: LAN-to-LAN. Соединение установлено с другим узлом 10.1.1.2. Отображаются алгоритмы шифрования и хеширования, а также время входа и продолжительность сеанса. Аналогичный результат можно получить для сайта в Дубае, как показано ниже:



9.4 Краткое содержание главы

Внедрение IPsec VPN-решений может быть очень утомительной задачей. Следовательно, включение VPN в решения сетевой безопасности является сложной задачей как для новичка, так и даже для специалиста по промежуточной безопасности. Соответственно, основной целью этой главы было как можно более понятное объяснение реализации VPN с использованием различных иллюстраций, снимков экрана и этапов настройки. В этой главе представлен общий обзор технологии VPN и кратко объяснено, как она работает. Кроме того, он представил сравнение фаз протокола IKE, режимов IPsec, протоколов IPsec и типов VPN. В этой главе основное внимание уделялось архитектуре IPsec VPN типа «сеть-сеть». Сценарии развертывания и рекомендации по внедрению были объяснены с использованием продуктов безопасности двух лидеров в этой области, а именно Juniper Networks и Cisco Microsystems.

Глава 10

Внедрение VPN-туннеля удаленного доступа против подслушивающих атак

10.1 Введение

Связь в любое время и в любом месте, обеспечивающая бесперебойную связь, является важным катализатором успешного делового и научного решения. Существует растущий спрос на такого рода подключения, но также растет обеспокоенность по поводу конфиденциальности информации в таких сетях. Поскольку это требование удовлетворяется, информационная безопасность и конфиденциальность являются очевидной проблемой, которая должна быть эффективно решена. IPsec VPN с удаленным доступом (виртуальная частная сеть) становится все более эффективным решением для обеспечения конфиденциальности данных в Интернете. В этой главе дается подробное объяснение решения безопасности IPsec VPN для удаленного доступа, которое позволяет удаленным пользователям за удаленным VPN-клиентом безопасно получать доступ к данным и сетевым ресурсам центрального сайта через VPN-туннель. Будучи интернет-технологией, она предлагает масштабируемое, недорогое, где угодно и когда угодно, решение для малого, среднего и крупного бизнеса.

VPN с удаленным доступом имеет решающее значение для любой системы безопасности сети предприятия, в основном из-за растущих приложений вне предприятия, которым требуется безопасный доступ к критически важным внутренним сетевым ресурсам. Типичный случай использования IPsec VPN с удаленным доступом - когда сотрудники хотят получить доступ к своим офисным компьютерам во время путешествий. Несмотря на безопасный доступ к сетевым ресурсам, который обеспечивает VPN с удаленным доступом, он часто открывает двери для серьезных угроз. Возможный метод проникновения - когда зараженная удаленная система ставит под угрозу меры безопасности защищенной сети. Следовательно, «Сетевой контроль доступа» (NAC) или сканирование соответствия выполняется на удаленном пользовательском компьютере. Это гарантирует, что на машине нет вредоносных программ или какого-либо вредоносного кода и что она полностью соответствует политикам безопасности защищенной сети. Кроме того, зашифрованный трафик VPN рассматривается как доверенный трафик, и поэтому он по умолчанию обходит политики безопасности защищенного сетевого брандмауэра. Для борьбы с этой угрозой необходимо установить межсетевой экран после шлюза VPN для выполнения политик безопасности в дешифрованном трафике VPN. Это требует наличия решения VPN как части комплексного решения безопасности, которое также включает в себя брандмауэр и систему защиты от вторжений.

Как и в предыдущей главе, здесь реализованы два решения IPsec VPN для удаленного доступа. Это дает четкое представление об основных компонентах, участвующих в процессе настройки VPN-туннеля.

Следующие аппаратные и программные средства необходимы для выполнения задач настройки:

* Беспроводное устройство Juniper Networks SSG20 *: шлюз VPN
* VPN-клиент удаленного доступа Juniper Networks †: VPN-клиент

* http://www.juniper.net
† http://www.juniper.net

* Устройство Cisco Microsystems ASA *: шлюз VPN
* VPN-клиент удаленного доступа Cisco Microsystems †: VPN-клиент

10.2 Лабораторная работа 10.1: VPN с удаленным доступом - первая реализация

10.2.1 Результат

Цель этого упражнения - научить студентов внедрять VPN с удаленным доступом с использованием технологии Juniper.

10.2.2 Описание

В отличие от VPN-соединений типа «сеть-сеть», для которых требуются как минимум два шлюза VPN, два основных компонента, составляющих VPN-сеть IPsec удаленного доступа, представляют собой программный компонент, называемый VPN-клиентом удаленного доступа, и VPN-шлюз, также называемый удаленным доступом. VPN-сервер.

Во-первых, программный компонент, называемый VPN-клиентом удаленного доступа, успешно устанавливается на клиентском компьютере, прежде чем предпринимать какие-либо попытки подключиться к сети центрального сайта. Основная роль VPN-клиента заключается в получении политик безопасности от второго компонента (VPN-сервера). Современные настольные операционные системы, такие как Windows, Linux, Macintosh и Solaris, предоставляют встроенную версию удаленного VPN-клиента. Здесь мы используем программное обеспечение Juniper для VPN-клиента. Существенным преимуществом использования VPN с удаленным доступом является то, что настройка и настройка клиента VPN с удаленным доступом чрезвычайно минимальны.

Второй компонент, который является VPN-шлюзом (сервером), обычно является аппаратным компонентом. Его роль очень похожа на шлюз VPN VPN типа «сеть-сеть»; однако, это требует, чтобы удаленный пользователь предоставил необходимые учетные данные для аутентификации перед установкой VPN-туннеля.

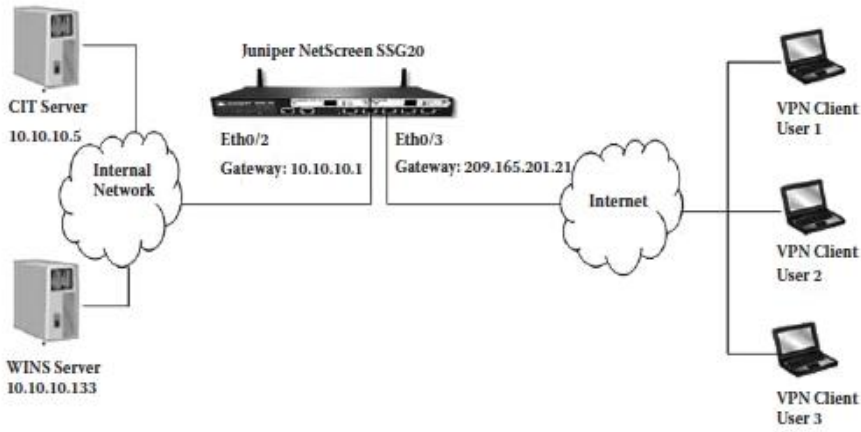
* http://www.cisco.com
† http://www.cisco.com

Этапы настройки обоих компонентов VPN с удаленным доступом описаны в разделе «Эксперимент» (раздел 10.2.3). Кроме того, необходимые процедуры тестирования проводятся, чтобы подтвердить, что VPN-туннель установлен и работает как требуется.

10.2.3 Эксперимент

Этапы настройки VPN для удаленного доступа выполняются с использованием Juniper NetScreen SSG20 с работающим ScreenOS 5.4.0r1.0 и Juniper NetScreen Remote VPN Client.

Следующий рисунок иллюстрирует сетевую архитектуру эксперимента, предназначенного для трех пользователей для удаленного доступа к внутренней сети через VPN в качестве примера. Три пользователя подключены к “Untrust”(недоверенной) зоне на Ethernet0/3.



Эксперимент состоит из следующих этапов:

Шаг 1. Сбросьте брандмауэр до значения по умолчанию.
Шаг 2. Назначьте IP-адреса компьютеров и интерфейсов брандмауэра.
Шаг 3: Создание пользователей.

Шаг 4: Настройте предложение фазы 1.
Шаг 5: Настройте предложение фазы 2.
Шаг 6: Создайте политику безопасности.
Шаг 7. Настройте удаленного VPN-клиента NetScreen и проверьте подключение.
Шаг 8: Проверьте установление VPN-туннеля.

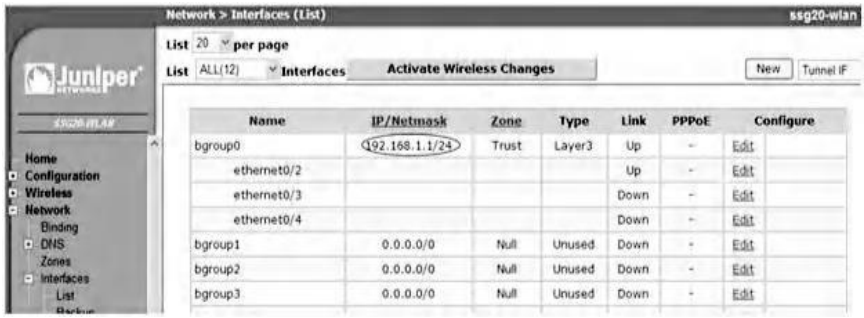
10. 2.3.1 Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию

Обратитесь к шагу 1 в первой лабораторной работе для VPN типа «сеть-сеть» (лабораторная работа 9.1) с использованием сетевого брандмауэра Juniper.

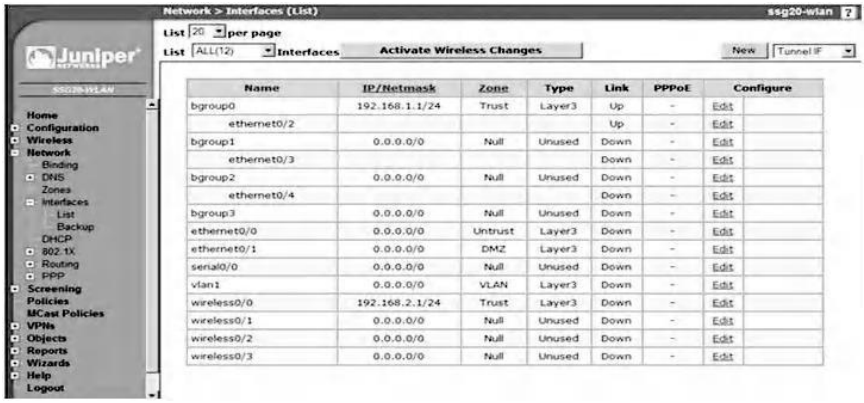
10. 2.3.2 Шаг 2. Назначьте IP-адреса компьютерам и интерфейсу брандмауэра

Обратитесь к шагу 1 в первой лабораторной работе для VPN типа «сеть-сеть» (лабораторная работа 9.1) с использованием сетевого брандмауэра Juniper, пока не отобразится экран настройки брандмауэра.

Здесь IP-адреса назначаются интерфейсу брандмауэра. Сначала нажмите “Network”(Сеть), затем “Interfaces”(Интерфейсы) и, наконец, “Lists”(Списки), чтобы увидеть экран, показанный ниже.

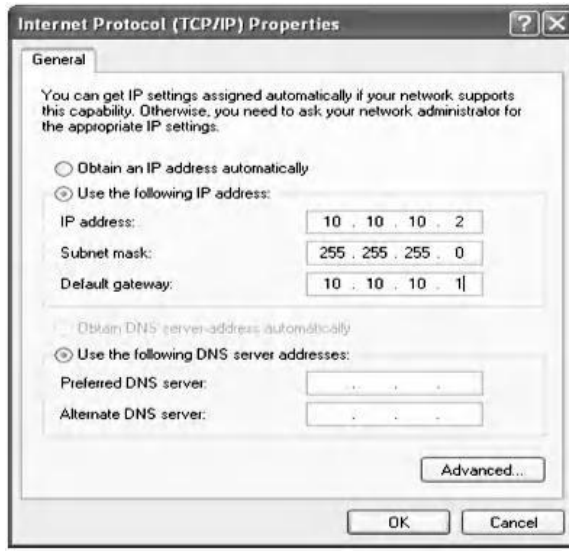


IP-адрес по умолчанию, назначенный интерфейсу bgroup0, - 192.168.1.1. Перед назначением IP-адресов интерфейсам интерфейсы Ethernet разделяются на различные “bgroups”(группы), как показано далее.

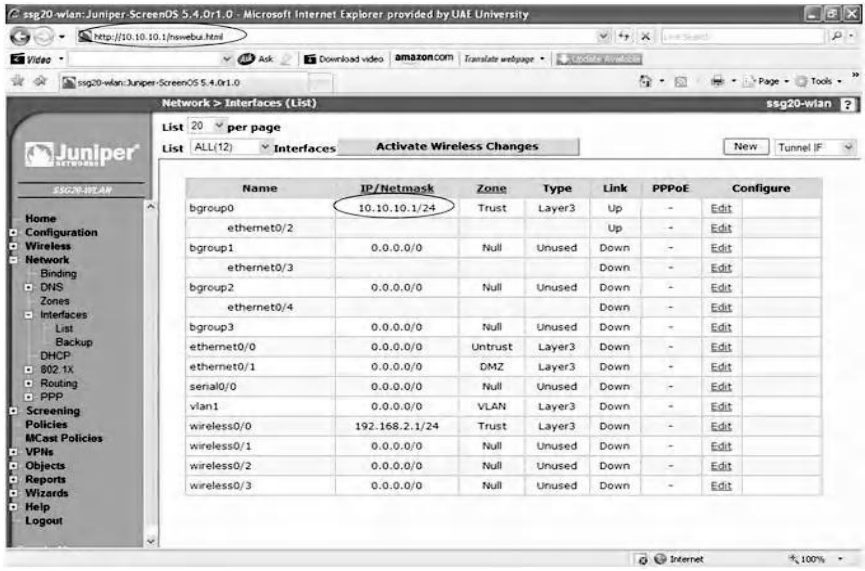


Нажмите на ссылку “Edit” (Редактировать) интерфейса bgroup0 и введите значения, как показано ниже. Убедитесь, что имя зоны указано как “Trust”(Доверие), а режим интерфейса - «NAT». Включите службы, которые будут использоваться в этой зоне (например, WebUI), что позволяет пользователю получать доступ к конфигурации брандмауэра с помощью веб-пользователя. интерфейс через eth0/2. Подтвердите настройку, нажав “Apply”(Применить), а затем «OK».

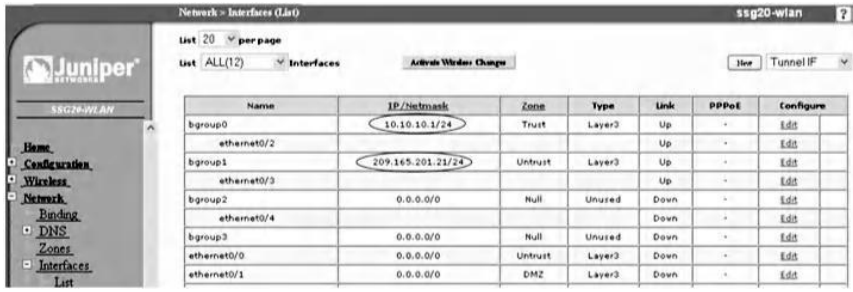
После изменения IP-адреса интерфейса веб-интерфейс Juniper автоматически выходит из системы. Поэтому измените IP-адрес ПК на 10.10.10.2/24, чтобы поддерживать связь, как показано ниже.



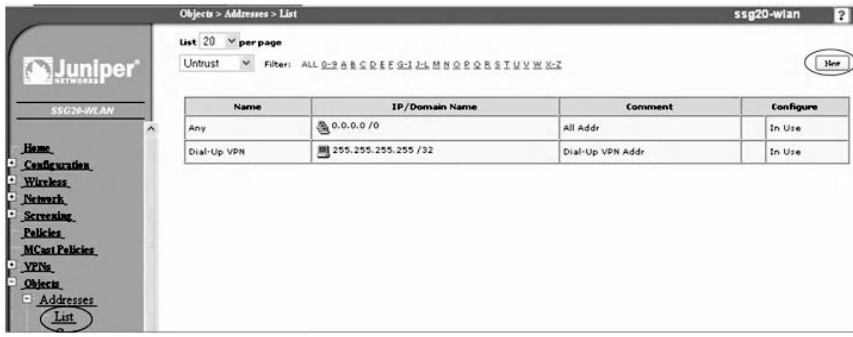
Используйте веб-браузер, чтобы перейти к http://10.10.10.1 для доступа к веб-интерфейсу пользователя. Выберите “Network”(Сеть), затем “Interfaces”(Интерфейсы) и, наконец, “List”(Список), который отображает следующий экран.



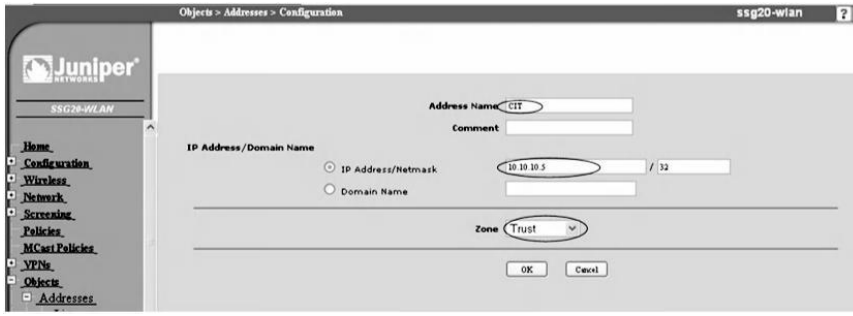
Нажмите на ссылку “Edit” интерфейса bgroup1 и введите значения, как показано ниже. Имя зоны - “Untrust”(Недоверие), когда удаленные пользователи пытаются получить доступ к доверенной зоне через VPN-туннель, который будет создан. Включите службы для использования в этой зоне, нажав “Apply”, а затем «ОК». Сконфигурированные IP-адреса назначаются интерфейсам eth0/2 и eth0/3.



Чтобы создать сетевой IP-адрес сервера, к которому будут подключаться удаленные пользователи, выберите “Objects”(Объекты), затем “Address”(Адрес) и, наконец, “List”(Список). Нажмите “New”, как указано ниже.

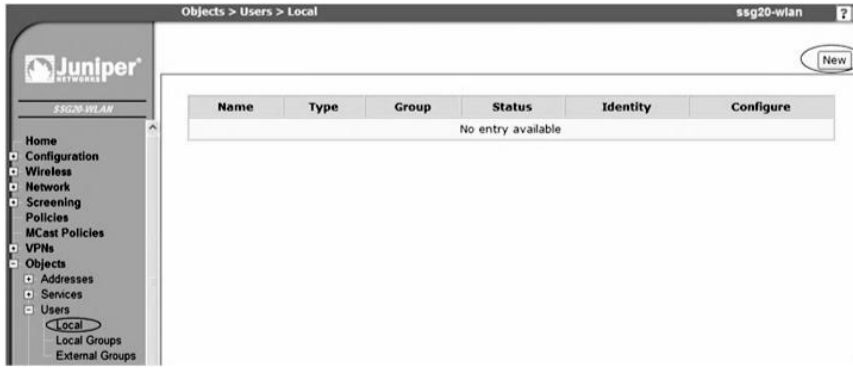


Заполните значения, как показано в следующем. Дайте адресу имя, которое в нашем примере - «CIT», чтобы облегчить выбор адреса назначения при настройке политики. Затем введите IP-адрес и маску сети, и, наконец, выберите зону “Trust”(Доверие) в раскрывающемся меню и подтвердите, нажав «ОК».

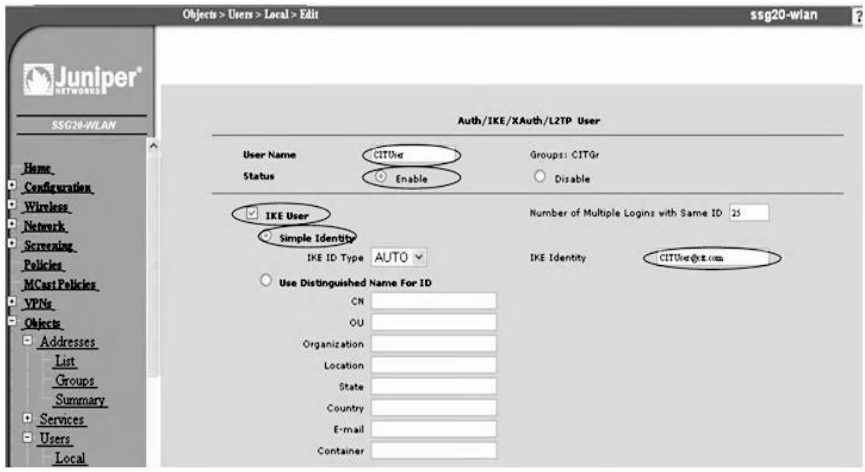


10.2.3.3 Шаг 3: Создание пользователей

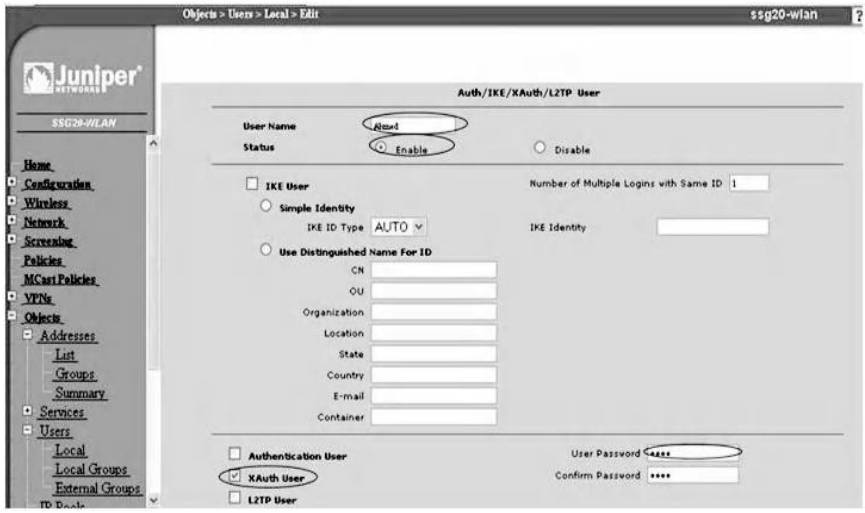
Чтобы создать пользователей для удаленного подключения через VPN, перейдите через “Objects”(Объекты), затем “Users”(Пользователи) и, наконец, “Local”(Локальный). Нажмите “New”, как указано ниже.

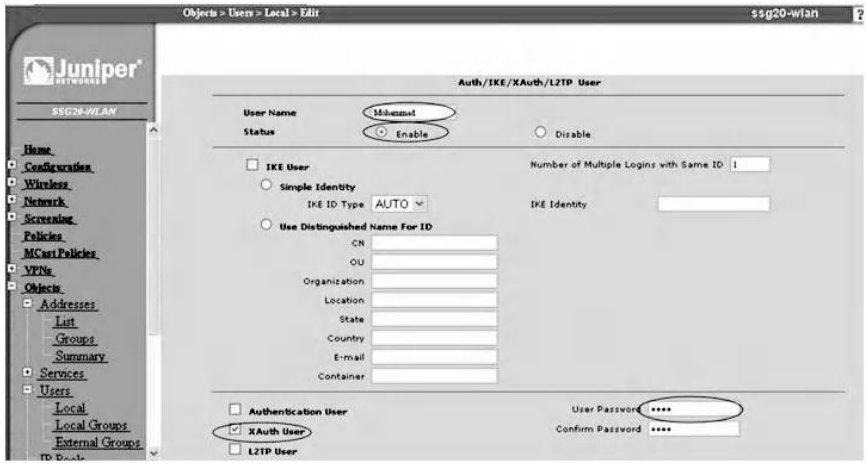


NetScreen предоставляет различные типы пользователей, и каждый тип имеет свои особенности. Введите имя пользователя и включите статус для пользователя. Затем выберите тип пользователя «IKE User», который использует локальную базу данных, предоставленную устройством NetScreen. Выберите опцию «Простая идентификация» и введите идентификационную информацию пользователя, которая называется “CITUser@cit.com.” Подтвердите настройки, нажав «ОК», как показано ниже.



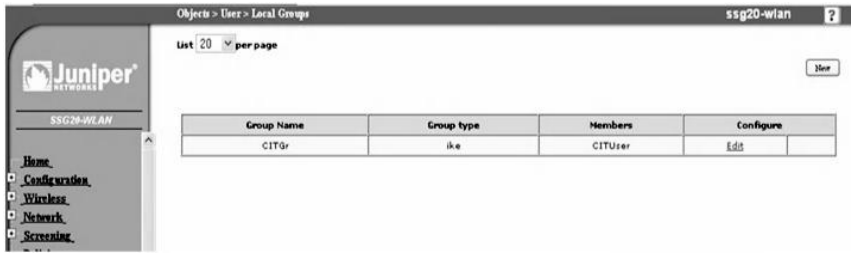
Теперь создайте еще двух пользователей с типом XAuth, чтобы гарантировать, что пользователям будет предложено аутентифицировать себя с помощью имени пользователя и пароля для установления соединения. Экраны показаны на следующих двух скриншотах для первого и второго пользователей XAuth.





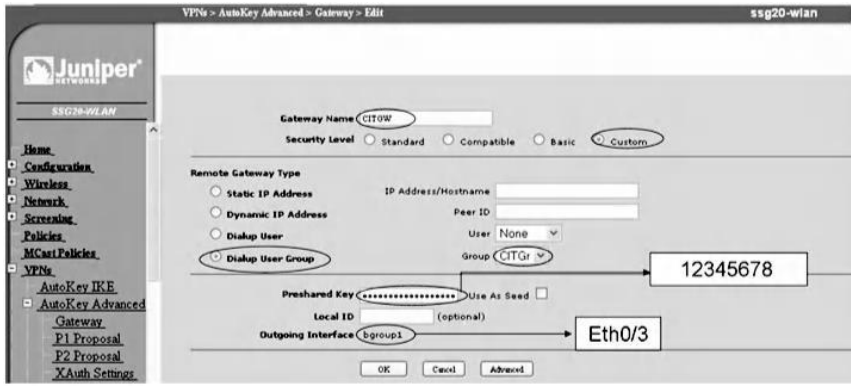
Затем создайте группу для пользователей, которые были созданы. Перейдите к “Objects”(Объектам), а затем “User Groups”(Группам пользователей) и, наконец, “Local”(Локальным). Укажите имя группы, затем выберите участников в области “Available Members”(Доступные участники) и добавьте их в текстовую область “Group Members”(Участники группы). Подтвердите, нажав «ОК», как показано на следующем скриншоте

Группа создается с ее членами, как показано ниже.

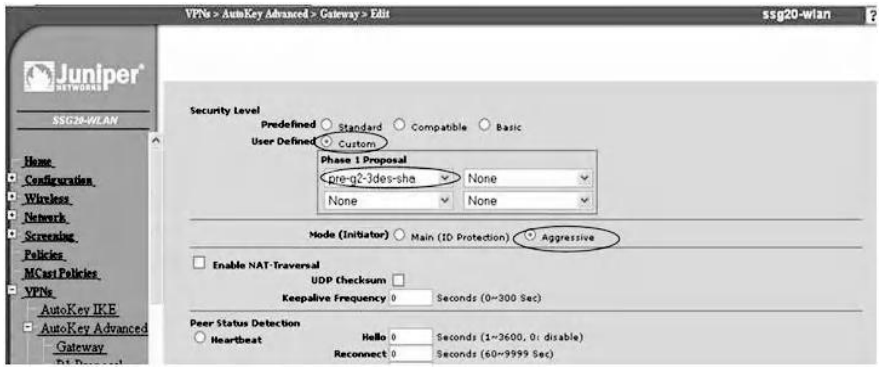


10.2.3.4 Шаг 4: Сконфигурируйте предложение Фазы 1

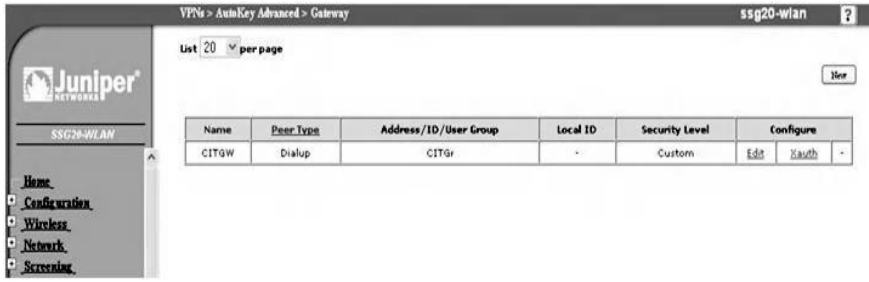
Чтобы создать предложение фазы 1, как показано на следующем снимке экрана, сначала перейдите к «VPN», затем «AutoKey Advanced» и далее “Gateway”(Шлюз) (AutoKey - это автоматический обмен ключами и согласование с сертификатом или предварительно предоставленным ключом, используемым протокол обмена ключами в Интернете). Далее нажмите “New” и введите название шлюза. Выберите уровень безопасности как “Custom”(Пользовательский), а также выберите тип удаленного шлюза как “Dialup User Group”(Группа пользователей удаленного доступа); затем выберите группу из выпадающего меню. Укажите предварительный общий ключ (в нашем примере это «12345678»). Выберите исходящий интерфейс, который является “Untrust” (недоверенным) интерфейсом (bgroub1) (см. Следующий экран).



Далее нажмите на кнопку “Advanced”(Дополнительно); Результат показан ниже (т. е. расширенный этап настройки VPN-шлюза, фаза 1).



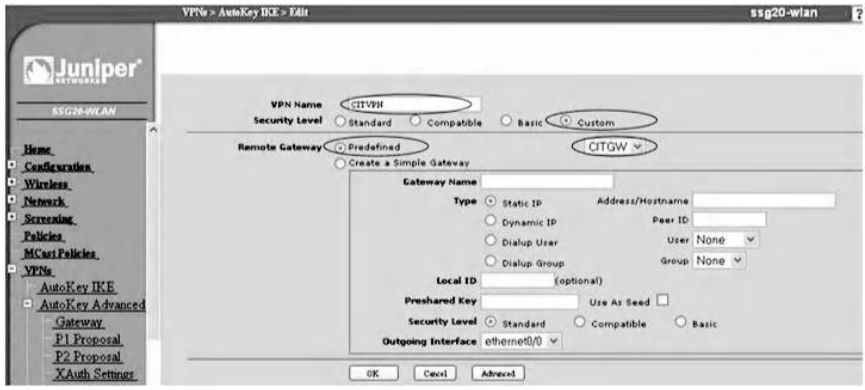
Укажите параметры фазы 1, выбрав “Custom”(Пользовательский) в качестве уровня безопасности. Далее выберите предложение фазы 1 из выпадающего меню. Он состоит из трех алгоритмов. Первый - группа Диффи-Хеллмана 2, которая используется для соглашения о секретном ключе между двумя концами. Второй алгоритм - 3DES, который используется для целей шифрования. Третий алгоритм - это SHA, который используется для аутентификации. Выберите aggressive mode(агрессивный режим) и нажмите “Return”(Вернуться); затем подтвердите, нажав «ОК», чтобы завершить этапы создания фазы 1, как показано ниже (этап 1 шлюза VPN завершен).



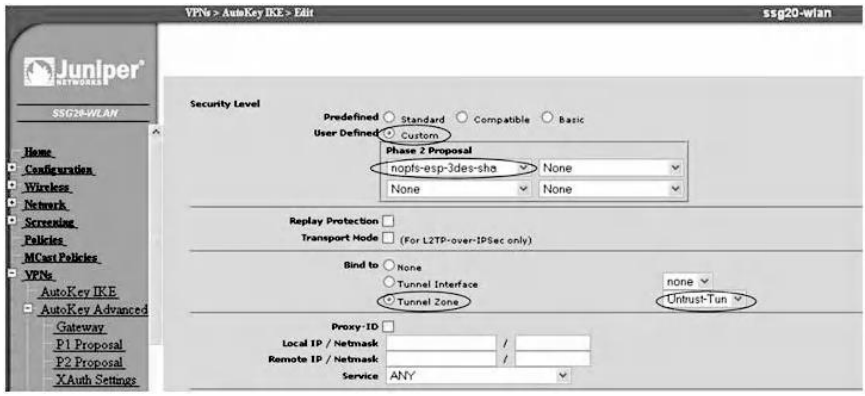
Поскольку пользователи Xauth настроены, сервер Xauth должен быть включен. Чтобы включить это, нажмите на ссылку «Xauth» и выберите «XauthServer»; затем выберите «Local Authentication» и выберите «Allow Any». Подтвердите, нажав «ОК». Настройки сервера Xauth показаны ниже.

10.2.3.5 Шаг 5: Настройте предложение фазы 2

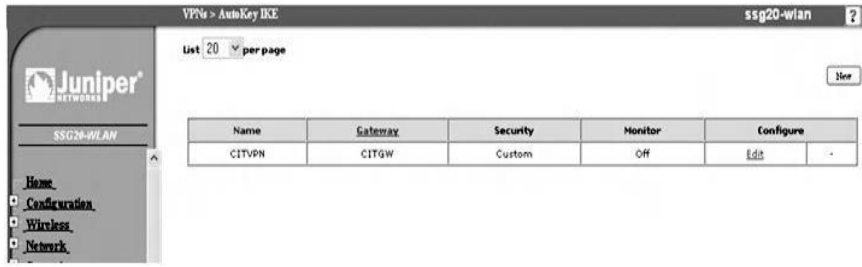
Как показано в базовой конфигурации следующего этапа 2, создайте предложение этапа 2, перейдя к «VPN», а затем «AutoKey IKE» и нажмите “New”. Введите имя VPN как «CITVPN» и выберите “Custom” в качестве защиты уровень. Выберите “Predefined”(Предопределенный) для удаленного шлюза, а затем выберите шлюз в раскрывающемся меню.



Далее нажмите “Advanced”(Дополнительно); результирующий экран (расширенная конфигурация шлюза VPN фазы 2):

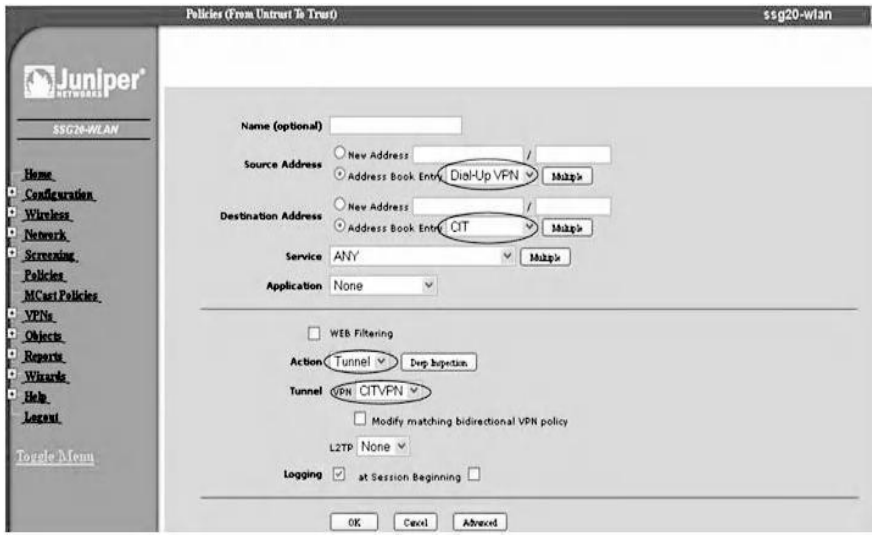


Теперь укажите параметры фазы 2, выбрав “Custom” для уровня безопасности. Затем выберите предложение фазы 2 из выпадающего меню. Он состоит из протокола ESP, алгоритма 3DES и алгоритма хеширования SHA. Выберите “Tunnel Zone”(Туннельная зона) для “Bind to” (Привязать к); затем выберите “Untrust”(Недоверие) из выпадающего меню. Нажмите “Return”(Вернуться), чтобы подтвердить настройки. Затем нажмите «OK», чтобы завершить создание фазы 2, как показано ниже для фазы 2 шлюза VPN.



10.2.3.6 Шаг 6: Создайте политику безопасности

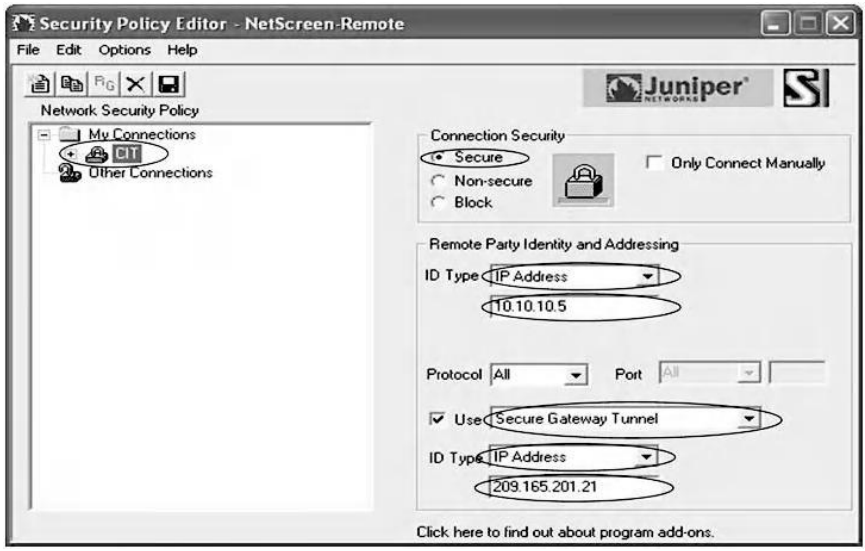
Чтобы пользователи могли подключаться удаленно, политика безопасности настраивается путем перехода к пункту “Policies”(Политики). Затем выберите раскрывающееся меню “Zones”(Зоны) из “Untrust” в “Trust” и нажмите “New”. Затем заполните записи, как показано на следующем экране создания политики безопасности.



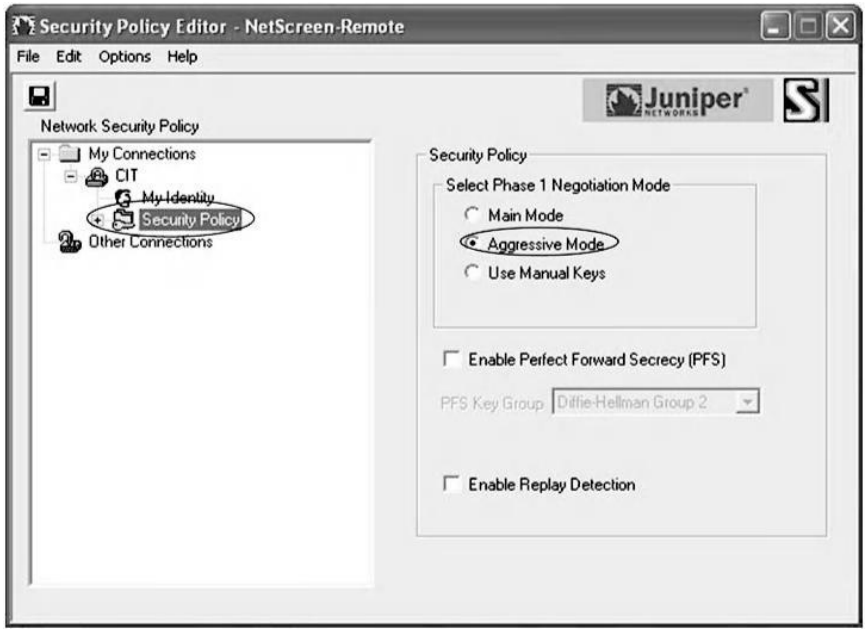
Укажите исходный адрес как «Dial-Up VPN» для удаленных пользователей, что является стороной “Untrust”(Недоверчивость). Укажите адрес назначения как «CIT», который является стороной “Trust”(Доверие), к которой будет подключаться удаленный пользователь. Действие политики должно быть “Tunnel”(Туннель), а полем туннеля является предварительно настроенный VPN, который называется «CITVPN». Подтвердите настройки, нажав «OK».

10. 2.3.7 Шаг 7. Настройте удаленный VPN-клиент Juniper NetScreen и проверьте подключение

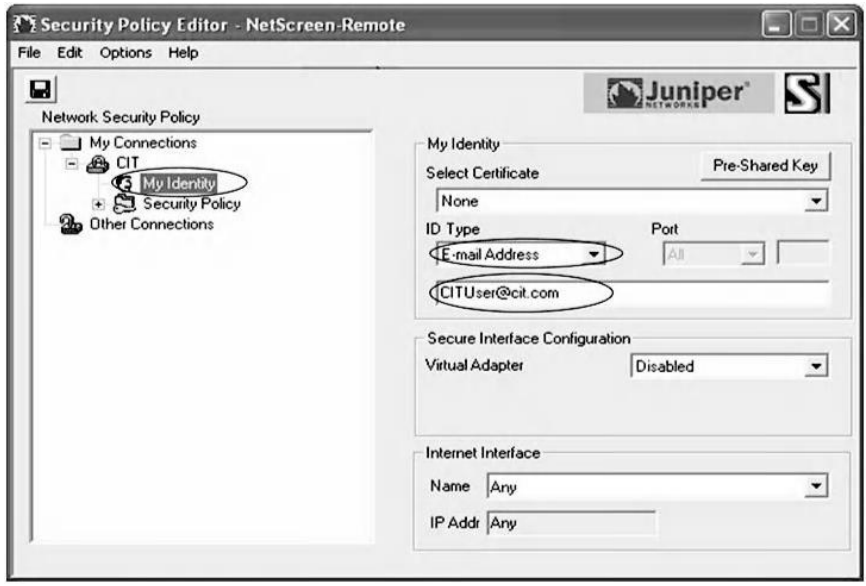
Установите программное обеспечение удаленного VPN-клиента NetScreen на клиентском компьютере и запустите программное обеспечение для его настройки. Сначала нажмите кнопку “New” соединение и введите имя соединения как «CIT». В области Connection Security (Безопасность соединения) выберите опцию “Secure” (Безопасный); для “Remote Party Identity and Addressing” (Идентификации и адресации удаленной стороны) выберите IP-адрес в качестве “ID Type” (Типа идентификатора). Затем введите IP-адрес. Наконец, включите “Use Secure Gateway Tunnel”(Использовать защищенный туннель шлюза) и введите IP-адрес удаленного шлюза. Конфигурация удаленного VPN-клиента Juniper NetScreen показана ниже.



Теперь разверните дерево соединения CIT и нажмите “Security Policy.”. Выберите “Aggressive Mode” для “Phase 1 Negotiation Mode”(Режим согласования фазы 1), чтобы соответствовать конфигурации шлюза VPN.

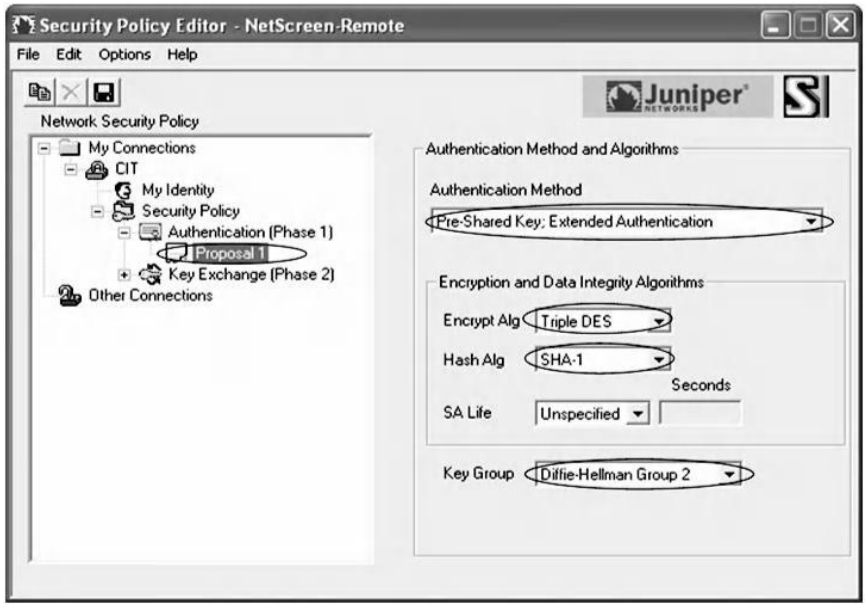


Выберите “My Identity”(Моя личность), а затем выберите “ID Type”(Тип идентификатора) в качестве адреса электронной почты в раскрывающемся меню. Введите адрес электронной почты, который должен быть идентичен тому, который вы настроили в брандмауэре: CITUser@cit.com.

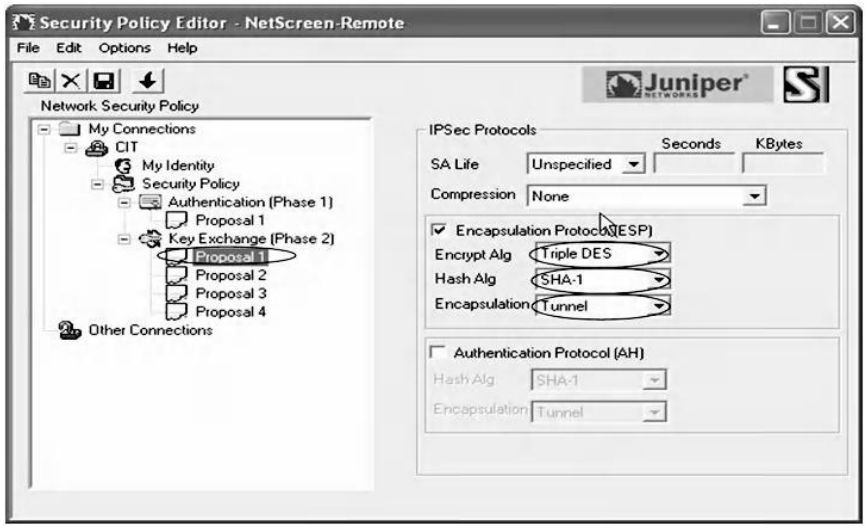


Затем нажмите кнопку “Pre-shared Key”(Предварительный общий ключ), а затем введите ключ, использованный в конфигурации шлюза VPN, который был «12345678», и нажмите «OK», чтобы завершить настройку, как показано ниже.

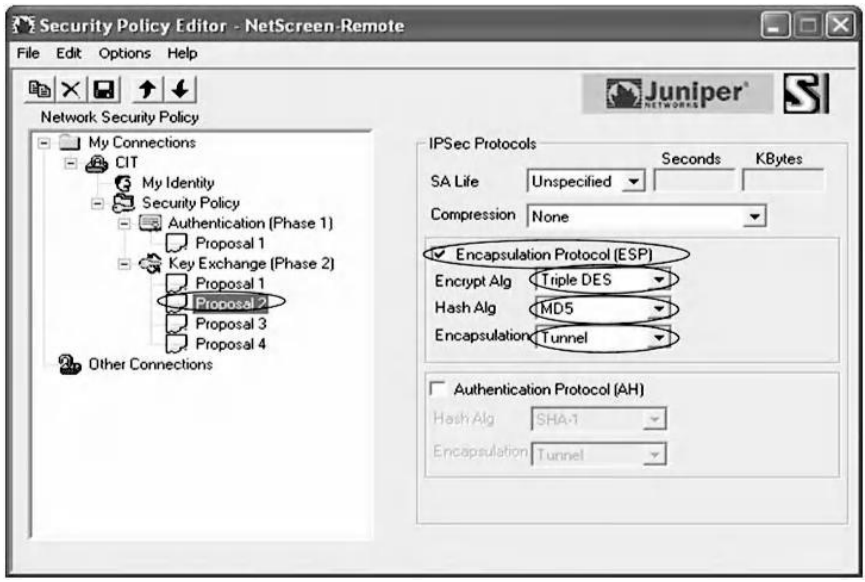
Теперь выберите “Security Policy”(Политика безопасности), затем “Authentication Phase 1” (Фаза аутентификации 1) и, наконец, “Proposal 1”(Предложение 1) Выберите “Pre-shared Key Extended Authentication”(Расширенная аутентификация с предварительным общим ключом) для “Authentication Method”(Способа аутентификации) и выберите “Triple DES”(Тройной DES) для алгоритма шифрования. Затем выберите «SHA-1» для алгоритма хеширования и, наконец, «Diffie-Hellman Group 2» для «Key Group». Варианты показаны ниже.



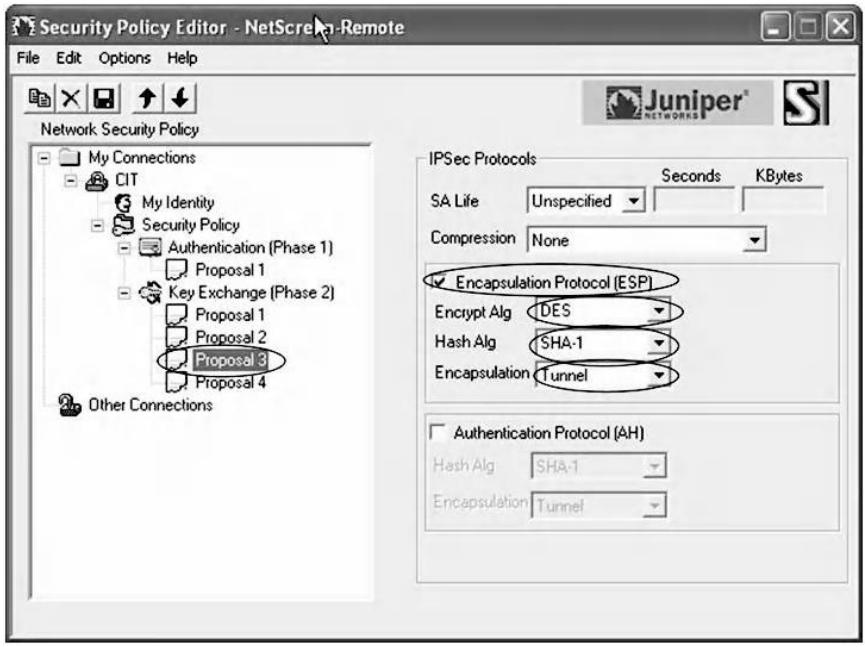
Затем выберите “Proposal 1” для “Key Exchange (Phase 2)”(Обмен ключами (этап 2) и включите протокол инкапсуляции. Затем выберите “Triple DES” для алгоритма шифрования и выберите «SHA-1» для алгоритма хеширования. Наконец, выберите “Tunnel” для инкапсуляции, как показано ниже (Фаза 2, Предложение 1).



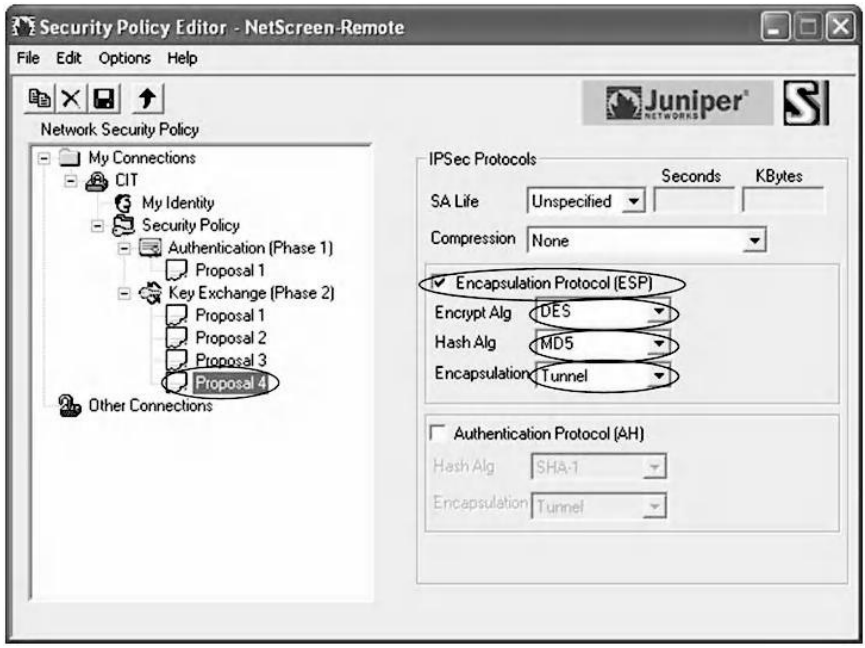
Создайте второе предложение в “Key Exchange Phase 2”(Фазе обмена ключами 2) и включите протокол инкапсуляции. Выберите «Triple DES» для алгоритма шифрования, а затем «MD5» для алгоритма хеширования. Наконец, выберите “Tunnel” для инкапсуляции, как показано ниже (Фаза 2, Предложение 2).



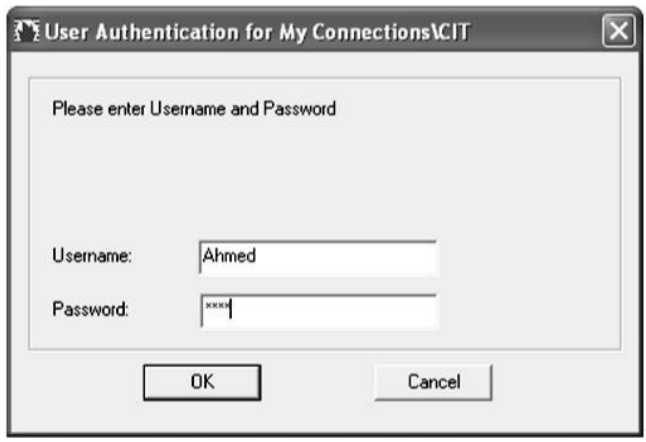
Затем создайте третье предложение в “Key Exchange Phase 2” и включите протокол инкапсуляции. Выберите «DES» для алгоритма шифрования и «SHA-1» для алгоритма хеширования. Наконец, выберите “Tunnel” для инкапсуляции, как показано ниже (Фаза 2, Предложение 3).



Теперь создайте четвертое предложение в “Key Exchange Phase 2” и включите протокол инкапсуляции. Выберите «DES» для алгоритма шифрования, а затем «MD5» для алгоритма хеширования. Наконец, выберите “Tunnel” для инкапсуляции, как показано на следующем экране (Фаза 2, Предложение 4).

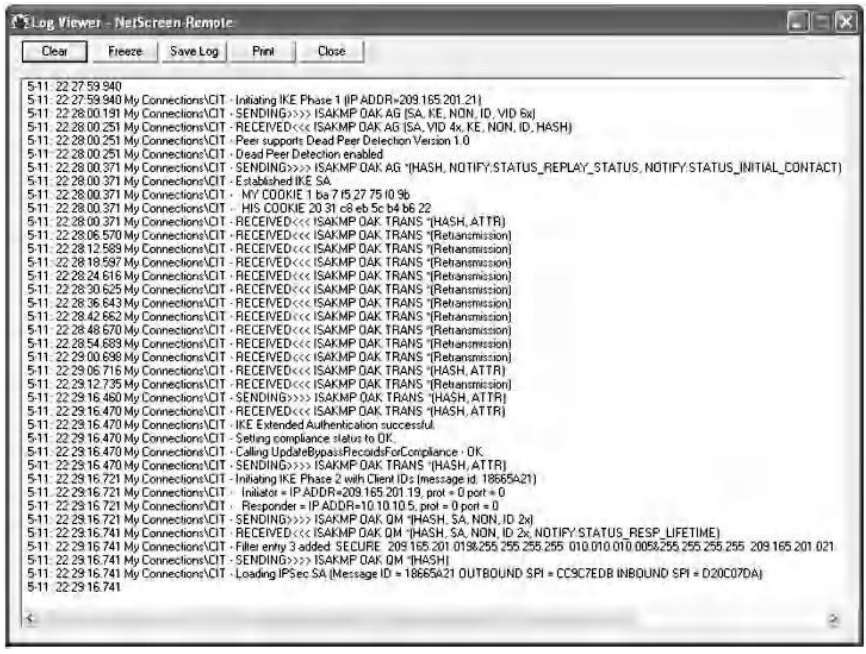


Наконец, щелкните значок “Save”(Сохранить) (значок дискеты), затем щелкните правой кнопкой мыши удаленного VPN-клиента Juniper NetScreen и выберите “Connect”(Подключиться). Появится окно аутентификации пользователя, как показано на следующем снимке экрана. Введите имя пользователя и пароль, которые были настроены ранее (конфигурация пользователя Xauth), и подтвердите, нажав «OK» (как показано).

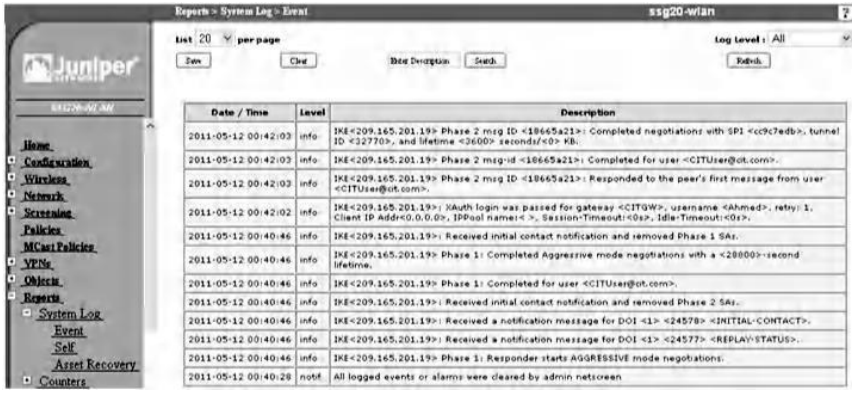


Указание на успешное соединение с удаленным пунктом назначения показано ниже.

Программа просмотра журнала записывает все переговоры, которые произошли через VPN-туннель. Следующий экран представляет записи журнала удаленного VPN-клиента. Как показано, начало этапа 1 началось с удаленного пользователя, который был подключен к шлюзу 209.165.201.21. Затем был получен ответ от его сверстника. После обмена предложением этапа 1 второй этап начался с того, что удаленный пользователь (209.165.201.19) начал переговоры со своим коллегой по предложению второго этапа. Последняя запись указывает на успешное соединение.

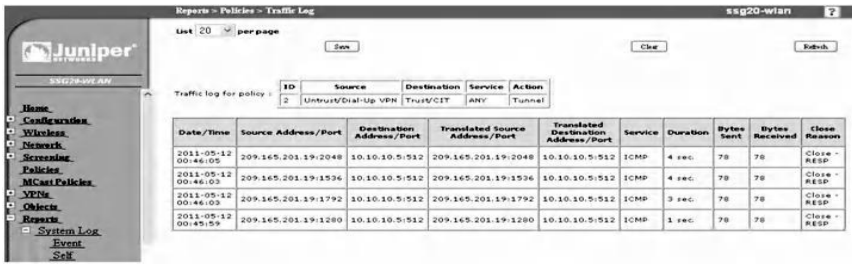


Чтобы увидеть подробности удаленного установления VPN-туннеля в устройстве брандмауэра, перейдите к “Reports”(Отчеты), затем “System Log”(Системный журнал), а затем “Event”(Событие), как показано ниже.



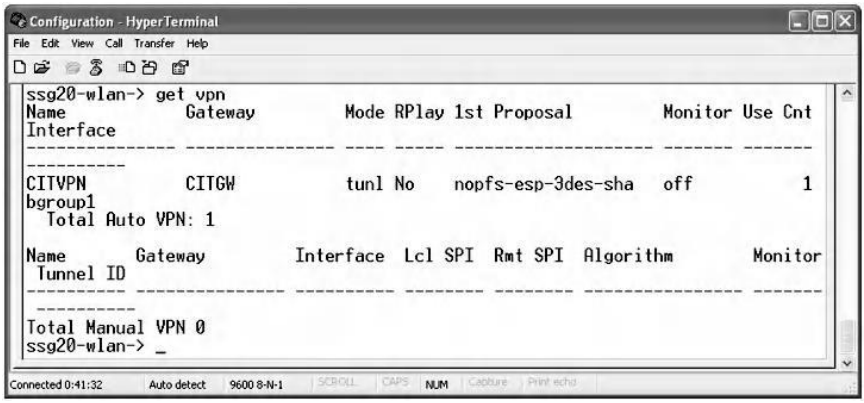
Чтобы проверить связь между двумя узлами, с удаленного пользовательского компьютера выдается команда ping для 10.10.10.5. Команда и ответ однорангового узла следующие:

Чтобы просмотреть ICMP-пакеты, полученные в результате пинга 10.10.10.5, нажмите “Traffic Log”(Журнал трафика) в окне политики. Результирующий экран:



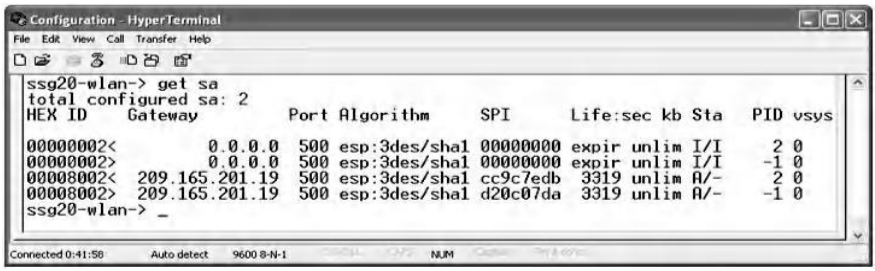
10.2.3.8 Шаг 8: Проверьте Установление VPN-туннеля

Чтобы проанализировать установление туннеля, проверьте сеансы VPN с помощью следующей команды:



Отображаются различные параметры, такие как “Name Interface”(Имя интерфейса), который является bgroup1 (CITVPN). “Gateway”(Шлюз) отображается как «CITGW». Режимом является туннельный режим, который шифрует заголовок IP и полезную нагрузку, так что весь пакет защищен. Первое предложение - это nopfs (без идеальной секретности), что означает, что в будущем не будет никаких изменений ключа. ESP (Encapsulation Security Payload) - это протокол, 3DES - это алгоритм шифрования, а SHA - используемый алгоритм аутентификации. Всего автоматический VPN равен 1.

Чтобы изучить параметры ассоциации безопасности, введите команду «get sa»:



Выходные данные показывают, что число настроенных sa равно двум. IP-адрес шлюза - 209.165.201.19, а порт IKE UDP - 500. Алгоритмы - 3des для шифрования и sha-1 для аутентификации. SPI - это индекс параметра безопасности. Есть два SPI, один для каждого sa.

10.3 Лабораторная работа 10.2: VPN с удаленным доступом - вторая реализация

10.3.1 Результат

Цель этого упражнения - научить студентов внедрять VPN с удаленным доступом с использованием технологии Cisco.

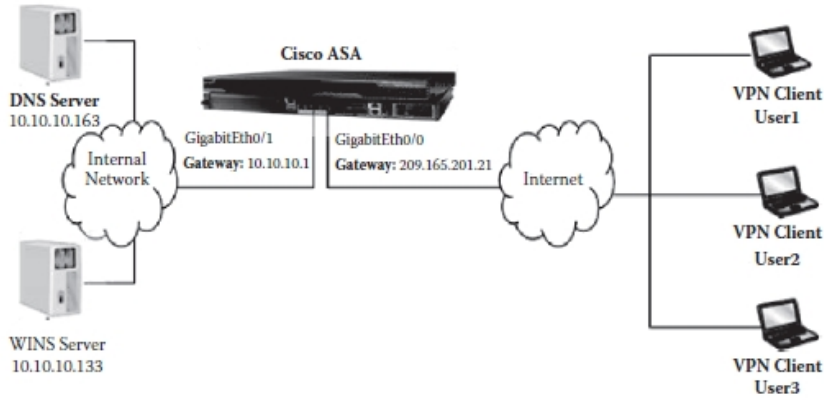
10.3.2 Описание

Сценарий для этой лабораторной работы аналогичен сценарию, описанному в лабораторной работе 10.1, за исключением использования другого оборудования.

10.3.3 Эксперимент

Чтобы объяснить, как настроить VPN с удаленным доступом, проводится эксперимент с использованием устройства Cisco Adaptive Security и клиента Cisco VPN.

На следующем рисунке показана сетевая архитектура эксперимента. Три пользователя пытаются получить доступ к внутренней сети через VPN-туннель, настроенный в Cisco ASA (Adaptive Security Appliance) под управлением ОС 7.0 (7). Три пользователя подключены к внешнему интерфейсу GigabitEthernet0/0.



Эксперимент состоит из следующих этапов:

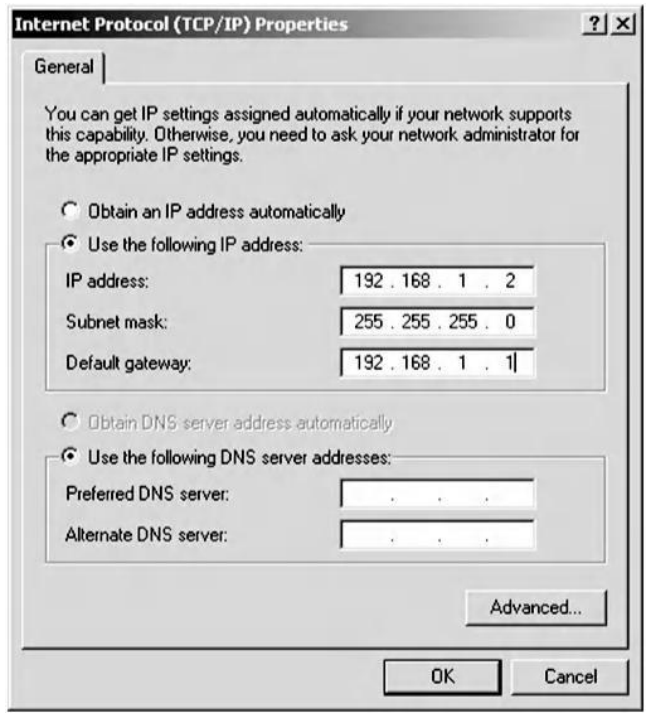
Шаг 1. Сбросьте брандмауэр до значения по умолчанию.
Шаг 2. Назначьте IP-адреса компьютерам и интерфейсам брандмауэра.
Шаг 3. Выберите тип VPN-туннеля для удаленного доступа и выберите клиенты удаленного доступа.
Шаг 4: Укажите имя группы VPN-туннелей и метод аутентификации.
Шаг 5: Настройте учетные записи пользователей.
Шаг 6: Настройте пул адресов.
Шаг 7: Настройте атрибуты клиента.
Шаг 8: Настройте политику IKE.
Шаг 9: Настройте параметры шифрования и аутентификации IPsec.
Шаг 10: Исключение трансляции адресов и разделенное туннелирование.
Шаг 11: Установите программное обеспечение клиента Cisco VPN.
Шаг 12: Запустите программное обеспечение и проверьте подключение.
Шаг 13: Проверьте установление VPN-туннеля.
Шаг 14: Контролируйте VPN-туннель в ASA.

10. 3.3.1 Шаг 1. Сбросьте настройки брандмауэра до настроек по умолчанию

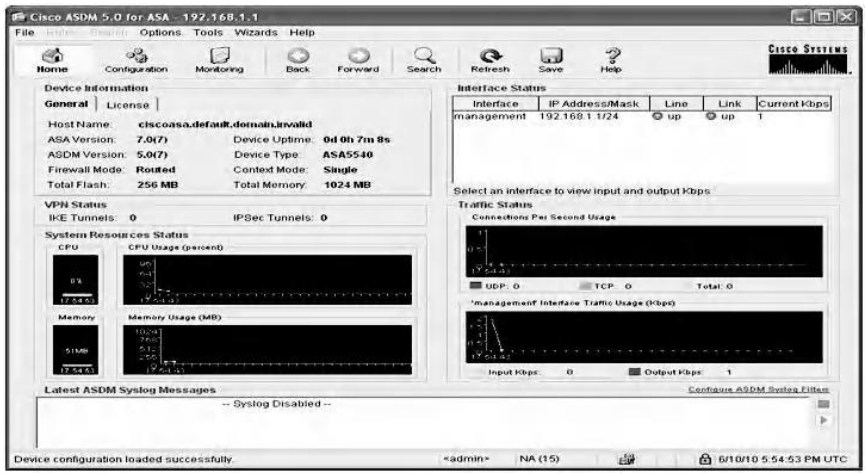
Чтобы начать упражнение, мы сбрасываем брандмауэр на настройки по умолчанию. Для этого подключите ПК к последовательной консоли брандмауэра через HyperTerminal, чтобы получить интерфейс командной строки брандмауэра. Введите команду «enable» в командной строке «ciscoasa>», а затем нажмите «Enter» для запроса пароля. Наконец, введите команду “configure factory-default”(настроить заводские настройки).

10. 3.3.2 Шаг 2. Назначьте IP-адреса компьютерам и интерфейсам брандмауэра

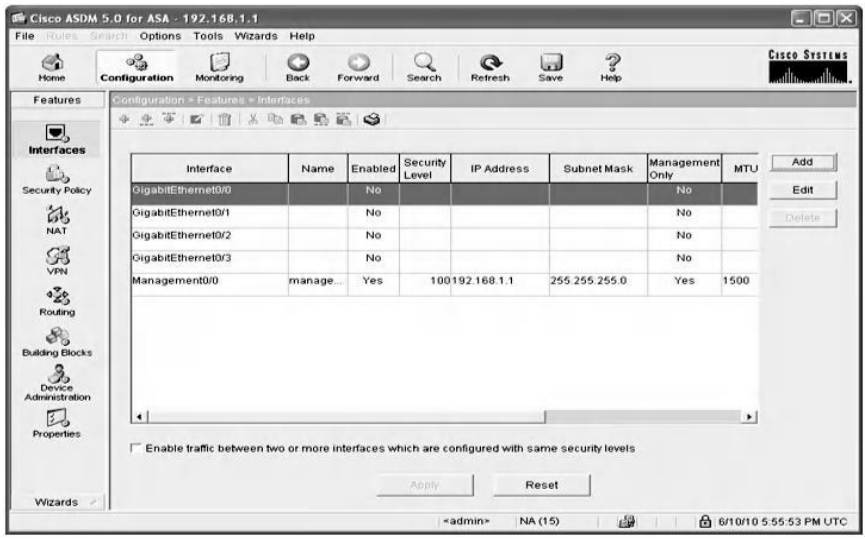
Чтобы назначить IP-адрес компьютерам и брандмауэру, повторите шаг 2 в лабораторной работе 9.1 главы 9, но с параметрами сети, показанными ниже.



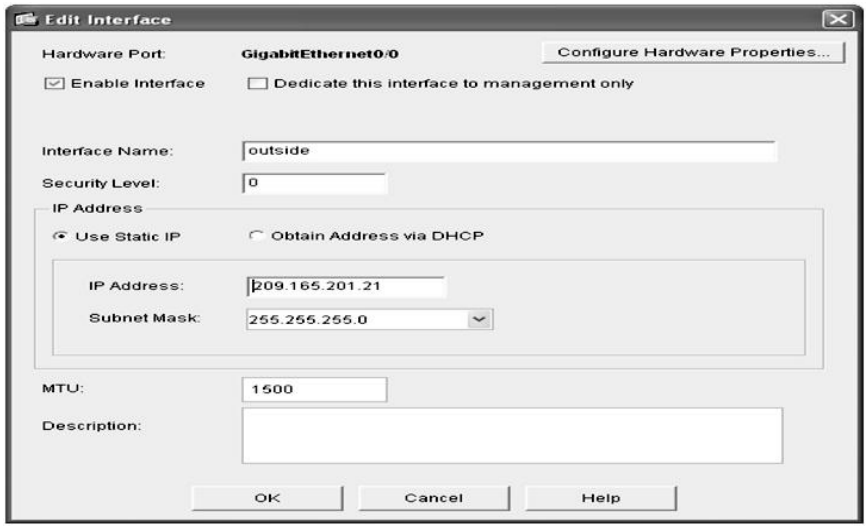
Завершите назначение IP-адреса, нажав кнопку «OK», а затем подключите ПК к порту управления брандмауэра, чтобы начать настройку, используя прямые кабели. Запустите веб-браузер и в поле URL-адреса перейдите по адресу https://192.168.1.1, чтобы открыть веб-интерфейс пользователя (WebUI). Диспетчер устройств адаптивной защиты (ADSM) ASA отображается, как показано ниже.



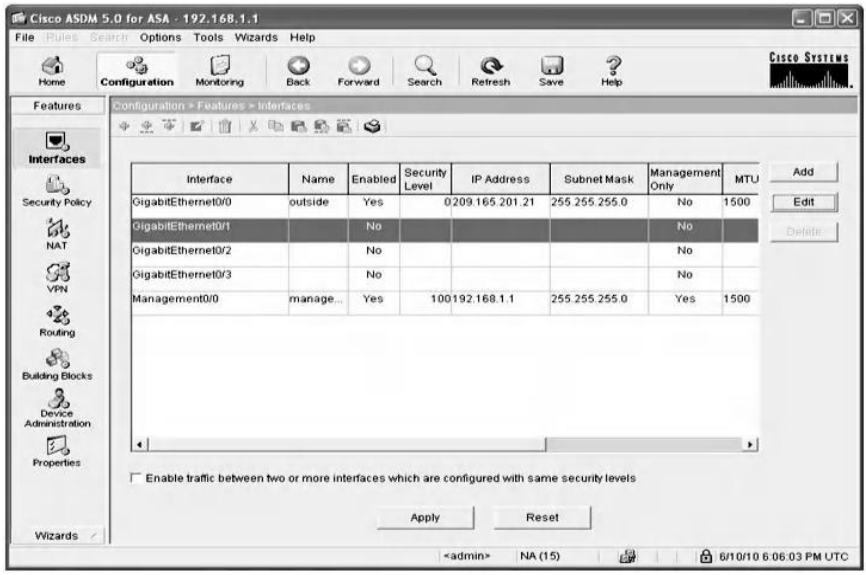
Нажмите на вкладку “Configuration”, чтобы отобразить все интерфейсы брандмауэра, как показано на следующем экране.



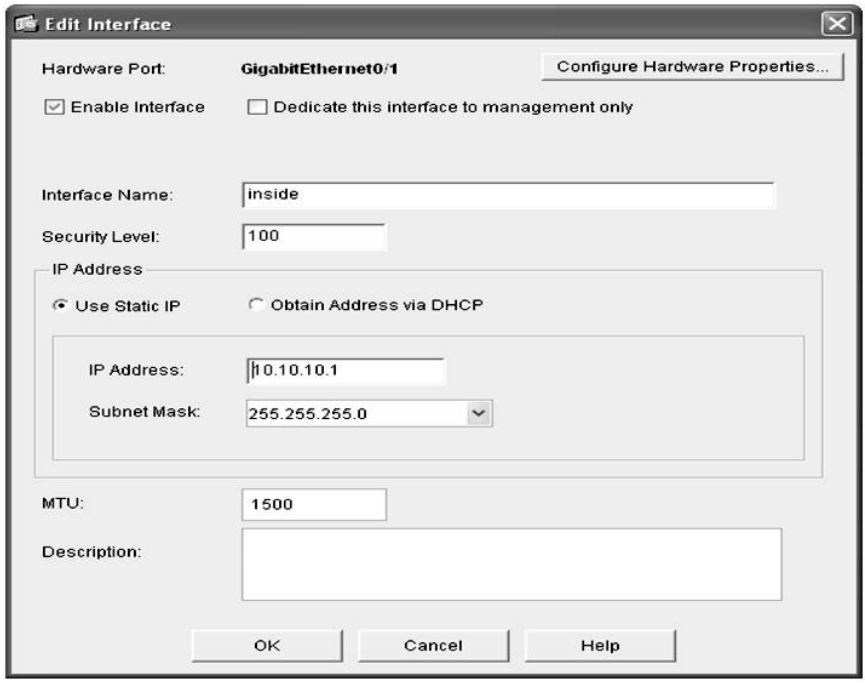
Теперь выберите GigabitEthernet0/0 в качестве внешнего интерфейса с уровнем безопасности 0 и нажмите кнопку “Edit”, чтобы назначить ему IP-адрес, как показано ниже.



Чтобы подтвердить настройку, нажмите кнопку «OK», чтобы убедиться, что интерфейсу будет назначен указанный IP-адрес, как показано на следующем экране.

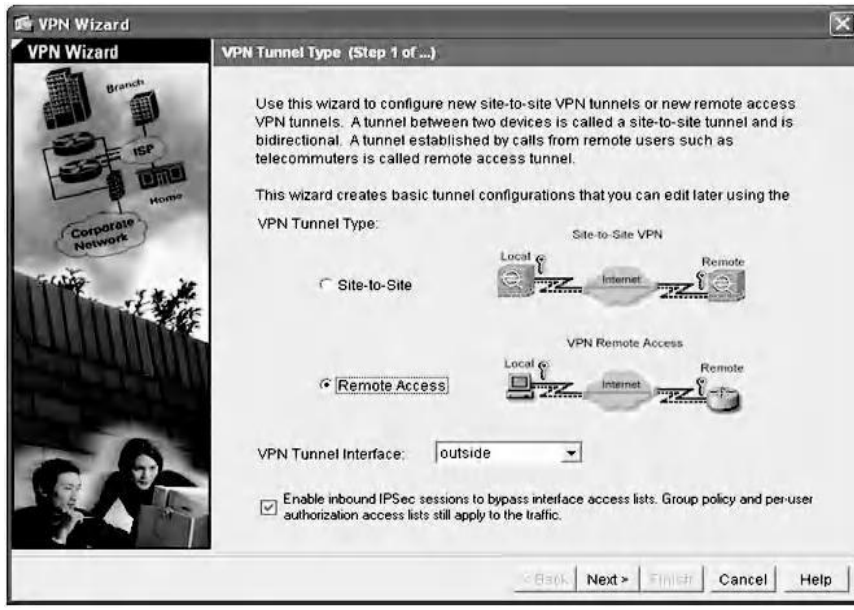


Повторите предыдущие шаги с интерфейсом GigabitEthernet0/1, который будет внутренним интерфейсом, как показано далее.



10.3.3.3 Шаг 3. Выберите тип VPN-туннеля для удаленного доступа и выберите клиенты для удаленного доступа.

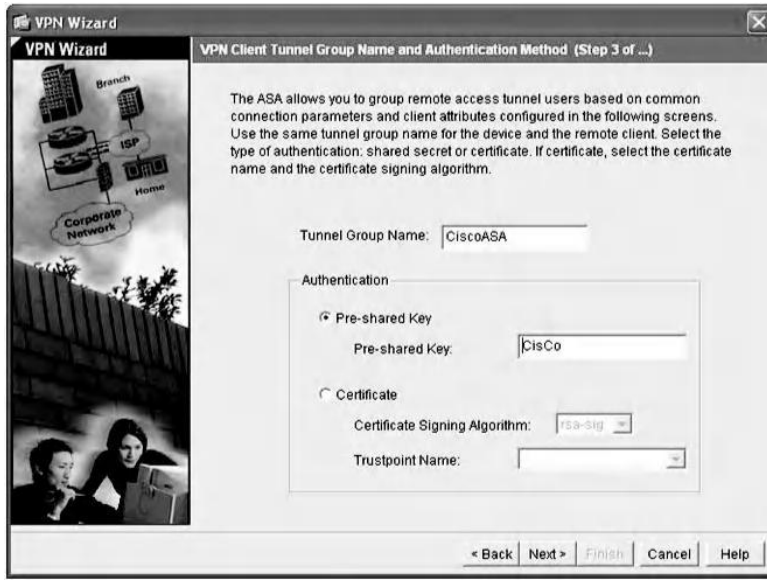
В раскрывающемся меню мастера выберите параметр мастера VPN, и отобразится окно, показанное ниже.



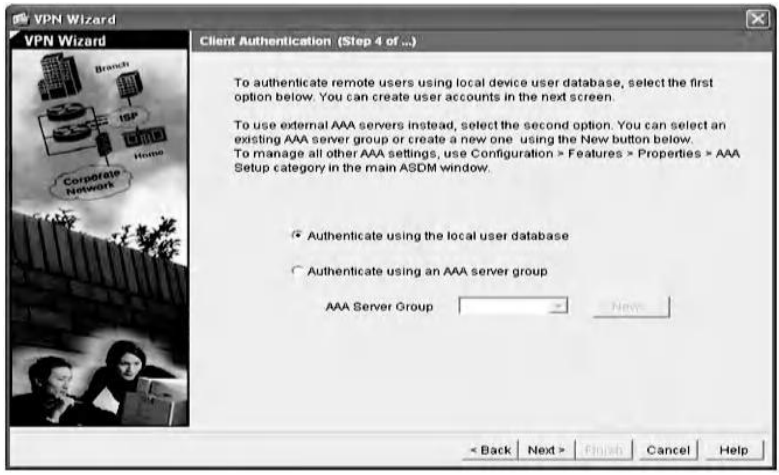
Выберите тип “Remote Access”(Удаленный доступ) и выберите внешний интерфейс в раскрывающемся меню как “VPN Tunnel Interface”(Интерфейс VPN-туннеля). Затем нажмите кнопку “Next” и выберите “VPN clients”(Клиенты VPN), как показано на следующем снимке экрана. Наконец, нажмите кнопку “Next”.

10. 3.3.4 Шаг 4: Укажите имя группы туннелей VPN и метод аутентификации

Введите имя группы туннелей для удаленных пользователей и выберите параметр предварительного общего ключа в качестве метода аутентификации, как показано на следующем снимке экрана.

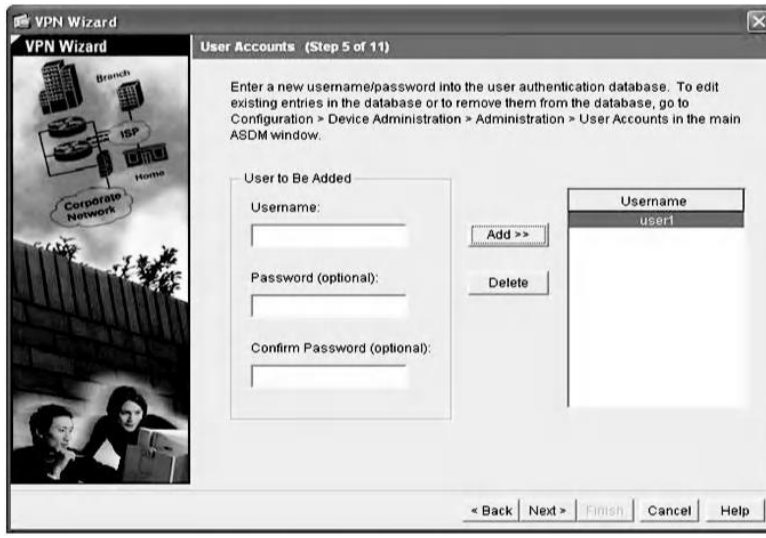


Нажмите кнопку “Next” и укажите базу данных аутентификации пользователя, нажав переключатель. В нашем сценарии мы выберем локальную базу данных пользователей, как показано на следующем снимке экрана, и нажмем “Next”.

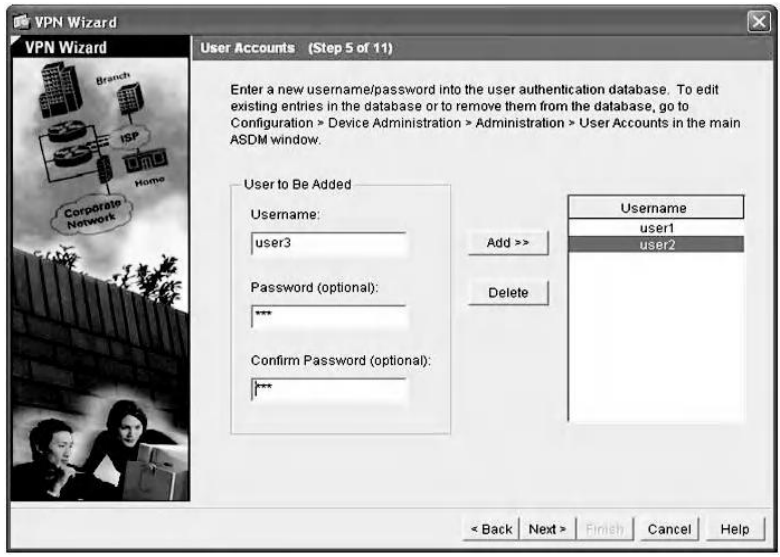


10.3.3.5 Шаг 5. Настройка учетных записей пользователей.

Введите имя пользователя и пароль для добавления в локальную базу данных аутентификации в качестве новой записи; затем нажмите кнопку “Add”(Добавить), как показано ниже.

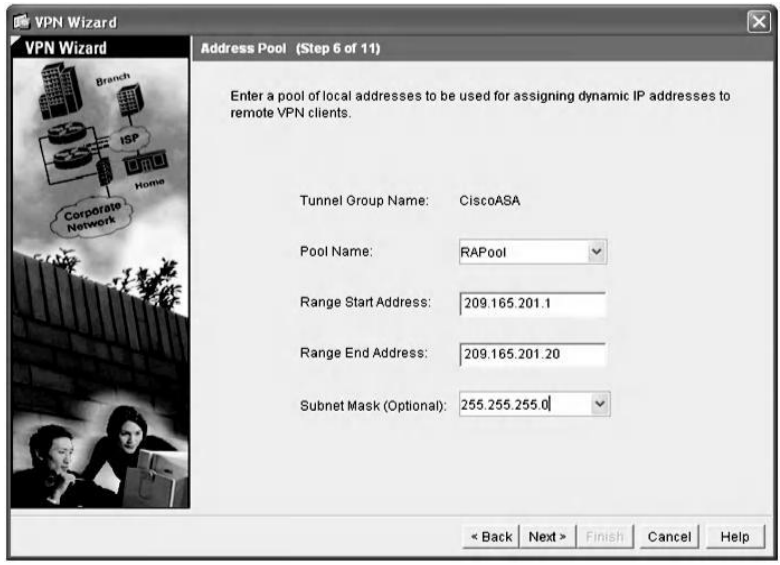


Повторите предыдущий шаг, если необходимо настроить более одного пользователя (как показано на следующем снимке экрана), и нажмите кнопку “Next”.



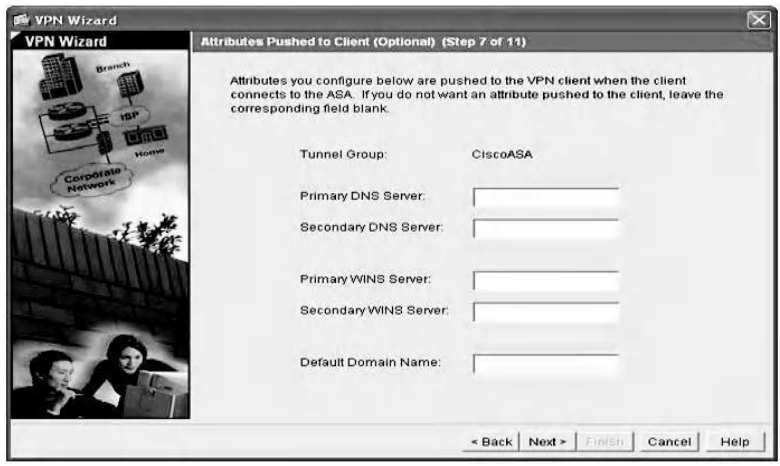
10.3.3.6 Шаг 6: Настройте пул адресов

Введите имя пула или выберите предварительно настроенное в раскрывающемся меню. Затем введите начальный диапазон пула и конец диапазона, введите маску подсети и нажмите “Next”, как показано на следующем снимке экрана.



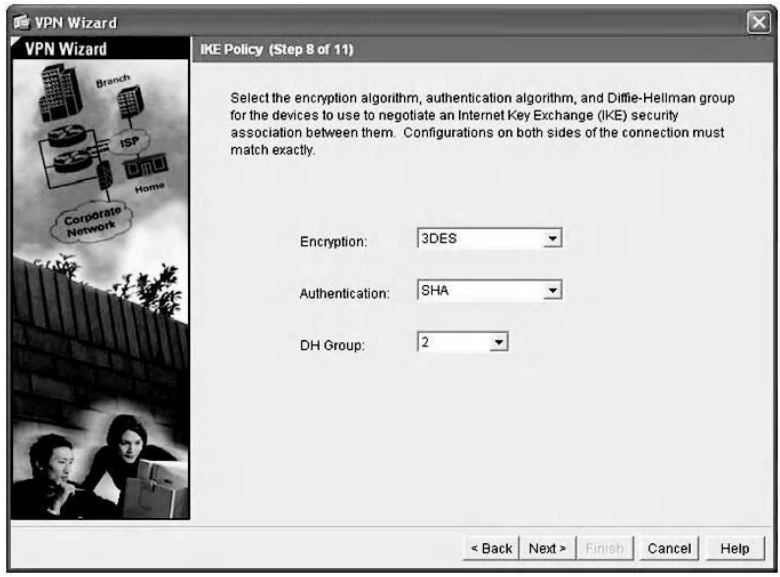
10.3.3.7 Шаг 7: Настройте атрибуты клиента

Введите дополнительную информацию о конфигурации сети, которая будет отправлена на удаленные клиенты (как показано ниже), и нажмите кнопку “Next”.



10.3.3.8 Шаг 8. Настройте политику IKE.

Сконфигурируйте предложение IKE Phase 1, выбрав алгоритм шифрования, алгоритм аутентификации и группу Диффи-Хеллмана для согласования SA, как показано в следующем окне, и нажмите кнопку “Next”.

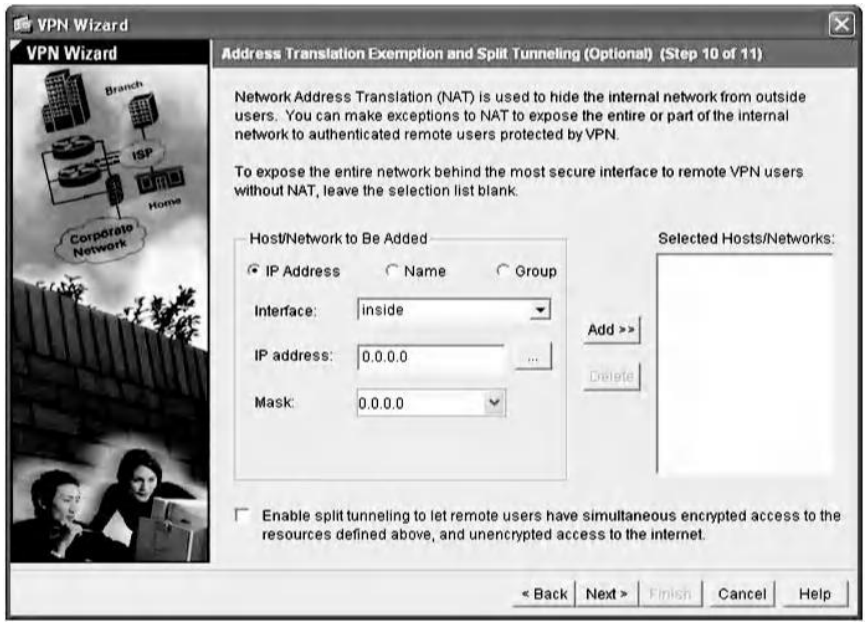


10.3.3.9 Шаг 9. Настройка параметров шифрования и аутентификации IPsec

Для конфигурации IKE Phase 2 выберите алгоритм шифрования в качестве 3DES и алгоритм аутентификации в качестве SHA, как показано ниже.

10. 3.3.10 Шаг 10: Исключение трансляции адресов и разделенное туннелирование

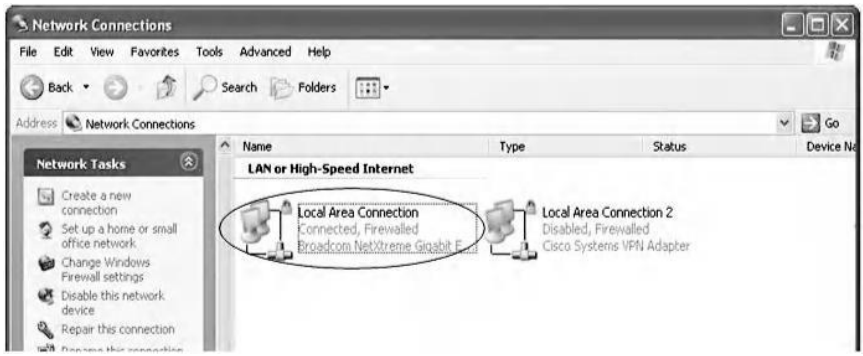
Трансляция сетевых адресов используется, чтобы скрыть внешний сетевой IP-адрес от внешнего воздействия, как показано ниже.



Исключения могут быть сделаны путем определения локальных хостов и сетей, адреса которых не будут переведены. Кроме того, раздельное туннелирование может быть включено, чтобы разрешить незашифрованный доступ пользователей к Интернету. Наконец, нажмите кнопку “Next”, чтобы открыть окно подтверждения, показанное ниже, а затем нажмите “Finish”.

10.3.3.11 Шаг 11. Установите клиентское программное обеспечение Cisco VPN.

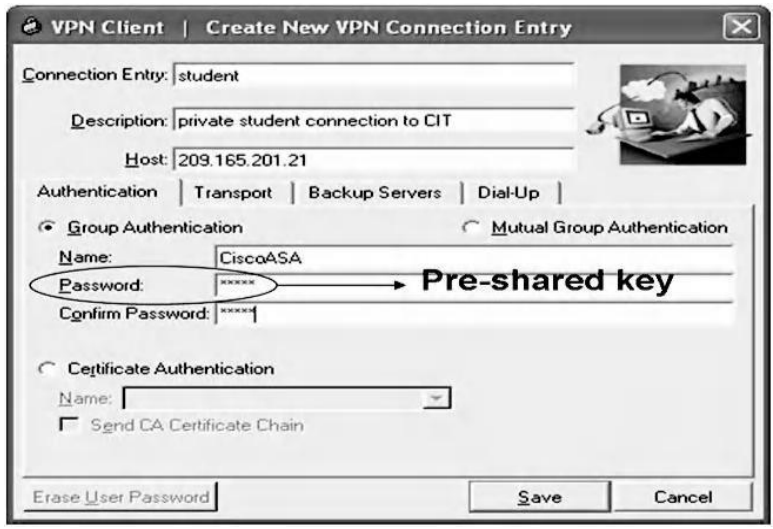
Установите VPN-клиент на машине, которая подключена к внешнему интерфейсу. Дважды щелкните значок “Local Area Connection” (Подключение по локальной сети) (не Cisco System VPN Adapter), как показано ниже.



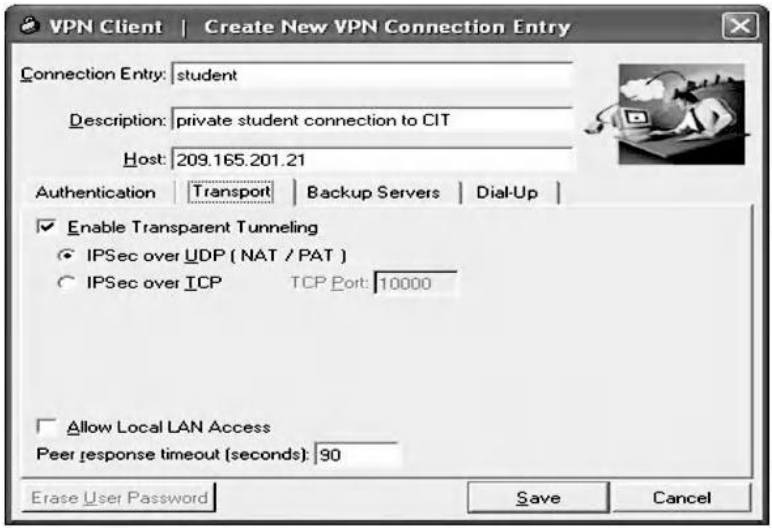
Присвойте машине следующий IP-адрес: 209.165.201.19, как показано ниже.

10. 3.3.12 *Шаг 12: Запустите программное обеспечение и проверьте подключение*

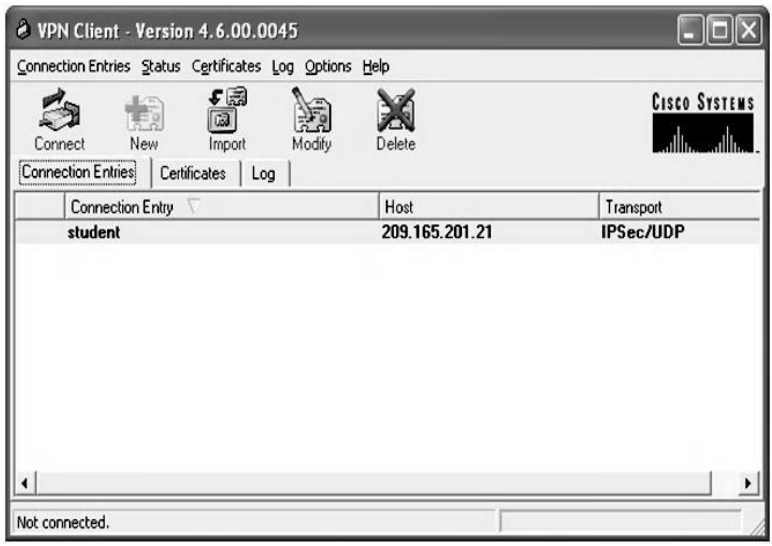
Сначала запустите системный VPN-клиент Cisco. Создайте новое соединение, нажав на иконку “New”. Заполните записи в окне «Connection Entry», введите имя для подключения и введите IP-адрес VPN-сервера, который равен 209.165.201.21. Затем введите имя группового туннеля и пароль, который является предварительным общим ключом, настроенным для VPN удаленного доступа в ASA. Детали показаны ниже.



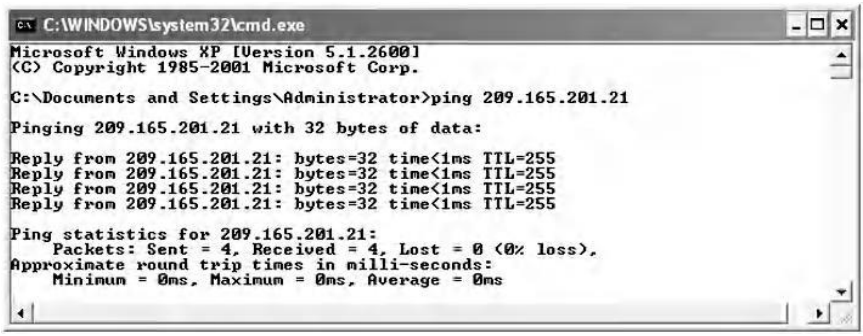
Затем нажмите на вкладку “Transport”(Транспорт) и выберите “Enable Transparent Tunneling”(Включить прозрачное туннелирование), которое позволяет зашифрованному трафику IPsec проходить через устройства трансляции сетевых адресов / трансляции адресов портов (NAT / PAT), такие как брандмауэры. Затем выберите IPsec через UDP (NAT / PAT), как показано на следующем экране.



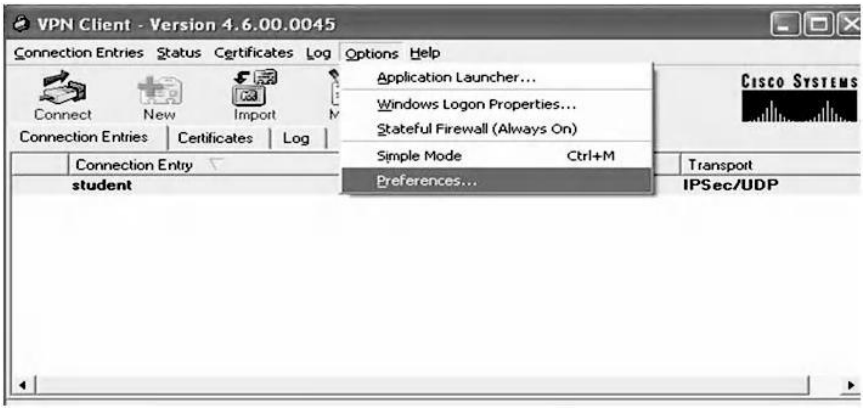
Нажмите кнопку “Save”(Сохранить), чтобы создать соединение, как показано далее.



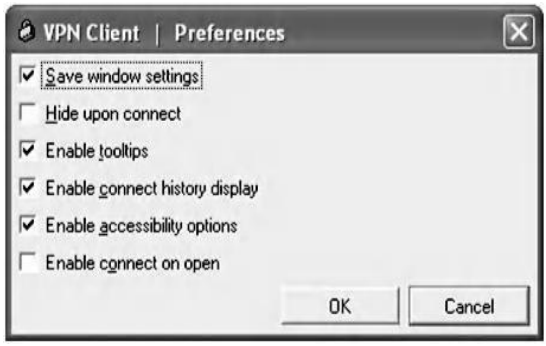
Чтобы проверить подключение к сети, выполните команду ping 209.165.201.21 с хоста клиента. Это должно быть успешно, как в следующей команде.



Перейдите в меню “Options”(Параметры) на VPN-клиенте и выберите параметры, как показано на следующем экране, чтобы получить дополнительные параметры.



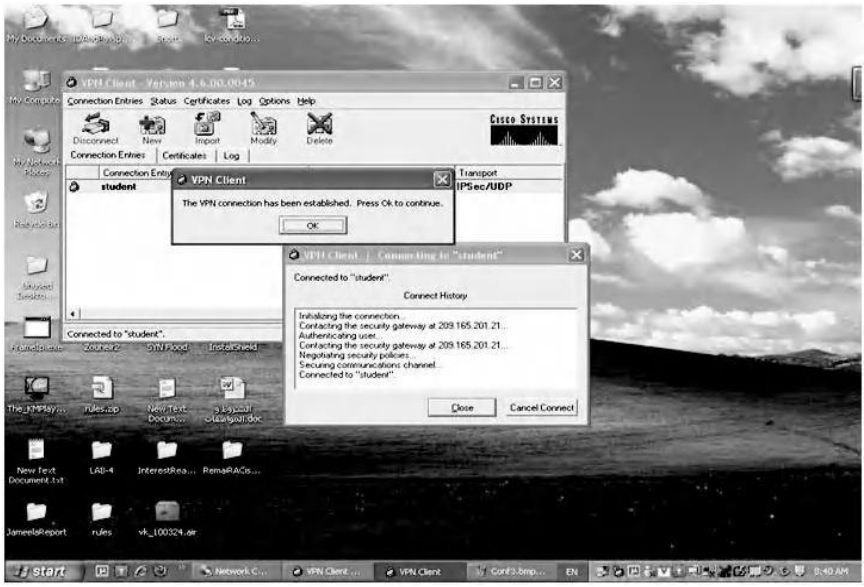
Выберите следующие “Preferences”: “Save window settings,” “Enable tool tips,” “Enable connect history display,” и “Enable accessibility options,”, как показано ниже.



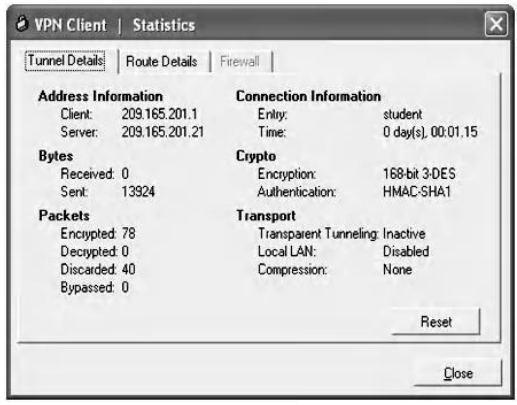
Затем нажмите кнопку “Connect”, которая открывает окно аутентификации пользователя, как показано на следующем экране.

Заполните поля имени пользователя и пароля как user1 и 123, как настроено в этом примере, и нажмите кнопку «ОК». Соединение будет инициализировано, и начнется согласование политик безопасности, как показано на следующем снимке экрана.

Как только пользователь подключится к VPN-шлюзу, появится другое всплывающее окно, подтверждающее, что соединение установлено, как показано на следующем снимке экрана.

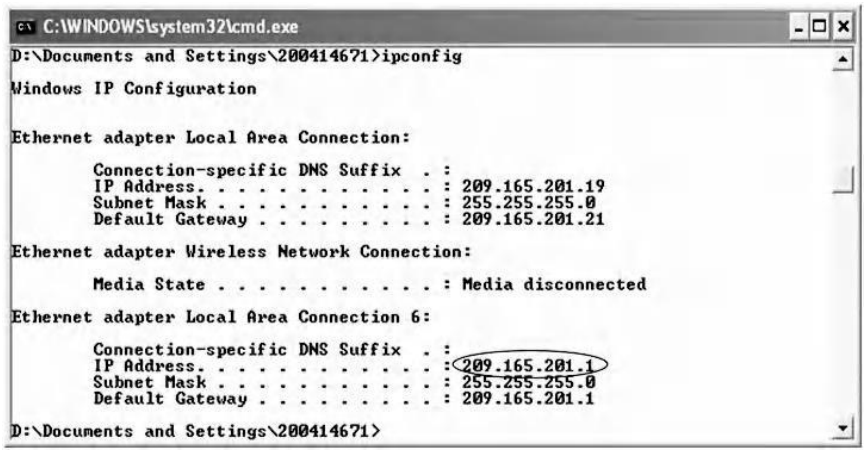


Чтобы просмотреть более подробную информацию о VPN-туннеле, перейдите в меню “Status” и выберите “Statistics” на VPN-клиенте. Как показано на следующем снимке экрана, удаленный клиент получил IP-адрес из предварительно сконфигурированного пула, это 209.165.201.1. Появится новое соединение, информация “student”. Количество зашифрованных пакетов равно 78, а алгоритмы шифрования и аутентификации - 3-DES и SHA-1 соответственно.



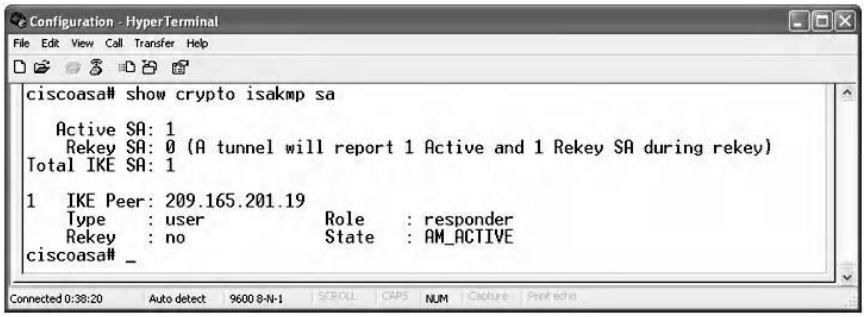
Чтобы просмотреть сведения об IP-адресе удаленного клиента, введите команду «ipconfig», как показано ниже, чтобы увидеть IP-адрес,

который был назначен пользователю из пула адресов на шлюзе VPN.



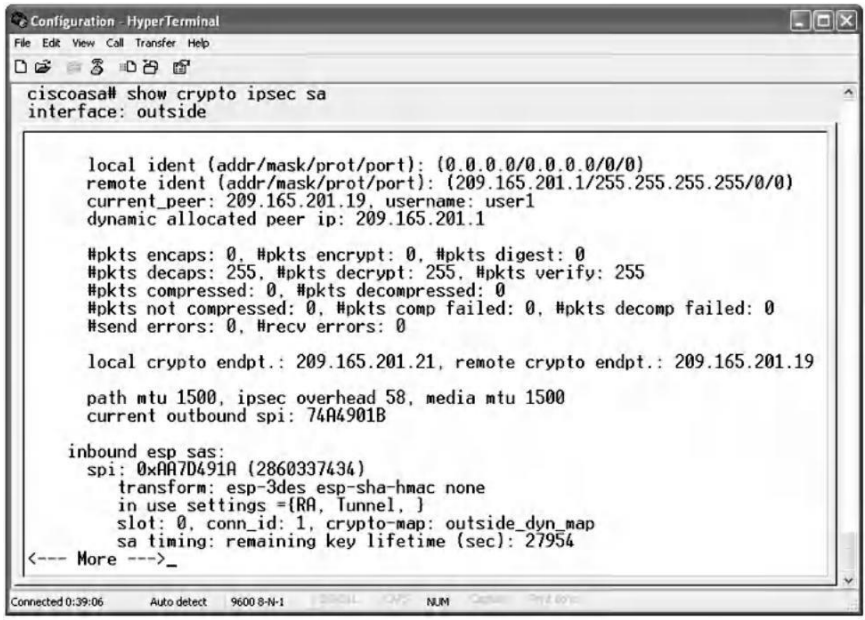
10.3.3.13 Шаг 13: Проверьте Установление VPN-туннеля

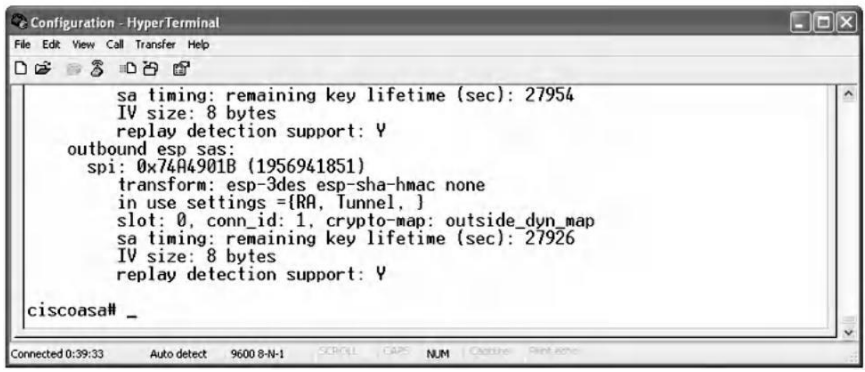
На ASA используйте команду «show crypto isakmp sa» для отображения согласованных параметров SA IKE фазы 1, как показано ниже:



Замечено, что количество активных сопоставлений безопасности равно 1, одноранговый узел IKE равен 209.165.201.19, тип подключения - VPN с удаленным доступом (пользователь), роль удаленного пользователя - респондент, а режим IKE фазы 1 агрессивен, так как обозначается AM-ACTIVE.”

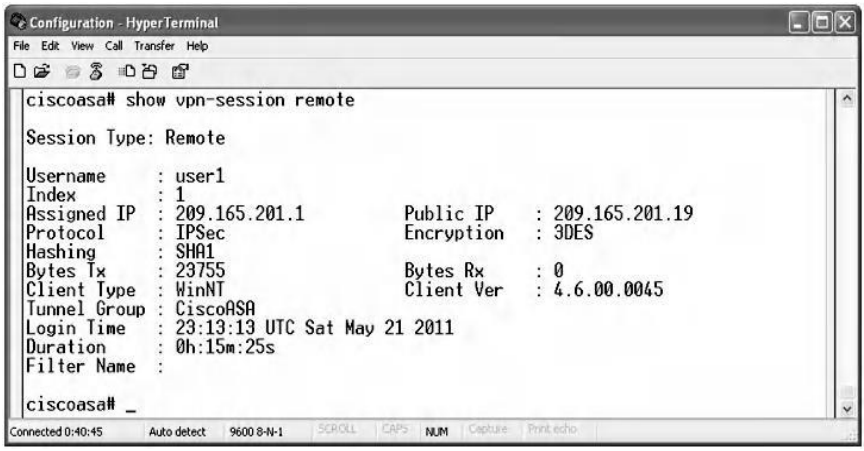
Чтобы отобразить сопоставление безопасности IKE Phase 2, введите следующую команду: «show crypto ipsec sa».





Замечено, что текущее количество инкапсулированных, зашифрованных и переваренных пакетов равно 0; количество декапсулированных, дешифрованных и проверенных пакетов составляет 255; количество сжатых и распакованных пакетов равно 0; режим IPsec - это туннельный режим; и есть два SA, один входящий и один исходящий, и каждый SA имеет свой собственный SPI.

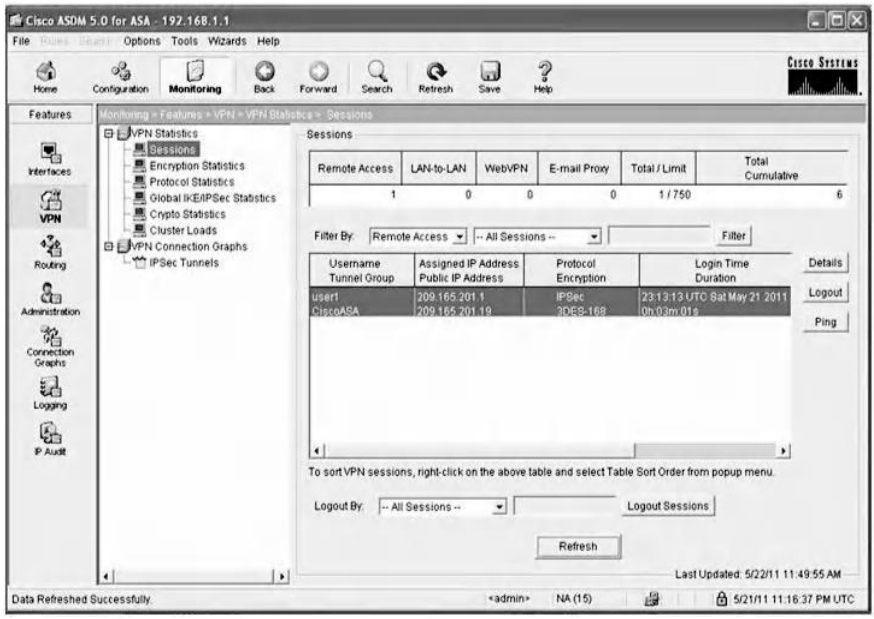
Чтобы просмотреть более подробную информацию о VPN-туннеле, введите следующую команду:



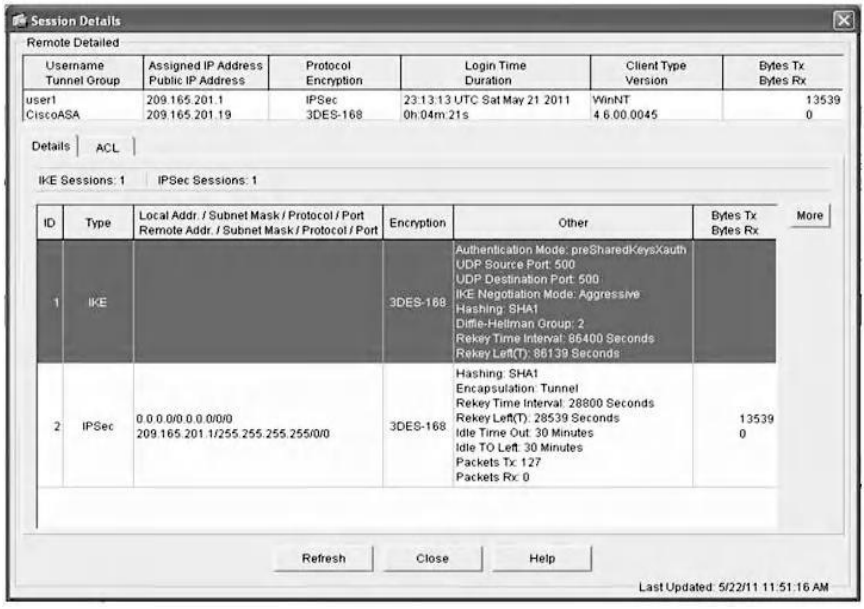
Отображаются несколько параметров сеанса, который произошел между одноранговыми узлами, например, тип сеанса удаленный, имя пользователя user1 и назначенный ему IP-адрес 209.165.201.1, протокол пользователя Ipsec, а алгоритмы шифрования и хэширования 3DES и SHA1 соответственно. Имя туннельной группы - Cisco ASA, и время входа и продолжительность сеанса определены.

10.3.3.14 Шаг 14: Контролируйте VPN-туннель в ASA

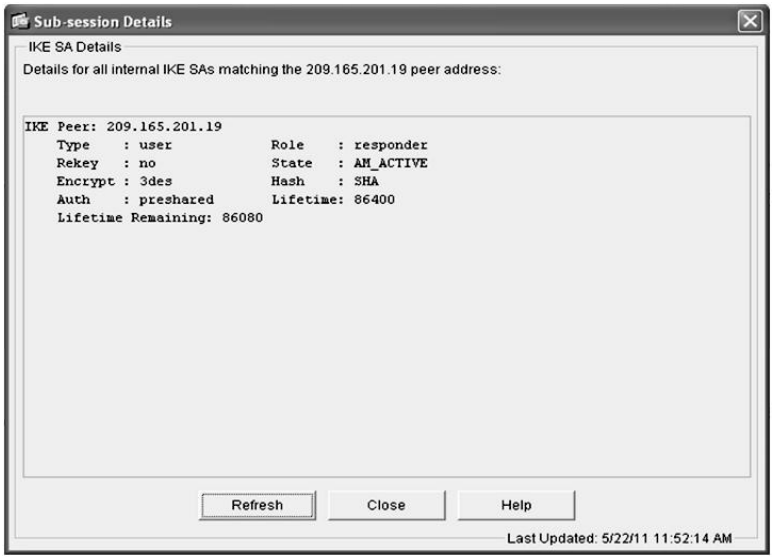
Чтобы подробно отслеживать сеансы, нажмите на вкладку “Monitoring” и в дереве статистики VPN выберите поддерево “Sessions”. Следующий снимок экрана показывает детали сеанса, такие как имя пользователя, которое является user1; его туннельная группа Cisco ASA; назначенный IP-адрес удаленного пользователя; используемый протокол IPsec; алгоритм шифрования; и время, когда пользователь вошел в систему.



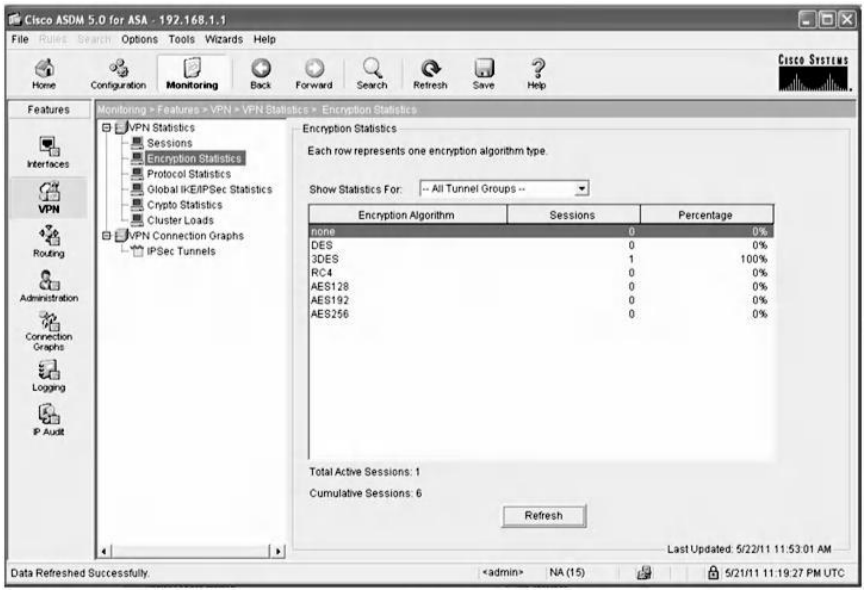
Для просмотра более подробной информации нажмите кнопку “Details” . На следующем снимке экрана показаны подробности сопоставлений безопасности фазы 1 и фазы 2. Кроме того, алгоритм шифрования и хеширования используются на каждом этапе.



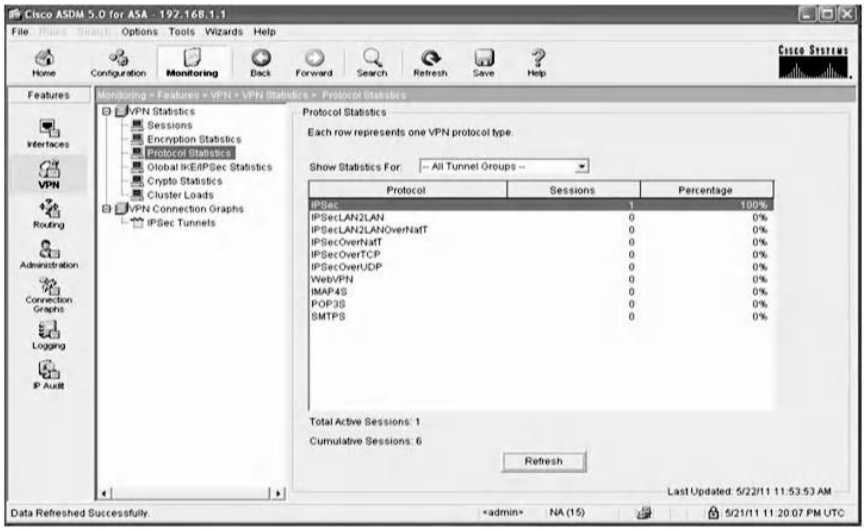
При нажатии на кнопку “More” при выборе строки IKE Phase 1, информация о IKE SA будет отображаться, как показано на следующем снимке экрана, на котором отображается узел IKE 209.165.201.19; тип пира, который является пользователем; роль, которую она играет, которая является ответчиком; шифрование; и алгоритмы хеширования, которые являются 3DES и SHA. Режим агрессивный; Кроме того, метод аутентификации является предварительным.



Затем выберите другие поддеревья, чтобы узнать больше о статистике шифрования. Один активный сеанс использует алгоритм шифрования 3DES 100% времени, как показано на следующем экране.

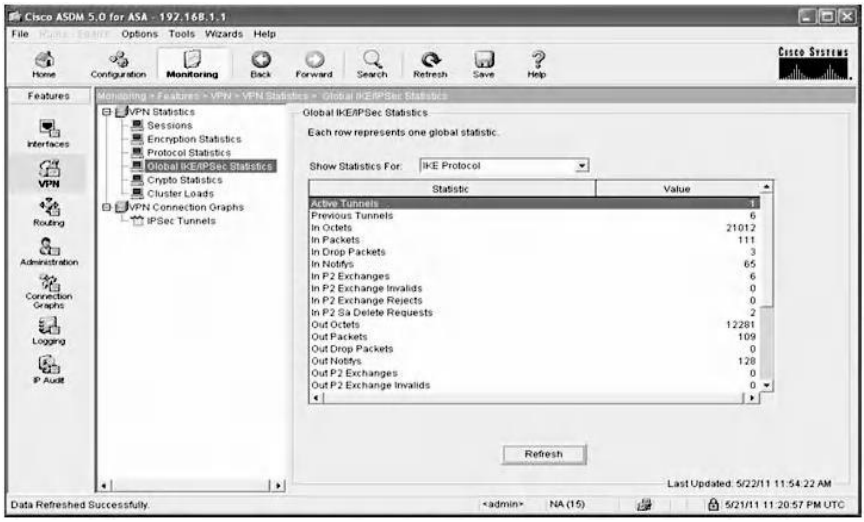


Выберите поддерево статистики протокола, чтобы просмотреть подробную информацию об используемом протоколе. Активный сеанс работает по протоколу IPsec 100% времени, как показано ниже.

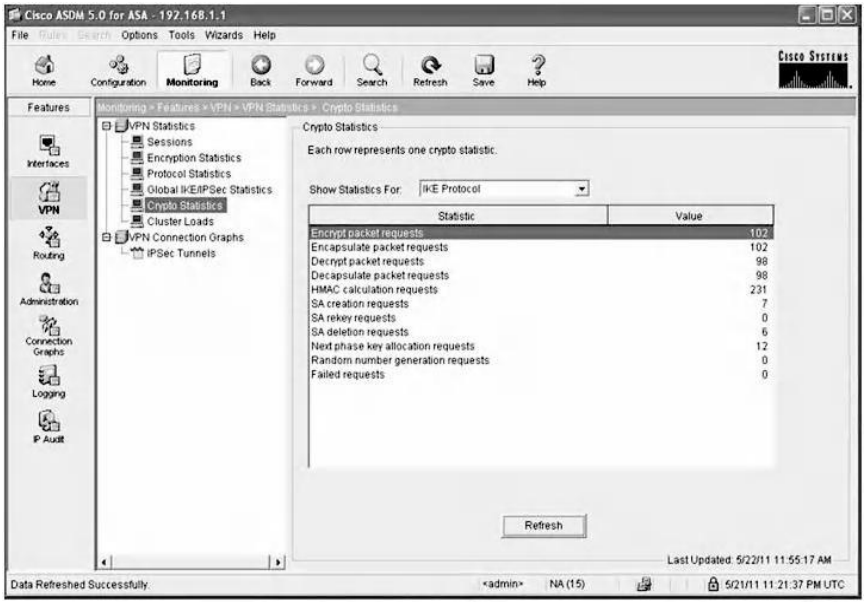


Из поддерева Глобальная статистика IKE / IPsec количество активных туннелей равно 1, а предыдущие туннели - 6. Есть 111 IP-пакетов и 3 в

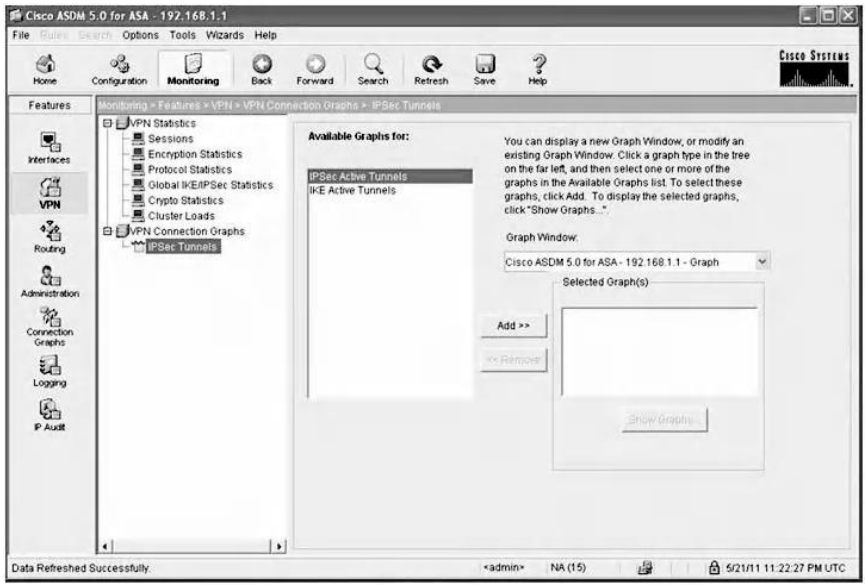
отбрасываемых пакетах. Кроме того, имеется 109 выходных пакетов и 0 выходных пакетов, как показано ниже.



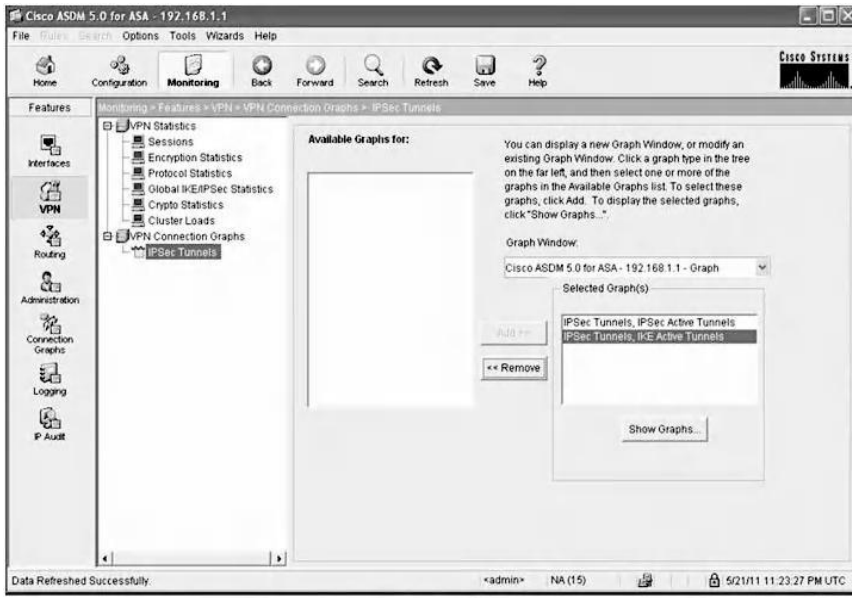
Выберите поддерево Crypto Statistics и проанализируйте его статистику. Имеется 102 запроса на шифрование пакета и пакета с инкапсуляцией и 98 запросов на дешифрование и декапсуляцию пакетов. Имеется 231 запрос на расчет HMAC, 7 запросов на создание SA и 6 запросов на удаление SA. Кроме того, есть 12 запросов о распределении ключей следующего этапа, как показано ниже.



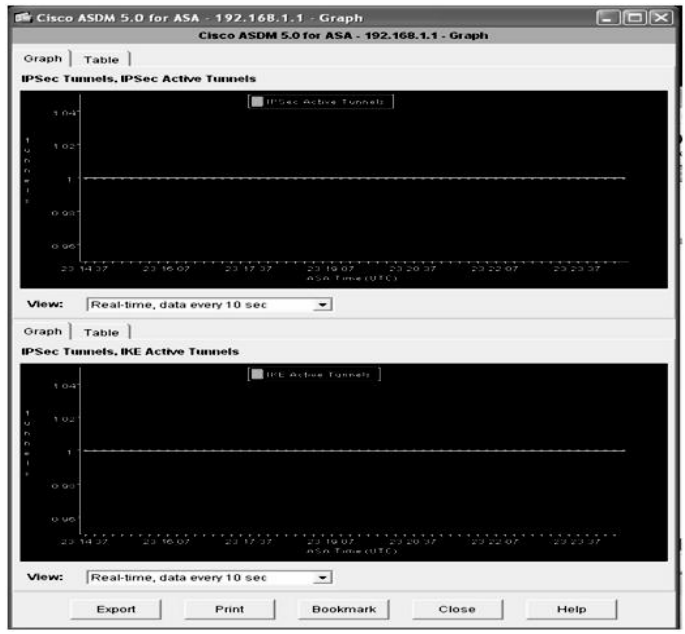
Чтобы просмотреть информацию о туннеле VPN в графической форме, выберите “VPN Connection Graph” (График VPN-подключения), а затем “IPsec tunnels” (Туннели IPsec), чтобы открыть окно, показанное ниже:



В текстовой области доступных графиков выберите «IPsec Active tunnel» и нажмите кнопку “Add”, чтобы открыть окно, показанное ниже. Повторите предыдущий шаг с активными туннелями IKE, чтобы информация об активных туннелях IKE и IPsec была показана на графике.



Нажмите “Show Graphs” (Показать графики), и устойчивая прямая зеленая линия указывает, что туннель все еще активен, как показано в следующем окне.



10.4 Краткое содержание главы

Поскольку потребность в любом месте и в любое время продолжает расти, удаленный доступ IPsec VPN все чаще оказывается наиболее эффективным решением для обеспечения конфиденциальности данных в Интернете. В этой главе представлено подробное объяснение решения безопасности IPsec VPN для удаленного доступа и подробно описаны основные компоненты, из которых состоит VPN IPsec удаленного доступа, а именно VPN-клиент удаленного доступа и VPN-сервер удаленного доступа. Он разделен на два раздела: обсуждение функций и конфигурации на основе устройства межсетевого экрана Juniper Networks NetScreen, а затем внедрение с использованием устройства адаптивной безопасности Cisco Microsystems. В этой главе были подробно рассмотрены и проанализированы основные концепции IPsec VPN для удаленного доступа, такие как согласование IKE Phase 1 SA и статистика пакетов IKE Phase 2.