Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
О.В. Фомичева
«22» 12 2023г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.03.03 Безопасность сетевой инфраструктуры
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 202 3 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «21» 11 202 3 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

СОДЕРЖАНИЕ

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по выполнению практических работ предназначены для организации работы на практических занятиях по МДК.03.03 «Безопасность компьютерных сетей», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по МДК.03.03 «Безопасность компьютерных сетей» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ПК 3.3. Осуществлять защиту информации в сети с использованием программно-аппаратных средств

ПК 3.6. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

В рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой по МДК.03.03 «Безопасность компьютерных сетей».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках МДК.03.03 «Безопасность компьютерных сетей» позволяет освоить комплекс работ по выполнению практических заданий по всем темам ПМ.03 «Эксплуатация объектов сетевой инфраструктуры».

Рабочая тетрадь по МДК.03.03 «Безопасность компьютерных сетей», имеют практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих МДК.03.03 «Безопасность компьютерных сетей».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками и выставляются в журнале теоретического обучения.

1. Перечень практических работ по МДК03.03 «Безопасность компьютерных сетей»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 3.1. Безопасность компьютерных сетей	– выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; – осуществлять диагностику и поиск неисправностей всех компонентов сети; – выполнять действия по устранению неисправностей	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 1 Составить сравнительную характеристику средств защиты информации	2
			Практическая работа № 2 Основные этапы допуска к ресурсам вычислительной системы.	2
			Практическая работа № 3 Использование динамически изменяющегося пароля.	2
			Практическая работа № 4 Взаимная проверка подлинности и другие случаи опознания.	2
			Практическая работа № 5 Обеспечение административного доступа AAA и сервера Radius	2
			Практическая работа № 6 Настройка политики безопасности брандмауэров	2
			Практическая работа № 7 Настройка безопасности на втором уровне на коммутаторах	2
			Практическая работа № 8 Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки	2
			Практическая работа № 9 Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM	2
			Практическая работа № 10 Базовая настройка шлюза безопасности ASA и настройка NAT	2
			Практическая работа № 11 Базовая настройка шлюза безопасности ASA и фильтрация трафика с помощью Access Lists	2
			Практическая работа № 12 Маршрутизация в шлюзе безопасности ASA	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Практическая работа № 213 TCP Advanced Options в шлюзе безопасности ASA	2
			Практическая работа № 14 Анализи внутрипротокольного трафика шлюза безопасности ASA	2
			Практическая работа № 15 Работа с логическими интерфейсами шлюза безопасности ASA	2
			Практическая работа № 16 Монитор вторжений Threat Detection шлюза безопасности ASA	2
			Практическая работа № 17 Перенаправления трафика из шлюза безопасности ASA в Firepower	2
			Практическая работа № 19 Расшифровка трафика в шлюзе безопасности ASA при помощи SSL Decryption	2
			Практическая работа № 20 Сбор статистики о трафике, проходящем через шлюз безопасности ASA	2
			Практическая работа № 20 Настройка AnyConnect Remote Access SSL VPN используя ASDM	2
Тема 3.2. Системы обнаружения вторжения	Устанавливать системы обнаружения и предотвращения вторжений	ОК 1 – ОК 9 ПК 3.3, ПК 3.6	Практическая работа № 21 Установка системы обнаружения и предотвращения вторжения Snort	2
			Практическая работа № 22 Настройка системы обнаружения и предотвращения вторжения Snort	2
	Работать с системой обнаружения и предотвращения вторжений		Практическая работа № 23 Установка MySQL для работы со Snort	2
			Практическая работа № 24 Запись предупреждений о вторжениях в MySQL	2
			Практическая работа № 25 Установка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort	2
			Практическая работа № 26	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort	
			Практическая работа № 27 Использование стандартных правил для Snort	2
			Практическая работа № 28 Создание собственных правил для Snort. Синтаксис правил	2
			Практическая работа № 29 Настройка виртуальной машины для эмуляции угроз ИБ	2
			Практическая работа № 30 Отслеживание действий в сети и создание своих правил	2

2. Описание порядка выполнения практических работ

Практическая работа № 1
Составить сравнительную характеристику средств защиты информации

Задание:

С помощью учебного пособия, конспекта, опыта выполнения практических работ и ресурсов Интернета заполнить следующую таблицу по системам обнаружения и предотвращения вторжений:

Продукт IDS/IPS	Поддерживаемые операционные системы	Дата последнего обновления и последняя версия	Стоимость продукта	Используемые методы обнаружения	Достоинства	Недостатки
Traffic Inspector Next Generation						
StoneGate IPS						
CISCO IDS/IPS						
Suricata						
Snort						
UserGate						

Практическая работа № 2
Основные этапы допуска к ресурсам вычислительной системы.

Задание:

1. Выписать из прайс-листа своего компьютера его конфигурацию.
2. Пояснить все параметры, используя приложения.
3. К какой конфигурации вы отнесете свой компьютер?

Практическая работа № 3
Использование динамически изменяющегося пароля.

Задание:

1.Прослушать интерактивный обучающий курс/вводную лекцию преподавателя по теме «Использование динамического пароля»в лекционном классе.
2.Изучить возможности парольной защиты с использованием метода динамического пароля.
3. Изучить функциональный метод составления динамического пароля.
4. Изучить метод «рукопожатия».
Работа в лаборатории
1. Ознакомиться с Практической работой № «Использование динамического пароля», повторить обучающий курс.
3. С использованием предложенных методов составить функцию ***У=(X mod 100)D+W , где X*** собственная дата рождения, записать их в отчет.
4. Создать документ Microsoft WORD, сохранить его с вводом пароля из трех знаков. Оценить стойкость пароля из трех знаков с использованием программы аудита паролей Advanced Office Password. Результаты занести в отчет.
5.Повторить пункт 4. с вводом пароля из 4 знаков, и 5 знаков.
6. Сравнить скорость вычисления паролей. Результаты занести в отчет. Сделать выводы

Практическая работа № 4
Взаимная проверка подлинности и другие случаи опознания.

Задание:

Задание.
Провести сравнение методов индификации и проверки подлинности.
Выделить их преимущества и недостатки.
Привести примеры ситуаций для их приоритетного использования.

Практическая работа № 5
Обеспечение административного доступа AAA и сервера Radius

Задание:

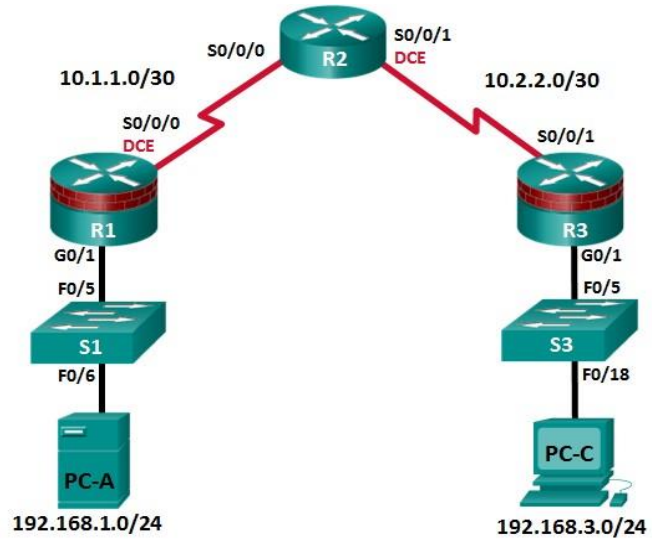


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

- Настройте основные параметры, такие как имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статическую маршрутизацию.

Часть 2. Настройка локальной аутентификации

- Настройте локального пользователя базы данных и локальный доступ для линий консоли, vty и aux.
- Проверьте конфигурацию.

Часть 3. Настройка локальной аутентификации с помощью AAA

- Настройте локальную базу данных пользователей с помощью Cisco IOS.
- Настройте локальную аутентификацию AAA с помощью Cisco IOS.
- Проверьте конфигурацию.

Часть 4. Настройка централизованной аутентификации с помощью AAA и RADIUS

- Установите на компьютер сервер RADIUS.
- Настройте пользователей на сервере RADIUS.

- На маршрутизаторе настройте сервисы AAA с помощью Cisco IOS, чтобы получить доступ к серверу RADIUS для аутентификации.
- Проверьте конфигурацию AAA и RADIUS.

Исходные данные/сценарий

Самым распространенным способом обеспечения безопасного доступа к маршрутизатору является создание паролей для линий консоли, vty и aux. При попытке доступа к маршрутизатору у пользователя будет запрашиваться только пароль. Настройка секретного пароля в привилегированном режиме повышает уровень безопасности, но в любом случае для каждого уровня доступа требуется только основной пароль.

Помимо основных паролей, в локальной базе данных маршрутизатора можно настроить отдельные имена или учетные записи пользователей с разными уровнями привилегий, которые могут применяться ко всему маршрутизатору. Когда для линий консоли, vty или aux настроено обращение к этой локальной базе данных, то при использовании любой из этих линий для доступа к маршрутизатору пользователю предлагается ввести имя и пароль.

Для дополнительного контроля над процессом входа может применяться метод аутентификации, авторизации и учета (AAA). Для обеспечения базовой аутентификации функцию AAA можно настроить на доступ к локальной базе данных при вводе имен пользователей. Кроме того, могут быть определены запасные процедуры. Однако данный подход не обладает хорошей масштабируемостью, так как его нужно настраивать на каждом маршрутизаторе. Для обеспечения максимальной масштабируемости и максимально эффективного применения AAA, данную функцию нужно использовать совместно с базой данных внешнего сервера TACACS+ или RADIUS. При попытке пользователя войти в систему маршрутизатор обращается к внешнему серверу базы данных для проверки действительности имени пользователя и пароля.

В данной лабораторной работе вы построите сеть из нескольких маршрутизаторов и настроите маршрутизаторы и хосты. Затем вам будет необходимо использовать команды CLI для настройки на маршрутизаторах базовой локальной аутентификации с помощью AAA. Вы установите на внешнем компьютере программное обеспечение RADIUS и будете использовать AAA для аутентификации пользователей с помощью сервера RADIUS. Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатора Cisco 1941 с ПО Cisco IOS Release 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. В зависимости от модели маршрутизатора и версии Cisco IOS, доступные команды и выходные данные могут отличаться от указанных в данной лабораторной работе.

Примечание. Перед началом работы убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 2 ПК (Windows 7 или 8.1, с установленным SSH-клиентом и WinRadius)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

В части 1 этой лабораторной работы вы создадите топологию сети и настроите основные параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Все операции должны быть выполнены на маршрутизаторах R1 и R3. На маршрутизаторе R2 необходимо выполнить только шаги 1, 2, 3 и 6. В качестве примера здесь показана процедура для маршрутизатора R1.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов согласно топологической схеме.
b. Настройте IP-адреса, как показано в таблице IP-адресов.
c. Настройте тактовую частоту маршрутизаторов с помощью DCE-кабеля, подключенного к последовательному интерфейсу каждого из них.

```
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
```

d. Чтобы маршрутизатор не пытался неправильно интерпретировать введенные команды как имена хостов, отключите функцию DNS-поиска.

```
R1(config)# no ip domain-lookup
```

Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.

a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из маршрутизатора R3 в R2.
b. Настройте статический маршрут из маршрутизатора R2 к LAN маршрутизатора R1 и статический маршрут из маршрутизатора R2 к LAN маршрутизатора R3.

Шаг 4: Настройте параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показано в таблице IP-адресов.

Шаг 5: Проверьте связь между компьютером PC-A и маршрутизатором R3.

a. Отправьте эхо-запрос с маршрутизатора R1 на маршрутизатор R3. Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.
b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, то это означает, что статическая маршрутизация настроена верно и работает исправно. Если эхо-запрос был выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами show run и show ip route, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 6: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Шаг 7: Сконфигурируйте и зашифруйте пароли на маршрутизаторах R1 и R3.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. В производственной сети рекомендуется использовать более сложные пароли.

На данном шаге настройте параметры одинаковым образом на маршрутизаторах R1 и R3. В качестве примера здесь показан маршрутизатор R1.

a. Задайте минимальную длину пароля.

Используйте команду security passwords, чтобы задать минимальную длину пароля в 10 символов.

```
R1(config)# security passwords min-length 10
```

b. Настройте пароль enable secret на обоих маршрутизаторах. Используйте алгоритм хеширования type 9 (SCRYPT).

R1(config)# enable algorithm-type scrypt secret cisco12345

Шаг 8: Настройте основную консоль, вспомогательный порт и линии vty.

a. Настройте пароль консоли и активируйте вход в систему для маршрутизатора 1. Для дополнительной безопасности команда exec-timeout обеспечивает выход из системы линии, если в течение 5 минут отсутствует активность. Команда logging synchronous предотвращает прерывание ввода команд сообщениями консоли. Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во время лабораторной работы, вы можете ввести команду exec-timeout с параметрами 0 0, чтобы отключить проверку истечения времени ожидания. Однако такой подход не считается безопасным.

R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous

b. Настройте пароль для порта AUX для маршрутизатора R1.

R1(config)# line aux 0

R1(config-line)# password ciscoauxpass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

a. Настройте пароль на линиях vty для маршрутизатора R1.

R1(config)# line vty 0 4

R1(config-line)# password ciscovtypass

R1(config-line)# exec-timeout 5 0

R1(config-line)# login

b. Зашифруйте пароли для консоли, aux и vty.

R1(config)# service password-encryption

c. Введите команду show run. Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

Шаг 9: Настройте предупреждающий баннер при входе в систему на маршрутизаторах R1 и R3.

a. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD) с помощью команды banner motd. При подключении пользователя к маршрутизатору до запроса на ввод авторизационных данных отображается баннер MOTD. В данном примере в начале и конце сообщения используется знак доллара ($).

R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit

b. Выйдите из привилегированного режима с помощью команды disable или exit, а затем нажмите Enter для начала работы.

Если баннер отображается некорректно, создайте его заново с помощью команды banner motd.

Шаг 10: Сохраните базовые конфигурации на всех маршрутизаторах.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

R1# copy running-config startup-config

Часть 2: Настройка локальной аутентификации

В части 2 данной лабораторной работы необходимо создать локальное имя пользователя и пароль, а также настроить способ доступа к линиям консоли, aux и vty через локальную базу данных маршрутизатора, где находятся действительные имена пользователей и пароли. Выполните все шаги на маршрутизаторах R1 и R3. Ниже показана процедура для маршрутизатора R1.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования MD5. Используйте алгоритм хеширования type 9 (SCRYPT).

R1(config)# username user01 algorithm-type scrypt secret user01pass

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

Шаг 2: Настройте локальную аутентификацию для линии консоли и входа в систему.

a. Настройте линию консоли на использование локально определенных имен пользователей и паролей.

R1(config)# line console 0

R1(config-line)# login local

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R1 con0 is now available. Press RETURN to get started.

c. Войдите в систему с помощью ранее настроенной учетной записи user01 и пароля.

Чем сейчас отличается вход через консоль от того, что было раньше?

d. После входа введите команду show run. Вам удалось отправить команду? Поясните ответ.

Войдите в привилегированный режим, используя команду enable. У вас был запрошен пароль? Поясните ответ.

Шаг 3: Проверьте новую учетную запись путем входа в рамках сеанса Telnet.

a. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A.

PC-A> telnet 192.168.1.1

b. Система запросила у вас учетные данные? Поясните ответ.

a. Настройте линию vty на использование ранее локально определенных учетных записей и паролей и сконфигурируйте команду transport input, чтобы разрешить Telnet.

R1(config)# line vty 0 4

R1(config-line)# login local

R1(config-line)# transport input telnet

R1(config-line)# exit

b. Повторно свяжитесь с маршрутизатором R1 с компьютера PC-A с помощью Telnet. PC-A> telnet 192.168.1.1

Система запросила у вас учетные данные? Поясните ответ.

c. Войдите в систему как пользователь user01 с паролем user01pass.

d. Во время сеанса Telnet с маршрутизатором R1 войдите в привилегированный режим с помощью команды enable.

Какой пароль вы использовали?

e. Для дополнительной безопасности настройте порт AUX на использование локально определенных учетных записей для входа.

R1(config)# line aux 0
R1(config-line)# login local

f. Завершите сеанс Telnet с помощью команды exit.

Шаг 4: Сохраните конфигурацию на маршрутизаторе R1.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

R1# copy running-config startup-config

Шаг 5: Выполните шаги 1–4 на маршрутизаторе R3 и сохраните конфигурацию.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

Часть 3: Настройка локальной аутентификации на маршрутизаторе R3 с помощью AAA

Задача 1: Настройка локальной базы данных пользователей с помощью Cisco IOS.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования SCRYPT.

R3(config)# username Admin01 privilege 15 algorithm-type scrypt secret Admin01pass

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

2: Настройка локальной аутентификации AAA с помощью Cisco IOS.

Включите сервисы на маршрутизаторе R3 с помощью команды aaa new-model в режиме глобальной настройки. Так как вы устанавливаете локальную аутентификацию, используйте ее в качестве первичного метода и метод без аутентификации – в качестве вторичного.

Если вы использовали метод аутентификации через удаленный сервер, например TACACS+ или RADIUS, вы должны были настроить вторичный метод аутентификации в качестве запасного, если сервер недоступен. Обычно вторичным методом является аутентификация по локальной базе данных. В нашем случае, если в локальной базе данных не настроены имена пользователей, маршрутизатор будет предоставлять доступ к устройству всем пользователям.

Шаг 1: Включите сервисы AAA.

R3(config)# aaa new-model

Шаг 2: Разверните сервисы AAA с помощью локальной базы данных.

a. Настройте список аутентификации для входа в систему по умолчанию с помощью команды aaa authentication login default *method1[method2][method3];* укажите список методов с помощью ключевых слов local и none.

R3(config)# aaa authentication login default local-case none

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Примечание. Параметр local-case используется для того, чтобы сделать имена пользователей зависимыми от регистра.

a. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться: R3 con0 is now available

Press RETURN to get started.

Войдите в консоль как Admin01 с паролем Admin01pass. Помните, что сейчас и имена пользователей, и пароли чувствительны к регистру. Вам удалось войти? Поясните ответ.

Примечание. Если ваш сеанс через порт консоли маршрутизатора истекает по времени, вам может потребоваться войти в систему с помощью списка методов аутентификации по умолчанию.

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться: R3 con0 is now available

Press RETURN to get started.

c. Попытайтесь войти в консоль как пользователь baduser с любым паролем. Вам удалось войти? Поясните ответ.

Шаг 3: Создайте профиль аутентификации AAA для Telnet с помощью локальной базы данных.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного метода без аутентификации, поэтому если в локальной базе данных не будет имен пользователей, доступ по Telnet будет отключен. Для создания профиля аутентификации, который не является профилем по умолчанию, укажите имя списка TELNET_LINES и примените его к линиям vty.

   R3(config)# aaa authentication login TELNET_LINES local

   R3(config)# line vty 0 4

   R3(config-line)# login authentication TELNET_LINES

b. Убедитесь, что профиль аутентификации используется при открытии сеанса Telnet с компьютера PC-C на маршрутизатор R3.

   PC-C> telnet 192.168.3.1

   Trying 192.168.3.1 ... Open

c. Войдите как Admin01 с паролем Admin01pass. Вам удалось войти? Поясните ответ.

Задача 3: Изучение отладки аутентификации AAA с помощью Cisco IOS.

В этом задании с помощью команды debug вы рассмотрите успешные и неуспешные попытки аутентификации.

Шаг 1: Убедитесь, что системное время и временные метки для отладки правильно настроены.

a. От имени пользователя маршрутизатора R3 или в привилегированном режиме введите команду show clock, чтобы определить, какое текущее время установлено на маршрутизаторе. Если время и дата установлены неправильно, установите их в привилегированном режиме по команде clock set HH:MM:SS DD month YYYY. Ниже приведен пример для маршрутизатора R3.

R3# clock set 14:15:00 13 September 2019

b. Убедитесь, что подробная информация о временных метках доступна в выходных данных отладки, с помощью команды show run. Эта команда отобразит все строки текущей конфигурации, в которых есть текст timestamps (временные метки).

R3# show run | include timestamps

service timestamps debug datetime msec service timestamps log datetime msec

c. Если команда service timestamps debug отсутствует, введите ее в режиме глобальной настройки.

```
R3(config)# service timestamps debug datetime msec
R3(config)# exit
```

d. Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

```
R3# copy running-config startup-config
```

Шаг 2: Используйте отладку для проверки доступа пользователя.

a. Включите отладку для аутентификации AAA.

```
R3# debug aaa authentication
AAA Authentication debugging is on
```

b. Запустите на маршрутизаторе R2 сеанс Telnet с маршрутизатором R3.

c. Войдите под именем пользователя Admin01 и паролем Admin01pass. Просмотрите события аутентификации AAA в окне сеанса консоли. Там должны отображаться сообщения об отладке, похожие на следующие.

```
R3#
Feb 20 08:45:49.383: AAA/BIND(0000000F): Bind i/f
Feb 20 08:45:49.383: AAA/AUTHEN/LOGIN (0000000F): Pick method list 'TELNET_LINES'
```

d. Из окна Telnet перейдите в привилегированный режим. Используйте пароль привилегированного доступа cisco12345. Там должны отображаться сообщения об отладке, похожие на следующие. Обратите внимание на имя пользователя в третьей строке (Admin01), номер виртуального порта (tty132) и адрес удаленного клиента Telnet (10.2.2.2). Также обратите внимание, что последняя строка о состоянии – PASS.

```
R3#
Feb 20 08:46:43.223: AAA: parse name=tty132 idb type=-1 tty=-1
Feb 20 08:46:43.223: AAA: name=tty132 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=132 channel=0
Feb 20 08:46:43.223: AAA/MEMORY: create_user (0x32716AC8) user='Admin01' ruser
Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): port='tty132' list='' action=LOGIN service=ENABLE
Feb 20 08:46:43.223: AAA/AUTHEN/START (2
R3#655524682): non-console enable - default to enable password
Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): Method=ENABLE

Feb 20 08:46:43.223: AAA/AUTHEN (2655524682): status = GETPASS
R3#
Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): continue_login (user='(undef)')
Feb 20 08:46:46.315: AAA/AUTHEN (2655524682): status = GETPASS
Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): Method=ENABLE
Feb 20 08:46:46.543: AAA/AUTHEN (2655524682): status = PASS
```

e. В окне Telnet выйдите из привилегированного режима с помощью команды disable. Попытайтесь перейти в привилегированный режим снова, но на этот раз используйте неправильный пароль. Просмотрите выходные данные отладчика на маршрутизаторе R3. Обратите внимание, что сейчас состояние – FAIL.

```
Feb 20 08:47:36.127: AAA/AUTHEN (4254493175): status = GETPASS
Feb 20 08:47:36.127: AAA/AUTHEN/CONT (4254493175): Method=ENABLE
Feb 20 08:47:36.355: AAA/AUTHEN(4254493175): password incorrect
Feb 20 08:47:36.355: AAA/AUTHEN (4254493175): status = FAIL
```

Feb 20 08:47:36.355: AAA/MEMORY: free_user (0x32148CE4) user='NULL' ruser='NULL' port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)
R3#

f. В окне Telnet выйдите из сеанса Telnet с маршрутизатором. Попытайтесь снова открыть сеанс Telnet с маршрутизатором, но на этот раз попытайтесь войти в систему как Admin01 с неправильным паролем. Выходные данные отладчика в окне консоли должны быть похожи на следующее.

Feb 20 08:48:17.887: AAA/AUTHEN/LOGIN (00000010): Pick method list 'TELNET_LINES' Какое сообщение было показано на экране клиента Telnet?

Часть 4: Настройка централизованной аутентификации с помощью AAA и RADIUS

В части 4 данной лабораторной работы необходимо установить программное обеспечение RADIUS на компьютере PC-A. Затем необходимо настроить доступ на маршрутизаторе R1 к внешнему серверу RADIUS для аутентификации пользователей. В этой части лабораторной работы используется бесплатный сервер WinRadius.

Задача 1: Восстановление базовой конфигурации маршрутизатора R1.

Чтобы избежать ошибок из-за созданной ранее конфигурации AAA RADIUS, начните с возврата базовых настроек на маршрутизаторе R1, как показано в частях 1 и 2 данной лабораторной работы.

Шаг 1: Повторно загрузите и восстановите сохраненную конфигурацию на маршрутизаторе R1.

На данном шаге верните базовые настройки на маршрутизаторе, сохраненные в частях 1 и 2.

a. Подключитесь к консоли маршрутизатора R1, войдите в систему как user01 с паролем user01pass.

b. Войдите в привилегированный режим с паролем cisco12345.

c. Перезагрузите маршрутизатор и ответьте no на запрос о сохранении конфигурации.

R1# reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

Шаг 2: Проверьте связь.

a. Проверьте связь, отправив эхо-запрос с компьютера PC-A на PC-C. Если запрос выполнился с ошибкой, устраните неисправности в настройках маршрутизатора и ПК.

b. Если вы вышли из консоли, войдите снова как user01 с паролем user01pass, затем войдите в привилегированный режим с паролем cisco12345.

Задача 2: Загрузка и установка на компьютере PC-A сервера RADIUS.

Существует несколько серверов RADIUS, как платных, так и бесплатных. В данной лабораторной работе используется WinRadius – стандартный бесплатный сервер RADIUS, работающий под управлением ОС Windows. Бесплатная версия этого ПО поддерживает лишь 5 имен пользователей.

Примечание. Zip-архив с программным обеспечением WinRadius можно запросить у своего инструктора.

Шаг 1: Загрузите программное обеспечение WinRadius.

a. Создайте папку с именем WinRadius на рабочем столе или в другом месте, куда будете сохранять файлы.

b. Распакуйте архив с WinRadius в папку, созданную на шаге 1a. Среди них не будет файла с установщиком. Распакованный файл WinRadius.exe является исполняемым.

Возможные решения:

a. Настройки для Compatibility (совместимость)

1) Щелкните правой кнопкой мыши значок WinRadius.exe и выберите Properties.

2) В диалоговом окне Properties перейдите на вкладку Compatibility. На этой вкладке установите флажок Run this program in compatibility mode for. Затем в раскрывающемся меню снизу выберите установленную на вашем компьютере операционную систему (например, Windows 7).

3) Нажмите OK.

b. Настройки для Run as Administrator

1) Щелкните правой кнопкой мыши значок WinRadius.exe и выберите Properties.

2) В диалоговом окне Properties перейдите на вкладку Compatibility. На этой вкладке установите флажок Run this program as administrator в разделе Privilege Level.

3) Нажмите OK.

c. Выберите Run as Administration для каждого запуска

1) Щелкните правой кнопкой значок WinRadius.exe и выберите Run as Administrator.

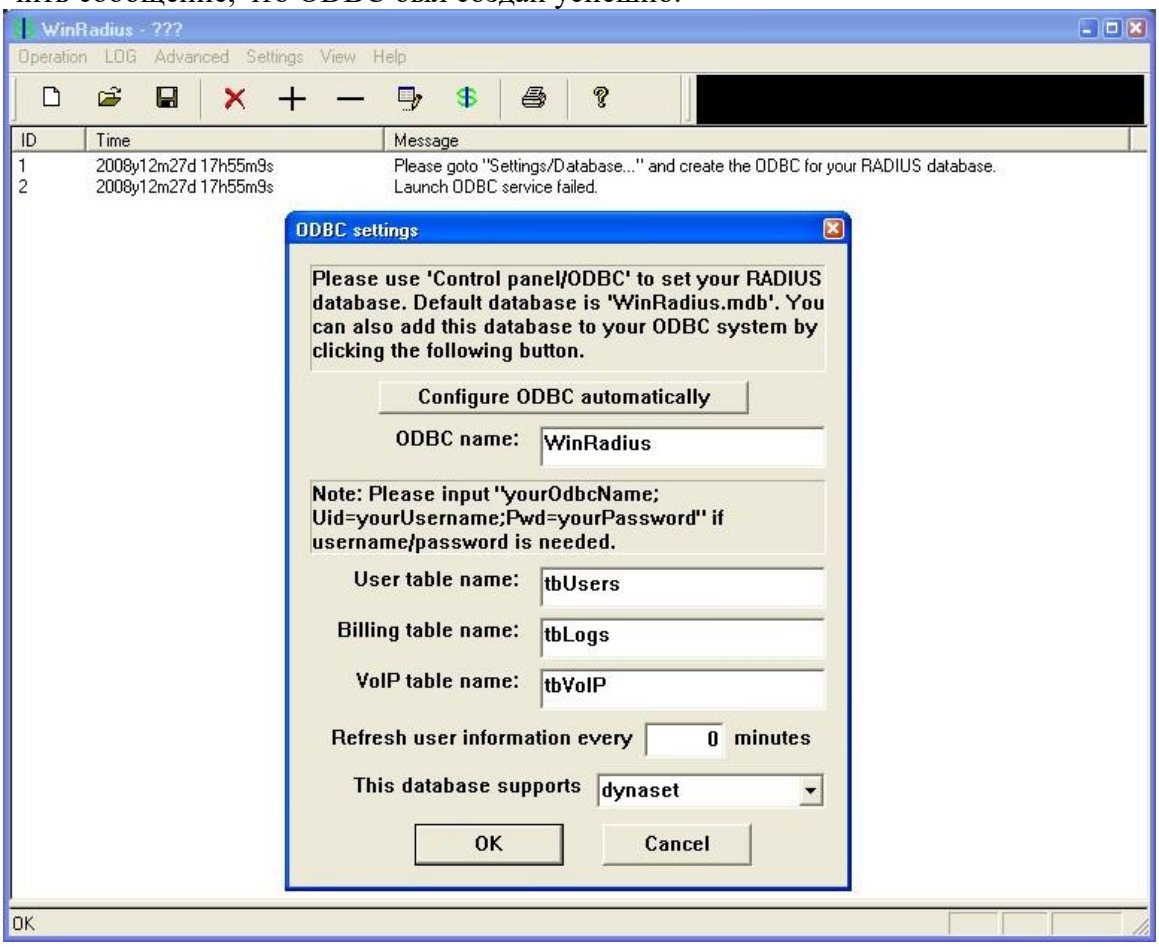
2) После запуска ПО WinRadius нажмите Yes в диалоговом окне User Account Control.

Шаг 2: Настройте базу данных сервера WinRadius.

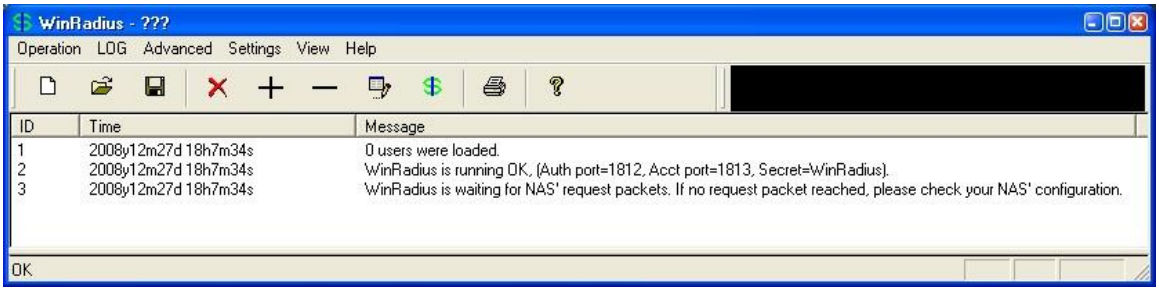
a. Запустите приложение WinRadius.exe. WinRadius использует локальную базу данных для хранения информации о пользователях. При первом запуске приложения появятся следующие сообщения:

Please go to “Settings/Database and create the ODBC for your RADIUS database.
Launch ODBC failed.

b. В главном меню выберите Settings > Database. Появится следующий экран. Нажмите кнопку Configure ODBC Automatically, затем нажмите OK. Вы должны получить сообщение, что ODBC был создан успешно.



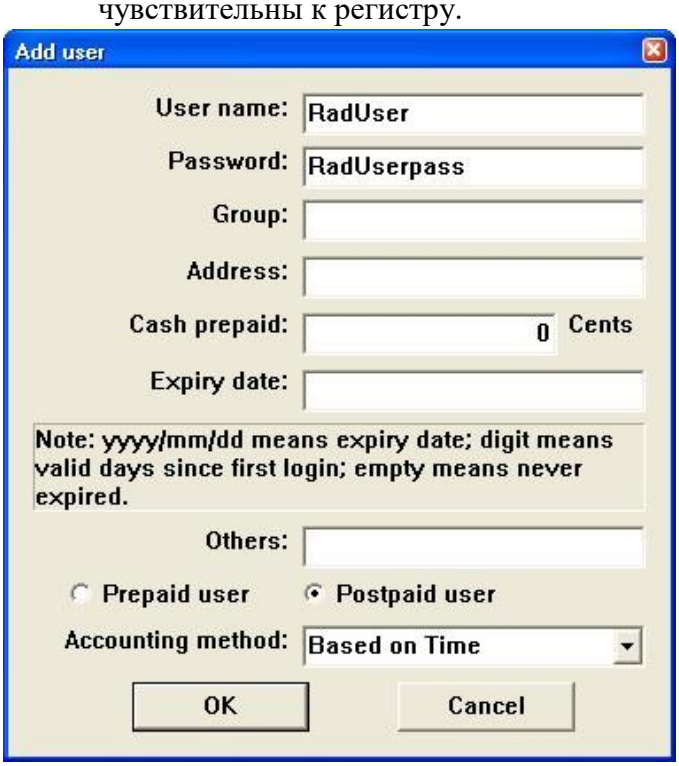
a. При повторном запуске WinRadius вы должны увидеть следующие сообщения.



Шаг 3: Настройте пользователей и пароли на сервере WinRadius.

a. В главном меню выберите Operation > Add User.

b. Введите имя пользователя RadUser и пароль RadUserpass. Помните, что пароли чувствительны к регистру.



c. Нажмите OK. Вы должны получить сообщение в окне журнала о том, что пользователь успешно добавлен.

Шаг 4: Очистите окно журнала.

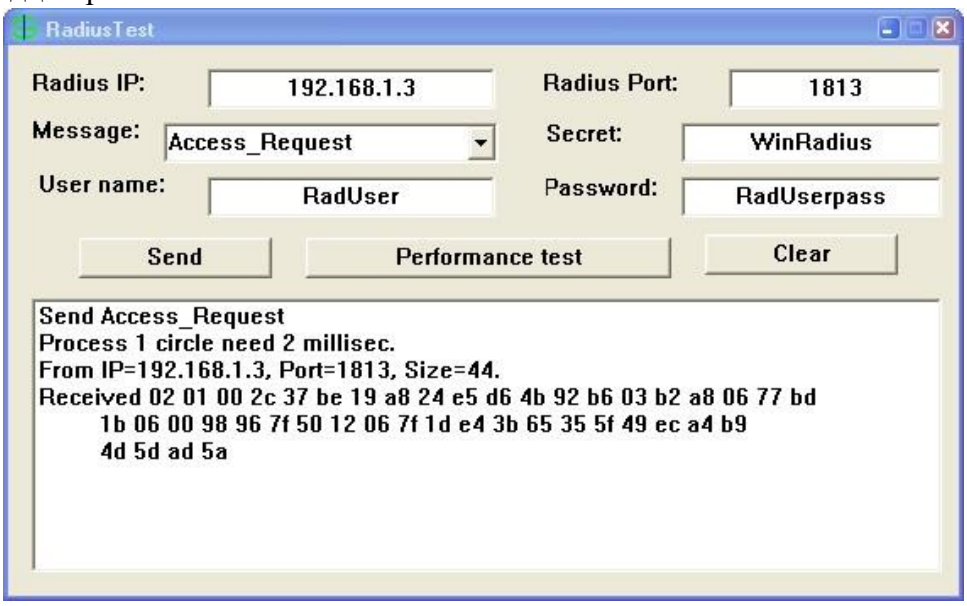
В главном меню выберите Log > Clear.

Шаг 5: Проверьте только что добавленного пользователя с помощью утилиты тестирования WinRadius.

a. В скачанном архиве находится утилита тестирования WinRadius. Перейдите в папку, куда вы распаковали WinRadius.zip, и найдите файл RadiusTest.exe.

b. Запустите приложение RadiusTest, введите IP-адрес сервера RADIUS (192.168.1.3), имя пользователя RadUser и пароль RadUserpass, как показано ниже. Не изменяйте номер порта RADIUS по умолчанию 1813 и пароль RADIUS WinRadius.

c. Нажмите Send, после чего вы должны увидеть сообщение Send Access_Request, в котором будет указано, что сервер по адресу 192.168.1.3 через порт 1813 получил 44 шестнадцатеричных символа.



a. Просмотрите журнал WinRadius и убедитесь, что пользователь RadUser был успешно аутентифицирован.

Задача 3: Настройка на маршрутизаторе R1 сервисов AAA и получение доступа к серверу RADIUS с помощью Cisco IOS.

Шаг 1: Включите AAA на маршрутизаторе R1.

Воспользуйтесь командой aaa new-model в режиме глобальной настройки, чтобы включить AAA.

R1(config)# aaa new-model

Шаг 2: Настройте список методов аутентификации при входе в систему по умолчанию.

a. Настройте список на первоочередное использование RADIUS для сервиса аутентификации, а далее – без аутентификации. Если сервер RADIUS недоступен и аутентификация не может быть выполнена, маршрутизатор глобально разрешает доступ без аутентификации. Это необходимо для случая, если маршрутизатор начнет работу без связи с активным сервером RADIUS.

R1(config)# aaa authentication login default group radius none

b. В качестве альтернативы вы можете настроить локальную аутентификацию в качестве запасного метода.

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Шаг 3: Укажите сервер RADIUS.

a. Используйте команду radius server для входа в режим настройки сервера RADIUS.

R1(config)# radius server CCNAS

b. Используйте символ ? для вывода списка команд подрежима для настройки сервера RADIUS.

```
R1(config-radius-server)# ?
RADIUS server sub-mode commands:
 address        Specify the radius server address   automate-tester  Configure server automated testing.
 backoff        Retry backoff pattern(Default is retransmits with constant                delay)   exit
Exit from RADIUS server configuration mode   key            Per-server encryption key   no
Negate a command or set its defaults   non-standard     Attributes to be parsed that violate RADIUS
standard   pac            Protected Access Credential key   retransmit       Number of retries to active
server (overrides default)   timeout          Time to wait (in seconds) for this radius server to reply
          (overrides default)
```

c. Используйте команду address для настройки IP-адреса для компьютера PC-A.

```
R1(config-radius-server)# address ipv4 192.168.1.3
```

d. Команда key используется для установки секретного пароля, который является общим для сервера RADIUS и маршрутизатора (в данном случае R1) и применяется для аутентификации соединения между маршрутизатором и сервером прежде, чем начнется процесс аутентификации пользователя. Используйте секретный пароль NAS по умолчанию WinRadius, указанный на сервере RADIUS (см. задачу 2, шаг 5). Помните, что пароли чувствительны к регистру.

```
R1(config-radius-server)# key WinRadius
R1(config-redius-server)# end
```

Задача 4: Проверка конфигурации AAA RADIUS.

Шаг 1: Проверьте связь между маршрутизатором R1 и компьютером, на котором работает сервер RADIUS.

Отправьте эхо-запрос с маршрутизатора R1 на компьютер PC-A.

```
R1# ping 192.168.1.3
```

Если запрос выполнен с ошибкой, проведите диагностику основных настроек компьютера и маршрутизатора перед тем, как продолжить.

Шаг 2: Проверьте конфигурацию.

a. Если вы перезапускали сервер WinRadius, вам потребуется заново создать пользователя RadUser с паролем RadUserpass путем выбора Operation > Add User.

b. Очистите журнал на сервере WinRadius путем выбора Log > Clear в главном меню.

c. На маршрутизаторе R1 перейдите на начальный экран маршрутизатора, на котором отображается:

```
R1 con0 is now available


Press RETURN to get started.
```

a. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя имя пользователя RadUser и пароль RadUserpass. Удалось ли вам получить доступ в привилегированный режим и если да, была ли задержка?

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

```
R1 con0 is now available
```

Press RETURN to get started.

c. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя несуществующее имя пользователя Userxxx и пароль Userxxxpass. Удалось ли вам получить доступ в привилегированный режим? Поясните ответ.

d. Были ли отображены какие-либо сообщения в журнале сервера RADIUS или при входе?

e. Почему несуществующему пользователю удалось получить доступ к маршрутизатору и при этом не были выведены сообщения в журнале сервера RADIUS?

f. Когда сервер RADIUS недоступен, после попыток входа в систему могут появляться примерно следующие сообщения:

*Dec 26 16:46:54.039: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.3:1645,1646 is not responding.

*Dec 26 15:46:54.039: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.3:1645,1646 is being marked alive.

Шаг 3: Устраните неполадки при связи между маршрутизатором и сервером RADIUS.

a. Проверьте номера портов Cisco IOS RADIUS UDP по умолчанию, используемые на маршрутизаторе R1: снова войдите в режим настройки сервера RADIUS с помощью команды radius server, а затем используйте функцию Cisco IOS Help в команде подрежима address.

R1(config)# radius server CCNAS

R1(config-radius-server)# address ipv4 192.168.1.3 ?

acct-port UDP port for RADIUS acco/unting server (default is 1646)

alias 1-8 aliases for this server (max. 8) auth-port UDP port for

RADIUS authentication server (default is 1645) <cr>

Каковы номера портов Cisco IOS UDP по умолчанию маршрутизатора R1 для сервера RADIUS?

Шаг 4: Проверьте номера портов по умолчанию на сервере WinRadius на компьютере PC-A.

В главном меню WinRadius выберите Settings > System.

Каковы номера портов WinRadius UDP по умолчанию?

Примечание. В документе RFC 2865 официально назначены номера портов 1812 и 1813 для RADIUS.

Шаг 5: Поменяйте номера портов RADIUS на маршрутизаторе R1 для соответствия с сервером WinRadius.

Если не указано иное, конфигурация Cisco IOS RADIUS по умолчанию настроена на номера портов UDP 1645 и 1646. Либо номера портов Cisco IOS должны быть изменены в соответствии с номерами портов сервера RADIUS, либо номера портов сервера RADIUS должны быть изменены в соответствии с номерами портов маршрутизатора Cisco IOS.

Снова введите команду подрежима address. На этот раз укажите номера портов 1812 и 1813, а также адрес IPv4.

R1(config-radius-server)# address ipv4 192.168.1.3 auth-port 1812 acct-port 1813

Шаг 6: Проверьте конфигурацию, войдя в консоль на маршрутизаторе R1.

a. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться: R1 con0 is now available, Press RETURN to get started.

b. Снова войдите под именем RadUser и паролем RadUserpass. Вам удалось войти? Была ли задержка на этот раз?

c. В журнале на сервере RADIUS должно появиться следующее сообщение.

User (RadUser) authenticate OK.

d. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R1 con0 is now available, Press RETURN to get started.

e. Снова войдите с именем Userxxx и паролем Userxxxpass. Вам удалось войти?

Какое сообщение появилось на маршрутизаторе?
В журнале на сервере RADIUS должны появиться следующие сообщения.
Reason: Unknown username

Шаг 7: Создайте список методов аутентификации для Telnet и протестируйте его.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного режима «без аутентификации», поэтому если доступ к серверу RADIUS отсутствует, то доступ по Telnet будет отключен. Назовите данный список TELNET_LINES.

R1(config)# aaa authentication login TELNET_LINES group radius

b. Примените список к линиям vty на маршрутизаторе, используя команду login authentication.

R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET_LINES

c. Подключитесь с компьютера PC-A к маршрутизатору R1 по Telnet и войдите с именем RadUser и паролем RadUserpass. Вам удалось получить доступ для входа? Поясните ответ.

d. Завершите сеанс Telnet, затем снова с компьютера PC-A подключитесь к маршрутизатору R1 по Telnet. Войдите с именем Userxxx и паролем Userxxxpass. Вам удалось войти? Поясните ответ.

Практическая работа № 6
Настройка политики безопасности брандмауэров

Задание:

Активизация встроенного межсетевого экрана

1. Откройте компоненту *Брандмауэр Windows.* Для этого выберите последовательно *Пуск —» Панель управления —> Система и безопасность* и выберите соответствующий компонент в списке.

Другой способ поиска данной компоненты осуществляется с помощью последовательного выбора *Пуск —> Панель управления —> Сеть и Интернет —> Центр управления сетями и общим доступом,* в котором в списке *См. также* находится ссылка на компоненту *Брандмауэр Windows* (рис. 6.2).

2. На вкладке *Включение и отключение брандмауэра Windows* в группе *Брандмауэр Windows* (рис. 6.3) выберите параметры размещения сети и включите брандмауэр для нужной сети. Для выполнения этого действия требуются *права администратора* (см. материал тем 2—5).

Запуск программ или компонентов через брандмауэр Windows

Для того чтобы разрешить, удалить или изменить разрешенные программы и порты, сделаем следующее: на вкладке *Разрешить запуск программы или компонента через брандмауэр Windows* в группе

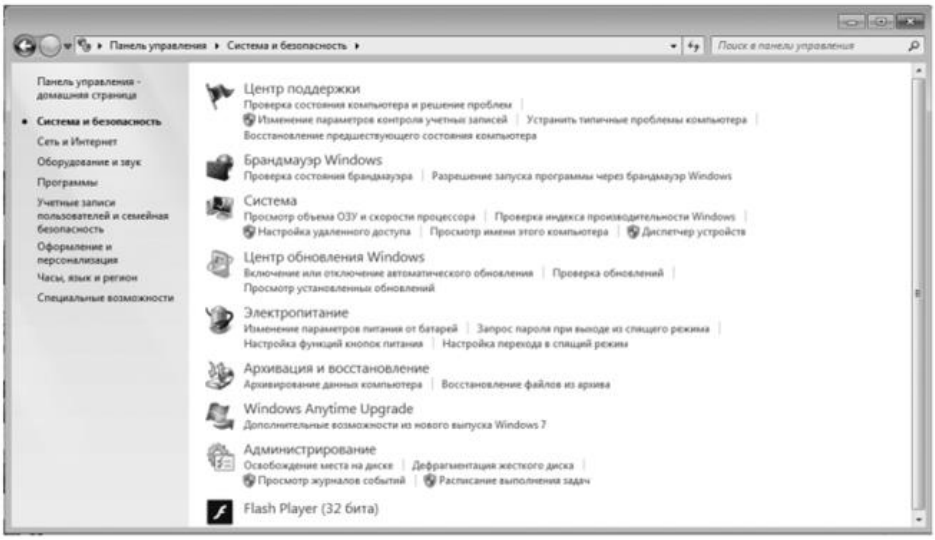


Рис. 6.2. Брандмауэр Windows

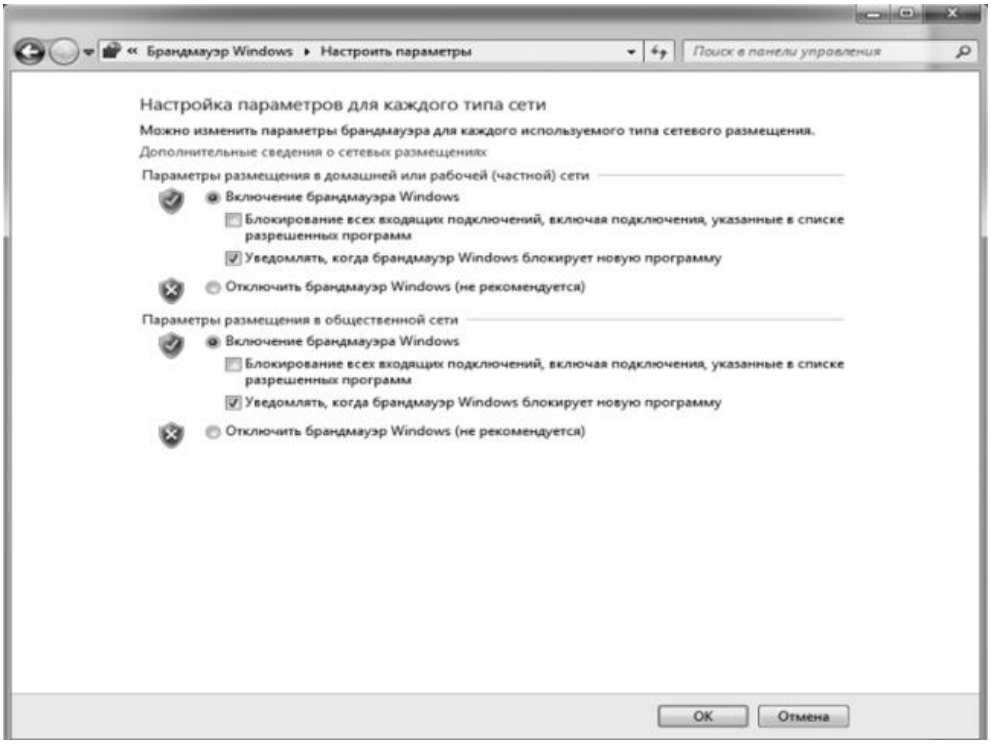


Рис. 6.3. Настройка параметров типов подключения

Брандмауэр Windows (рис. 6.4) выбираем и отмечаем галочками программы, которым мы хотим дать доступ к сети.

3041?

Практическая работа № 7
Настройка безопасности на втором уровне на коммутаторах

Задание:

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Задачи

Часть 1. Настройка топологии и установка исходного состояния устройства

Часть 2. Настройка базовых параметров устройств и проверка подключения Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1

Настройте доступ по протоколу SSH.
Измените параметры SSH.
Проверьте конфигурацию SSH.
Часть 4. Настройка и проверка параметров безопасности для S1
Настройте и проверьте общие функции безопасности.
Настройте и проверьте функцию безопасности порта.
Исходные данные/Сценарий
На компьютерах и серверах следует ограничивать доступ, устанавливая качественную систему безопасности. На ваших устройствах сетевой инфраструктуры, например коммутаторах и маршрутизаторах, тоже важно настраивать функции безопасности.
В ходе данной лабораторной работе вам нужно настроить функции безопасности на коммутаторах LAN в соответствии с практическими рекомендациями. Вам следует разрешить только сеансы протокола SSH и безопасного протокола HTTPS. Кроме того, вам предстоит настроить и проверить работу функции безопасности порта, направленную на блокировку любого устройства с MAC-адресом, который неизвестен коммутатору.
Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторных работах используется коммутатор Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под

управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.
Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена, и они не содержат файлов загрузочной конфигурации. Если вы не уверены, обратитесь к преподавателю или вернитесь к процедурам инициализации и перезагрузки устройств, описанных в предыдущей лабораторной работе.
Необходимые ресурсы:
1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
1 ПК (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
консольные кабели для настройки устройств Cisco IOS через консольные порты;
кабели Ethernet, расположенные в соответствии с топологией.
Часть 1. Настройка топологии и инициализация устройств
В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.
Шаг 1: Подключите кабели в сети в соответствии с топологией.
Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.
Если ранее на маршрутизаторе или коммутаторе были сохранены конфигурационные файлы, выполните инициализацию и перезагрузку устройств, чтобы восстановить базовые настройки.
Часть 2. Настройка базовых параметров устройств и проверка подключения

Во второй части лабораторной работы вам предстоит настроить базовые параметры маршрутизатора, коммутатора и ПК. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Шаг 1: Настройте IP-адрес на PC-A.

Шаг 2: Настройте базовые параметры на маршрутизаторе R1.

Задайте имя устройства.

Отключите поиск DNS.

Настройте IP-адрес интерфейса в соответствии с таблицей адресации.

Назначьте class в качестве пароля привилегированного режима EXEC.

Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

Зашифруйте все незашифрованные пароли.

Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 3: Выполните базовую настройку коммутатора S1.

Не рекомендуется назначать административный IP-адрес коммутатора для сети VLAN 1 (или любой другой VLAN с конечными пользователями). На данном этапе вам предстоит создать VLAN 99 на коммутаторе и назначить этой сети IP-адрес.

Задайте имя устройства.

Отключите поиск DNS.

Назначьте class в качестве пароля привилегированного режима EXEC.

Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.

Настройте шлюз по умолчанию для коммутатора S1 с помощью IP-адреса маршрутизатора R1.

Зашифруйте все незашифрованные пароли.

Сохраните текущую конфигурацию в загрузочную конфигурацию.

Создайте на коммутаторе сеть VLAN 99 и назовите её Management.

S1(config)# vlan 99 S1(config-vlan)# name Management S1(config-vlan)# exit S1(config)#

i. Настройте IP-адрес интерфейса административной сети VLAN 99 в соответствии с таблицей адресации и включите интерфейс.

S1(config)# interface vlan 99

S1(config-if)# ip address 172.16.99.11 255.255.255.0

S1(config-if)# no shutdown S1(config-if)# end S1#

Выполните команду show vlan на коммутаторе S1. В каком состоянии находится сеть VLAN 99?

Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?

Почему протокол выключен несмотря на то, что вы выполнили команду no shutdown для интерфейса VLAN 99?

Назначьте порты F0/5 и F0/6 для сети VLAN 99 на коммутаторе.

S1# config t

S1(config)# interface f0/5

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 99

S1(config-if)# interface f0/6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 99

S1(config-if)# end

m. Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол? _____

Примечание. При сходимости состояний портов может произойти небольшая задержка.

Шаг 4: Проверьте наличие подключения между всеми устройствами.

От компьютера PC-A отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
От компьютера PC-A отправьте эхо-запрос на адрес управления коммутатора S1. Успешно ли выполнены эхо-запросы? _____
От коммутатора S1 отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Если появится запрос на ввод имени пользователя пароля, оставьте имя пользователя пустым, а в качестве пароля введите class. Если появится запрос о защищённом подключении, ответьте No. Удалось ли вам получить доступ к веб-интерфейсу на коммутаторе S1?
Закройте сеанс браузера на компьютере PC-A.
Примечание. Незащищённый веб-интерфейс (сервер HTTP) коммутатора Cisco 2960 включён по умолчанию. Для обеспечения безопасности рекомендуется отключить данную службу, как описано в части 4.
Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1
Шаг 1: Настройте доступ к протоколу SSH на коммутаторе S1.
Включите SSH на S1. В режиме глобальной конфигурации создайте имя домена CCNA-Lab.com.
S1(config)# ip domain-name CCNA-Lab.com
Создайте запись локальной базы данных пользователей, которую вы будете использовать для подключения к коммутатору через SSH. Пользователь должен обладать правами доступа администратора.
Примечание. Используемый пароль не является надёжным. Он используется исключительно в рамках лабораторной работы.
S1(config)# username admin privilege 15 secret sshadmin
Настройте вход транспортировки таким образом, чтобы в каналах VTY были разрешены только подключения по протоколу SSH. Для аутентификации используйте локальную базу данных.
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local S1(config-line)# exit
d. Создайте ключ шифрования RSA с использованием модуля 1024 бит.
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 3 seconds)
e. Проверьте конфигурацию протокола SSH и ответьте на следующие вопросы.
S1# show ip ssh
Какую версию SSH использует коммутатор? _____
Сколько попыток аутентификации разрешает SSH? _____
На какое значение настроен лимит времени по умолчанию для SSH? _____
Шаг 2: Измените конфигурацию SSH на коммутаторе S1.
Измените конфигурацию SSH по умолчанию.
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
Сколько попыток аутентификации разрешает SSH? _____
На какое значение настроен лимит времени для протокола SSH? _____
Шаг 3: Проверьте конфигурацию SSH на коммутаторе S1.

С помощью клиентского программного обеспечения SSH на компьютере PC-A (например Tera Term), настройте SSH-подключение к коммутатору S1. Если в вашей клиентской программе SSH появилось сообщение о ключе узла, примите его. Войдите в систему, используя admin в качестве имени пользователя, и cisco в качестве пароля.
Удалось ли настроить связь? _____ Какой запрос был отображён на коммутаторе S1? Почему?
Чтобы завершить сеанс SSH на коммутаторе S1, введите exit.
Часть 4. Настройка и проверка параметров безопасности для S1
В четвёртой части лабораторной работы вам предстоит закрыть неиспользуемые порты, выключить определённые сервисы, работающие на коммутаторе, и настроить функцию безопасности порта на основе MAC-адресов. Коммутаторы могут быть подвержены переполнению таблицы MAC-адресов, спуфинг-атакам и попыткам неавторизованных подключений к портам коммутатора. Вам нужно будет настроить функцию порта безопасности, чтобы ограничить количество MAC-адресов, которые могут быть получены портом коммутатора, а также отключить порт при превышении этого количества.
Шаг 1: Настройка общих функций безопасности на коммутаторе S1.
Настройте баннер MOTD (сообщение дня) для коммутатора S1 в виде соответствующего предупреждения.
Выполните команду show ip interface brief на коммутаторе S1. Какие физические порты включены?
Выключите все неиспользуемые физические порты коммутатора. Используйте команду interface range.
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown S1(config-if-range)# end S1#
d. Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии находятся порты от F0/1 до F0/4?
e. Введите команду show ip http server status.
В каком состоянии находится сервер HTTP? _____
Какой порт сервера он использует? _____
В каком состоянии находится защищённый сервер HTTP? _____
Какой порт сервера он использует? _____
Сеансы HTTP отправляют все данные в незашифрованном виде. Вам нужно отключить сервис HTTP, который работает на коммутаторе S1.
S1(config)# no ip http server
В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Что у вас получилось?
В компьютере PC-A откройте защищённый сеанс веб-браузера по адресу https://172.16.99.11. Примите сертификат. Войдите в систему без имени пользователя, используйте пароль class. Что у вас получилось?
Закройте сеанс браузера на компьютере PC-A.
Шаг 2: Настройка и проверка работы функции безопасности порта на коммутаторе S1.
a. Запишите MAC-адрес интерфейса G0/1 маршрутизатора R1. В интерфейсе командной строки маршрутизатора R1 выполните команду show interface g0/1 и запишите MAC-адрес интерфейса.
R1# show interface g0/1
Каков MAC-адрес интерфейса G0/1 маршрутизатора R1?

В интерфейсе командной строки S1 выполните команду show mac address-table в привилегированном режиме. Найдите динамические записи для портов F0/5 и F0/6. Запишите их ниже.
MAC-адрес интерфейса F0/5: _____
MAC-адрес интерфейса F0/6: _____
Настройка базовой безопасности порта.
Примечание. Как правило, эту процедуру выполняют на всех портах доступа коммутатора. Интерфейс F0/5 представлен в качестве примера.
1) Из интерфейса командной строки коммутатора S1 войдите в режим конфигурации интерфейса для порта, который подключается к R1.
S1(config)# interface f0/5 2) Выключите порт.
S1(config-if)# shutdown
Включите функцию безопасности порта на интерфейсе F0/5.
S1(config-if)# switchport port-security
Примечание. Выполнение команды switchport port-security позволит установить максимальное количество MAC-адресов на значение 1. При попытке нарушения безопасности порт будет выключен. Команды switchport port-security maximum и switchport port-security violation можно использовать для того, чтобы изменить настройки по умолчанию.
Настройте статическую запись для MAC-адреса интерфейса G0/1 маршрутизатора R1, записанного на шаге 2a.
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
(Настоящий MAC-адрес интерфейса G0/1 маршрутизатора имеет формат xxxx.xxxx.xxxx).
Примечание. При желании вы можете использовать команду switchport port-security macaddress, чтобы добавить в текущую конфигурацию коммутатора защищённые MAC-адреса, которые были динамически получены на порте (до заданного максимального значения).
Включите порт коммутатора.
S1(config-if)# no shutdown S1(config-if)# end
d. Проверьте функцию безопасности порта на интерфейсе F0/5 коммутатора S1 с помощью команды show port-security interface.
S1# show port-security interface f0/5
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
В каком состоянии находится порт F0/5?
Из командной строки маршрутизатора R1 отправьте эхо-запрос на компьютер PC-A, чтобы проверить подключение.
R1# ping 172.16.99.3
Далее, изменив MAC-адрес интерфейса маршрутизатора, вы нарушите систему безопасности.
Войдите в режим конфигурации интерфейса для G0/1 и выключите его.
R1# config t
R1(config)# interface g0/1

R1(config-if)# shutdown
Настройте новый MAC-адрес для интерфейса, используя aaaa.bbbb.cccc в качестве адреса.
R1(config-if)# mac-address aaaa.bbbb.cccc
По возможности, одновременно с этим шагом установите консольное подключение на коммутаторе S1. В консольном подключении к коммутатору S1 вы увидите различные сообщения о нарушении системы безопасности. Включите интерфейс G0/1 маршрутизатора R1.
R1(config-if)# no shutdown
Из привилегированного режима коммутатора R1 отправьте эхо-запрос на компьютер PC-A.
Успешно ли выполнен эхо-запрос? Поясните свой ответ.
На коммутаторе проверьте функцию безопасности порта с помощью команд, указанных ниже.
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)

Fa0/5 1 1 1 Shutdown

Total Addresses in System (excluding one mac per port) :0 Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1

S1# show interface f0/5
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05) MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
Secure Mac Address Table

Vlan Mac Address Type Ports Remaining Age
(mins)
---- ----------- ---- ----- -------------
99 30f7.0da3.1821 SecureConfigured Fa0/5 -

Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192

k. На маршрутизаторе выключите интерфейс G0/1, удалите жёстко запрограммированный MACадрес из маршрутизатора и повторно включите интерфейс G0/1.
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown R1(config-if)# end
Из маршрутизатора R1 повторите эхо-запрос на компьютер PC-A по адресу 172.16.99.3. Успешно ли выполнен эхо-запрос? _____
Чтобы определить причину неудачи эхо-запроса, выполните команду show interface f0/5. Запишите полученные результаты.
Очистите состояние выключения порта F0/5 в результате сбоя S1.
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown S1(config-if)# no shutdown
Примечание. При сходимости состояний портов может произойти небольшая задержка.
Чтобы убедиться, что порт F0/5 вышел из состояния выключения в результате сбоя, на коммутаторе S1 выполните команду show interface f0/5.
S1# show interface f0/5
Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185) MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Из командной строки маршрутизатора R1 повторите эхо-запрос на компьютер PC-A. Эхо-запрос должен пройти успешно.

Практическая работа № 8
Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки

Задание:

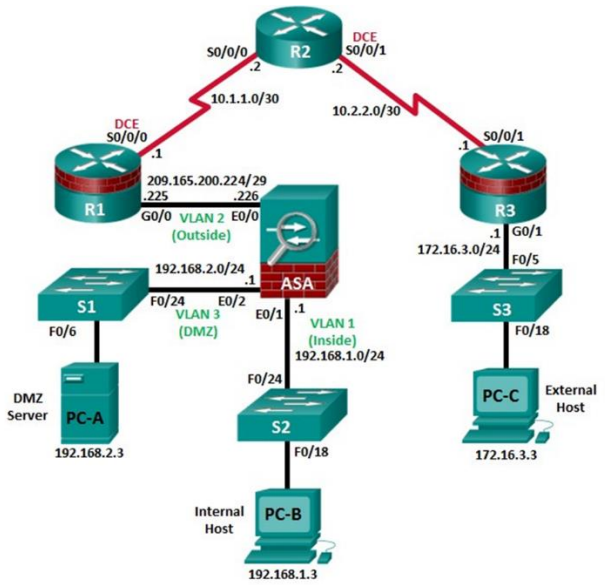


Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора

R1	G0/0	209.165.200.225	255.255.255.248	Н/П	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

- Подключите сетевые кабели и сбросьте предыдущие настройки на устройствах.
- Сконфигурируйте основные параметры для маршрутизаторов и коммутаторов.
- Настройте статическую маршрутизацию, включая маршруты по умолчанию, между маршрутизаторами R1, R2 и R3.
- Включите HTTP-сервер на маршрутизаторе R1, настройте пароли привилегированного доступа и пароли VTY.
- Сконфигурируйте параметры IP для хоста.
- Проверьте связь.

Порядок выполнения:

Шаг 1: Подключение сетевых кабелей и сброс предыдущих настроек на устройствах.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Шаг 2: Конфигурирование основных параметров для маршрутизаторов и коммутаторов.

a. Задайте имена хостов для каждого маршрутизатора, как показано на топологической схеме.

b. Настройте IP-адреса интерфейсов маршрутизаторов, как показано в таблице IP-адресов.

c. Настройте тактовую частоту маршрутизаторов с помощью последовательного кабеля DCE, подключенного к последовательному интерфейсу. В качестве примера показан маршрутизатор R1.

R1(config)# **interface S0/0/0**
R1(config-if)# **clock rate 64000**

d. Настройте имена хостов для коммутаторов. Остальные параметры коммутаторов можно оставить по умолчанию. IP-адрес для управления сетью VLAN для коммутаторов задавать необязательно.

Шаг 3: Настройка статической маршрутизации на маршрутизаторах.

a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из R3 в R2.

R1(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

R3(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

b. Настройте статический маршрут из маршрутизатора R2 к подсети Fa0/0 на R1 (подключенной к интерфейсу ASA E0/0) и статический маршрут из маршрутизатора R2 к LAN R3.

R2(config)# **ip route 209.165.200.224 255.255.255.248 10.1.1.1**
R2(config)# **ip route 172.16.3.0 255.255.255.0 10.2.2.1**

Шаг 4: Конфигурирование и шифрование паролей на маршрутизаторе R1.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, а сами пароли были упрощены для облегчения выполнения лабораторной работы. В производственной сети рекомендуется использовать более сложные пароли.

a. Задайте минимальную длину пароля. Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

b. Установите на обоих маршрутизаторах пароль привилегированного доступа **cisco12345**. Используйте алгоритм хеширования type 9 (SCRYPT).

c. Создайте локальную учетную запись **admin01,** установите для нее пароль **admin01pass.** Используйте алгоритм хеширования type 9 (SCRYPT) и установите уровень привилегий 15.

d. Настройте линии консоли и VTY на использование локальной базы данных для входа. В целях дополнительной безопасности настройте эти линии на выход из системы через 5 минут при отсутствии активности. Используйте команду **logging synchronous** для предотвращения прерывания ввода команд сообщениями консоли.

e. Включите доступ к HTTP-серверу на маршрутизаторе R1. Используйте локальную базу данных для аутентификации HTTP.

Примечание. Доступ к серверу HTTP будет использован для демонстрации инструментов ASDM в части 3.

Шаг 5: Конфигурирование параметров IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A, PC-B и PC-C, как показано в таблице IP-адресов.

Шаг 6: Проверка связи.

Между устройствами, подключенными к ASA, не будет связи, так как ASA является центральным узлом для сетевых зон и оно не было сконфигурировано. Однако у компьютера PC-C должна быть возможность отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. С компьютера PC-C отправьте эхо-запрос на IP-адрес интерфейса G0/0 маршрутизатора R1 (**209.165.200.225**). Если запросы завершаются с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запросы с компьютера PC-C на интерфейсы G0/0 и S0/0/0 маршрутизатора R1 выполнены успешно, это означает, что адресация настроена верно и статическая маршрутизация настроена и работает исправно.

Шаг 7: Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора.

Практическая работа № 9
Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM

Задание:

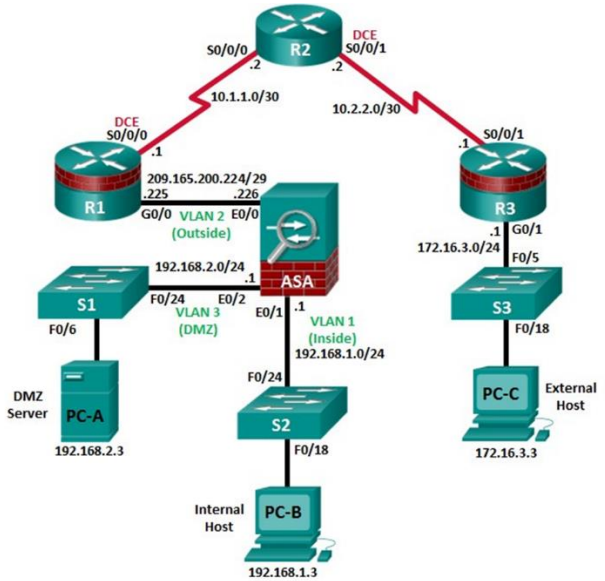


Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсе-ти	Шлюз по умолчанию	Порт комму-татора
R1	G0/0	209.165.200.225	255.255.255.248	Н/П	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Получите доступ к консоли ASA. Проверьте настройки аппаратного обеспечения, программного обеспечения и конфигурации.
Сбросьте предыдущие настройки конфигурации ASA.
Пропустите режим настройки (Setup) и сконфигурируйте интерфейсы ASDM VLAN.
Сконфигурируйте ASDM и проверьте доступ к ASA.
Получите доступ к ASDM и изучите графический интерфейс пользователя (GUI).

Порядок выполнения:
Шаг 1: Доступ к консоли ASA.
Доступ к ASA через консольный порт ничем не отличается от доступа к нему через маршрутизатор или коммутатор Cisco. Подключитесь к консольному порту ASA при помощи инверсного кабеля.
Используйте эмулятор терминала для доступа к CLI. Установите следующие настройки последовательного порта: 9600 бод, 8 бит данных, без проверки четности, 1 стоповый бит, без управления потоком.
При получении запроса на вход в режим интерактивной настройки межсетевого экрана (режим установки) ответьте no.
Войдите в привилегированный режим при помощи команды enable и пароля (если установлен). По умолчанию пароль пустой, поэтому просто нажмите Enter. Если пароль был изменен на указанный в данной лабораторной работе, введите пароль cisco12345. Имя хоста ASA по умолчанию и приглашение – ciscoasa>.
ciscoasa> enable
Password: cisco12345 (or press Enter if no password is set)
Шаг 2: Сброс предыдущих настроек конфигурации ASA.
С помощью команды write erase удалите файл startup-config из флеш-памяти.
ciscoasa# write erase
Erase configuration in flash memory? [confirm]
[OK] ciscoasa# ciscoasa# show start
No Configuration
Примечание. Команда IOS erase startup-config не поддерживается на ASA.
Используйте команду reload для перезагрузки ASA. При этом ASA загрузится в режиме настройки CLI. Если вы получите сообщение: “System config has been modified. Save? [Y]es/[N]o:”, введите n и нажмите Enter.
ciscoasa# reload
Proceed with reload? [confirm] <Enter>
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45 <output omitted>
Шаг 3: Пропуск режима настройки и конфигурирование интерфейсов ASDM VLAN.
После перезагрузки ASA оно должно определить, что не хватает файла startup-config, и выполнить серию интерактивных запросов для конфигурирования основных параметров ASA. Если переход в данный режим не выполняется, повторите шаг 2.

При запросе на предварительную настройку межсетевого экрана с помощью интерактивных запросов (режим установки) ответьте no.
Pre-configure Firewall now through interactive prompts [yes]? no
Войдите в привилегированный режим при помощи команды enable. На данном этапе пароль должен быть пустым (отсутствовать).
Войдите в режим глобальной настройки при помощи команды conf t. При первом после перезагрузки входе в режим настройки вы получите запрос на включение анонимной отправки отчетов. Ответьте no.

Настройте внутренний интерфейс VLAN 1 для подготовки к доступу через ASDM. Уровень безопасности должен быть автоматически установлен на наивысший уровень 100. Логический интерфейс VLAN 1 будет использоваться компьютером PC-B для доступа к ASDM на физическом интерфейсе E0/1 устройства ASA.
ciscoasa(config)# interface vlan 1 ciscoasa(config-if)# nameif inside
INFO: Уровень безопасности для внутреннего интерфейса inside установлен на значение 100 по умолчанию.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 ciscoasa(config-if)# security-level 100 ciscoasa(config-if)# exit
Компьютер PC-B подключен к коммутатору S2. Коммутатор S2 подключен к порту E0/1 на ASA. Почему не нужно добавлять физический интерфейс E0/1 к этой VLAN?
Примечания по интерфейсу в ASA 5505.
Модель 5505 отличается от других моделей ASA серии 5500. На других устройствах ASA, к примеру на маршрутизаторе Cisco, физическому порту можно непосредственно назначить IP-адрес 3-го уровня. ASA 5505 имеет 8 встроенных портов коммутатора, являющихся портами уровня 2. Для назначения параметров уровня 3 необходимо создать виртуальный интерфейс коммутатора (SVI) или логический интерфейс VLAN и затем назначить ему один или несколько физических портов уровня 2.
По умолчанию все физические интерфейсы ASA административно отключены (down), за исключением случаев, когда была запущена утилита установки (Setup) или были сброшены заводские настройки. Так как никакие физические интерфейсы в сети VLAN 1 не включены, VLAN 1 находится в состоянии down/down. Чтобы в этом убедиться, используйте команду show interface ip brief.
ciscoasa(config)# show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	unassigned	YES	unset	administratively down	up
Ethernet0/1	unassigned	YES	unset	administratively down	up
Ethernet0/2	unassigned	YES	unset	administratively down	up
Ethernet0/3	unassigned	YES	unset	administratively down	up
Ethernet0/4	unassigned	YES	unset	administratively down	down
Ethernet0/5	unassigned	YES	unset	administratively down	down
Ethernet0/6	unassigned	YES	unset	administratively down	down
Ethernet0/7	unassigned	YES	unset	administratively down	down
Internal-Data0/0	unassigned	YES	unset	up	up
Internal-Data0/1	unassigned	YES	unset	up	up

e. Включите интерфейс E0/1 с помощью команды no shutdown и проверьте состояние интерфейсов E0/1 и VLAN 1. Состояние и протокол для интерфейсов E0/1 и VLAN 1 должны быть up/up.
ciscoasa(config)# interface e0/1 ciscoasa(config-if)# no shut ciscoasa(config-if)# exit
ciscoasa(config)# show interface ip brief

```
Interface        IP-Address    OK? Method Status                Protocol
Ethernet0/0      unassigned    YES unset  administratively down up
Ethernet0/1      unassigned    YES unset  up                    up
Ethernet0/2      unassigned    YES unset  administratively down up

Ethernet0/3      unassigned    YES unset  administratively down up
Ethernet0/4      unassigned    YES unset  administratively down down
Ethernet0/5      unassigned    YES unset  administratively down down
Ethernet0/6      unassigned    YES unset  administratively down down
Ethernet0/7      unassigned    YES unset  administratively down down
Internal-Data0/0 unassigned    YES unset  up                    up
Internal-Data0/1 unassigned    YES unset  up                    up
Vlan1            192.168.1.1   YES manual up                  up
Virtual0         127.0.0.1     YES unset  up                    up
```

Выполните предварительную настройку внешнего интерфейса VLAN 2, добавьте физический интерфейс E0/0 к VLAN 2 и активируйте интерфейс E0/0. Назначьте IP-адрес с помощью ASDM.

```
ciscoasa(config)# interface vlan 2 ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# security-level 0 ciscoasa(config-if)# interface e0/0
ciscoasa(config-if)# switchport access vlan 2 ciscoasa(config-if)# no shut ciscoasa(config-if)# exit
```

Проверьте связь с ASA, послав эхо-запрос с компьютера PC-B на IP-адрес интерфейса VLAN 1 ASA 192.168.1.1. Эхо-запрос должен быть выполнен успешно.

Шаг 4: Настройка ASDM и проверка доступа к ASA.

Настройте на ASA прием подключений HTTPS с помощью команды http, чтобы разрешить доступ к ASDM любому хосту во внутренней сети 192.168.1.0/24.

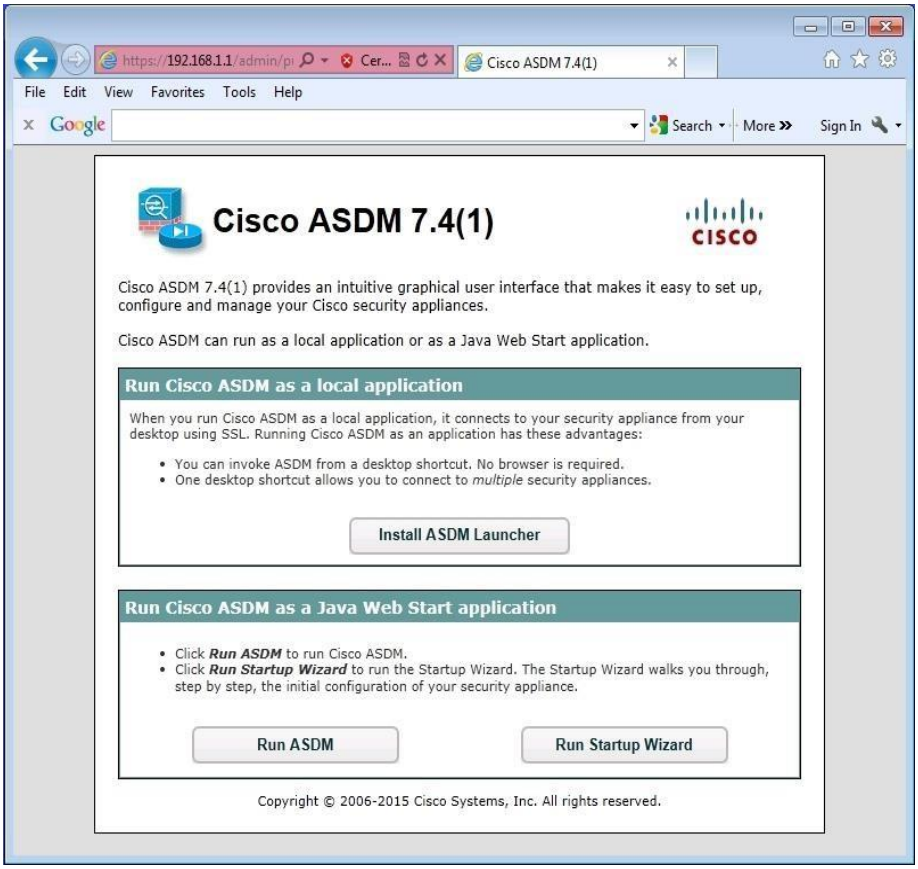
```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

Откройте браузер на компьютере PC-B и введите https://192.168.1.1., чтобы проверить HTTPS-доступ к устройству ASA.

Примечание. Убедитесь, что в URL-адресе указан протокол HTTPS.

Шаг 5: Доступ к ASDM и изучение GUI.

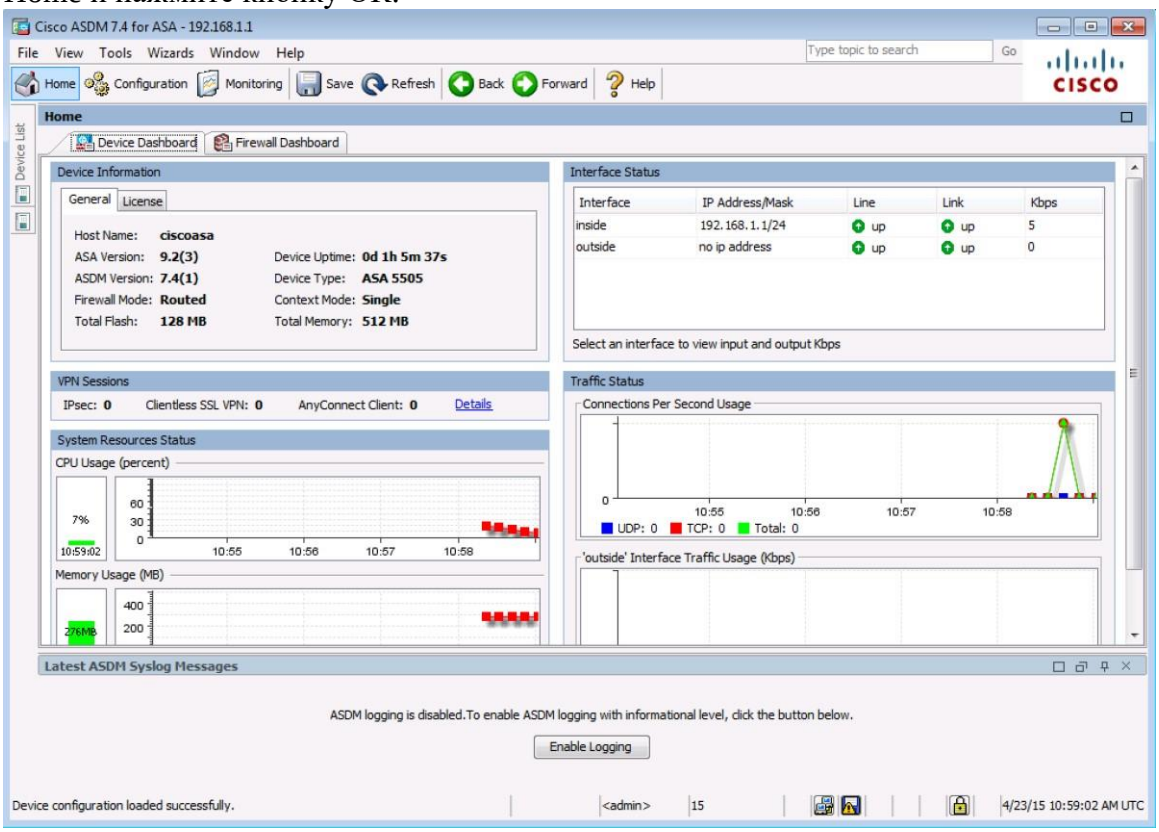
a. После ввода указанного выше URL-адреса должно появиться предупреждение системы безопасности о сертификате безопасности сайта. Щелкните Continue to this website. Появится начальная страница ASDM. На этой странице можно запустить ASDM как локальное приложение на ПК (что приведет к установке ASDM на компьютере), как браузерное Java-приложение напрямую из ASA либо запустить мастер запуска.



На все другие предупреждения системы безопасности отвечайте Yes. Должно появиться окно Cisco ASDM-IDM Launcher, в котором нужно ввести имя пользователя и пароль. Оставьте эти поля пустыми, так как эти значения еще не были сконфигурированы.

Для продолжения щелкните OK. ASDM загрузит текущую конфигурацию в GUI. Появляется начальный экран GUI, содержащий различные области и параметры. Меню в верхней левой части экрана содержит три основных раздела:: Home, Configuration и Monitoring. Раздел Home является разделом по умолчанию и состоит из двух информационных панелей: Device и Firewall. Экраном по умолчанию является информационная панель Device, на которой отображается информация об устройстве, например тип (ASA 5505), версии ASA и ASDM, объем памяти и режим межсетевого экрана (routed). На информационной панели Device имеются пять зон: o Device Information o Interface Status o VPN Sessions o System Resources Status o Traffic Status

Примечание. Если появляется окно Cisco Smart Call Home, выберите Do not enable Smart Call Home и нажмите кнопку OK.

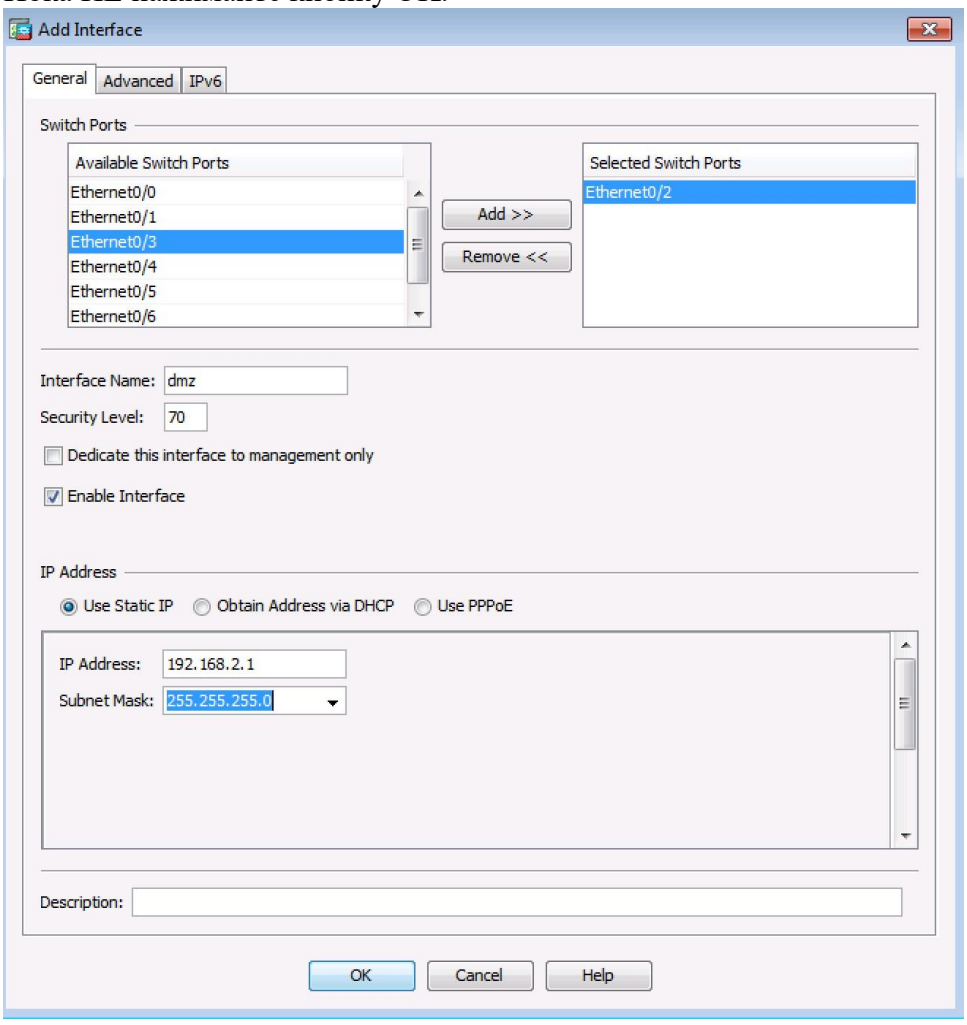


Нажмите кнопки Configuration и Monitoring, чтобы познакомиться с их расположением и увидеть доступные опции.

Практическая работа № 10
Базовая настройка шлюза безопасности ASA и настройка NAT

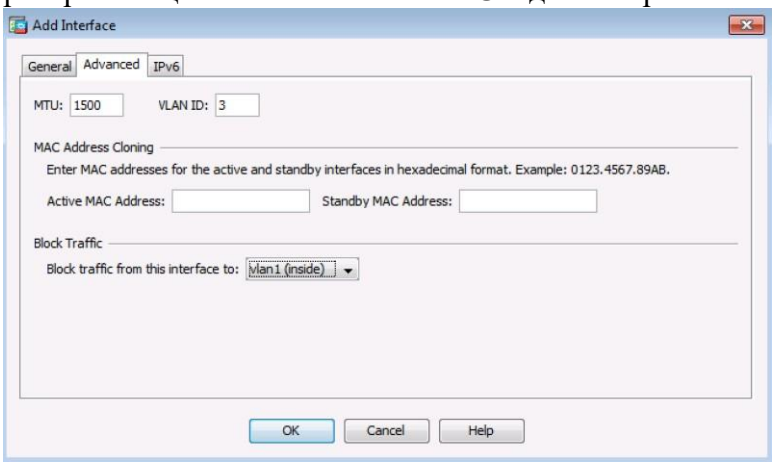
Задание:

Шаг 1: Настройка интерфейса ASA DMZ VLAN 3.
На данном шаге необходимо создать новый интерфейс VLAN 3 с именем dmz, назначить физический интерфейс E0/2 для сети VLAN, установить уровень безопасности 70 и ограничить передачу данных из этого интерфейса на внутренний (VLAN1) интерфейс.
На экране Configuration в меню Device Setup нажмите Interfaces. По умолчанию отображается вкладка Interface, на которой указываются внутренние (VLAN 1, E0/1) и внешние (VLAN 2, E0/0) интерфейсы. Нажмите Add для создания нового интерфейса.
В диалоговом окне Add Interface выберите порт Ethernet0/2 и нажмите Add. Вы получите запрос на изменение интерфейса из внутренней сети. Нажмите OK в этом сообщении, чтобы удалить порт из внутреннего интерфейса и добавить его в новый интерфейс. В окне Interface Name введите для интерфейса имя dmz, назначьте ему уровень безопасности 70 и убедитесь, что установлен флажок Enable Interface.
Убедитесь, что выбрана опция Use Static IP, введите IP-адрес 192.168.2.1 и маску подсети 255.255.255.0.
Пока НЕ нажимайте кнопку OK.

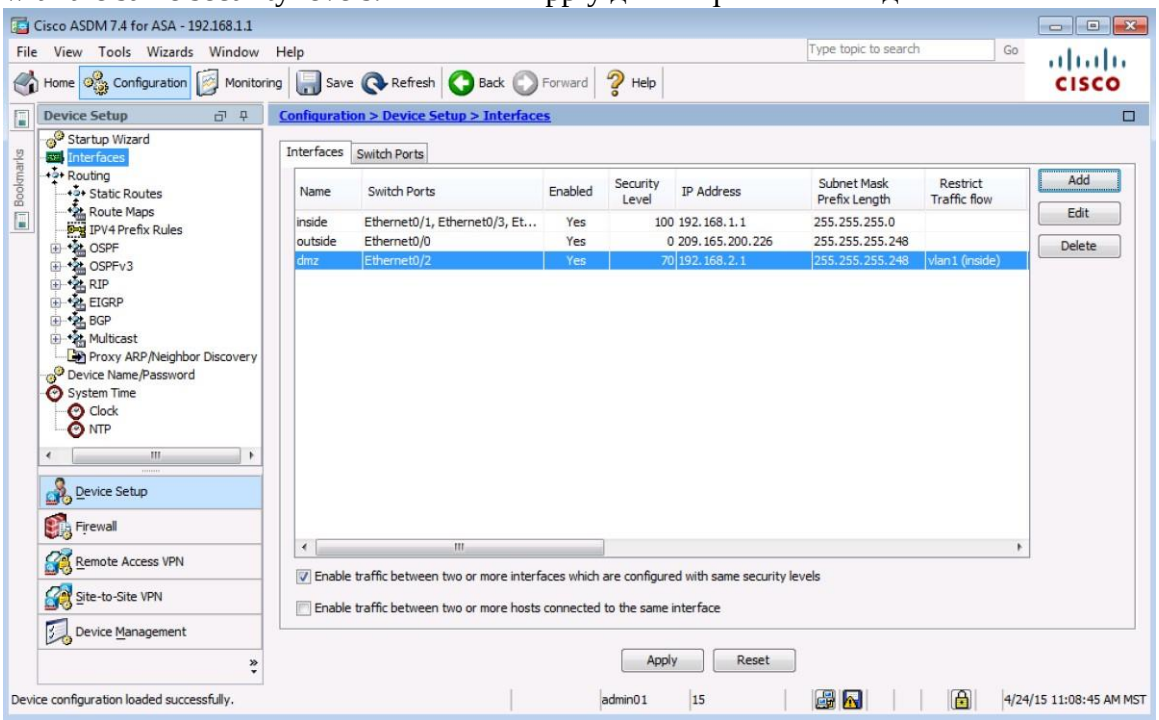


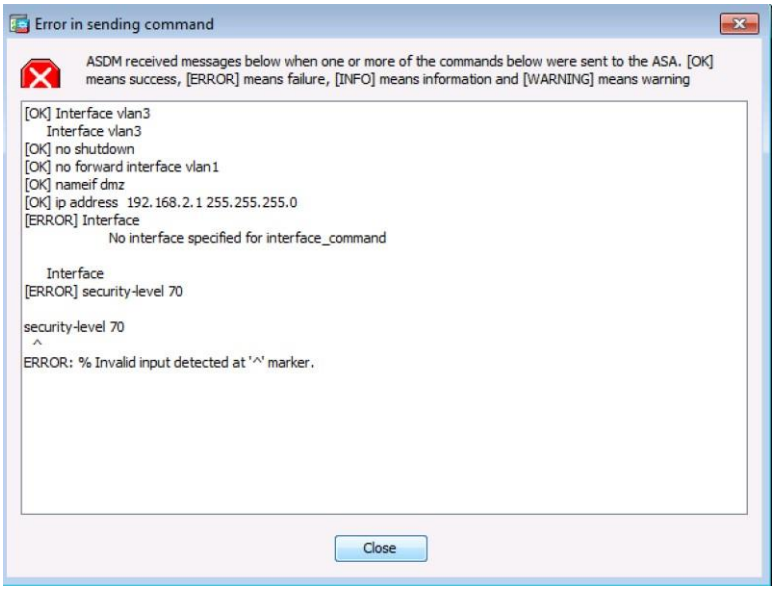
ASDM по умолчанию настроит этот интерфейс как VLAN ID 12. Перейдите на вкладку Advanced и определите этот интерфейс как VLAN ID 3, после чего нажмите кнопку OK, чтобы добавить интерфейс.

Примечание. Если вы работаете с базовой лицензией на ASA 5505, вы можете создать максимум три именованных интерфейса. Однако вам придется отключить связь между третьим интерфейсом и одним из других интерфейсов. Так как серверу DMZ не нужно инициировать связь с внутренними пользователями, вы можете отключить передачу данных на интерфейсы VLAN 1. На вкладке Advanced нужно заблокировать трафик, передаваемый из данного интерфейса VLAN 3 (dmz) в интерфейс VLAN 1 (внутренний). В области Block Traffic выберите vlan1 (inside) в раскрывающемся меню. Нажмите OK для возврата в окно Interfaces.



Кроме внешних и внутренних интерфейсов, теперь должен отображаться новый интерфейс с именем dmz. Установите флажок Enable traffic between two or more interfaces which are configured with the same security levels. Нажмите Apply для отправки команд на ASA.

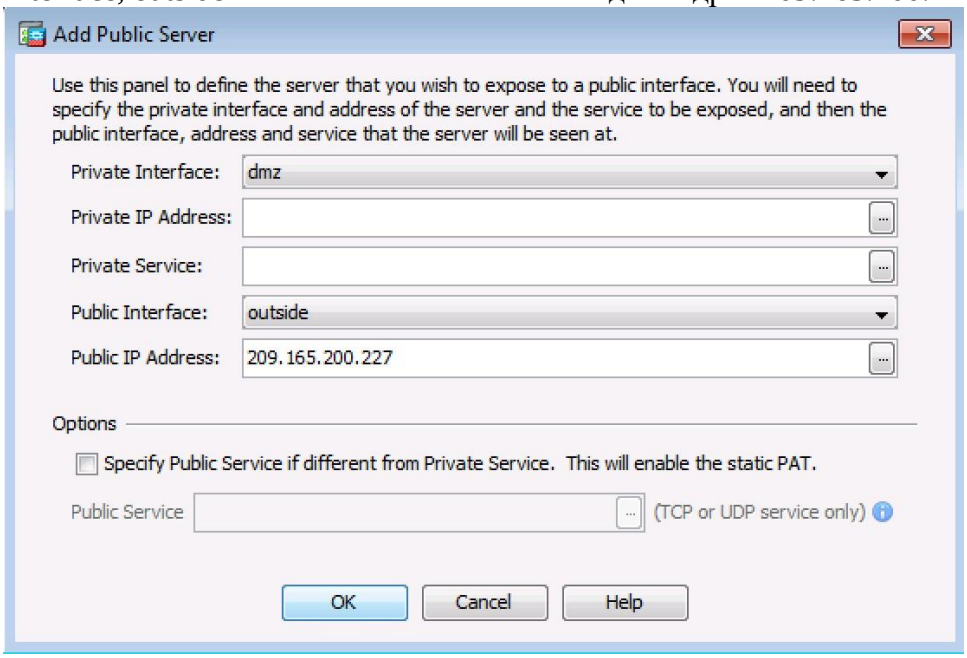




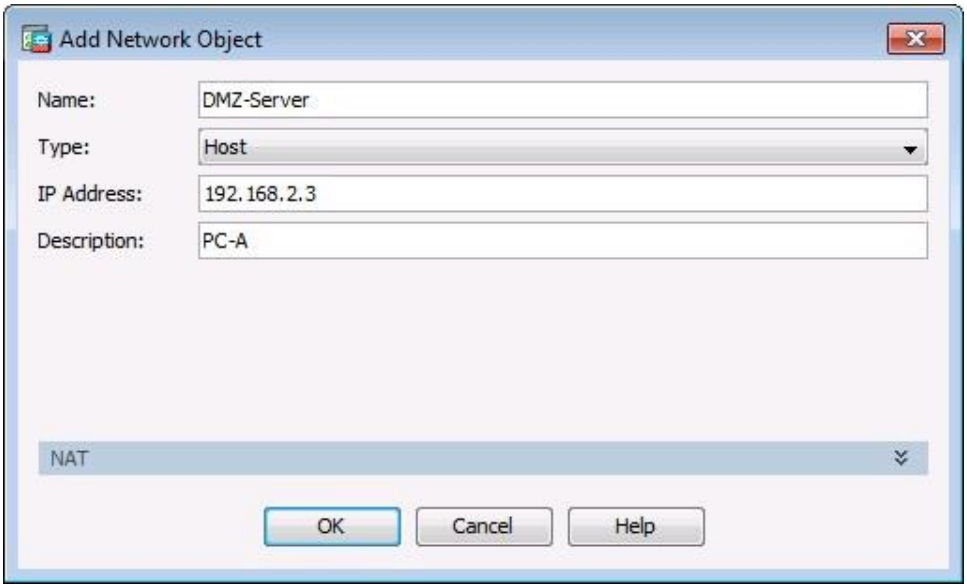
Шаг 2: Настройка сервера DMZ и статического преобразования NAT.

Для согласования добавления сервера DMZ и веб-сервера нужно будет использовать другой адрес из назначенного диапазона адресов ISP 209.165.200.224/29 (.224-.231). Интерфейс G0/0 маршрутизатора R1 и интерфейс ASA уже используют адреса 209.165.200.225 и 226. Для доступа к серверу с преобразованием адресов вы будете использовать общедоступный адрес 209.165.200.227 и статический NAT.

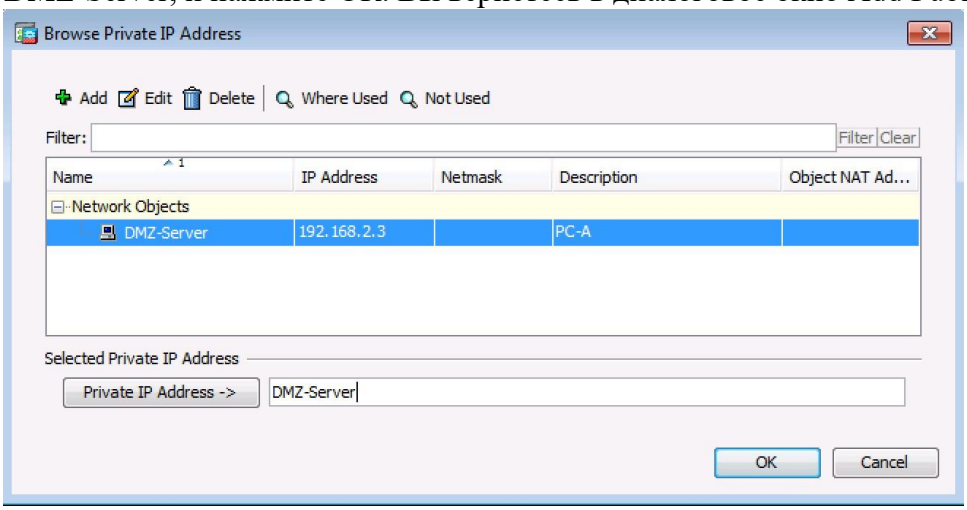
Для определения сервера DMZ и предоставляемых сервисов выберите в меню Firewall опцию Public Servers и нажмите Add. В диалоговом окне Add Public Server укажите dmz в поле Private Interface, outside в поле Public Interface и введите адрес 209.165.200.227 в поле Public IP address.



Нажмите кнопку выбора справа от поля Private IP Address. В окне Browse Private IP Address нажмите Add, чтобы определить сервер в качестве сетевого объекта (Network Object). Введите имя DMZ-Server, в раскрывающемся меню Type выберите Host, введите значения в поля IP Address (192.168.2.3) и Description (PC-A).

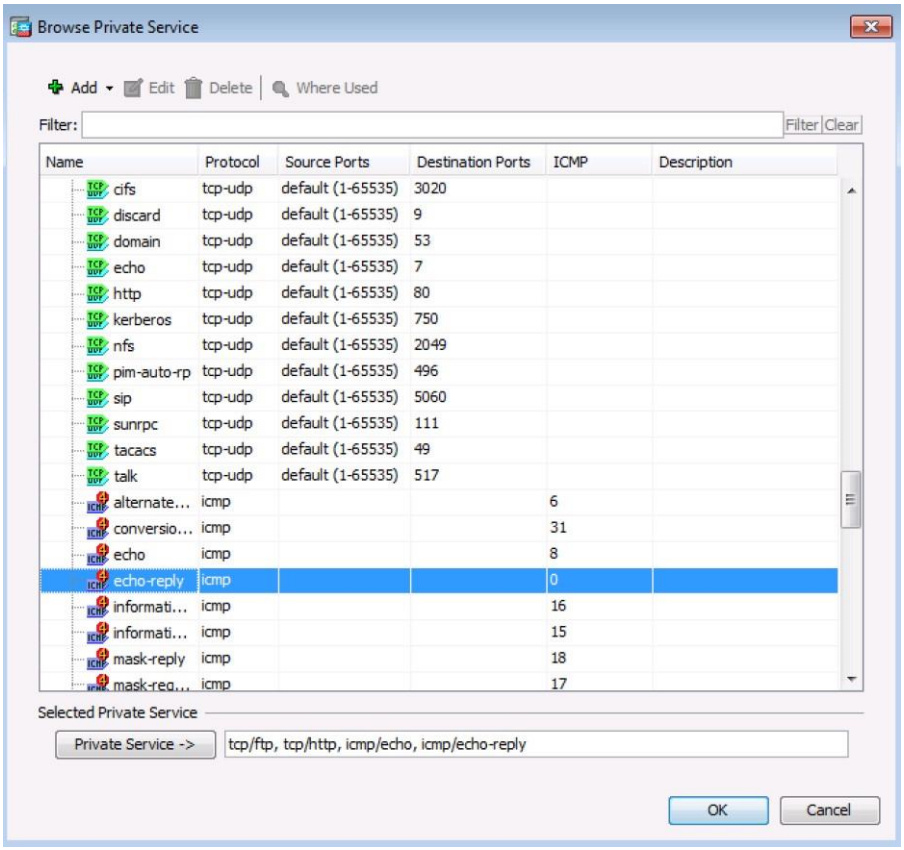


В окне Browse Private IP Address убедитесь, что в поле Selected Private IP Address отображается DMZ-Server, и нажмите OK. Вы вернетесь в диалоговое окно Add Public Server.

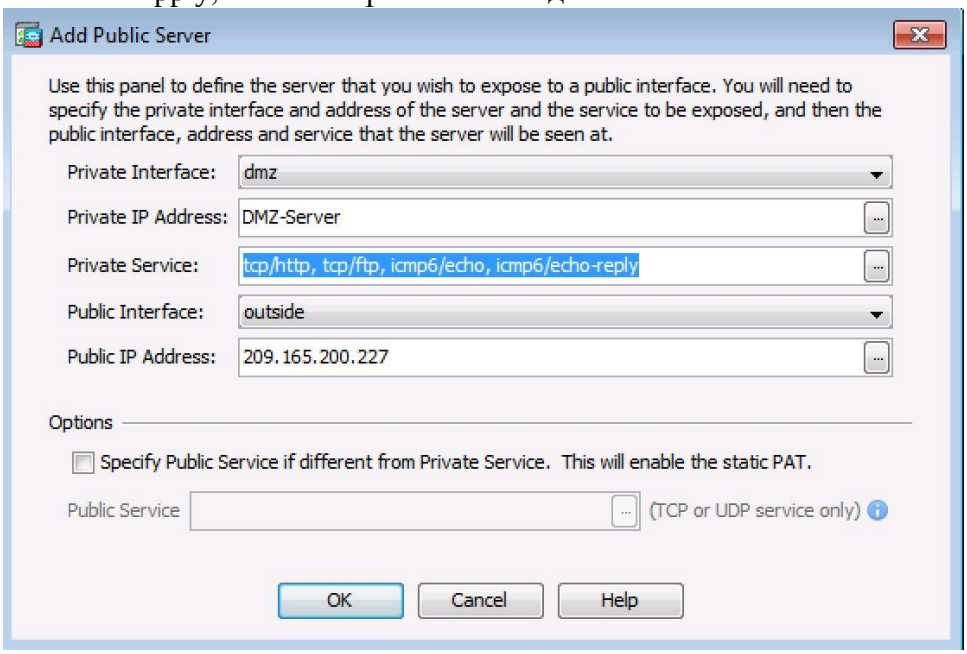


В диалоговом окне Add Public Server нажмите кнопку выбора, расположенную справа от поля Private Service. В окне Browse Private Service дважды щелкните следующие сервисы: tcp/ftp, tcp/http, icmp/echo, и icmp/echo-reply (чтобы увидеть все сервисы, используйте полосу прокрутки). Нажмите OK для продолжения и возврата в диалоговое окно Add Public Server.

Примечание. Вы можете определить общедоступные сервисы, если они не совпадают с частными, используя опцию на этом экране.



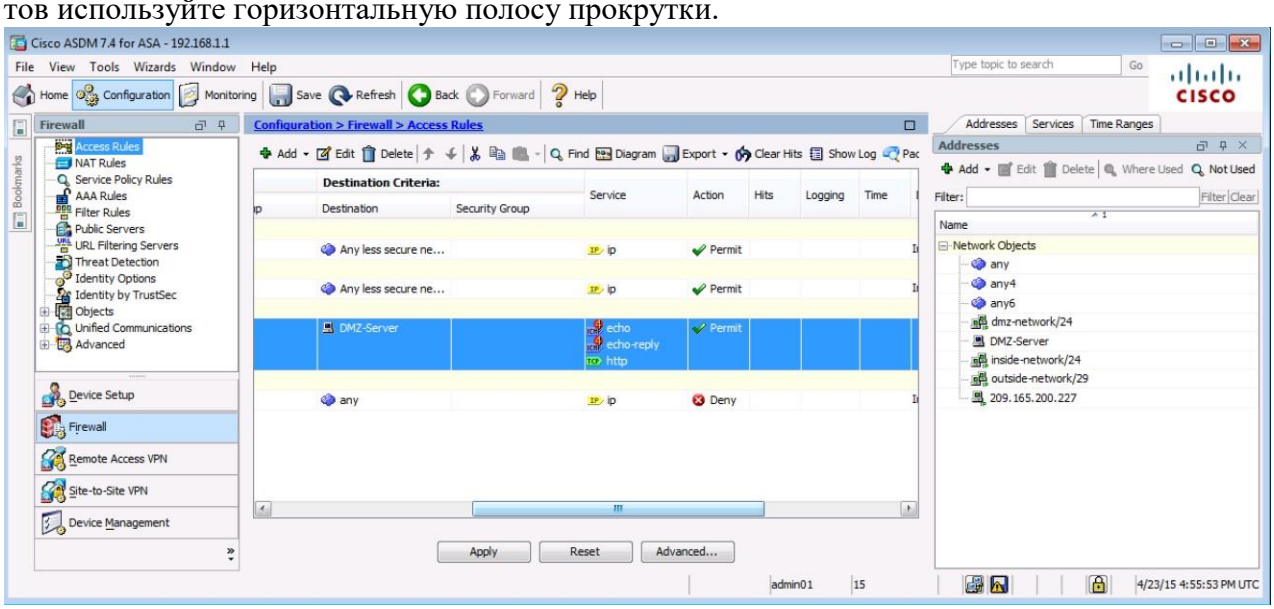
После ввода всей информации в диалоговом окне Add Public Server оно должно выглядеть примерно так, как показано ниже. Нажмите OK, чтобы добавить сервер. На экране Public Servers нажмите Apply, чтобы отправить команды на ASA.



Шаг 3: Просмотр правила доступа к DMZ, сгенерированного в ASDM.

После создания объекта «сервер DMZ» и выбора сервисов диспетчер ASDM автоматически генерирует правило доступа (ACL), разрешающее соответствующий доступ к серверу, и применяет его к внешнему интерфейсу во входящем направлении.

Чтобы увидеть это правило ACL в ASDM, выберите Configuration > Firewall > Access Rules. Оно будет показано как внешнее входящее правило. Для выбора правила и просмотра его компонентов используйте горизонтальную полосу прокрутки.



Примечание. Вы также можете посмотреть сгенерированные команды в меню Tools > Command Line Interface с помощью команды show run.

Шаг 4: Проверка доступа к серверу DMZ из внешней сети.

С компьютера PC-C отправьте эхо-запрос (ping) на IP-адрес общедоступного сервера со статическим NAT (209.165.200.227). Эхо-запрос должен быть выполнен успешно.

Так как уровень безопасности внутреннего интерфейса VLAN 1 ASA равен 100 (наивысший), а интерфейса DMZ (VLAN 3) – 70, вы также можете получить доступ к серверу DMZ с хоста из внутренней сети. ASA функционирует как маршрутизатор между двумя сетями. Отправьте эхо-запрос с хоста PC-B (192.168.1.X) внутренней сети на внутренний адрес (192.168.2.3) сервера DMZ (PC-A). Эхо-запрос должен быть выполнен успешно благодаря уровню безопасности интерфейса и тому факту, что на внутреннем интерфейсе с помощью глобальной политики выполняется инспектирование ICMP.

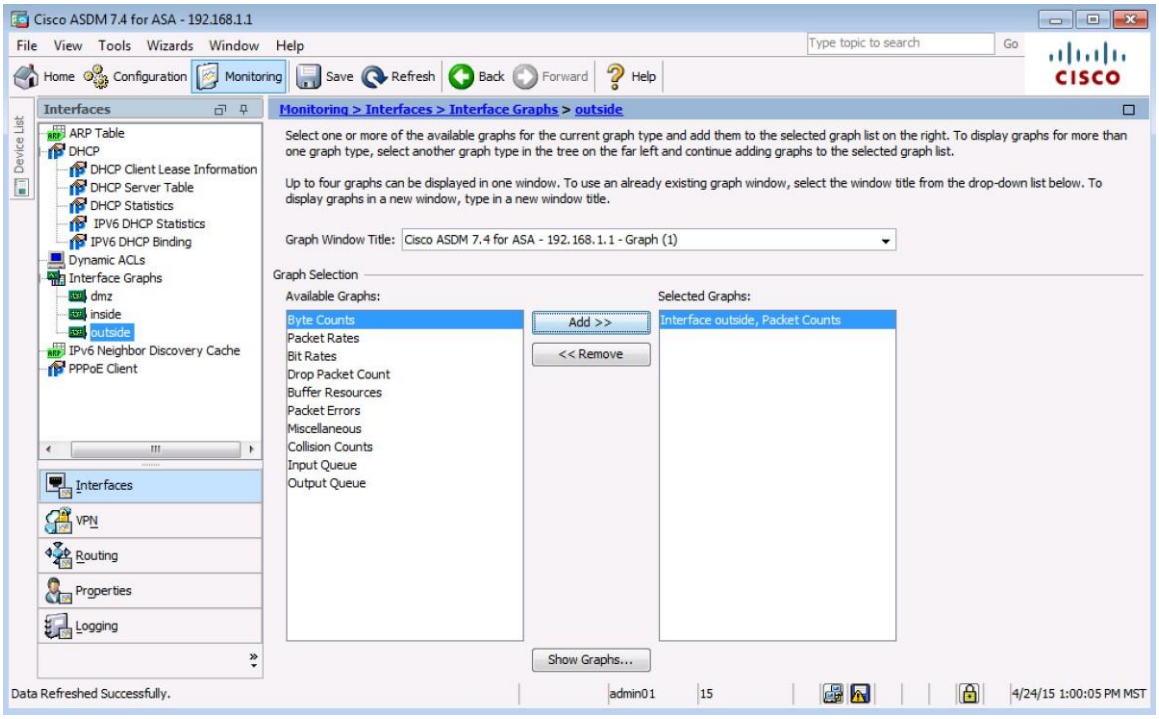
Сервер DMZ не может выполнять эхо-запрос компьютера PC-B во внутренней сети. Это объясняется тем, что интерфейс DMZ VLAN 3 имеет более низкий уровень безопасности, и тем фактом, что во время создания интерфейса VLAN 3 было необходимо задать команду no forward.

Попытайтесь отправить эхо-запрос с сервера DMZ на PC-A на компьютер PC-B по IP-адресу 192.168.1.X. Эти запросы должны завершаться ошибкой.

Шаг 5: Использование мониторинга ASDM для отслеживания активности пакетов.

С помощью экрана Monitoring можно отслеживать различные параметры ASA. Основными категориями для этого экрана являются Interfaces, VPN, Routing, Properties и Logging. На данном шаге необходимо создать график для отслеживания активности пакетов для внешнего интерфейса.

На экране Monitoring в меню Interfaces выберите Interface Graphs > outside. Выберите Packet Counts и нажмите Add, чтобы добавить график. На рисунке ниже показано, что добавлена информация о количестве пакетов (Packet Counts).



Нажмите Show Graphs, чтобы показать график. Изначально, трафик не отображается.

В командной строке в привилегированном режиме на маршрутизаторе R2 смоделируйте интернет-трафик, поступающий на ASA, путем отправки эхо-запроса на общедоступный адрес сервера DMZ с количеством повторов 1000. При необходимости количество повторов можно увеличить.

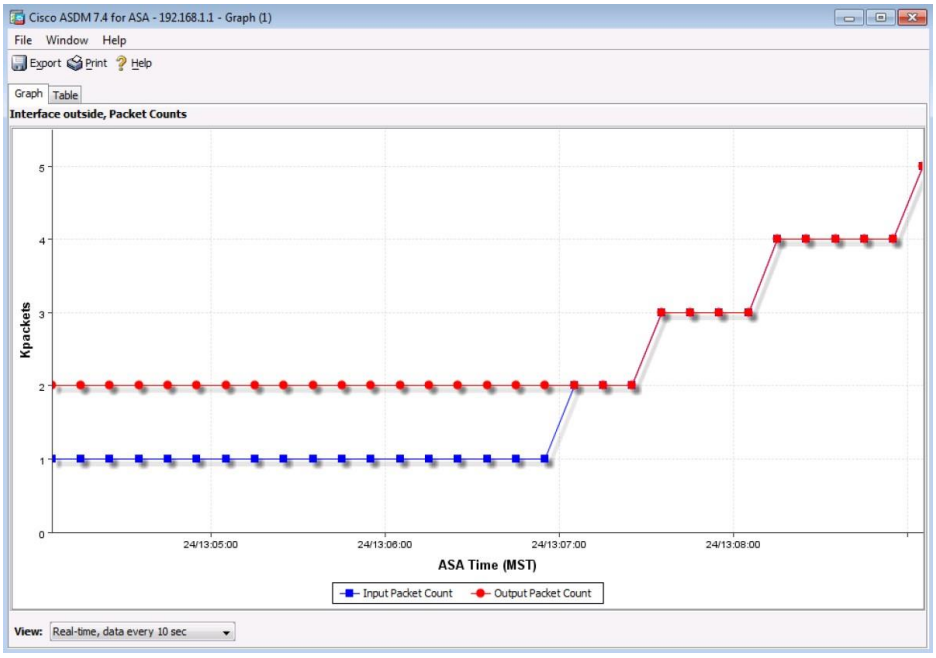
R2# ping 209.165.200.227 repeat 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
!!!
!!! <output omitted>
!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/12 ms

Вы должны увидеть результат эхо-запросов с маршрутизатора R2 на графике в виде показателя Input Packet
Count. Масштаб графика изменяется автоматически и зависит от объема трафика. Если перейти на вкладку Table, то данные также можно будет увидеть в табличном формате. Обратите внимание, что для режима представления (View) в левой нижней части экрана Graph установлено значение Real-time: данные обновляются каждые 10 секунд. Щелкните раскрывающийся список, чтобы увидеть другие доступные опции.

Отправьте эхо-запрос с компьютера PC-B на интерфейс S0/0/0 маршрутизатора R1 по адресу 10.1.1.1 с использованием параметра –n (количество пакетов) и укажите 100 пакетов.

C:>\ ping 10.1.1.1 –n 100

Примечание. Ответ от ПК будет получен не очень быстро, и изменения на графике в показателе Output Packet Count могут появиться не сразу. На графике ниже показаны дополнительные 4000 входящих пакетов, а также количество входящих и исходящих пакетов.



Практическая работа № 11

Базовая настройка шлюза безопасности ASA и фильтрация трафика с помощью Access Lists

Задание:

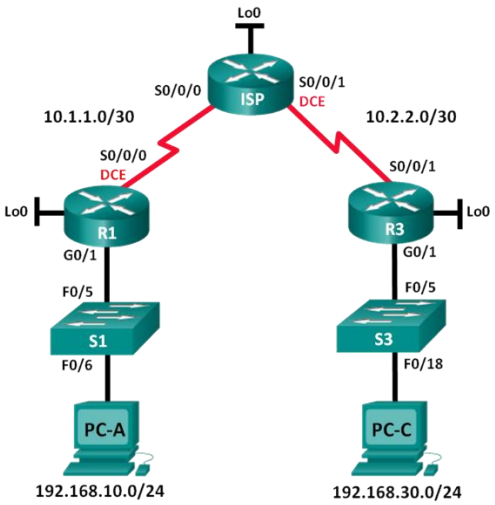


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	**G0/1**	**192.168.10.1**	**255.255.255.0**	**N/A**
	Lo0	**192.168.20.1**	**255.255.255.0**	**N/A**
	S0/0/0 (DCE)	**10.1.1.1**	**255.255.255.252**	**N/A**
ISP	**S0/0/0**	**10.1.1.2**	**255.255.255.252**	**N/A**
	S0/0/1 (DCE)	**10.2.2.2**	**255.255.255.252**	**N/A**
	Lo0	**209.165.200.225**	**255.255.255.224**	**N/A**
R3	**G0/1**	**192.168.30.1**	**255.255.255.0**	**N/A**
	Lo0	**192.168.40.1**	**255.255.255.0**	**N/A**
	S0/0/1	**10.2.2.1**	**255.255.255.252**	**N/A**
S1	**VLAN 1**	**192.168.10.11**	**255.255.255.0**	**192.168.10.1**
S3	**VLAN 1**	**192.168.30.11**	**255.255.255.0**	**192.168.30.1**
PC-A	**NIC**	**192.168.10.3**	**255.255.255.0**	**192.168.10.1**
PC-C	**NIC**	**192.168.30.3**	**255.255.255.0**	**192.168.30.1**

Часть 1. Настройка топологии и установка исходного состояния устройства

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2. Конфигурация устройств и проверка подключения

- Назначьте компьютерам статический IP-адрес.
- Настройте базовые параметры на маршрутизаторах.
- Настройте базовые параметры на коммутаторах.
- Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.
- Проверьте наличие подключения между всеми устройствами.

Часть 3. Настройка и проверка стандартных нумерованных списков ACL и стандартных именованных ACL-списков

- Настройте, примените и проверьте работу нумерованных стандартных ACL-списков.
- Настройте, примените и проверьте работу стандартных именованных ACL-списков.

Часть 4. Изменение стандартного ACL-списка

- Измените и проверьте работу стандартного именованного ACL-списка.
- Проверьте работу ACL-списка.

Исходные данные/сценарий

Обеспечение сетевой безопасности является важным аспектом при разработке и управлении IPсетями. Ценным навыком является умение применять соответствующие правила для фильтрации пакетов на основе установленной политики безопасности.

В данной лабораторной работе вы настроите правила фильтрации для двух офисов, представленных маршрутизаторами R1 и R3. Руководство определило некоторые правила в рамках политики безопасности для сетей LAN, расположенных на маршрутизаторах R1 и R3, которые вы должны реализовать. На маршрутизаторе ISP, расположенном между R1 и R3, ACL-списки не будут использоваться. У вас не будет прав административного доступа к маршрутизатору ISP, поскольку вы можете управлять только собственным оборудованием.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсе маршрутизатора в конце этой лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 3 маршрутизатора (Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universal) или аналогичная модель);
- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 2 ПК (под управлением ОС Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet и последовательные кабели в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети и при необходимости удалить все текущие настройки.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Часть 2: Настройка устройств и проверка подключения

Во второй части вам предстоит настроить базовые параметры маршрутизаторов, коммутаторов и компьютеров. Имена и адреса устройств указаны в топологии и таблице адресации.

Шаг 1: Настройте IP-адреса на PC-A и PC-C.

Шаг 2: Настройте базовые параметры маршрутизаторов.

a. Отключите поиск DNS.
b. Присвойте имена устройствам в соответствии с топологией.
c. Создайте интерфейсы loopback на каждом маршрутизаторе в соответствии с таблицей адресации.
d. Настройте IP-адреса интерфейсов в соответствии с топологией и таблицей адресации.
e. Установите пароль **class** для доступа к привилегированному режиму EXEC.
f. Установите тактовую частоту на **128000** для всех последовательных интерфейсов DCE.
g. Назначьте **cisco** в качестве пароля консоли.
h. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте доступ через Telnet.

Шаг 3: Настройка базовых параметров на коммутаторах (дополнительно). a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.
c. Назначьте административный IP-адрес интерфейса в соответствии с таблицами топологии и адресации.
d. Установите пароль **class** для доступа к привилегированному режиму EXEC.
e. Настройте шлюз по умолчанию.
f. Назначьте **cisco** в качестве пароля консоли.
g. Назначьте **cisco** в качестве пароля виртуального терминала VTY и активируйте доступ через Telnet.

Шаг 4: Настройте маршрутизацию EIGRP на маршрутизаторах R1, ISP и R3.

a. Настройте автономную систему (AS) номер 10 и объявите все сети на маршрутизаторах R1, ISP и R3. Отключите автоматическое суммирование маршрутов.
b. После настройки EIGRP на маршрутизаторах R1, ISP и R3 убедитесь, что все маршрутизаторы имеют заполненные таблицы маршрутизации с необходимыми для работы сетями. В случае необходимости выполните поиск и устранение неполадок.

Шаг 5: Проверьте наличие подключения между всеми устройствами.

Примечание. Соединение важно проверять **перед** настройкой и применением списков доступа! Удостовериться в правильной работе сети необходимо до начала фильтрации трафика.

a. От узла PC-A отправьте эхо-запрос на PC-C и интерфейс loopback маршрутизатора R3. Успешно ли выполнены эхо-запросы? _____
b. От маршрутизатора R1 отправьте эхо-запрос на PC-C и loopback-интерфейс на маршрутизаторе R3. Успешно ли выполнены эхо-запросы? _____
c. От узла PC-C отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1. Успешно ли выполнены эхо-запросы? _____
d. От маршрутизатора R3 отправьте эхо-запрос на PC-A и интерфейс loopback маршрутизатора R1.

Успешно ли выполнены эхо-запросы? _____

Часть 3: Настройка и проверка стандартных нумерованных ACLсписков и стандартных именованных ACL-списков

Шаг 1: Настройка стандартного именованного ACL-списка.

Стандартные ACL-списки фильтруют трафик, исходя только из адреса источника. Согласно принятой рекомендации стандартные ACL-списки следует настраивать и применять как можно ближе к назначению. Для первого списка доступа создайте стандартный нумерованный ACL-список, который пропускает трафик от всех узлов в сети 192.168.10.0/24 и всех узлов в сети 192.168.20.0/24 ко всем узлам в сети 192.168.30.0/24. Согласно политике безопасности в конце всех ACL-списков должна содержаться запрещающая запись контроля доступа **deny any** (ACE), которую также называют оператором ACL-списка.

Какую шаблонную маску вы будете использовать, чтобы разрешить всем узлам из сети 192.168.10.0/24 доступ к сети 192.168.30.0/24?

Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?

На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Настройте ACL-список на маршрутизаторе R3. В качестве номера списка доступа используйте 1.

R3(config)# **access-list 1 remark Allow R1 LANs Access**
R3(config)# **access-list 1 permit 192.168.10.0 0.0.0.255** R3(config)# **access-list 1 permit 192.168.20.0 0.0.0.255**
R3(config)# **access-list 1 deny any**

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

R3(config)# **interface g0/1**

R3(config-if)# **ip access-group 1 out**

c. Проверьте нумерованный ACL-список.

Использование команды **show** поможет вам при проверке синтаксиса и размещении списков ACL в вашем маршрутизаторе.

Какую команду вы будете использовать для просмотра полного списка доступа 1 со всеми записями ACE?

Какую команду вы будете использовать, чтобы просмотреть, где и в каком направлении был применён список доступа?

_ 1) На маршрутизаторе R3 выполните команду **show access-lists 1**.

R3# **show access-list 1**

Standard IP access list 1

10 permit 192.168.10.0, wildcard bits 0.0.0.255

20 permit 192.168.20.0, wildcard bits 0.0.0.255

30 deny any

2) На маршрутизаторе R3 выполните команду **show ip interface g0/1**.

R3# **show ip interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Internet address is 192.168.30.1/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.10

Outgoing access list is 1

Inbound access list is not set

Output omitted

3) Проверьте, пропускает ли ACL-список трафик из сети 192.168.10.0/24 в сеть 192.168.30.0/24. Из командной строки узла PC-A отправьте эхо-запрос на IP-адрес PC-C. Успешно ли выполнен эхо-запрос? _____

4) Проверьте, пропускает ли ACL-список трафик из сети 192.168.20.0/24 в сеть 192.168.30.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R1 в качестве источника. Отправьте эхо-запрос на IP-адрес узла PC-C. Успешно ли выполнен эхо-запрос? _____

R1# **ping**

Protocol [ip]:

Target IP address: **192.168.30.3** Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]: Extended commands [n]: **y**

Source address or interface: **192.168.20.1** Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.20.1 !!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

d. Из командной строки маршрутизатора R1 снова отправьте эхо-запрос на IP-адрес узла PC-C.
R1# **ping 192.168.3.3**
Успешно ли выполнен эхо-запрос? Поясните свой ответ.

Шаг 2: Настройте стандартный именованный ACL-список.

Создайте стандартный именованный ACL-список, который соответствует следующему правилу: список должен разрешать доступ для трафика со всех узлов из сети 192.168.40.0/24 ко всем узлам в сети 192.168.10.0/24. Кроме того, доступ в сеть 192.168.10.0/24 должен быть разрешён только для узла PCC. Этот список доступа должен быть назван BRANCH-OFFICE-POLICY.
Следуя практическим рекомендациям Cisco, на каком маршрутизаторе вы разместите ACL-список?
На каком интерфейсе вы разместите этот список? В каком направлении вы его примените?

a. Создайте стандартный ACL-список под именем BRANCH-OFFICE-POLICY на маршрутизаторе R1.

R1(config)# **ip access-list standard BRANCH-OFFICE-POLICY**
R1(config-std-nacl)# **permit host 192.168.30.3**
R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**
R1(config-std-nacl)# **end**
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
Взгляните на первую запись ACE в списке доступа и ответьте, можно ли записать это иначе?

b. Примените ACL-список к подходящему интерфейсу в нужном направлении.

R1# **config t**
R1(config)# **interface g0/1**
R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

c. Проверьте именованный ACL-список.

1) На R1 выполните команду **show access-lists.**

R1# **show access-lists**
Standard IP access list BRANCH-OFFICE-POLICY
  10 permit 192.168.30.3
  20 permit 192.168.40.0, wildcard bits 0.0.0.255
Существуют ли различия между ACL-списком на маршрутизаторе R1 и ACL-списком на маршрутизаторе R3? Если да, в чём они заключаются?
На маршрутизаторе R1 выполните команду **show ip interface g0/1**.
R1# **show ip interface g0/1**
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.10.1/24
 Broadcast address is 255.255.255.255
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is BRANCH-OFFICE-POLICY
 Inbound access list is not set
<Output omitted>

3) Проверьте работу ACL-списка. Из командной строки узла PC-C отправьте эхо-запрос на IPадрес узла PC-A. Успешно ли выполнен эхо-запрос? _____
4) Проверьте ACL-список, чтобы удостовериться, что доступ к сети 192.168.10.0/24 настроен только на узле PC-C. Вам нужно выполнить расширенный эхо-запрос и ис-

пользовать адрес G0/1 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос? _____

5) Проверьте, пропускает ли ACL-список трафик из сети 192.168.40.0/24 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на маршрутизаторе R3 в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос? _____

Часть 4: Изменение стандартного ACL-списка

Политика безопасности нередко претерпевает изменения. По этой причине ACL-списки тоже необходимо изменять. В четвёртой части вам предстоит изменить один из ранее настроенных вами ACL-списков для соответствия новой политике безопасности.

Руководство решило, что пользователи из сети 209.165.200.224/27 должны получить полный доступ к сети 192.168.10.0/24. Также руководство хочет, чтобы правила в ACL-списках на всех их маршрутизаторах выполнялись последовательно. В конце всех ACL-списков должна быть внесена запись ACE **deny any**. Вам необходимо изменить ACL-список с именем BRANCH-OFFICE-POLICY.

Также вам предстоит добавить в этот список ACL две дополнительные строки. Это можно сделать двумя способами:

Вариант 1: Выполните команду **no access-list standard BRANCH-OFFICE-POLICY** в режиме глобальной конфигурации. Это исключит весь ACL-список из маршрутизатора. В зависимости от IOS маршрутизатора, произойдет один из следующих вариантов: вся фильтрация пакетов будет отменена, и все пакеты будут пропускаться через маршрутизатор; либо, поскольку команда **ip access-group** в интерфейс G0/1 активна, фильтрация останется прежней. В любом случае, когда ACL-список будет удалён, вы сможете заново ввести весь ACL-список или вырезать и вставить записи из текстового редактора.

Вариант 2: ACL-списки можно изменить, не удаляя, добавив или удалив конкретные строки из ACLсписка. Этот вариант наиболее удобен, особенно в случае если ACL-список содержит много записей.

При повторном вводе всего ACL-списка или при вырезании и копировании могут возникнуть ошибки. В изменении определённых строк в списках ACL нет ничего сложного.

Примечание. В ходе данной лабораторной работы используйте вариант 2.

Шаг 1: Изменение стандартного именованного ACL-списка.

a. В привилегированном режиме маршрутизатора R1 выполните команду **show access-lists**.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
   10 permit 192.168.30.3 (8 matches)
   20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

b. Добавьте две дополнительные строки в конец ACL-списка. В режиме глобальной конфигурации измените ACL-список с именем BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. Проверьте ACL-список.

1) На R1 выполните команду **show access-lists.**

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
   10 permit 192.168.30.3 (8 matches)
   20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

30 permit 209.165.200.224, wildcard bits 0.0.0.31
40 deny any

Нужно ли вам применить список под именем BRANCH-OFFICE-POLICY на интерфейсе G0/1 маршрутизатора R1?

Из командной строки ISP выполните расширенный эхо-запрос. Проверьте, пропускает ли список ACL трафик из сети 209.165.200.224/27 в сеть 192.168.10.0/24. Вам нужно выполнить расширенный эхо-запрос и использовать loopback-адрес 0 на ISP в качестве источника. Отправьте эхо-запрос на IP-адрес компьютера PC-A. Успешно ли выполнен эхо-запрос?

Практическая работа № 12
Маршрутизация в шлюзе безопасности ASA

Задание:

Настроить Learning Routes

Существует несколько способов для Learning Routes:

Directly connected networks - это сети, прописанные непосредственно на интерфейсах ASA. Такие маршруты добавляются в Routing Table автоматически.

Static routes - маршруты, прописанные вручную.

Dynamic Routing protocols - Автоматичекое распространие информации по маршрутизации. ASA поддерживает RIP, EIGRP, OSPF

Static routes

Как уже было сказано, статические маршруты прописываются вручную, - поэтому такие маршруты остаются на месте даже

если есть назначения уже отсутствует, т.е. такие маршруты статичны.

Default Gateway - пример статического маршрута.

```
route outside 0.0.0.0 0.0.0.0 62.105.149.225 1
```

Здесь 1 - Administrative Distance для данного маршрута.

Еще пример статического маршрута

```
route inside 192.168.22.0 255.255.255.0 192.168.1.1
```

Проверка:

```
show route
```

OSPF

```
router ospf 10
 network 192.168.2.0 255.255.255.0 area 0
 network 192.168.253.0 255.255.255.0 area 0
 log-adj-changes
```

Все настройки такие же как на роутере, за исключением того что в ASA нигде не используются Wildcard Masks

EIGRP

```
router eigrp 1
 network 192.168.1.0 255.255.255.0
 network 192.168.2.0 255.255.255.0
```

Проверка

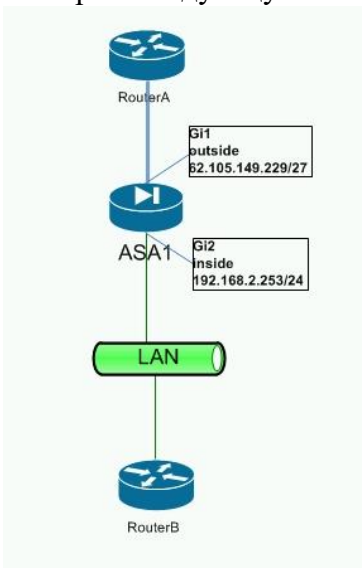
```
show running-config router
```

Практическая работа № 13
TCP Advanced Options в шлюзе безопасности ASA

ASA, как устройство для обеспечения безопасности, по умолчанию может выполнять некоторые хитрые манипуляции с TCP, которые могут оказаться вредными для нашей сети.
Мы рассмотрим некоторые подобные случаи и методы их обхода.

BGP и ASA

Рассмотрим следующую схему.



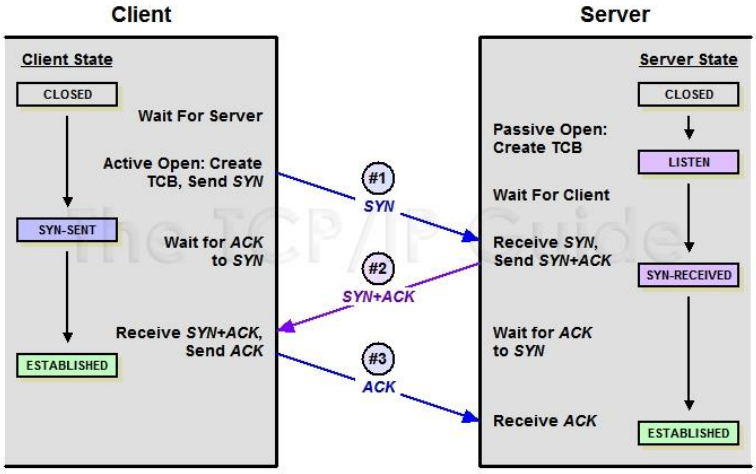
На двух роутерах поднят BGP. Проблема возникнет если BGP использует Authentication.
На ASA функционирует модуль, который называется **Normalizer** - он анализирует проходящий трафик и может менять TCP пакеты и их заголовки по своему усмотрению.
Дело в том, что BGP для Аутентификации использует *Option 19*, а Normalizer её удаляет.
Также мы отключим ISN Randomizing.
Для выполнения данной задачи мы также будем использовать политики + **TCP Map**.
TCP Map - собственно задаёт поведение ASA при обработке пакетов TCP.

```
tcp-map OPTION-19
 tcp-options range 19 19 allow
class-map BGP
 match port tcp eq bgp
policy-map global_policy
 class BGP
  set connection advanced-options OPTION-19
  set connection conn-max 0 embryonic-conn-max 0 per-client-max 0 per-client-embryonic-conn-max 0 random-sequence-null
```

TCP State Bypass и Asymmetric Routing

Рассмотрим как происходит инициализация соединения TCP:

1. Инициатор отправляет **SYN** на Destionation IP адрес
2. Ответ **Syn + Ack**
3. Инициатор шлёт **Ack**



Проблема может возникнуть, если по каким либо причинам запросы и ответы идут разными путями (asymmetric routing), и ASA видит только часть этого "разговора". В этом случае ASA (а точнее Normalizer) не будет пропускать такое соединение, посчитав его "неправильным".
Для решения данной ситуации мы будем использовать **TCP State Bypass**.

```
tcp-map all-traffic
 match any
policy-map global_policy
 class all-traffic
  set connection advanced-options tcp-state-bypass
```

TCP intercept (syn-flood)

Syn-Flood Attack - это атака при которой инициатор в пакете SYN ставит подложный *Source IP address* либо игнорирует ответы от сервера Syn + Ack. При открытии тысяч таких половинчатых сессий тратятся ресурсы сервера, который вынужден запоминать параметры каждой и в итоге может отказать.
Для решения данной проблемы ASA использует TCP SYN Cookies: ASA защищает сервер и не транслирует на него все соединения. Вместо того чтобы запоминать все эти половинчатые сессии, ASA тупо отвечает на каждую из них, но фактическое соединение с сервером осуществляет только при получении 3-го ответа **Ack**.

```
access-list outside_mpc line 1 extended permit tcp any object dmz-server real
class-map no-syn-flood-class
 match access-list outside_mpc
policy-map NO-SYN-FLOOD
 class no-syn-flood-class
  set connection conn-max 0 embryonic-conn-max 5 per-client-max 0 per-client-embryonic-conn-max 0 random-sequence-number enable
service-policy NO-SYN-FLOOD interface outside
```

Здесь **embryonic-conn-max 5** означает, что максимум будет разрешени до 5 половинчатых соединений.

Практическая работа № 14
Анализи внутрипротокольного трафика шлюза безопасности ASA

Теоритические основы:
DENIED — пакеты NetFlow, в которых говорится о том, какой трафик был заблокирован, количество трафика всегда будет равно нулю во входящем или исходящем поле, поэтому данный тип мы будем игнорировать;

CREATED, UPDATED — пакеты NetFlow, в которых указывается инициализация (**CREATED**), и периодическое обновление трафика после инициализации (**UPDATED**), данные типы также не будут учитываться нами для учета трафика (объяснение ниже);

DELETED (Torn Down) — пакеты NetFlow, в которых указана полная информация о трафике, который был завершен, сумма входящего и исходящего трафика «всегда» должна удовлетворять следующей формуле **CREATED + UPDATED = DELETED**, этот тип мы и будем учитывать.

Для того, чтобы не было "**удвоения**" трафика, необходимо использовать либо **CREATED + UPDATED** пакеты, либо только **DELETED**. Если использовать и то и другое, то ваш реальный трафик будет отображаться как реальный трафик умноженный на два! В идеале нужно учитывать трафик **CREATED + UPDATED**, так как эти 2 типа дают более точное представление о том, насколько загружен ваш Интернет в текущий момент времени. **DELETED** — это та информация о трафике, в которой сессия прекратила свое существование, и например, если кто-то в компании поставит загрузку очень большого файла с утра и закончит скачивать его только вечером, то данные о большом трафике отобразятся **ТОЛЬКО** вечером!

Увы, но пришлось вести учет трафика по типу **DELETED**, так как имеется баг в связке **Cisco NetFlow + nfcapd (nfdump) + UPDATED**. Баг заключается в том, что с определенной частотой при парсинге **nfdump** в пакетах **UPDATED**, встречается трафик размером **4,3 GB**. Мне не удалось выяснить чем вызван этот баг, или реализацией самим оборудованием **Cisco**, где в пакете содержится какая-то «хитрая» информация, которую не может обработать **nfdump**, либо баг в самой реализации **nfcapd + nfdump**. В пакетах **DELETED** такого бага не было замечено за пару месяцев работы оборудования.
Как вести учет по NetFlow, включая VPN трафик

Понятно, что мы хотим считать и учитывать только "**реальный**" трафик, который поступает **ТОЛЬКО** от провайдера. И мы не хотим, чтобы к этому трафику добавлялся локальный трафик, например трафик между **LAN** и **DMZ**, или трафик между всеми "**white**" хостами вашей подсети (подсеть IP адресов, выделенная вашим провайдером). Здесь все просто, считаем только такой трафик из NetFlow пакета, где наш какой-либо локальный хост идет куда-либо в Интернет и фильтруем трафик, который идет либо в **DMZ**, либо на какой-либо ваш "**white**" IP адрес, либо любую **VPN** подсеть (почему игнорируем **VPN** подсети описано ниже).

Вся загвоздка заключается с учетом **реального** трафика, где используется любой тип **VPN**. Например такие маршруты **VPN** трафика: **LAN(DMZ)-to-VPN, VPN-to-LAN(DMZ), VPN-to-VPN, VPN-to-INTERNET**. Так вот, после долого анализа файлов, с использованием утилиты **nfdump**, мной были сделаны следующие выводы о том, как учитывать трафик с такими маршрутами. Если вы хотите узнать, сколько потребляется **VPN** трафика вашими сотрудниками, например **LAN(DMZ)-to-VPN, VPN-to-VPN**, то вы просто должны учесть это трафик как есть, то есть просто посчитать количество трафика, которое идет из вашей локальной подсети или

DMZ на **VPN** подсети, или **VPN-to-VPN** (это количество будет почти точно отображать количество потребляемого **VPN** трафика). Полученное количество **VPN** трафика нельзя использовать для "**реального**" учета трафика, так как "**реальный**" трафик будет отображен между белыми IP адресами, например между вашим IP офиса и IP удаленного клиента, или между белыми IP 2ух офисов. Во-первых, такое количество будет полностью отображать количество **VPN** трафика между белыми хостами, а во-вторых, это количество будет значительно выше количества трафика **ANY-to-VPN**, так как в этом количестве будет учитываться такой трафик как **VPN-to-INTERNET**, а также дополнительный системный трафик.

Таким образом учет трафика необходимо делать по вашим **WAN** подсетям наравне с **LAN**. Делаем 2 подсчета трафика: **WAN-to-!(LAN, DMZ, VPN, YOUR WAN)** и **!(LAN, DMZ, VPN, YOUR WAN)-to-WAN**. Так мы точно учтем весь "**реальный**" трафик, а также тот трафик, который инициализируется на самих **Cisco ASA**, либо приходит из вне. Учет трафика **VPN-to-INTERNET** учитывается точно также, как и **LAN(DMZ)-to-INTERNET**.

Итоговая формула подсчета **реального** трафика по NetFlow: **(LOCAL-to-INTERNET) + (INTERNET-to-LOCAL)**

LOCAL — это все подсети типа **WAN, LAN, DMZ, VPN**;
INTERNET — весь остальной трафик, который не относится к **WAN, LAN, DMZ, VPN**.

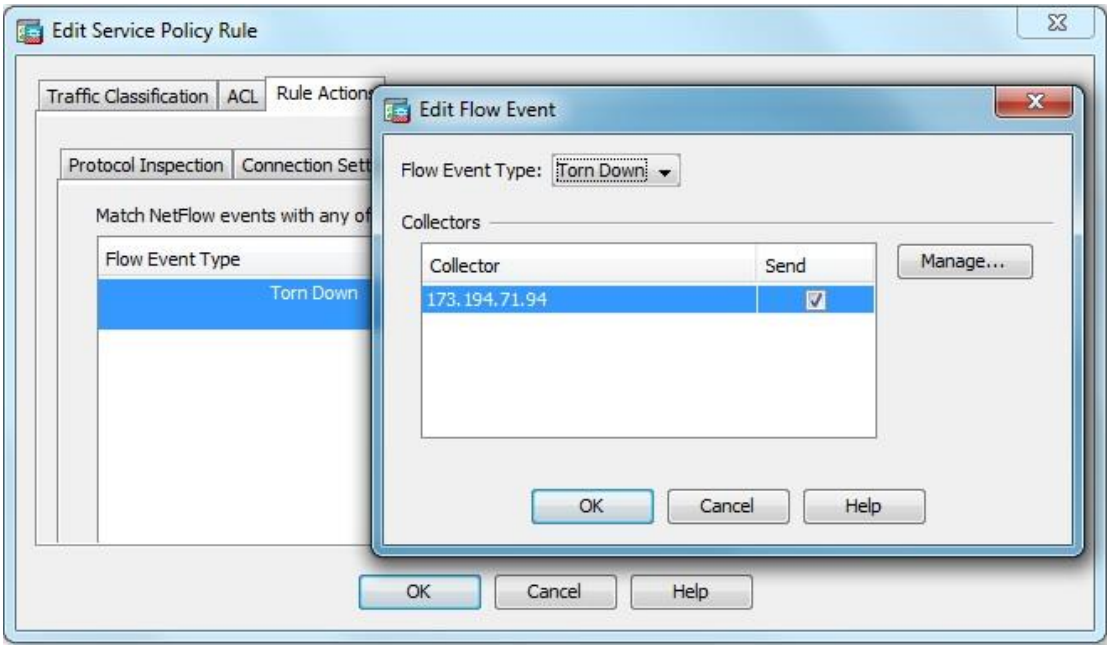
На практике при подсчете трафика типа "**INTERNET-to-LOCAL**" у вас будет считаться только трафик типа "**INTERNET-to-WAN**", так как других NetFlow данных у вас не будет, например не будет данных по типу "**INTERNET-to-(LAN, DMZ, VPN)**".

Итоговая формула подсчета **VPN** трафика по NetFlow: **LOCAL-to-VPN**

LOCAL — это все подсети типа **WAN, LAN, DMZ, VPN**

Этот **VPN** трафик **НЕЛЬЗЯ** суммировать с реальным трафиком, так как он уже включает в себя полную статистику по всем **VPN** сессиям между "**VPN_REMOTE_HOST-to-WAN**", "**WAN-to-VPN_REMOTE_HOST**". Данный трафик отображает только примерное количество трафика, которое идет по **VPN** сессиям.
От теории к практики или делаем подготовку сенсора и коллектора

Задание:
1. Установить:
Cisco ASA — **ASDM 7.1.6**, **ASA 9.1.5**
(http://software.cisco.com/download/type.html?mdfid=279513399)
Коллектор (PC Core2Duo, **2GB RAM**, 160GB HDD) — **Debian 7.4**, **MySQL 5.5.35**, **Apache 2.2.22**, **PHP 5.4.4-14**
nfdump 1.6.12 (http://sourceforge.net/projects/nfdump/files/stable/)
Мы условились, что учитывать будем только пакеты NetFlow с типом **DELETED**. Поэтому в **ASDM** выставим отправку только этого типа пакетов.



Теперь нам надо подготовить коллектор. Все что нам нужно, это скачать исходники и скомпилировать их с поддержкой **NSEL**:

- 1) ./configure --enable-nsel
- 2) make
- 3) make install

2 Подготовка MySQL базы под NetFlow на коллекторе:

- 1) Создадим базу: CREATE DATABASE NetFlow CHARACTER SET utf8 COLLATE utf8_general_ci;
- 2) Добавим пользователя netflow: GRANT ALL PRIVILEGES ON NetFlow.* TO 'netflow'@'%' IDENTIFIED BY 'nfpass' WITH GRANT OPTION;
- 3) Сбрасываем привелегии: FLUSH PRIVILEGES;
- 4) Импорт чистой базы: mysql -u**root** -p**root_pass** NetFlow < /var/www/netflow/setup/netflow.sql (где **root_pass**, пароль от вашего сервера **MySQL**).

3 Оптимизация MySQL:

В нашем случае понадобится изменение настроек по умолчанию, так как база будет использовать больше ресурсов, чем прописано в дефолтном конфиге **MySQL**. Например, только один запрос по **INSERT** может быть несколько мегабайт. Основная задача — это добиться того, чтобы все запросы **INSERT** проходили, и при этом не терялись данные, как у меня было в самом начале исследования. А также оптимизировать работу запросов **SELECT**, чтобы база отдавала данные в приемлемое время. У меня не получилось оптимизировать базу под **InnoDB**, поэтому использую **MyISAM**.

Напомню, что у меня на коллекторе установлено **2GB RAM**, поэтому в вашем случае параметры могут отличаться как в большую, так и в меньшую сторону. Приведу свои настройки, которые мне помогли оптимизировать **MySQL**:

skip-innodb
default-storage-engine = MyISAM
sort_buffer_size = 4M
myisam_sort_buffer_size = 256M
key_buffer = 256M

max_allowed_packet = 32M
read_rnd_buffer_size = 2M
thread_stack = 2M
thread_cache_size = 16
query_cache_limit = 32M
query_cache_size = 128M
Перегружаем **MySQL**: /etc/init.d/mysql restart
Если у вас возникнут проблемы с оптимизацией, воспользуйтесь **perl**-скриптом с сайта http://mysqltuner.com/
Все подробности использования и оптимизации написаны на сайте, а также при выполнении скрипта.

4 Определяем свои подсети в базе:

Откройте ваш браузер и перейдите по ссылке **/netflow/networks**
Опишите все ваши локальные подсети по типу **LAN, DMZ, WAN, VPN**
Далее укажите те подсети, которые относятся к **VPN**, например подсети удаленного офиса или подсети удаленных клиентов.

5 Запускаем наш коллектор:

Перед запуском проверте, что у вас установлен плагин **php5-mysql** или **php5-mysqlnd**
/usr/local/bin/nfcapd -t 600 -w -p 9995 -l /netflow/nflogs -D -x '/usr/bin/php5 /var/www/netflow/scripts/netflow.php %d/%f'
"/netflow/nflogs" — это путь к логам;
"/usr/bin/php5 /var/www/netflow/scripts/netflow.php %d/%f" — это запуск **php**-скрипта, после того как файл с логами будет создан.
Этот скрипт "**сердце**" учета трафика, который собирает статистику каждые 10 минут, обрабатывает ее и кладет в базу данные о трафике, а также чистит устаревшие данные. Скрипт оптимизирован под временной интервал сбора статистики каждые 10 минут, поэтому не меняйте параметр "**-t 600**".
Если все сделано правильно, то на ваш коллектор будут приходить NetFlow пакеты. Посмотреть можно командой: "**tcpdump port 9995**". Если пакеты приходят от вашего оборудования на порт, значит все хорошо, иначе вы неправильно настроили свою циску.

Практическая работа № 15
Работа с логическими интерфейсами шлюза безопасности ASA

Задание:

Выполнить настройку логических интерфейсов

1 VLANs and Subinterfaces

Хорошей практикой является разделение внутренней сети на несколько Security Zones, или Layer 3 subnets, которые контролируются и защищаются с помощью ASA. Для контроля security zones для каждой зоны нужен отдельный физический или логический интерфейс.
Также каждая Security Zone живёт в своём VLAN.
Cisco ASA поддерживает создание транка с использованием протокола **802.1q** или Subinterfaces.

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# no nameif
ciscoasa(config-if)# no security-level
ciscoasa(config-if)# no ip address
ciscoasa(config-if)# exit
!
ciscoasa(config)# interface gigabitethernet 0/1.1
```

ciscoasa(config-subif)# vlan 10
ciscoasa(config-subif)# nameif inside1
ciscoasa(config-subif)# security-level 80
ciscoasa(config-subif)# ip address 192.168.1.1 255.255.255.0
!
ciscoasa(config)# interface gigabitethernet 0/1.2
ciscoasa(config-subif)# vlan 20
ciscoasa(config-subif)# nameif inside2
ciscoasa(config-subif)# security-level 90
ciscoasa(config-subif)# ip address 192.168.2.1 255.255.255.0
Etherchannel
2 Etherchannel - это технология, которая позволяет объединить несколько физических интерфейсов в один логический, тем самым увеличивая пропускную способность.
Cisco ASA поддерживает протокол LACP.
interace gigabitethernet2
channel-group 1 mode Active
!
interace gigabitethernet3
channel-group 1 mode Active
!
interface port-channel1
prot-channel load-balance src-port
port-channel min-bundle 1
lacp max-bundle 1
no shutdown
speed auto
duplex auto
nameif dmz
security-level 50
ip address 172.16.0.1 255.255.255.0

Практическая работа № 16
Монитор вторжений Threat Detection шлюза безопасности ASA

Задание:
1 Настройка Basic Threat Detection
Basic Threat Detection включена по умолчанию.
Вручную включить можно командой:
threat-detection basic-threat
Либо через ASDM: **Configuration>Firewall>Threat Detection**
Просмотр статистики:
show threat-detection rate

	Average(eps)	Current(eps)	Trigger	Total events
10-min ACL drop:	**2**	**0**	**0**	**1334**
1-hour ACL drop:	**0**	**2**	**0**	**2017**
10-min SYN attck:	**0**	**0**	**0**	**267**
1-hour SYN attck:	**0**	**0**	**0**	**699**
10-min Scanning:	**3**	**1**	**4**	**1926**
1-hour Scanning:	**1**	**3**	**0**	**3726**

10-min Bad pkts:	**0**	**0**	**0**	**18**
1-hour Bad pkts:	**0**	**0**	**0**	**65**
10-min Firewall:	**2**	**1**	**0**	**1659**
1-hour Firewall:	**0**	**2**	**0**	**3027**
10-min DoS attck:	**0**	**0**	**0**	**307**
1-hour DoS attck:	**0**	**0**	**0**	**945**
10-min Interface:	**2**	**0**	**0**	**1720**
1-hour Interface:	**1**	**1**	**0**	**3671**

Здесь нас больше всего интересует столбец **Trigger**: в данном примере было обнаружено 4 атаки типа Scanning.

Посмотреть установки Basic Threat Detection events:

show running-config all threat-detection

Установки можно поменять.

Advanced Threat Detection

Advanced threat detection - это также лишь статистика, но более подробная.

Advanced Threat Detection позволяет определить traffic rates для hosts, ports, protocols, ACLs.

Advanced threat detection может перегрузить ресурсы системы!!!

Включение:

threat-detection statistics port number-of-rate 1 - статистика по TCP/UDP портам

threat-detection statistics protocol number-of-rate 1 - статистика по протоколам IP, non-TCP/UDP.

threat-detection statistics host number-of-rate 1 - статистика по хостам.

threat-detection statistics access-list - статистика по ACL

threat-detection statistics tcp-intercept

hpm topN enable

Здесь *number-of-rate* означает количество отслеживаемых rate intervals. Доступно 1-3 и чем больше, тем больше необходимо ресурсов.

1-отслеживается за 1 hour.

2-отслеживается за 1 hour, 8 hours.

3-отслеживается за 1 hour, 8 hours, and 24 hours.

threat-detection statistics port number-of-rate 1

threat-detection statistics protocol number-of-rate 1

threat-detection statistics host number-of-rate 1

threat-detection statistics access-list

threat-detection statistics tcp-intercept

hpm topN enable

Scanning Threat Detection

Scanning Threat Detection способна также и блокировать attacker.

Scanning Threat Detection может перегрузить ресурсы системы!!!

Конфигурация:

threat-detection scanning-threat shun

threat-detection scanning-threat shun duration 3600

threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.0

Проверка:

show threat-detection shun

show threat-detection scanning-threat

Поведение в реальных ситуациях

В случае подозрения что у нас какие-то проблемы, первое что следует сделать - открыть ASDM, и посмотреть Firewall Dashboard.

Ниже приведён пример реакции ASA на сканирование извне через nmap. Поскольку при сканировании перебираются порты, мы получим массу ACL Dropped и Possble Scans.

Далее смотрим логи:

May 05 2017 10:41:03: %ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 4 per second, max configured rate is 10; Current average rate is 12 per second, max configured rate is 5; Cumulative total count is 7530

May 05 2017 10:41:03: %ASA-4-733100: [Scanning] drop rate-2 exceeded. Current burst rate is 0 per second, max configured rate is 8; Current average rate is 5 per second, max configured rate is 4; Cumulative total count is 18327

May 05 2017 10:41:23: %ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 4 per second, max configured rate is 10; Current average rate is 12 per second, max configured rate is 5; Cumulative total count is 7517

Как видно, в логах валятся ругань на threat category [Scanning].

Соответственно мы увидим что будут расти счётчики Scanning:

show threat-detection rate

msk-asa-01# show threat-detection rate

	Average(eps)	Current(eps)	Trigger	Total events
10-min ACL drop:	9	8	0	5709
1-hour ACL drop:	4	8	0	17583
10-min SYN attck:	0	0	0	200

1-hour SYN attck: 0 0 0 1458
10-min Scanning: 10 9 599 6164
1-hour Scanning: 5 9 559 20978
10-min Bad pkts: 0 0 0 19
1-hour Bad pkts: 0 0 0 176
10-min Firewall: 9 9 0 5964
1-hour Firewall: 5 8 0 19520
10-min DoS attck: 0 0 0 236
1-hour DoS attck: 0 0 0 1761
10-min Interface: 12 27 0 7684
1-hour Interface: 5 8 0 20677

Трафик массово дропается, посмотрим причины:

show asp drop

msk-asa-01# show asp drop

Frame drop:
No valid adjacency (no-adjacency) 208
No route to host (no-route) 248
Flow is denied by configured rule (acl-drop) 146493
First TCP packet not SYN (tcp-not-syn) 5668
TCP Dual open denied (tcp-dual-open) 30
TCP data send after FIN (tcp-data-past-fin) 8
TCP failed 3 way handshake (tcp-3whs-failed) 2374
TCP RST/FIN out of order (tcp-rstfin-ooo) 8020
TCP packet SEQ past window (tcp-seq-past-win) 671
TCP Out-of-Order packet buffer full (tcp-buffer-full) 3
TCP Out-of-Order packet buffer timeout (tcp-buffer-timeout) 700
TCP RST/SYN in window (tcp-rst-syn-in-win) 7
TCP dup of packet in Out-of-Order queue (tcp-dup-in-queue) 9
TCP packet failed PAWS test (tcp-paws-fail) 37
Slowpath security checks failed (sp-security-failed) 86550
ICMP Inspect bad icmp code (inspect-icmp-bad-code) 72
ICMP Inspect seq num not matched (inspect-icmp-seq-num-not-matched) 2
FP L2 rule drop (l2_acl) 38192
Interface is down (interface-down) 5
Dropped pending packets in a closed socket (np-socket-closed) 575
Connection to PAT address without pre-existing xlate (nat-no-xlate-to-pat-pool) 29377

Last clearing: Never

Flow drop:
Inspection failure (inspect-fail) 896

Last clearing: Never

Повторяем эту команду несколько раз и получим, что увеличивается счетчик

Flow is denied by configured rule (acl-drop)

Ну и наконец вычисляем кто именно нас атакует:

capture drop type asp-drop real-time

msk-asa-01# capture drop type asp-drop real-time

Warning: using this option with a slow console connection may
result in an excessive amount of non-displayed packets
due to performance limitations.

Use ctrl-c to terminate real-time capture

1: 10:54:16.344876 192.168.2.49.137 > 192.168.2.255.137: udp 50
2: 10:54:16.369655 195.112.100.134.40584 > 46.28.95.136.10778: S 2228624278:2228624278(0) win 1024
3: 10:54:16.370220 195.112.100.134.40584 > 46.28.95.136.16113: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
4: 10:54:16.371288 195.112.100.134.40584 > 46.28.95.136.7025: S 2228624278:2228624278(0) win 1024
5: 10:54:16.371410 195.112.100.134.40584 > 46.28.95.136.6779: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
6: 10:54:16.372310 195.112.100.134.40584 > 46.28.95.136.1198: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
7: 10:54:16.373271 195.112.100.134.40584 > 46.28.95.136.31337: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
8: 10:54:16.373378 195.112.100.134.40584 > 46.28.95.136.2170: S 2228624278:2228624278(0) win 1024
9: 10:54:16.374004 195.112.100.134.40584 > 46.28.95.136.9485: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
10: 10:54:16.375102 195.112.100.134.40584 > 46.28.95.136.45100: S 2228624278:2228624278(0) win 1024 Drop-reason: (acl-drop) Flow is denied by configured rule
Это будет сразу видно по большому количеству дропов трафика от одного источника, т.е. от 195.112.100.134.

Практическая работа № 17
Перенаправления трафика из шлюза безопасности ASA в Firepower

Модуль Cisco ASA FirePOWER, который также называется ASA SFR, предоставляет сервисы межсетевого экрана следующего поколения, среди которых:

- Система предотвращения вторжений следующего поколения (NGIPS)
- Мониторинг и контроль работы приложений (AVC)
- Фильтрация по URL-адресам
- Защита от сложного вредоносного ПО (AMP)

Примечание. Модуль ASA SFR можно использовать в режиме Single Context или Multiple Context, а также в режиме Routed или Transparent.

Задание:

1 Установка модуля SFR на устройство ASA

Выполните следующие действия для установки модуля SFR на устройство ASA:

1. Загрузите системное программное обеспечение ASA SFR с веб-сайта Cisco.com на сервер HTTP, HTTPS или FTP, который доступен из интерфейса управления ASA SFR.

2. Переместите загрузочный образ на устройство. Сделать это можно с помощью диспетчера устройств Cisco Adaptive Security Device Manager (ASDM) или интерфейса командной строки ASA. Примечание. Не передавайте системное программное обеспечение; оно будет загружено позже на твердотельный накопитель (SSD).Для того чтобы переместить загрузочный образ с помощью ASDM, выполните следующие действия: Переместите загрузочный образ на рабочую станцию или разместите его на сервере FTP, TFTP, HTTP, HTTPS, Server Message Block (SMB) или Secure Copy (SCP).В ASDM выберите Tools > File Management (Сервис > Управление

файлами).Выберите соответствующую команду для передачи файла: Between Local PC and Flash (Между локальным ПК и флеш-памятью) или Between Remote Server and Flash (Между удаленным сервером и флеш-памятью).Переместите загрузочное программное обеспечение на флеш-диск (disk0) устройства ASA.Для того чтобы переместить загрузочный образ с помощью интерфейса командной строки устройства ASA, выполните следующие действия:Переместите загрузочный образ на сервер FTP, TFTP, HTTP или HTTPS.Введите команду copy в интерфейсе командной строки, чтобы передать загрузочный образ на флеш-диск. Вот пример, в котором используется протокол HTTP (замените <HTTP_Server> IP-адресом или именем хоста своего сервера):

ciscoasa# **copy http://<*HTTP_SERVER*>/asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500xboot-5.3.1-152.img**

3. Для того чтобы настроить местоположение загрузочного образа ASA SFR на флешдиске устройства ASA, введите следующую команду: ciscoasa# **sw-module module sfr recover configure image disk0:/*file_path*** Например:

ciscoasa# **sw-module module sfr recover configure image disk0:**
/asasfr-5500x-boot-5.3.1-152.img

4. Для того чтобы загрузить загрузочный образ ASA SFR, введите следующую команду: ciscoasa# **sw-module module sfr recover boot**

В ходе выполнения этой команды, если на устройстве ASA включить debug moduleboot, отображаются следующие сообщения отладки: ciscoasa# **sw-module module sfr recover boot**

5. Дождитесь загрузки модуля ASA SFR (приблизительно 5–15 минут), а затем откройте сеанс консоли для рабочего загрузочного образа ASA SFR.

2 Установка загрузочного образа ASA SFR

Для того чтобы настроить установленный загрузочный образ ASA SFR, выполните следующие действия:

1. После открытия сеанса нажмите Enter, чтобы появилось приглашение входа в систему. Примечание. Имя пользователя по умолчанию — admin, пароль по умолчанию — Admin123.Например:

ciscoasa# **session sfr console** Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Cisco ASA SFR Boot Image 5.3.1 asasfr login: admin Password: Admin123

Совет: Если загрузка модуля ASA SFR не завершена, команда session выполнена не будет и появляется сообщение о том, что системе не удается установить соединение по TTYS1. В этом случае дождитесь завершения загрузки модуля и повторите попытку.

2. Введите команду setup для настройки системы так, чтобы можно было установить пакет системного программного обеспечения:

asasfr-boot> **setup** Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []

Появится приглашение на ввод следующей информации:Имя хоста: может содержать до 65 буквенно-цифровых символов без пробелов. Можно использовать

дефисы.Сетевой адрес: может быть статическим адресом IPv4 или IPv6. Можно также использовать DHCP для автоматического задания адреса IPv4 или IPv6 без сохранения состояния.Информация DNS. Необходимо указать хотя бы один сервер системы доменных имен (DNS), а также можно задать доменное имя и домен для поиска.Информация NTP. Можно включить протокол NTP и настроить серверы NTP для задания системного времени.
3. Введите команду system install для установки образа системного программного обеспечения:
asasfr-boot >**system install [noconfirm]** ***url***
Укажите параметр noconfirm, если не хотите отвечать на подтверждающие сообщения. Замените ключевое слово url местоположением файла .pkg. Например:
asasfr-boot >**system install http://<*HTTP_SERVER*>/asasfr-sys-5.3.1-152.pkg** Verifying
Downloading
Extracting
Package Detail
Description: Cisco ASA-FirePOWER 5.3.1-152 System Install
Requires reboot: Yes
Do you want to continue with upgrade? [y]: y Warning: Please do not interrupt the process or turn off the system. Doing so might leave system in unusable state.
Upgrading Starting upgrade process ...
Populating new system image Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Jun 23 09:28:38 2014):
The system is going down for reboot NOW!
Console session with module sfr terminated.
Примечание. После завершения установки выполняется перезагрузка системы. Установка компонентов приложения и запуск сервисов ASA SFR занимает 10 минут и более. Выходные данные команды show module sfr должны указывать, что все процессы Up выполняются.

3 Настройка программного обеспечения FirePOWER
Для того чтобы настроить программное обеспечение FirePOWER, выполните следующие действия:

1. Откройте сеанс работы с модулем ASA SFR.

Примечание. Откроется еще одно приглашение ввода учетных данных, поскольку теперь происходит вход в систему на полностью работоспособном модуле.Например:
ciscoasa# **session sfr** Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Sourcefire ASA5555 v5.3.1 (build 152)
Sourcefire3D login:

2. Войдите в систему, используя имя пользователя admin и пароль Admin123.
3. Выполните настройку системы, следуя приглашениям, которые отображаются в следующем порядке: Прочитайте и примите лицензионное соглашение с конечным пользователем (EULA).Измените пароль администратора.При появлении соответствующих запросов задайте адрес управления и параметры DNS. Примечание. Для интерфейса управления можно задать оба (IPv4 и IPv6).Например:

ciscoasa# **session sfr** Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
Sourcefire ASA5555 v5.3.1 (build 152)
Sourcefire3D login:

4. Дождитесь, пока система изменит свою конфигурацию.

Настройка FireSIGHT Management Center

Для управления политикой безопасности и модулем ASA SFR необходимо зарегистрировать его в FireSIGHT Management Center. С помощью FireSIGHT Management Center нельзя выполнить следующие действия:

- Настройка интерфейсов модуля ASA SFR
- Завершение работы, перезапуск и прочие действия по управлению процессами модуля ASA SFR
- Создание резервных копий и восстановление из резервных копий на устройства модуля ASA SFR
- Правила контроля доступа с правом на запись для сопоставления трафика с использованием условий тега VLAN

Перенаправление трафика к модулю SFR

Для перенаправления трафика к модулю ASA SFR необходимо создать политику обслуживания, которая определяет нужный трафик. Для того чтобы настроить перенаправление трафика к модулю ASA SFR, выполните следующие действия:

1. Выберите необходимый трафик с помощью команды access-list. В данном примере перенаправляется весь трафик со всех интерфейсов. Перенаправление также можно задать и для определенного трафика. ciscoasa(config)# **access-list sfr_redirect extended permit ip any any**
2. Создайте class-map для сопоставления трафика со списком контроля доступа:

ciscoasa(config)# **class-map sfr**
ciscoasa(config-cmap)# **match access-list sfr_redirect**

3. Задайте режим развертывания. Устройство можно настроить в пассивном (только мониторинг) или транзитном (обычном) режиме развертывания.

Примечание. Нельзя одновременно настроить на устройстве ASA и пассивный и транзитный режим. Разрешено использовать только политику безопасности только одного типа.В транзитном развертывании после отбрасывания нежелательного трафика и выполнения всех остальных действий, которые применяются политикой, трафик возвращается на устройство ASA для дальнейшей обработки и окончательной передачи. В данном примере показано создание карты политик (policy-map) и настройка модуля ASA SFR в транзитном режиме:

ciscoasa(config)# **policy-map global_policy** ciscoasa(config-pmap)# **class sfr** ciscoasa(config-pmap-c)# **sfr fail-open**

В пассивном развертывании копия трафика передается на сервисный модуль SFR, но это не возвращается на устройство ASA. Пассивный режим позволяет просматривать действия, которые модуль SFR выполнил бы в отношении трафика. Он также позволяет оценить содержимое трафика, не оказывая влияния на сеть.

Для настройки модуля SFR в пассивном режиме используйте ключевое слово monitoronly (как показано в следующем примере). Если это ключевое слово не используется, трафик передается в транзитном режиме. ciscoasa(config-pmap-c)# **sfr fail-open monitor-only**

********** Warning **********: Режим monitor-only не позволяет сервисному модулю SFR запрещать или блокировать вредоносный трафик.Внимание. : Можно было бы настроить устройство ASA в режиме monitor-only с использованием команды traffic-forward sfr monitor-only уровня интерфейса; однако эта конфигурация предназначена только для демонстрационных целей, ее не следует использовать на устройстве ASA в производственной среде. Центр технической поддержки Cisco TAC не оказывает помощи в устранении любых неполадок, обнаруженных в этой демонстрационной функции. Если вы хотите развернуть сервис ASA SFR в пассивном режиме, используйте для настройки policy-map.

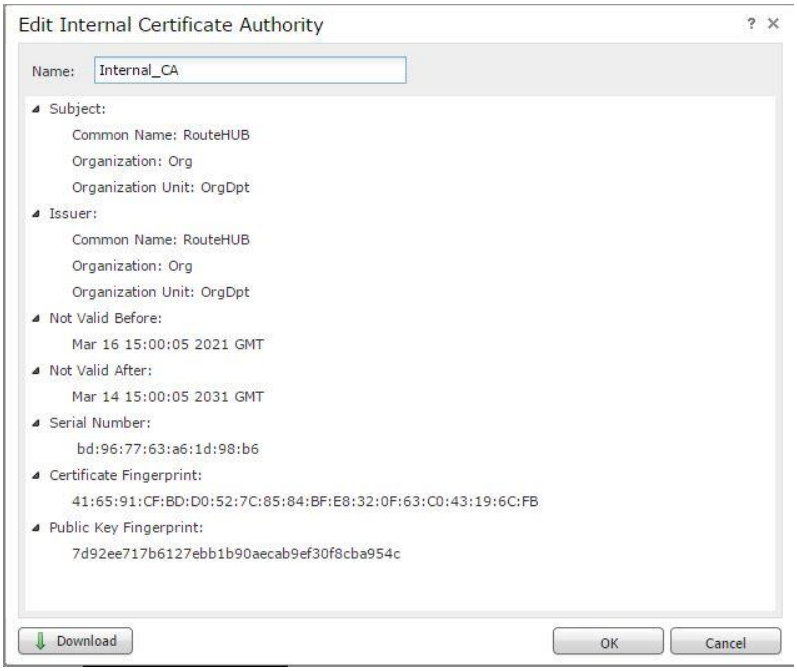
4. Укажите местоположение и примените политику. Политику можно применить глобально или к определенному интерфейсу. Для переопределения глобальной политики на интерфейсе можно применить политику обслуживания к этому интерфейсу.
Ключевое слово global применяет карту политик ко всем интерфейсам, а ключевое слово interface применяет данную политику к одному интерфейсу. Допускается только одна глобальная политика. В данном примере политика применена глобально: ciscoasa(config)# **service-policy global_policy global**
Внимание. : Карта политик global_policy является политикой по умолчанию. Если вы используете эту политику и хотите удалить ее на своем устройстве, чтобы выполнить поиск и устранения неполадок, убедитесь, что понимаете последствия.

Практическая работа № 18
Расшифровка трафика в шлюзе безопасности ASA при помощи SSL Decryption

SSL Decryption позволяет расшифровать трафик от пользователей на сайты https, чтобы затем выполнить проверку на настроенные политики.

Задание:
1. Создадим Internal CA:
Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal CAs -> Generate CA

Загрузим сертификат созданного CA:



Мы загрузим файл типа PKCS12. Данный тип файл содержит в себе сертификат + Private key de620fda-8666-11eb-9046-96de488b71b8.p12

Идём на страницу SSL policy:

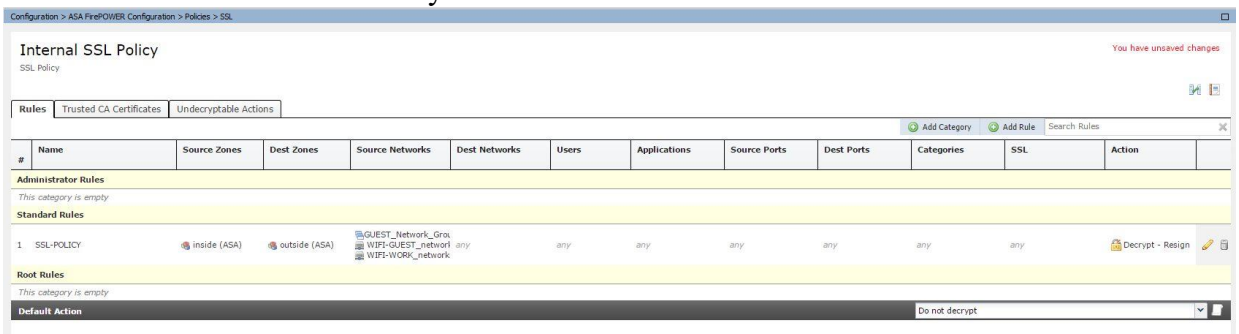
Configuration > ASA FirePOWER Configuration > Policies > SSL

Создадим SSL Policy Rule, которое будет определять, какой типа трафика будет подвергаться SSL Decryption.

Поскольку SSL Decryption "тяжелая" операция, рекомендуется создавать достаточно узкие правила.

Но наше правило учебное.

Также поменяем имя SSL Policy.

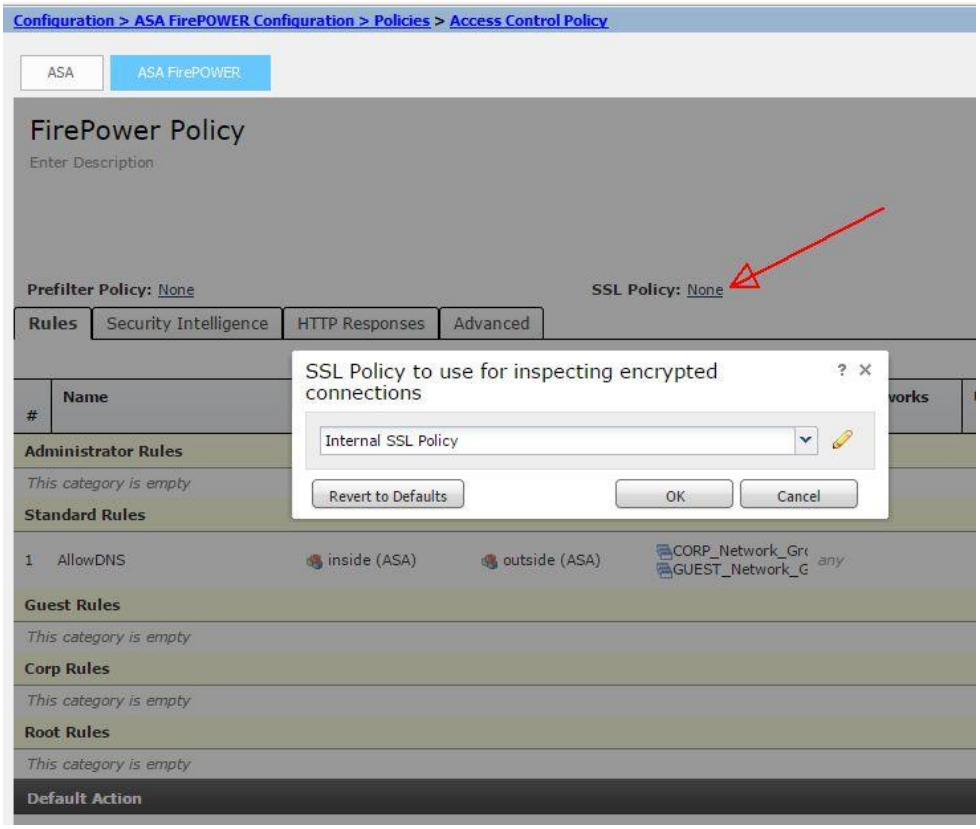


Сохраняем:

Store ASA FirePOWER Changes

Далее мы должны привязать SSL policy к Access Control Policy:

Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy



Сохраняем:

- Store ASA FirePOWER Changes

- Deploy FirePOWER Changes

Далее нам понадобится файл с сертификатом.

Сертификат необходимо установить клиентским компам, чтобы они не ругались на сертификат.

Вытаскиваем Private Key:

C:\temp>G:\PROGRA~2\GnuWin32\bin\openssl.exe pkcs12 -nocerts -in CA.p12 -out CAkey.pem

Вытаскиваем сам сертификат:

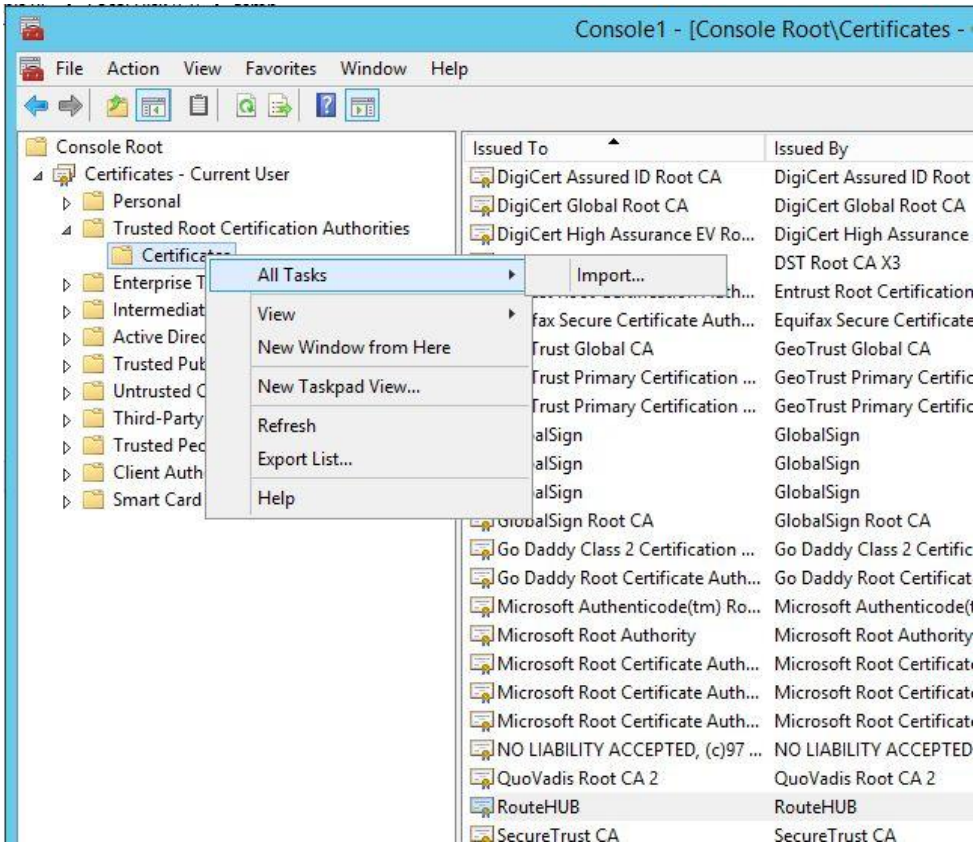
C:\temp>G:\PROGRA~2\GnuWin32\bin\openssl.exe pkcs12 -clcerts -in CA.p12 -out CAcert.pem

В итоге мы получим два файла:

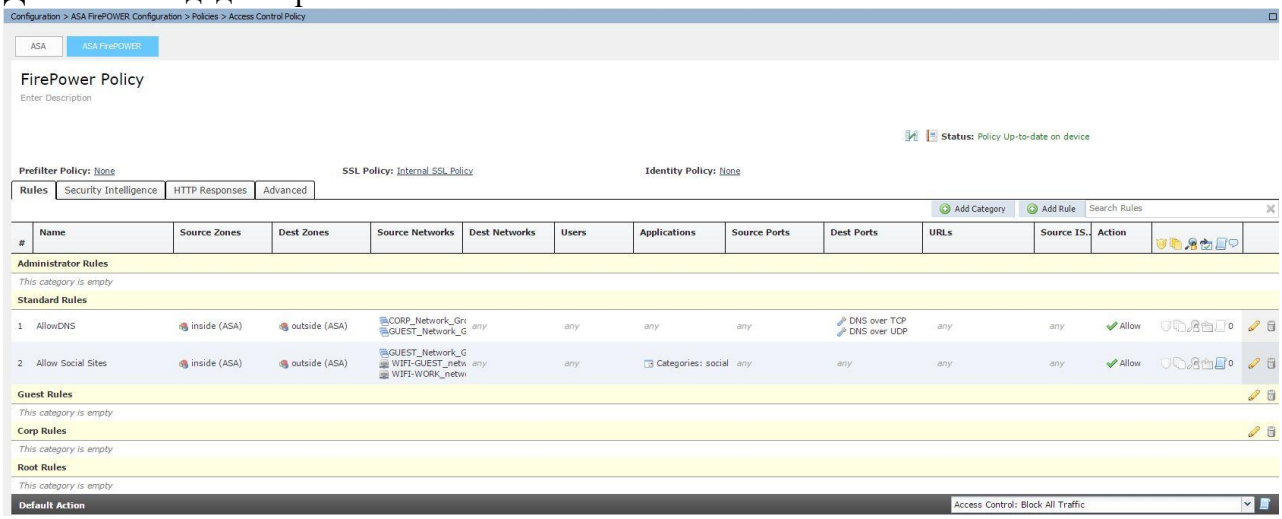
CAcert.pem

CAkey.pem

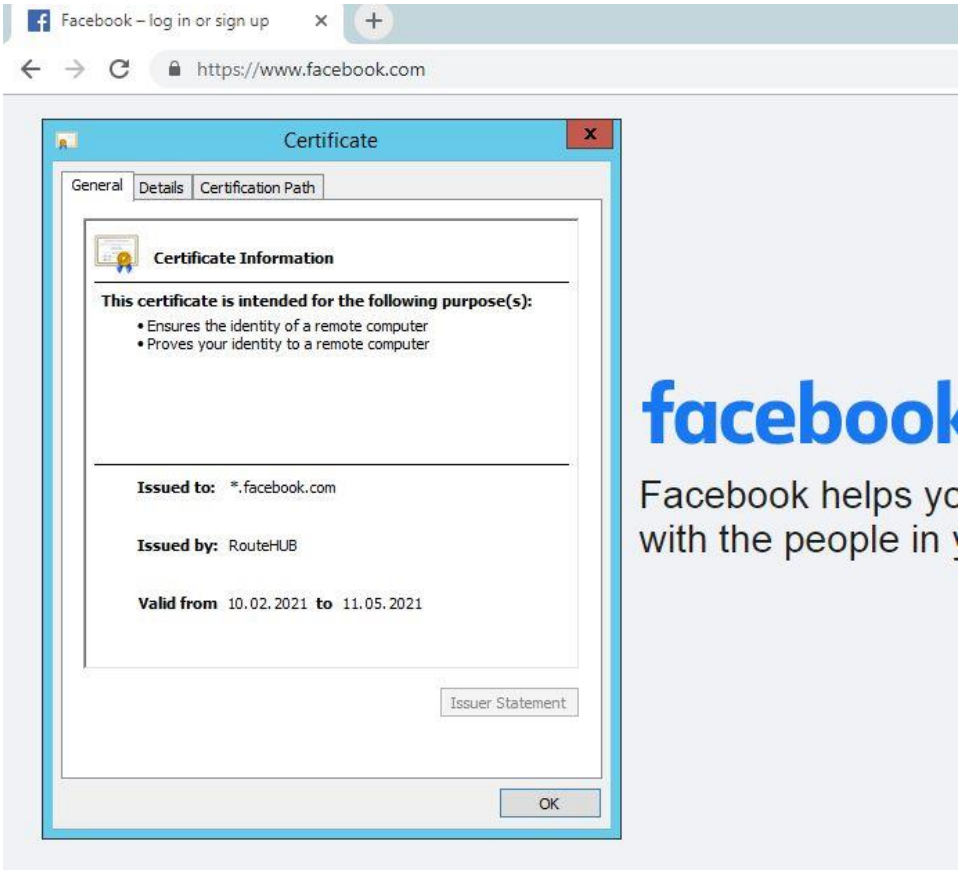
Переносим файл CAkey.pem на виндовую машину, и в mmc Certificates делаем Import в Trusted Root Certification Authorities:



Для теста создадим правило:

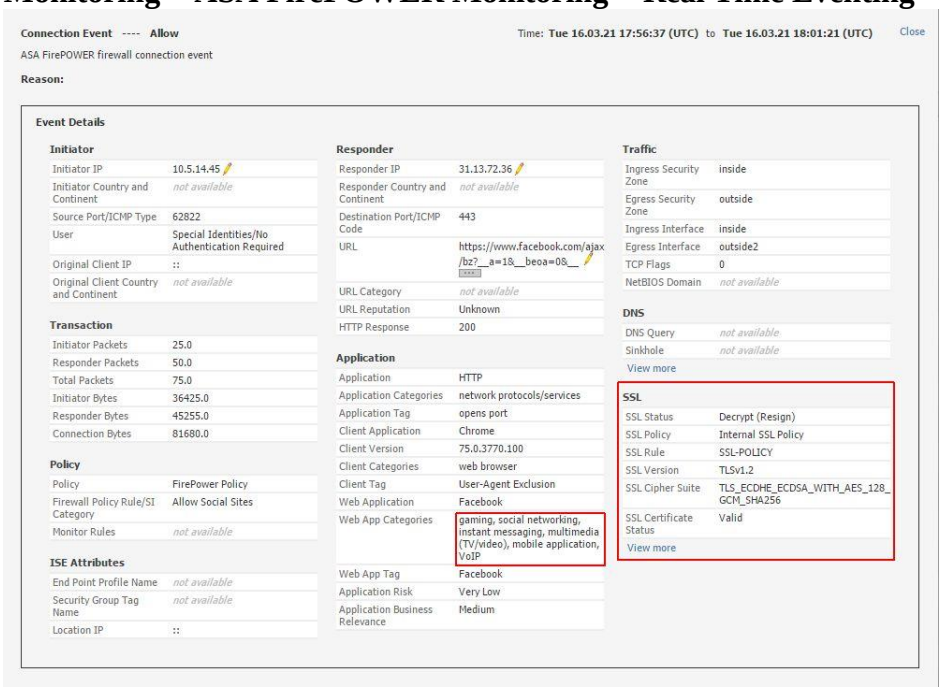


2 Тестирование SSL Decryption

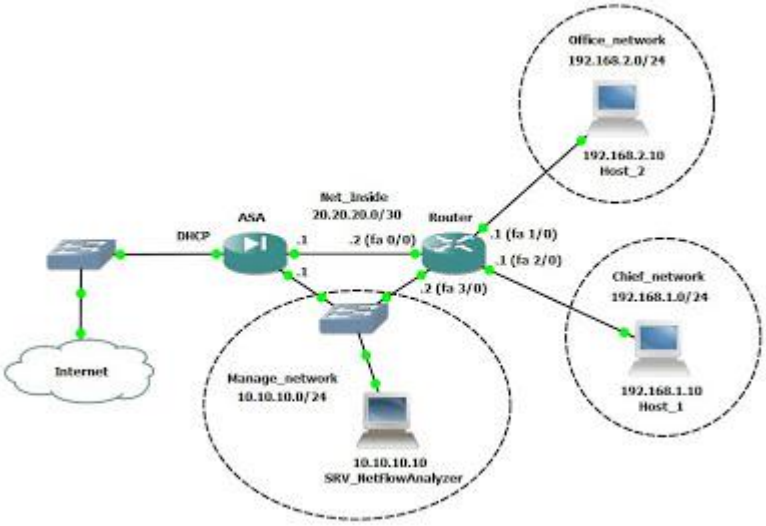


Monitoring:

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing



Практическая работа № 19
Сбор статистики о трафике, проходящем через шлюз безопасности ASA



Задание:

1. Настроить мониторинг и QoS на cisco ASA

Есть небольшая (упрощенная) сеть предприятия, состоящая из роутера cisco и устройства безопасности cisco ASA. Имеется четыре сети:

- 1. Chief_network (192.168.1.0/24), где находятся рабочие станции руководства. Для проверки используется Host_1 с IP-адресом 192.168.1.10;
- 2. Office_network (192.168.2.0/24), где находятся рабочие станции пользователей. Для проверки используется Host_2 с IP-адресом 192.168.2.10;
- 3. Manage_network (10.10.10.0/24), где находится сервер сбора статистики (IP-адрес 10.10.10.10.);
- 4. Промежуточная сеть Net_inside (20.20.20.0/30) предназначенная для соединения роутера и устройства безопасности. Данная сеть подключена к cisco ASA к интерфейсу inside.

Внешний интерфейс cisco ASA (outside) получает IP-адрес по протоколу DHCP. Для выхода в интернет настроен динамический NAT в данный IP-адрес (PAT).

Задача. Организовать и настроить сбор статистики использования полосы пропускания (скорости) канала связи с интернет, количества трафика, посещаемых сайтах и другой сопутствующей информации. Организовать распределение выделенной скорости (или полосы пропускания) конкретным сетям (хостам) (другими словами – настроить QoS).

Немного пояснений, как создать такую схему в GNS3. В качестве Host_1, Host_2 и SRV_NetFlowAnalyzer используются "VirtualBox guest"-элементы с настроенными на них UDPTunnel-ми в качестве сетевых интерфейсов. В роутере (cisco 3640) присутствуют 4-ре слота (NM-1FE-TX) по одному FastEthernet порту. Cisco ASA используется с IOS версии 8.4 (как запустить ASA с данным IOS можно посмотреть вот тут). Подключение к интернет реализовано через элемент "Cloud" с привязанным к нему сетевым интерфейсом VMNet8, который используется VMWare Workstation 9 для организации подключения типа NAT. Здесь следует учитывать тот факт, что по умолчанию VMWare Workstation 9 для сети за NAT-ом использует диапазон 192.168.158.128-254/24, шлюзом по умолчанию для которого является адрес 192.168.158.**2**, а не 192.168.158.**1**, как могло показаться. Данный адрес (192.168.158.2) следует выставить в качестве IP-адреса DNS-сервера на конечных хостах. Элементы "Ethernet Switch" используются для соединения ASA и "Cloud" и соединения ASA, Router и SRV_NetFlowAnalyzer соответственно.

Для решения задачи сбора подробной статистики будем использовать NetFlow и в качестве

collector-a – сервер с установленным на нем NetFlow Analyzer от компании ManageEngine. Я пробовал еще программы PRTG и Scrutinizer Flow Analyzer, но они мне менее понравились. Чем примечателен NetFlow Analyzer от компании ManageEngine, так это тем, что, несмотря на его платность ?, после окончания trial-периода он оставляет работоспособным мониторинг 2-х интерфейсов в полном объеме (а этого вполне достаточно для работы, имея inside и outside на cisco ASA).
Итак, приступим. Как всегда, для начала, организуем сетевую доступность и выход пользователей и руководства в интернет. Начнем с роутера:

R1#conf t
R1(config)#hostname Router - **задаем имя устройству**;
Router(config)#int fa 0/0
Router(config-if)#ip address 20.20.20.2 255.255.255.252 - **назначаем IP-адрес на интерфейсе, смотрящем в сторону ASA**;
Router(config-if)#no shutdown - **включаем интерфейс**;
Router(config-if)#exit
Router(config)#int fa 3/0
Router(config-if)#ip address 10.10.10.2 255.255.255.0 - **назначаем IP-адрес на интерфейсе, смотрящем в сеть Manage_Network**;
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int fa 1/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0 - **назначаем IP-адрес на интерфейсе, смотрящем в сеть Office_Network**;
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#int fa 2/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0 - **назначаем IP-адрес на интерфейсе, смотрящем в сеть Chief_Network**;
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 20.20.20.1 - **прописываем маршрут по умолчанию через cisco ASA**;
Router(config)#exit
Router#wr
Router#

Теперь перейдем на cisco ASA:

ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)#
ciscoasa(config)# int gi 0
ciscoasa(config-if)# ip address dhcp – **настраиваем, чтобы IP-адрес на интерфейс устанавливался по DHCP**;
ciscoasa(config-if)# no sh – **включаем интерфейс**;
ciscoasa(config-if)# nameif outside – **определяем, что этот интерфейс будет outside. Соответственно security-level автоматически назначается равным "0"**;

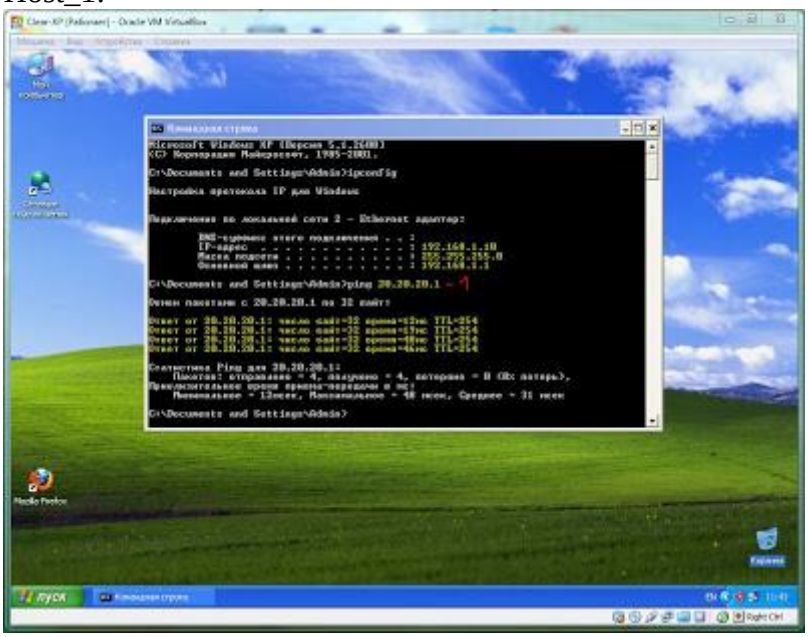
ciscoasa(config-if)# exit
ciscoasa(config)# int gi 1
ciscoasa(config-if)# nameif inside – **определяем, что этот интерфейс будет inside. Соответственно security-level автоматически назначается равным "100"**;
ciscoasa(config-if)# ip address 20.20.20.1 255.255.255.252 – **назначаем IP-адрес интерфейсу**;
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)# int gi 2
ciscoasa(config-if)# nameif manage – **определяем, что этот интерфейс будет manage**;
ciscoasa(config-if)# security-level 50 – **устанавливаем security-level в значение "50"**;
ciscoasa(config-if)# ip address 10.10.10.1 255.255.255.0
ciscoasa(config-if)# no sh
ciscoasa(config-if)# exit
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.158.2 – **прописываем маршрут по умолчанию через outside**;
ciscoasa(config)# route inside 192.168.1.0 255.255.255.0 20.20.20.2 – **так как мы не используем здесь динамическую маршрутизацию, то прописываем статические маршруты в сети пользователей, находящиеся за роутером, через интерфейс inside**;
ciscoasa(config)# route inside 192.168.2.0 255.255.255.0 20.20.20.2
ciscoasa(config)# object network OFFICE – **из-за специфики настройки NAT в IOS 8.4 создаем object network для каждой из сетей пользователей. В данном случае для сети Office_network**;
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0 – **определяем соответствующую подсеть**;
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface – **включаем динамический NAT (PAT) непосредственно для данной object network. В прошлых IOS-ах, насколько вы помните, NAT включался из глобального режима**;
ciscoasa(config-network-object)# exit
ciscoasa(config)# object network CHIEF
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config-network-object)# exit

Следующие настройки обычно уже присутствуют на реальном оборудовании. Это настройки для инспектирования различного вида трафика. Если их нет, то некоторый трафик может не проходить. Так что советую вам их добавить, если у вас их нет:

ciscoasa(config)# class-map inspection_default – **создаем класс трафика**;
ciscoasa(config-cmap)# match default-inspection-traffic – **определяем тип трафика, попадающий в данный класс**;
ciscoasa(config-cmap)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
ciscoasa(config-pmap-p)# policy-map global_policy – **определяем глобальную политику инспектирования**;
ciscoasa(config-pmap)# class inspection_default – **подключаем к ней ранее созданный класс**;
ciscoasa(config-pmap-c)# inspect dns preset_dns_map – **определяем, что делать с данным трафиком (в данном случае просто проводить инспекцию)**;

ciscoasa(config-pmap-c)# inspect ftp
ciscoasa(config-pmap-c)# inspect h323 h225
ciscoasa(config-pmap-c)# inspect h323 ras
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# inspect netbios
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# service-policy global_policy global – **включаем политику глобально на всем устройстве**;
ciscoasa(config)#exit
ciscoasa#wr

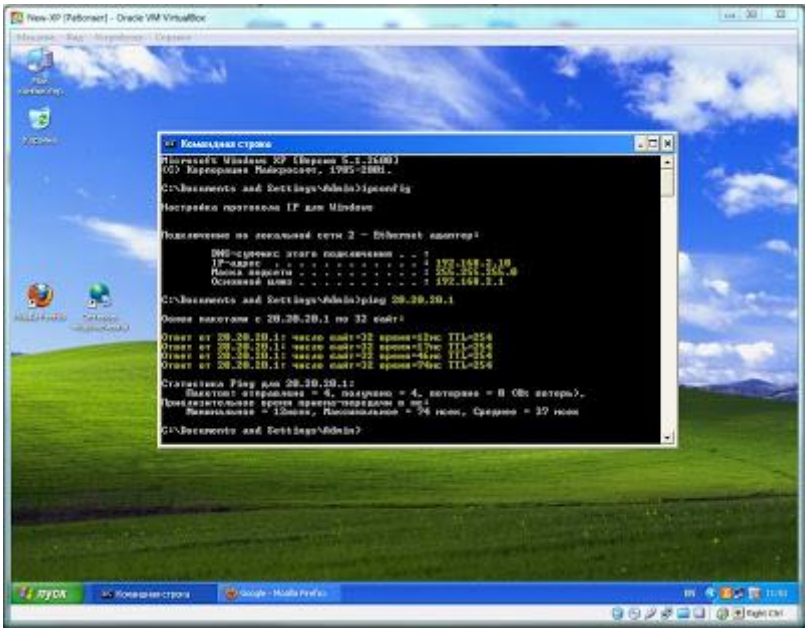
Основные сетевые настройки закончили. Давайте проверимся. Зайдем на Host_1 и Host_2 и посмотрим наличие доступа в интернет.
Host_1:

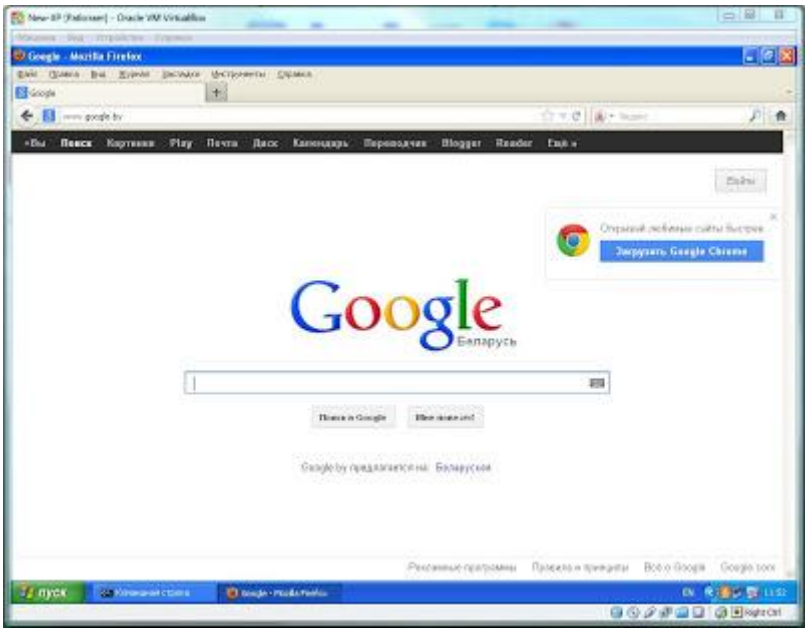


где:

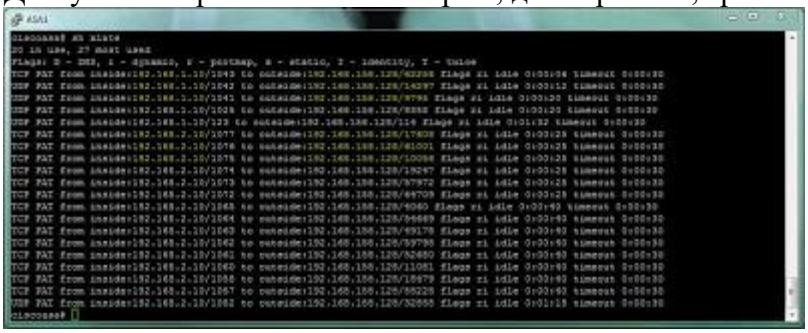
- 1 – IP-адрес интерфейса inside ASA.

Host_2:



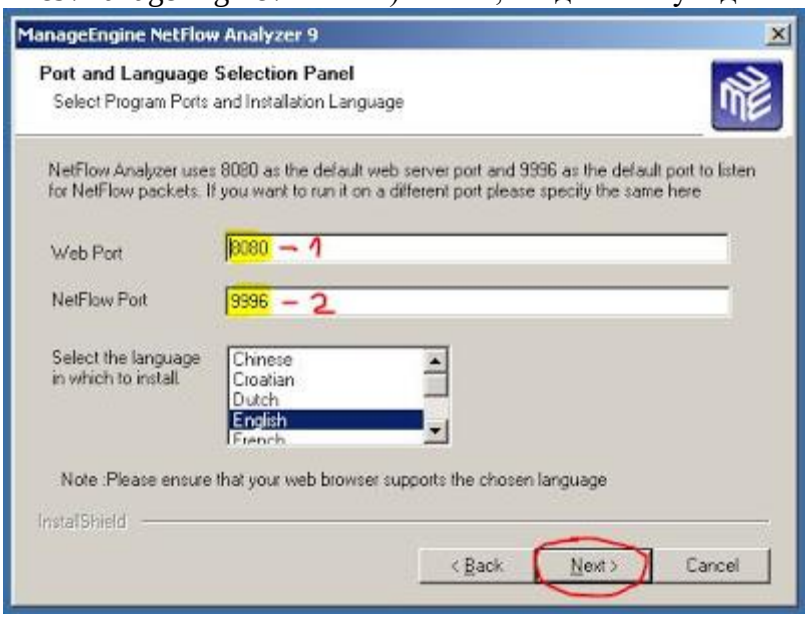


Доступ в интернет есть. Посмотрим, для верности, трансляцию адресов на cisco ASA:

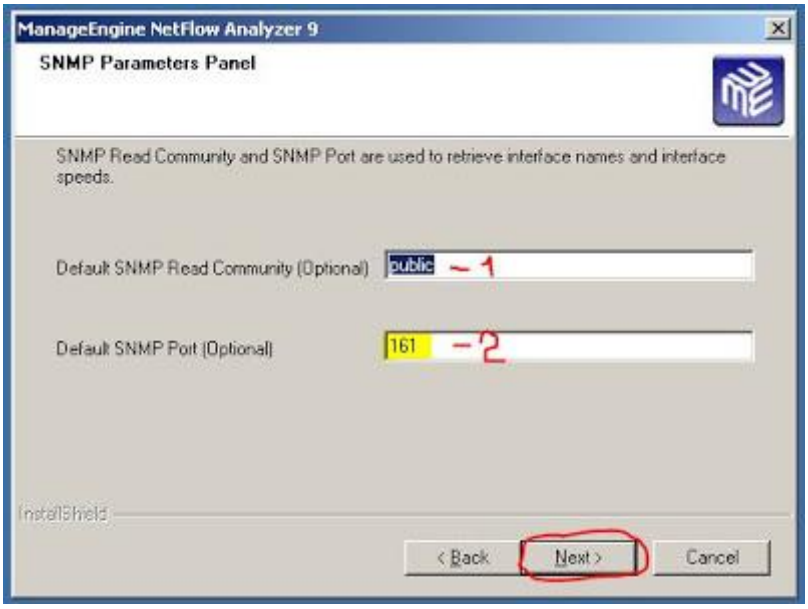


Как видно, трансляция отлично работает.
На данный момент мы настроили сетевую доступность и обеспечили выход в интернет всем за-

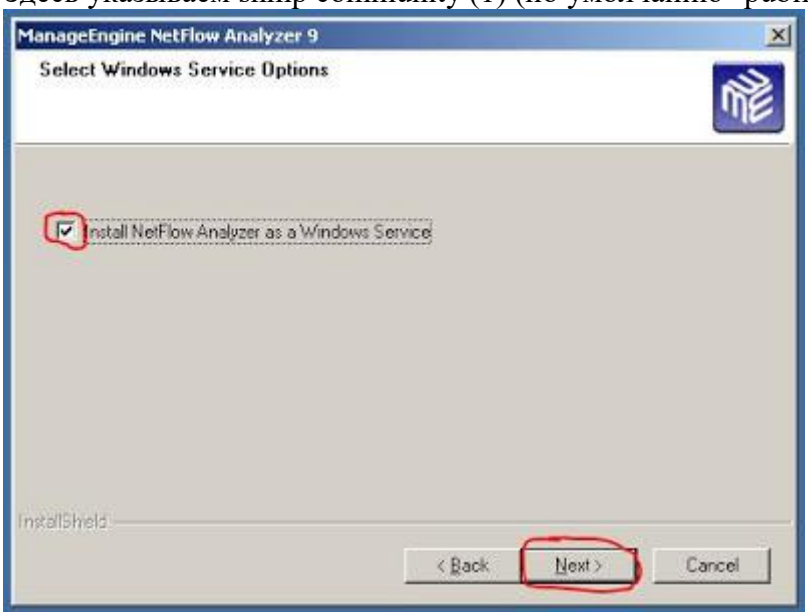
интересованным лицам, но сейчас каждый ходит куда хочет и занимает максимально доступную полосу канала (ну или использует скорость канала по полной :)).
Для организации контроля над всем этим делом, давайте установим и настроим сервер мониторинга, проанализируем, кто куда ходит, и затем настроим приоритеты и разграничение скорости.
Для этого, переходим на сервер SRV_NetFlowAnalyzer (установлена win 2003 со службой IIS) и установим программу NetFlow Analyzer (скачать можно вот здесь). Запускаем скачанный файл. В приветственном окне нажимаем "Next". В следующем соглашаемся с лицензией ("Yes"). Затем выбираем папку, куда будет установлена программа (по умолчанию C:\Program Files\ManageEngine\NetFlow). Затем, вы должны увидеть следующее окно:



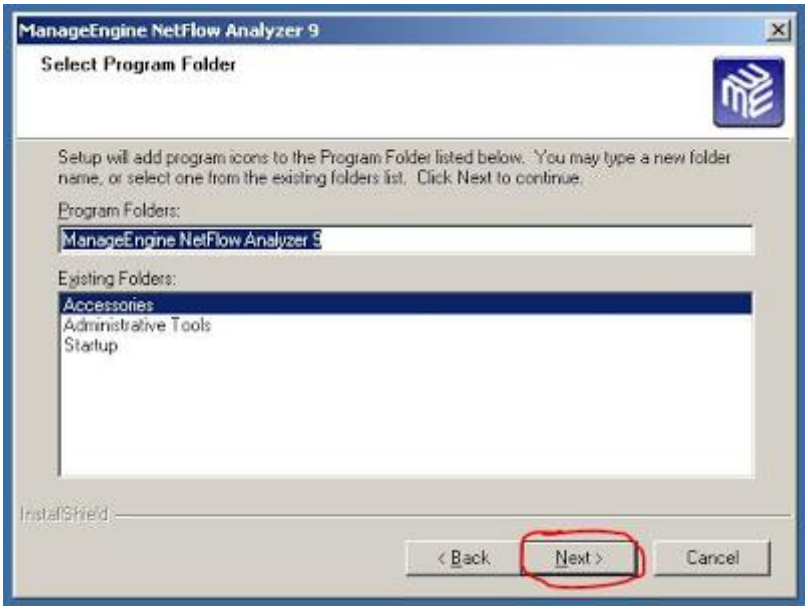
Здесь указываем порт для доступа через web-интерфейс (1) и порт, на который NetFlow Analyzer будет принимать пакеты NetFlow (2). Можно оставить все по умолчанию. Следует так же проверить, чтобы порт для web (8080) работал и "слушался" установленной службой IIS. Нажимаем "Next":



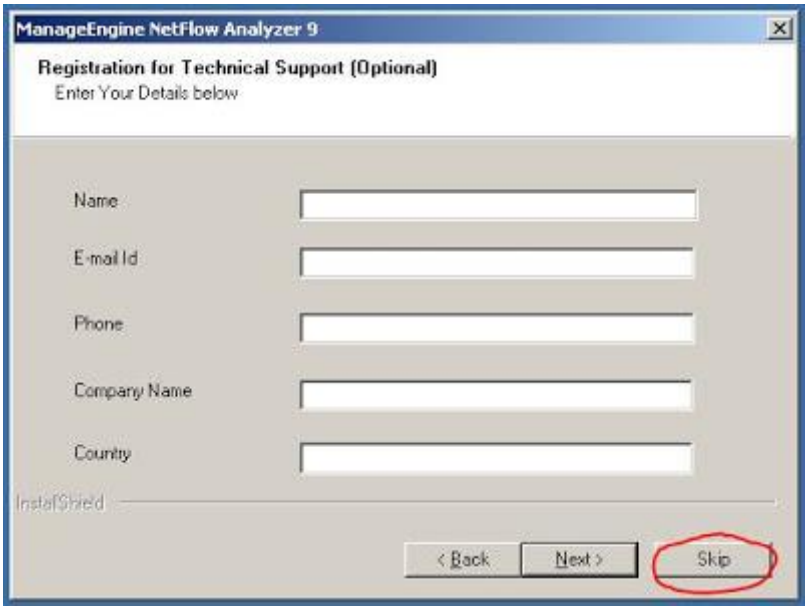
Здесь указываем snmp community (1) (по умолчанию "public") и порт (2). Нажимаем "Next":



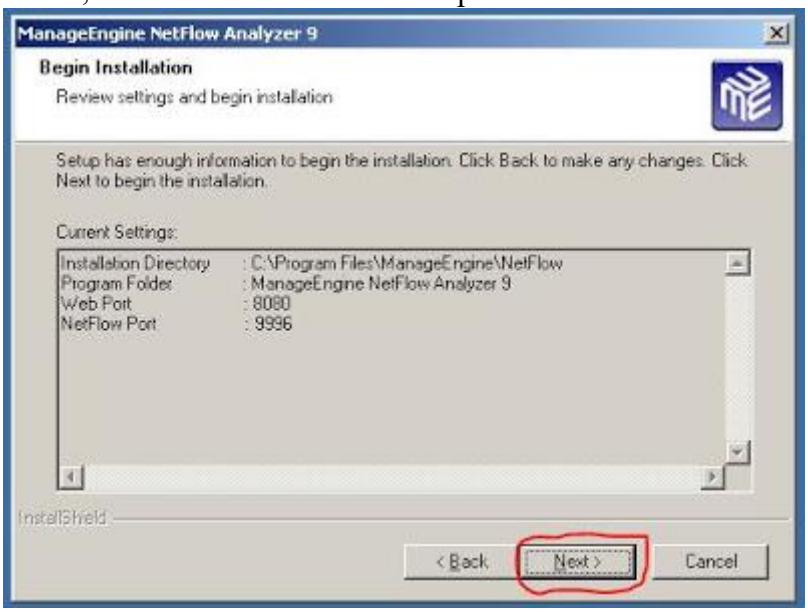
Здесь отмечаем пункт, чтобы NetFlow Analyzer установился в качестве сервиса windows. В дальнейшем, за счет этого, он будет запускаться при старте системы автоматически. Нажимаем "Next":



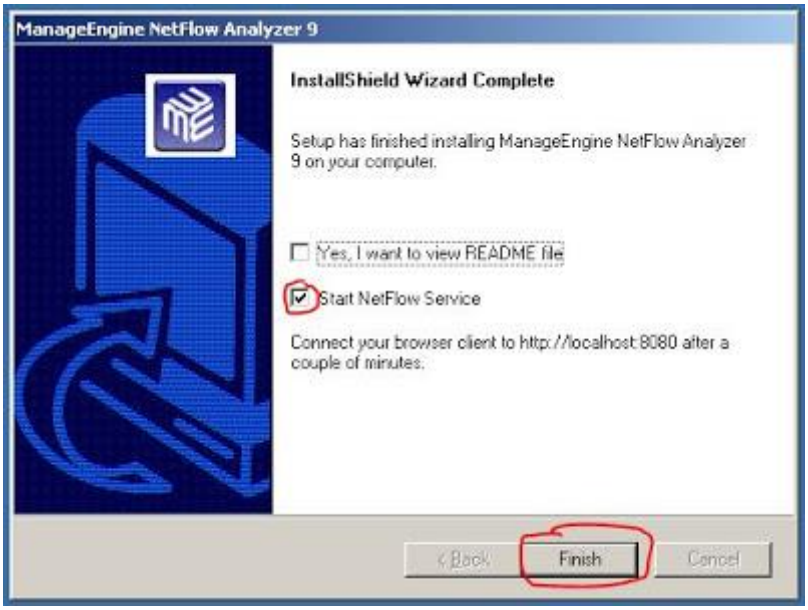
В этом окне указываем, какую папку создаст для себя программа. Нажимаем "Next":



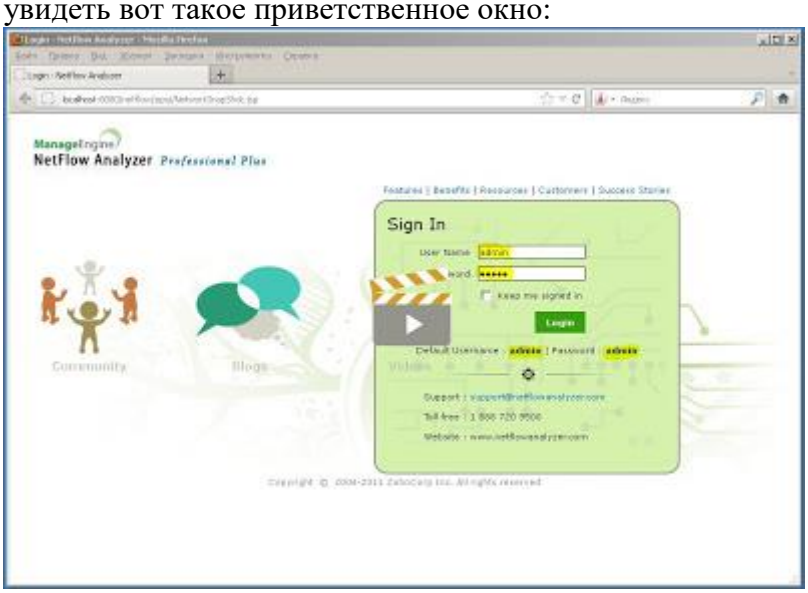
Здесь просят ввести данные для технической поддержки. Если вам она необходима, то заполняйте, если нет – нажимайте "Skip":



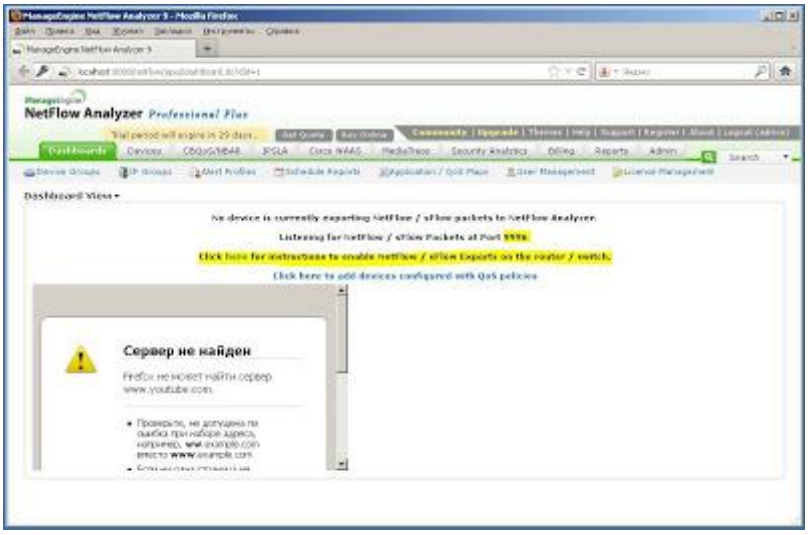
В данном окне нам предлагают проверить параметры установки. Если все верно, нажимаем "Next". Начнется процесс установки программы. После окончания установки вы должны увидеть следующее окно:



Отказываемся от просмотра файла "Readme" и отмечаем пункт запуска сервиса NetFlow Analyzer. Нажимаем "Finish". После запуска сервиса (будет видно соответствующее окно), если у вас в панели задач windows (внизу) видна некая непонятная закладка и при наведении на нее пишет "do not close", не пугайтесь, можете просто перегрузить сервер win 2003, и при следующей загрузке этой закладки уже не будет. Находим ярлык программы на рабочем столе и дважды кликаем по нему (или можно открыть браузер и ввести http://localhost:8080). Вы должны увидеть вот такое приветственное окно:



Стандартный логин и пароль: admin/admin. Вводим его и заходим в консоль управления:



Это главное окно программы. Как вы можете заметить, оно пустое. Проверьте в нем лишь порт для NetFlow, который мы указывали ранее, чтобы он совпадал. Можете полазить там по вкладкам, посмотреть, все они будут пустыми. Вернемся на наши сетевые устройства и настроим на них NetFlow.
Чем мне еще понравился данный продукт, так это Help-ом. Там есть примеры настройки NetFlow на оборудовании. Но вот как раз настройку NetFlow на cisco ASA я не нашел :).
Так как у нас на данный момент есть возможность мониторинга более 2-х интерфейсов со всем функционалом, то грех этим не воспользоваться. Поэтому настроим NetFlow не только на cisco ASA, но еще и на роутере (cisco 3640). С него и начнем:

Router#conf t
Router(config)#ip flow-export destination 10.10.10.10 9996 – **определяем IP-адрес и порт collector-а, куда будут отправляться пакеты (cache) NetFlow**;
Router(config)#ip flow-export source fastEthernet 3/0 – **указываем, какой из интерфейсов будет использоваться в качестве источника, для отправки NetFlow пакетов**;
Router(config)#ip flow-export version 9 – **определяем версию NetFlow (существует еще версия 5)**;
Router(config)#ip flow-cache timeout active 1 – **определяем интервал времени (в минутах) через которое устройство будет делать так называемые сэмплы (выборку) пакетов и отправлять их на collector**;
Router(config)#ip flow-cache timeout inactive 15 – **определяем интервал времени (в секундах) неактивности трафика. Т.е. каждые 15 секунд устройство будет проверять наличие соответствующего трафика**;
Router(config)#ip flow-top-talkers – **для возможности просмотра основных потребителей трафика непосредственно на устройстве создадим группу Top-talkers. В дальнейшем, чтобы посмотреть этот список на устройстве, используйте команду *show ip flow top-talkers***;
Router(config-flow-top-talkers)#top 10 – **указываем количество отображаемых элементов**;
Router(config-flow-top-talkers)#cache-timeout 60000 – **интервал (в миллисекундах) сбора статистики**;
Router(config-flow-top-talkers)#sort-by bytes – **метод сортировки результатов**;
Router(config-flow-top-talkers)#exit
Router(config)#snmp-server community public ro – **определяем snmp community и даем права read only**;

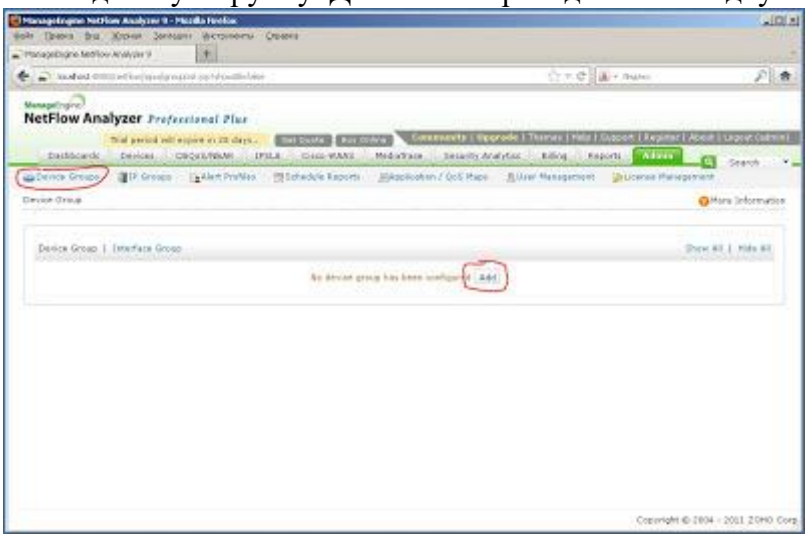
Router(config)#snmp-server ifindex persist – **включаем "разрешение имен интерфейсов". За счет этого на сервере имена интерфейсов устройства будут отображаться корректно**;
Router(config)#int fa 0/0
Router(config-if)#ip flow ingress – **указываем собирать статистику по входящему трафику**;
Router(config-if)#ip flow egress – **указываем собирать статистику по исходящему трафику**;
Router(config-if)#ip route-cache flow – **включаем NetFlow export на интерфейсе**;
Router(config-if)#exit
Router(config)#int fa 1/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config-if)#ip route-cache
Router(config-if)#exit
Router(config)#int fa 2/0
Router(config-if)#ip flow ingress
Router(config-if)#ip flow egress
Router(config-if)#ip route-cache
Router(config-if)#exit
Router(config)#exit
Router#wr
Router#

Теперь перейдем на cisco ASA и настроим NetFlow там. Настройки будут отличаться от роутера. Кроме основных настроек, нам необходимо будет создать специальный класс, специальный список, который будет отлавливать необходимый нам трафик, создать затем политику и применить ее глобально на устройстве. Но, обо всем по порядку:

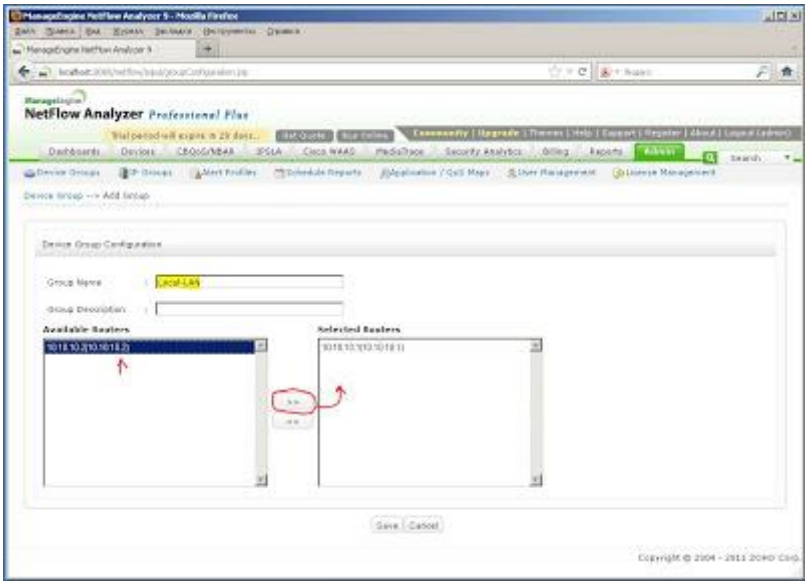
ciscoasa# conf t
ciscoasa(config)# snmp-server community public – **прописываем snmp community**;
ciscoasa(config)# access-list For-NetFlow extended permit ip any any – **создаем список доступа для захвата нужного трафика. Так как нам нужно отслеживать весь проходящий через ASA трафик, то делаем этот список как можно шире**;
ciscoasa(config)# flow-export destination manage 10.10.10.10 9996 – **как и на роутере, указываем IP-адрес и порт collector-а, только еще указываем, что он находится за интерфейсом "manage"**;
ciscoasa(config)# flow-export delay flow-create 60 – **устанавливаем интервал (в секундах) сэмплов (выборок) трафика для последующей отсылки на NetFlow collector**;
ciscoasa(config)# flow-export template timeout-rate 1 – **время неактивности (в минутах)**;
ciscoasa(config)# class-map NetFlow – **создаем класс для NetFlow трафика**;
ciscoasa(config-cmap)# match access-list For-NetFlow – **привязываем к этому классу ранее созданный список доступа. Теперь весь трафик, проходящий через ASA, будет попадать в этот класс**;
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy – **заходим в настройки глобальной политики**;
ciscoasa(config-pmap)# class NetFlow – **привязываем к политике созданный класс**;
ciscoasa(config-pmap-c)# flow-export event-type all destination 10.10.10.10 – **указываем какое действие делать с трафиком, относящимся к данному классу. В частности весь этот трафик будет отправлен на collector с IP-адресом 10.10.10.10**;
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit

```
ciscoasa(config)# exit
ciscoasa# wr
```

Ну что же, с настройками на устройствах вроде как закончили, теперь перейдем на сервер мониторинга (SRV_NetFlowAnalyzer) и настроим наш collector (NetFlow Analyzer).
Открываем web-консоль управления (можно через ярлык или через http://localhost:8080). Вполне возможно вы уже увидите в главном окне два устройства и какой-то трафик, но создадим для них отдельную группу. Для этого переходим на вкладку Devices Groups:

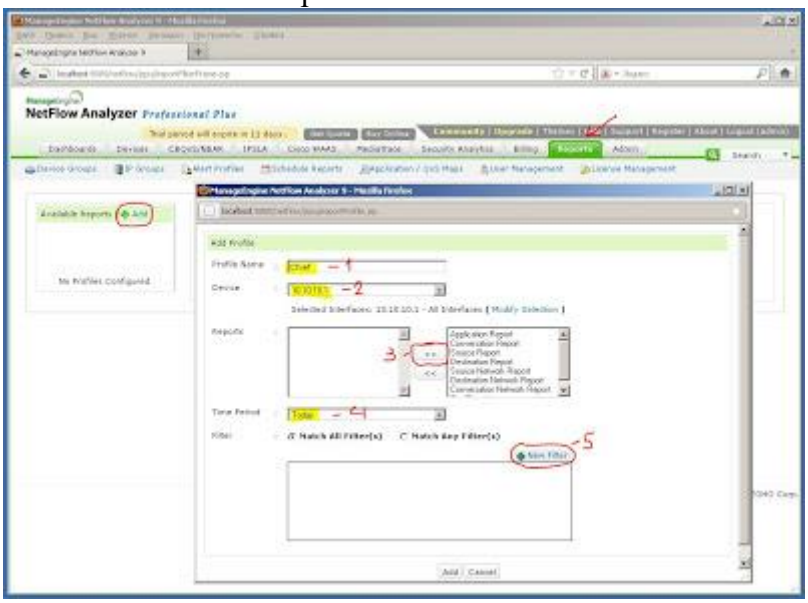


Нажимаем "Add":

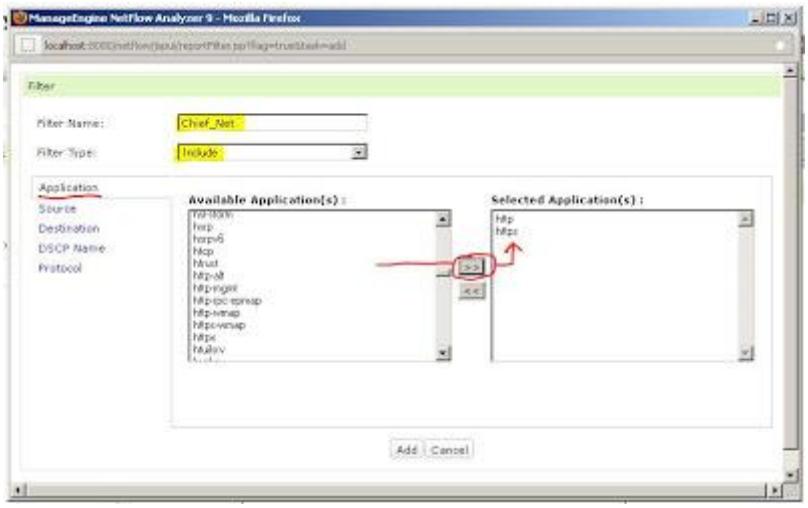


Видимые collector-у устройства будут отображаться слева (если их нет, подождите немного, необходимо, чтобы прошел какой-нибудь трафик через эти устройства, для этого, попускайте ping-и например). Нажимаем на кнопку переноса и переносим их в правый список. После этого нажимаем "Save". Как результат, вы должны увидеть в закладке "Device Groups" созданную группу с двумя устройствами в ней.
Вернувшись на главную страницу ("Dashboards") вы увидите приблизительно вот это:

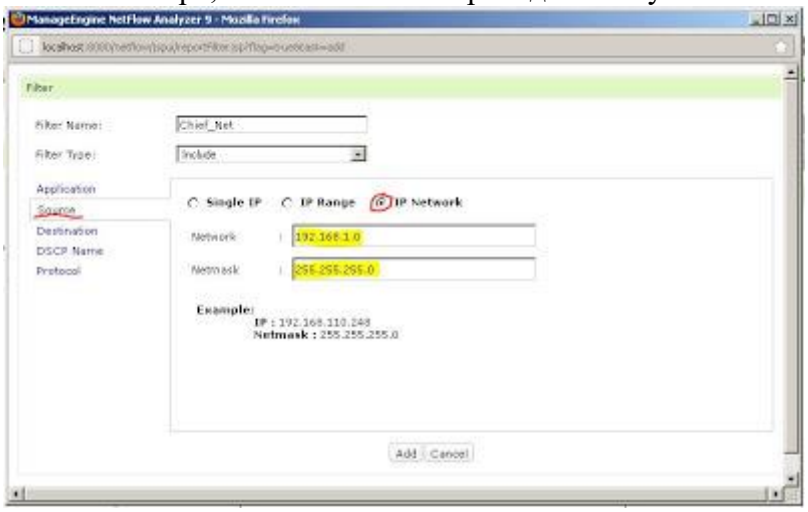
Уже красиво :). Уже можно посмотреть, какой трафик у нас бегает через устройства. Для более удобного просмотра статистики по трафику я предлагаю создать определенные правила (вид отчетов). Для этого, переходим на вкладку "Reports" и слева около надписи "Available Reports" нажимаем "Add". Откроется вот такое окно:



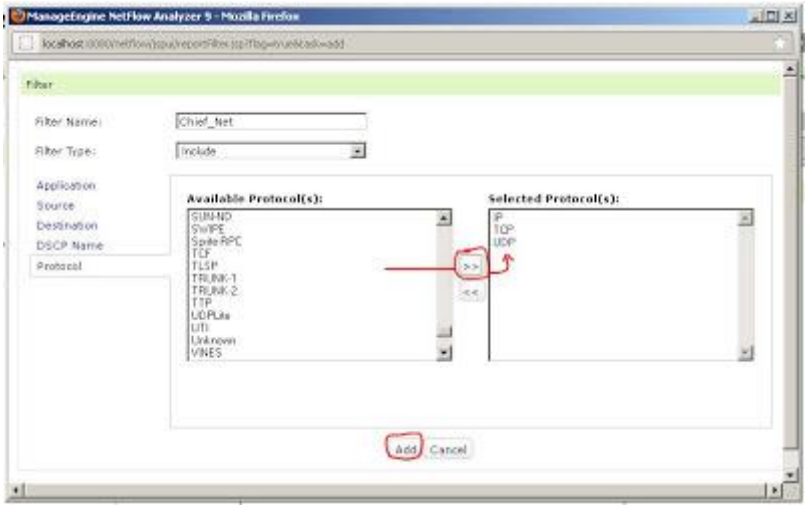
Здесь создаем первый "Report". Указываем ему имя (1), затем выбираем устройство из списка (2) (я выбрал cisco ASA 10.10.10.1). Далее из левой части списка выбираем виды отчетов и переносим их в правую часть (3). Для простоты я выбрал все. Далее выбираем период, за который мы хотим получать отчет (4). Теперь, прежде чем добавить отчет, необходимо указать, какой тип трафика, какие протоколы и так далее ему показывать. Для этого необходимо создать специальный фильтр. Нажимаем на "New Filter" (5). Откроется еще одно окно:



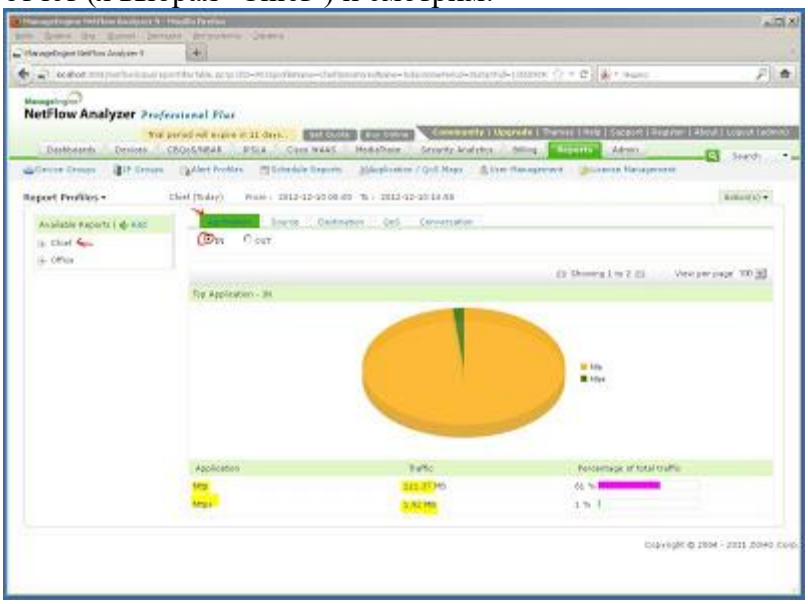
Здесь, так же задаем имя фильтра, указываем тип "Include". В пункте "Application" из левого списка выбираем интересующие нас виды приложений (http и https) и переносим их в правый список. Теперь, в этом же окне переходим на пункт "Source":



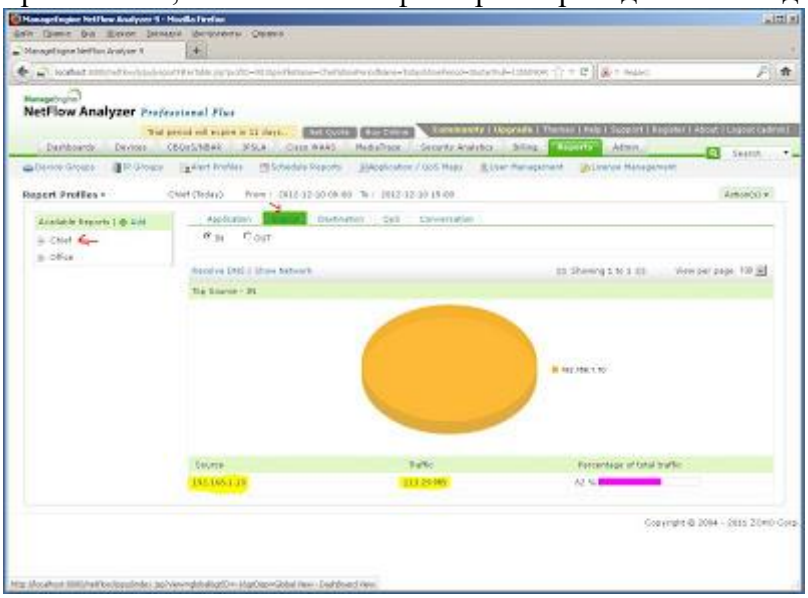
Здесь указываем сеть, для которой мы создаем фильтр. В данном случае указываем Chief_Network (192.168.1.0/24). Не закрывая окно, переходим к пункту "Protocol":



Снова из списка справа выбираем нужные нам протоколы (IP, TCP, UDP) и переносим их в правую часть. Все, нажимаем на "Add".
Фильтр должен появиться в нижнем списке. Отмечаем его и нажимаем "Add" уже в окне добавления отчета. Точно такие же действия проделайте для создания отчета по сети Office_Network. В итоге, у вас в списке должны присутствовать два отчета.
Теперь, если еще ничего не отображается, необходимо полазит в интернете с конечных хостов, чтобы наработать какой-нибудь трафик и собрать статистику. Если после этого тоже ничего не отображается, то перегрузите сервер с установленным NetFlow Analyzer.
Для просмотра статистики и отчетов снова возвращаемся во вкладку "Reports", выбираем любой отчет (я выбрал "Chief") и смотрим:

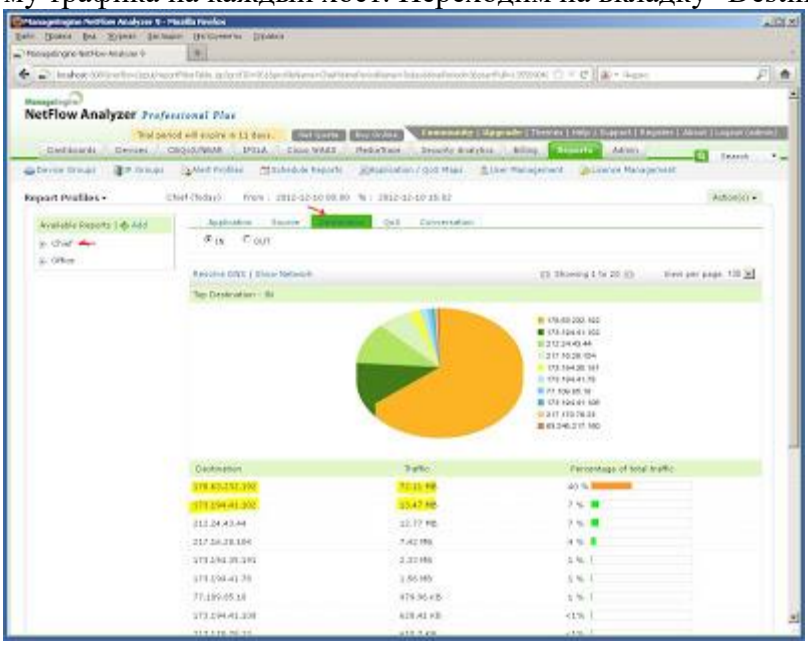


На закладке "Application" отображается общая информация по объему трафика по каждому виду приложения, отмеченного в фильтре. Переходим на вкладку "Source":

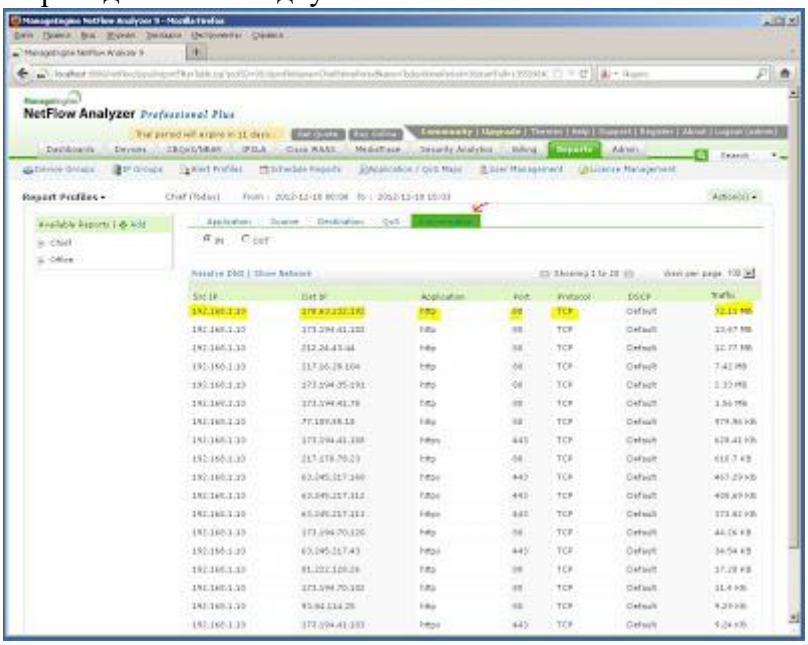


Здесь мы видим список источников трафика (ну у меня он один, а в реальной жизни тут будут

все хосты, которые находятся в заданной сети). Информация тут представлена по общему объему трафика на каждый хост. Переходим на вкладку "Destination":



Здесь показывается статистика по самым популярным посещаемым узлам (по объему трафика). Переходим на закладку "Conversations":



Здесь нам показана подробная статистика о соединениях (кто с кем, объем трафика, порты и так далее).
Я привел лишь базовую настройку этой программы, но, если у вас есть желание, то можете проиграться побольше. Ну а мы идем дальше.
Вторая задача, после сбора статистики - это настройка распределения пропускной способности (скорости) канала (Quality of Service). Если все обобщить, то это просто обработка пакетов согласно настроенным очередям. Есть три основных способа использования QoS на cisco ASA:
1. ***Traffic Prioritization***. Принцип состоит в том, что некоторому типу трафика (обычно Voice)

присваивается приоритет и после этого, он "обслуживается" в первую очередь, по сравнению с другим типом трафика. В cisco ASA можно задать лишь два приоритета - приоритетный (Priority QoS) и не приоритетный (Nonpriority QoS). Применяется этот вид QoS только на исходящий (egress) трафик. Настроить его можно с помощью следующих команд:

ASA(config)#policy map <название политики> - ***создаем политику;***
ASA(config-pmap)#class <название класса> - ***перед этим его нужно создать отдельно и определить тип трафика, который необходимо приоритезировать;***
ASA(config-pmap-c)#priority
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)#priority-queue <имя интерфейса> - ***включаем на интерфейсе.***
Так как у нас нет Voice, то настраивать это мы не будем.
2. ***Traffic Shaping***. Принцип действия основан на том, что настраивается "потолок" полосы пропускания (скорости), затем назначается средний размер пакета (burst size) который будет отсылаться через определенный промежуток времени. Другими словами, если у нас, например, полоса пропускания для shaping-а 2 Mbps, а размер burst size 16 Kbps и интервал времени 8 msec, то получается что каждые 8 msec ASA будет отсылать 16 Kbps информации.
Как всегда есть свои ограничения. 1) Если интервал времени задать большим, то устройство передаст информацию быстрее и будет ждать следующего момента, т.е. чувствительные к задержкам сервисы (VoIP) могут работать плохо. 2) Данный тип QoS применим только для трафика, который входит в class-default, создаваемый cisco ASA по умолчанию, т.е. ко всему трафику,. Другими словами, вы не можете создать специальный класс для shaping-а, но можете создать polucy-map. 3) Нельзя применить Traffic-Shaping глобально на устройстве.
Это нам так же не подойдет, так как мы хотим разграничить полосу пропускания (скорости) конкретным сетям (хостам). Но, если кто то хочет его настроить, то вот настройки:

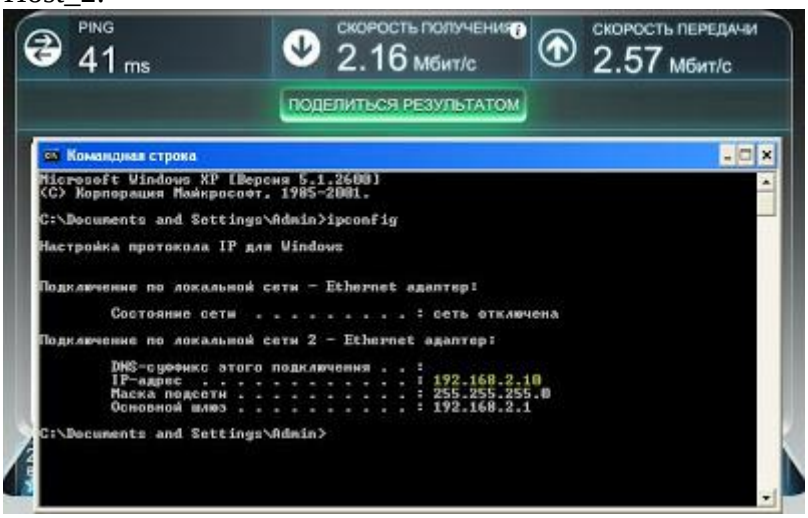
ASA(config)#policy map <название политики> - ***создаем политику;***
ASA(config-pmap)#class class-default - ***применим ТОЛЬКО для данного класса;***
ASA(config-pmap-c)# shape average [burst_size] - ***задаем нужные значения;***
ASA(config-pmap-c)#exit
ASA(config-pmap)#exit
ASA(config)# service-policy <название политики> interface <название интерфейса> - ***привязываем политику к конкретному интерфейсу;***

3. ***Traffic policing (traffic rate-limiting)***. Принцип основан на том, что задается верхний "потолок" полосы пропускания (скорости), которую может обеспечить интерфейс и любой трафик, который превышает этот лимит просто сбрасывается в конец очереди. Строго и со вкусом :).
Вот это то что нам надо, его мы и будем настраивать.
Хочу лишь заметить еще кое что:

- - нельзя сначала сделать трафику Priority, а затем еще и Shaping;
- - нельзя сначала сделать трафику Policing, а затем еще и Shaping;
- - нельзя сначала сделать трафику Shaping, а затем еще и Policing.

С небольшим экскурсом в теорию разобрались. Не судите строго, писал так, как понимаю сам и на звание эксперта не претендую :). За остальной информацией можно обратиться в интернет.
А мы двигаемся дальше и давайте, для начала, убедимся, что сейчас ограничения скорости нет ни у кого.
Host_1:

Host_2:

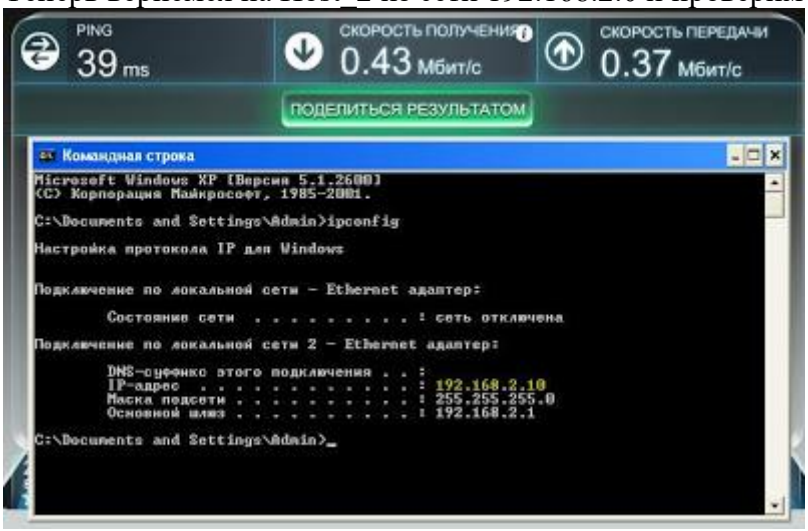


Как видно, ограничений нет. Ну что же, давайте ограничим скорость для Office_Network до 512 Кбит/с, думаю им хватит :). "Шефу" оставим полный канал. Для этого переходим на cisco ASA:

ciscoasa# conf t
ciscoasa(config)# access-list LIMIT_Office_Net extended permit ip 192.168.2.0 255.255.255.0 any - **создаем список доступа для интересующего нас трафика. В данном случае, когда из внутренней сети 192.168.2.0/24 идут во "внешний мир"**;
ciscoasa(config)# access-list LIMIT_Office_Net extended permit ip any 192.168.2.0 255.255.255.0 - **в данном случае, трафик идет из "внешнего мира" во внутреннюю сеть 192.168.2.0/24**;
ciscoasa(config)# class-map LIMIT_Speed - **создаем свой класс**;
ciscoasa(config-cmap)# match access-list LIMIT_Office_Net - **привязываем к нему ранее созданный список доступа**;
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map FOR_Office_Net - **создаем свою политику**;
ciscoasa(config-pmap)# class LIMIT_Speed - **привязываем к данной политике ранее созданный класс**;
ciscoasa(config-pmap-c)# police input 512000 96000 conform-action transmit exceed-action drop - **назначаем действие, которое необходимо выполнить с input трафиком, привязанным к**

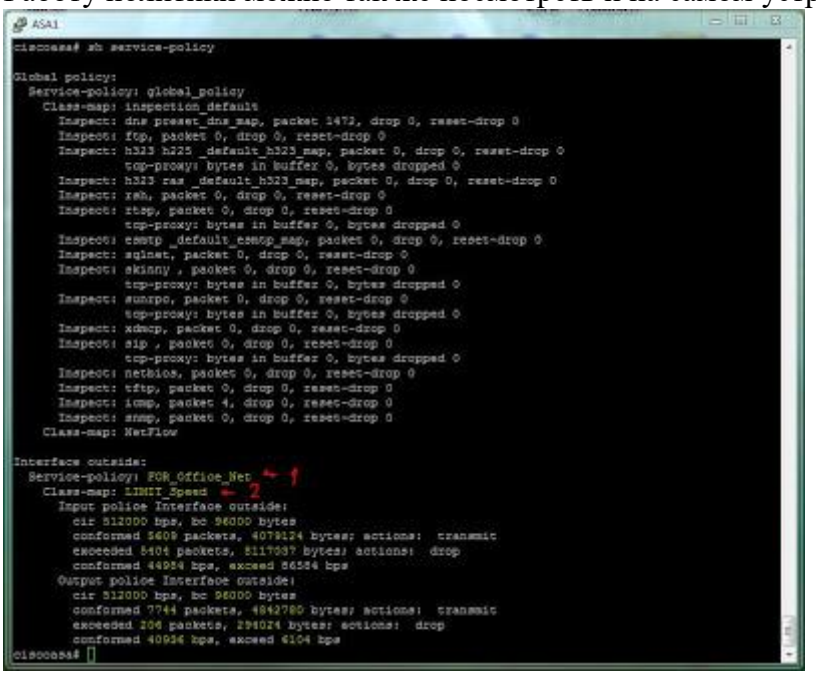
классу. В данном случае выставляется максимальная скорость (confirm rate) 512 Кбит/с и максимальное количество бит (burst size) 96000 (формула для расчета: Burst size = (confirm rate)/8*1.5), все, что подпадает под эти значения - пропускается, все что выходит за рамки - сбрасывается;
ciscoasa(config-pmap-c)# police output 512000 96000 conform-action transmit exceed-action drop - **назначаем действие, которое необходимо выполнить с output трафиком, привязанным к классу**;
ciscoasa(config)# service-policy FOR_Office_Net interface inside - **привязываем созданную политику к интерфейсу inside**;
ciscoasa(config)# exit
ciscoasa# wr
ciscoasa#

Конечно, я здесь привел пример "широкого" списка доступа, но он может быть организован намного строже. А именно для конкретного хоста, для конкретного порта и так .далее. Но это уже, если надо, вы попробуйте сами.
Теперь вернемся на Host_2 из сети 192.168.2.0 и проверим скорость сейчас:



Ну что же, ограничения вступили в силу :). Проверим, не урезали ли мы скорость для начальства. Переходим на Host_1:

Как видим ограничений нет (не смотрите что поменялась скорость передачи, просто видимо на момент проверки канал был немного загружен :)).
Работу политики можно так же посмотреть и на самом устройстве cisco ASA:

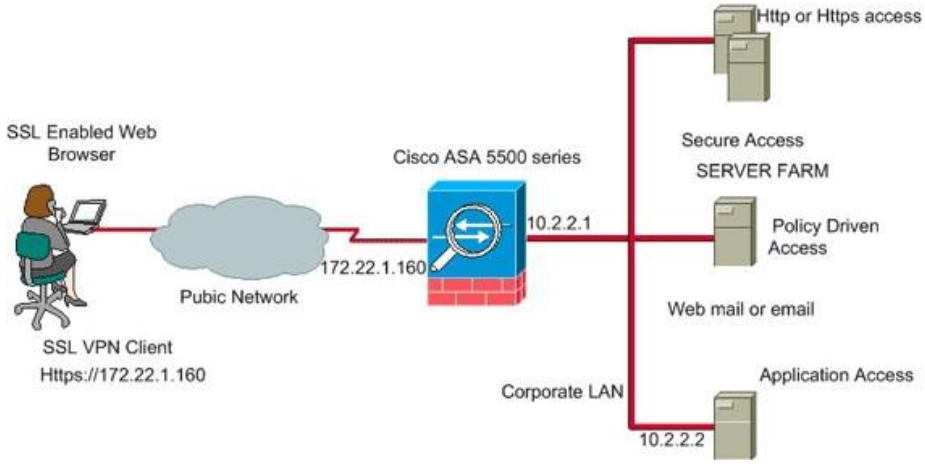


где:

- 1 - созданная политика;
- 2 - привязанный к политике класс.

Практическая работа № 20
Настройка AnyConnect Remote Access SSL VPN используя ASDM

Удаленный пользователь подключается к IP-адресу ASA с помощью веб-браузера с поддержкой SSL. После успешной аутентификации на клиентский компьютер загружается SVC, и пользователь получает полный доступ ко всем разрешенным ресурсам корпоративной сети в рамках шифрованного защищенного сеанса.



Задание:

Настройка SSL VPN Client на базе ASA

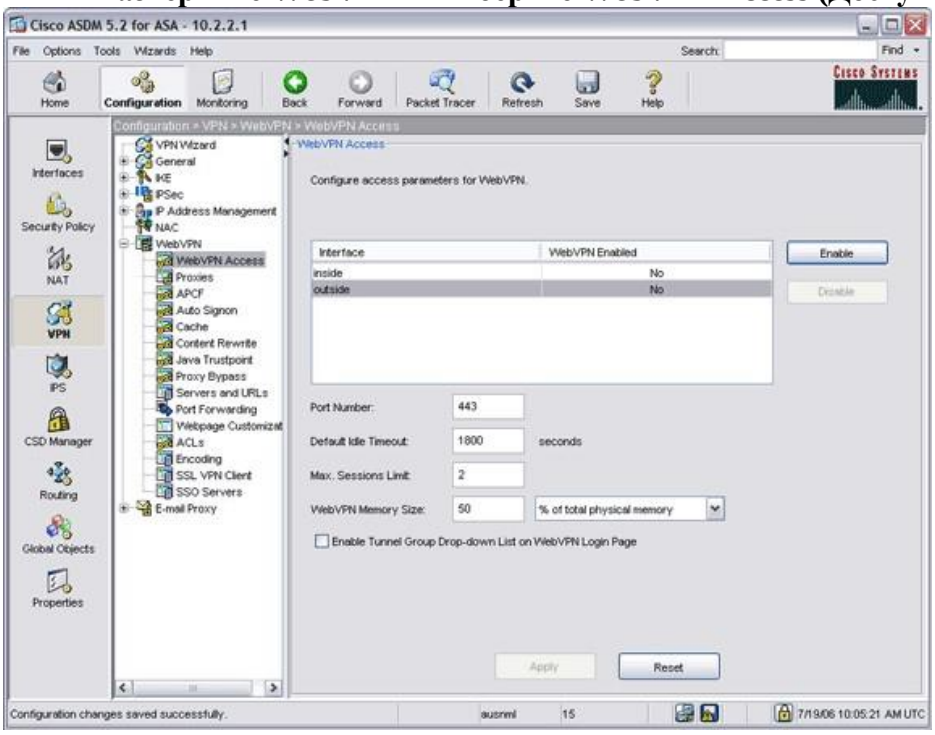
Чтобы настроить the SSL VPN Client на базе ASA, выполните следующие действия:

1. Включите WebVPN Access на ASA
2. Установите и включите VPN-клиента SSL (SVC) на ASA
3. Включите установку SVC на клиентах
4. Включите повторно вводят параметры

Шаг 1. Включение доступа к WebVPN для ASA

Чтобы включить доступ к WebVPN для ASA, выполните следующие действия:

1. **В приложении ASDM выберите Configuration (Настройка), затем выберите VPN.**
2. **Разверните WebVPN и выберите WebVPN Access (Доступ к WebVPN).**

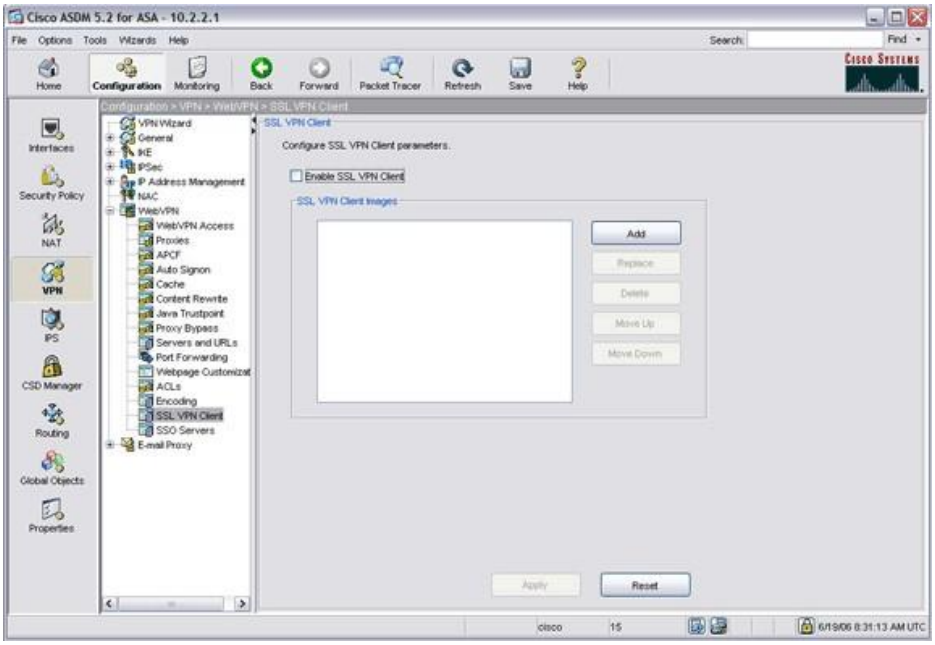


3. **Выберите интерфейсы, для которых необходимо включить WebVPN и нажмите Enable.**

Шаг 2. Установка и включение SSL VPN Client на ASA

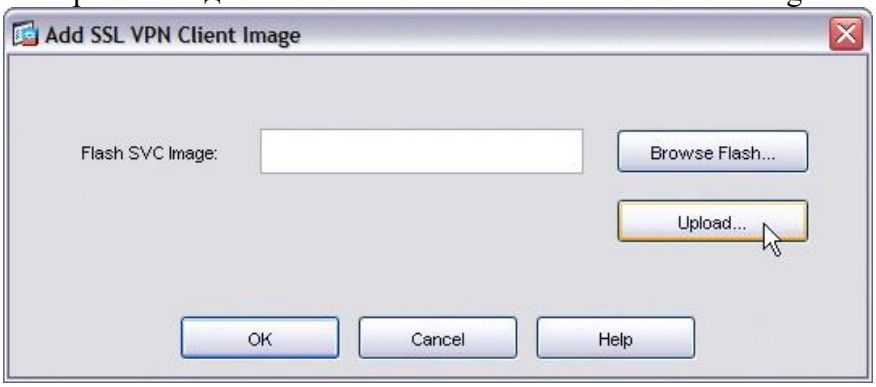
Чтобы установить и включить VPN-клиента SSL (SVC) на ASA, выполните эти шаги:

1. **Нажмите Configuration, затем VPN.**
2. **В навигационной панели разверните WebVPN и выберите SSL VPN Client.**



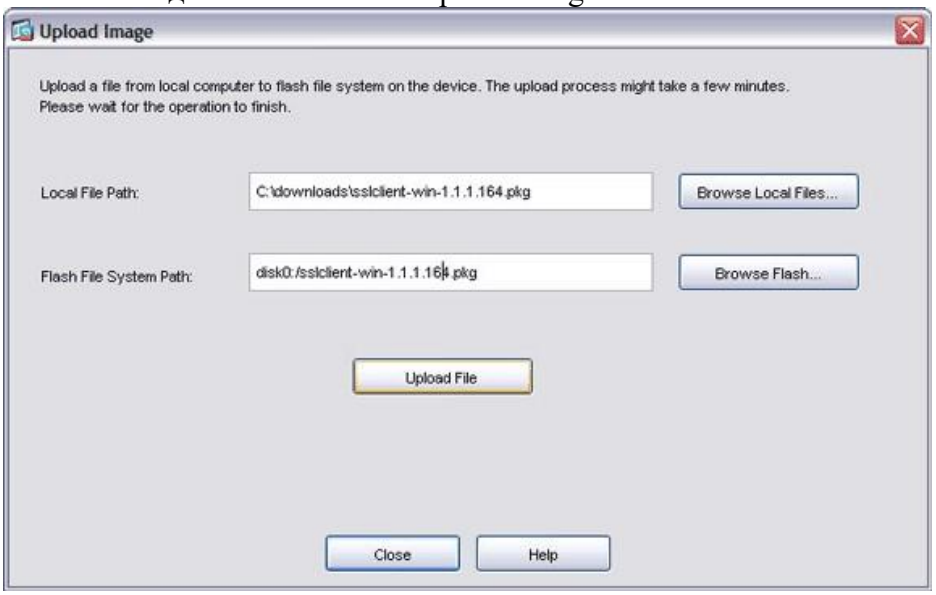
3. **Нажмите кнопку Add.**

Отображается диалоговое окно "Add SSL VPN Client Image".

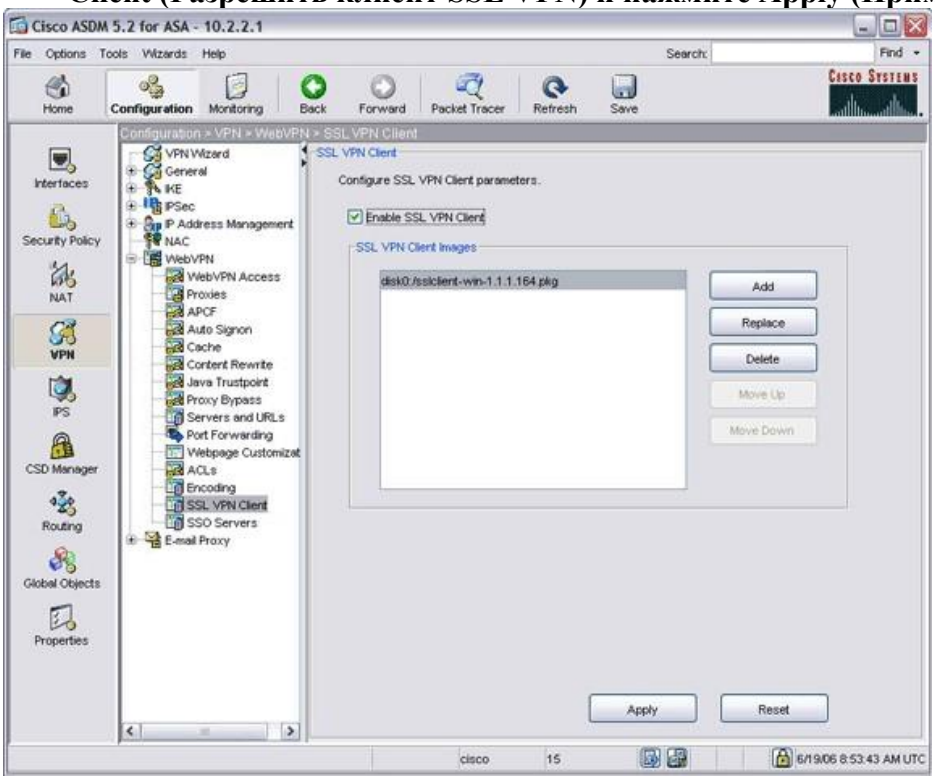


4. **Нажмите Upload.**

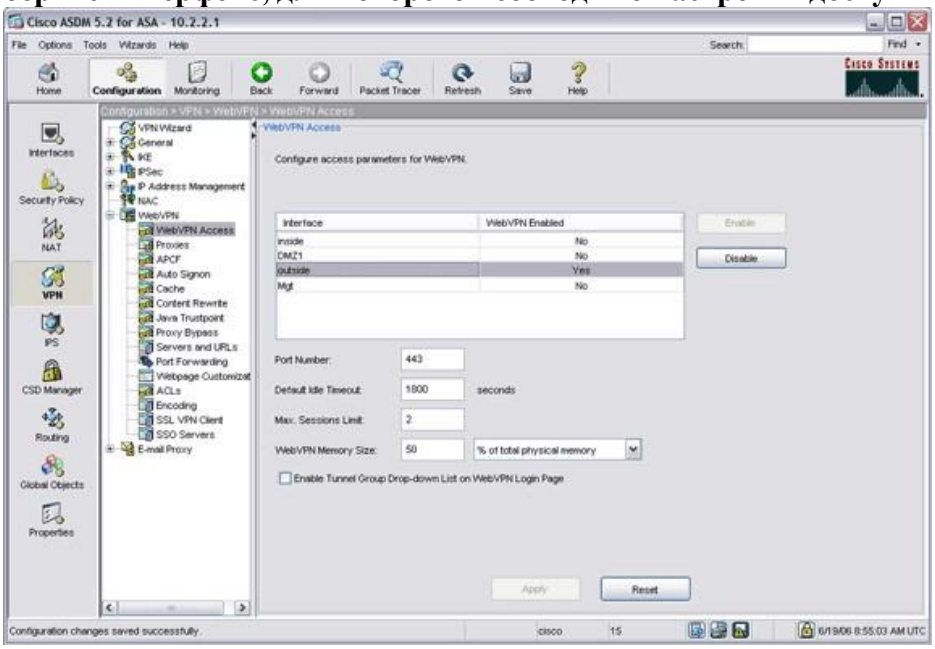
Появляется диалоговое окно "Upload Image".



5. **Нажмите Browse Local Files для выбора файла на локальном компьютере или Browse Flash для выбора файла в файловой системе флэш-диска.**
6. **Найдите файл образа клиента и нажмите OK.**
7. **Нажмите Upload File, а затем Close.**
8. **После загрузки образа клиента во флэш-память установите флажок Enable SSL VPN Client (Разрешить клиент SSL VPN) и нажмите Apply (Применить).**



Примечание: Если вы получаете сообщение об ошибках, проверяете, что включен доступ WebVPN. **В навигационной панели разверните WebVPN и выберите WebVPN Access. Выберите интерфейс, для которого необходимо настроить доступ и нажмите Enable.**

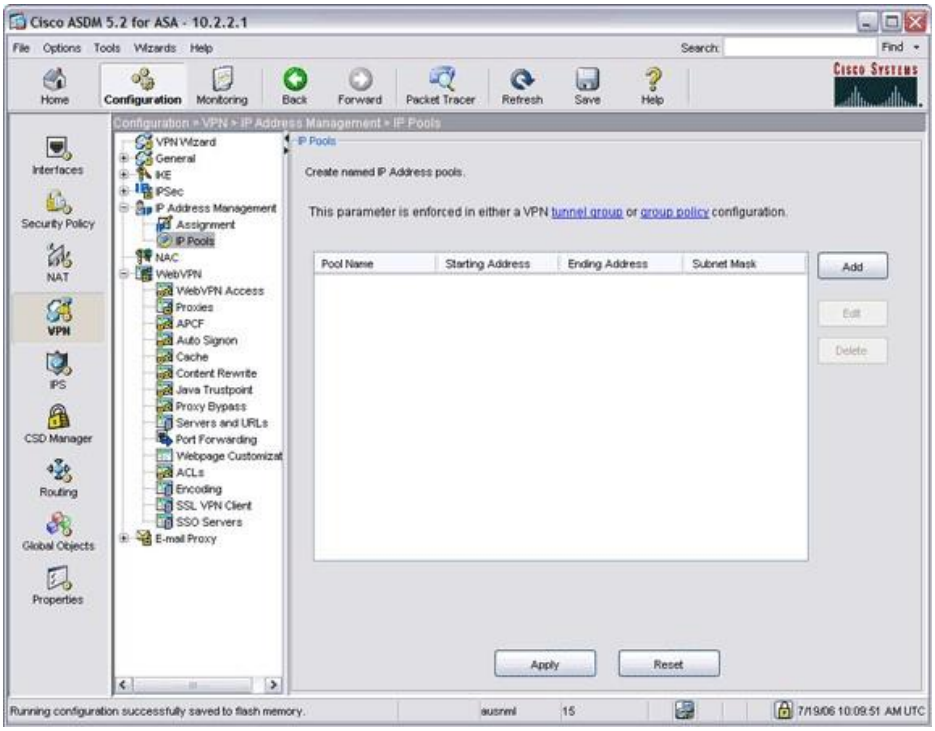


9. **Нажмите Save и Yes, чтобы принять изменения.**

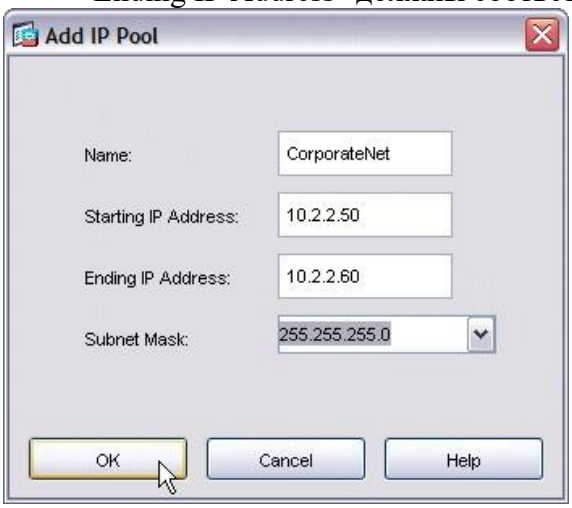
Шаг 3. Включение установки SVC на клиентах

Чтобы разрешить установку SVC на клиентах, выполните следующие действия:

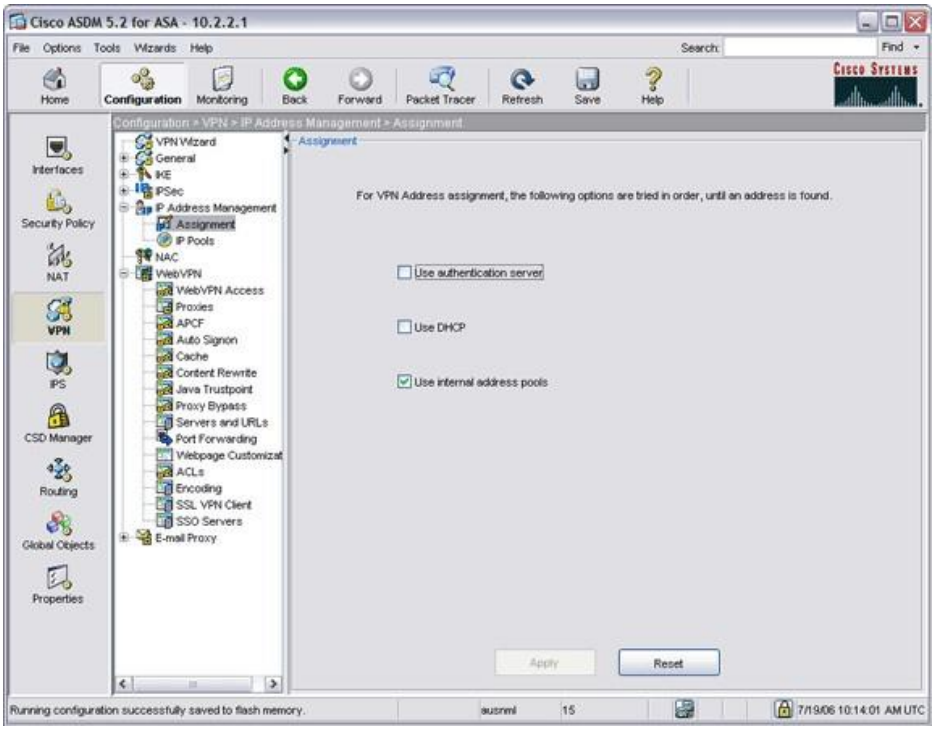
1. **В навигационной панели разверните IP Address Management и выберите IP Pools.**



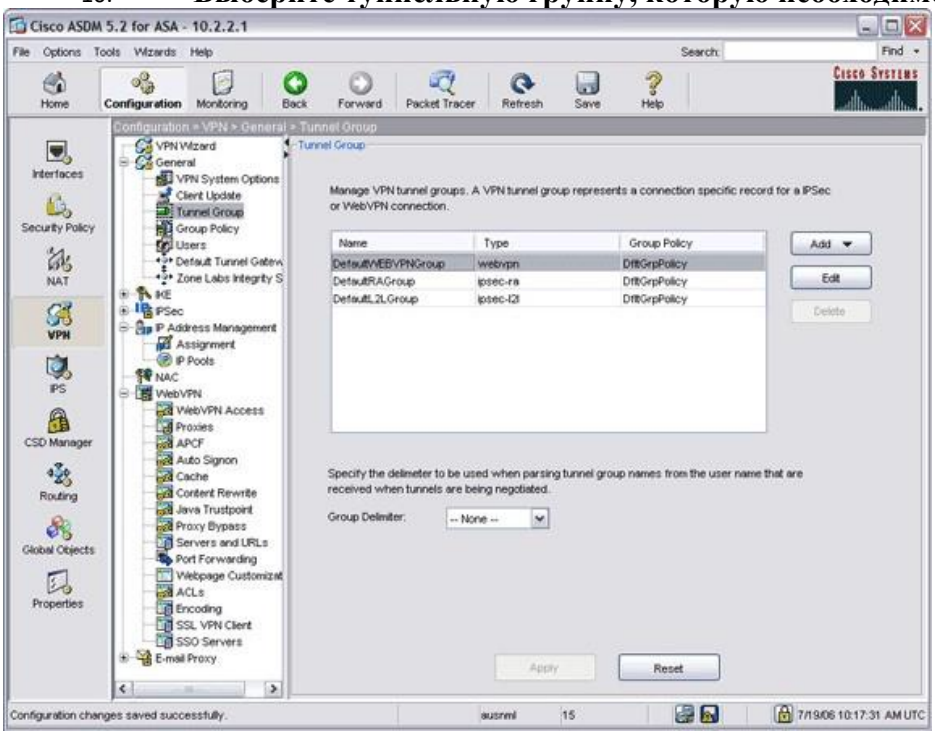
2. **Нажмите Add, введите значения в полях "Name", "Starting IP Address", "Ending IP Address" и "Subnet Mask".** IP-адреса, введенные в полях "Starting IP Address" и "Ending IP Address" должны соответствовать подсетям внутренней сети.



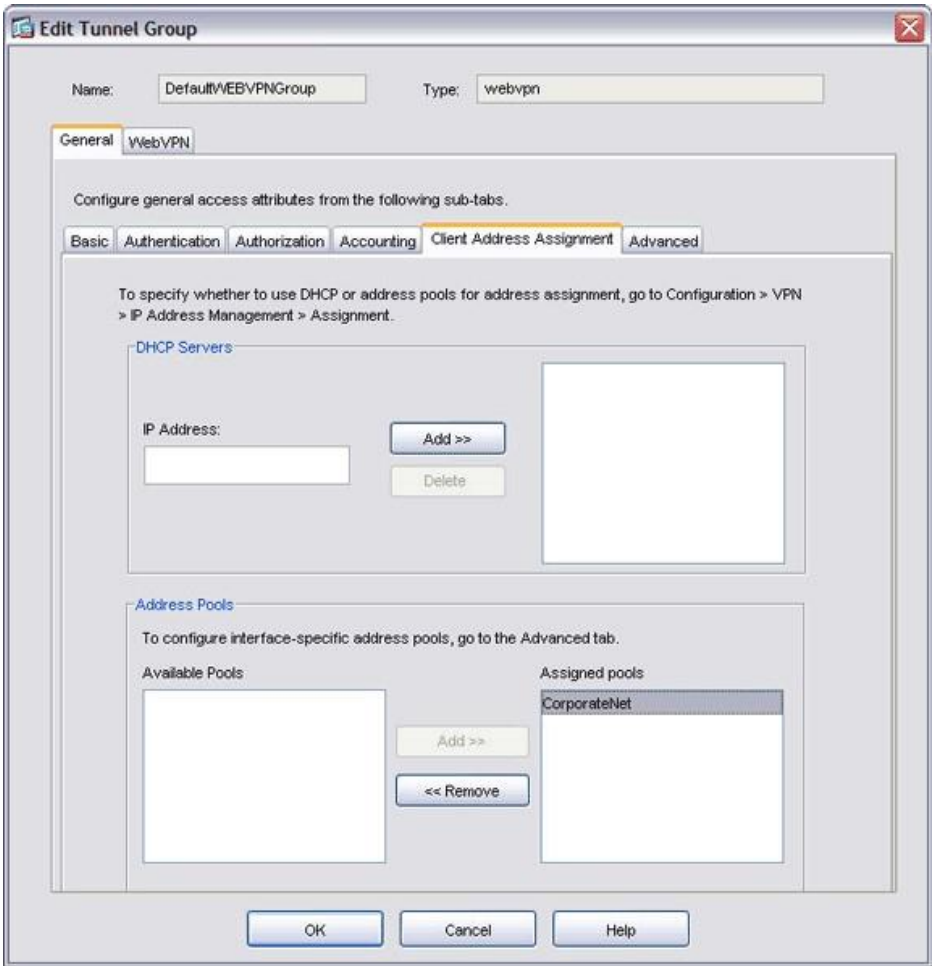
3. **Нажмите кнопку OK, а затем нажмите Apply.**
4. **Нажмите Save и Yes, чтобы принять изменения.**
5. **В навигационной панели разверните IP Address Management и выберите Assignment.**
6. **Установите флажок Use internal address pools, затем снимите флажки Use authentication server и Use DHCP.**



7. **Щелкните "Применить".**
8. **Нажмите Save и Yes, чтобы принять изменения.**
9. **В навигационной панели разверните General и выберите Tunnel Group.**
10. **Выберите туннельную группу, которую необходимо изменить и нажмите Edit.**



11. **Щелкните вкладку Client Address Assignment и выберите новый пул IP-адресов в списке "Available Pools".**

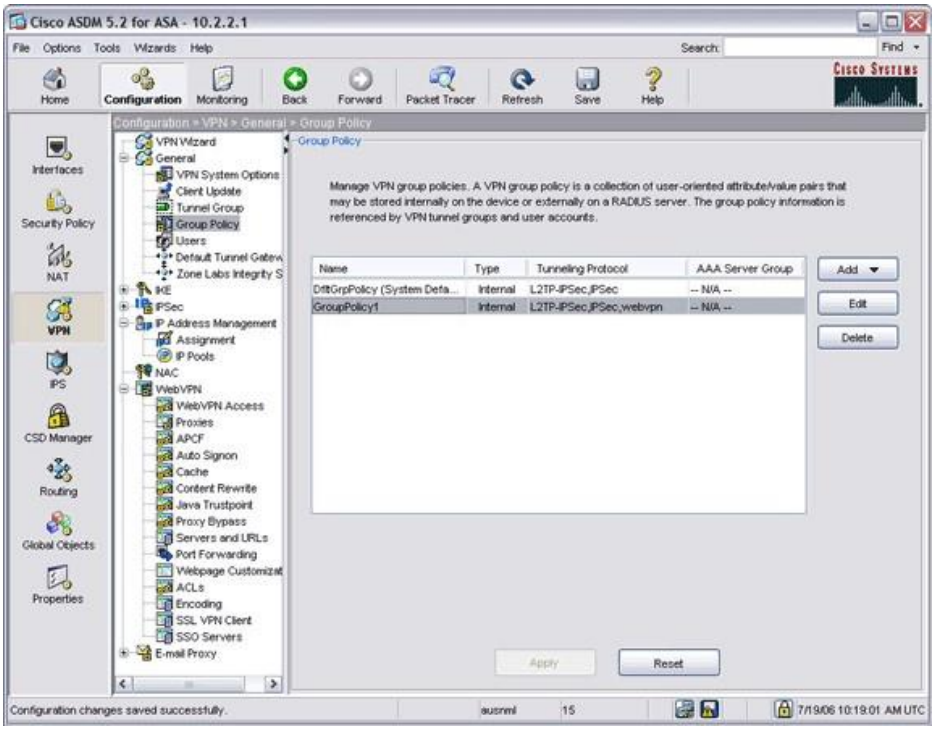


12. **Нажмите Add, а затем OK.**
13. **В окне приложения ASDM нажмите Apply.**
14. **Нажмите Save и Yes, чтобы принять изменения.**

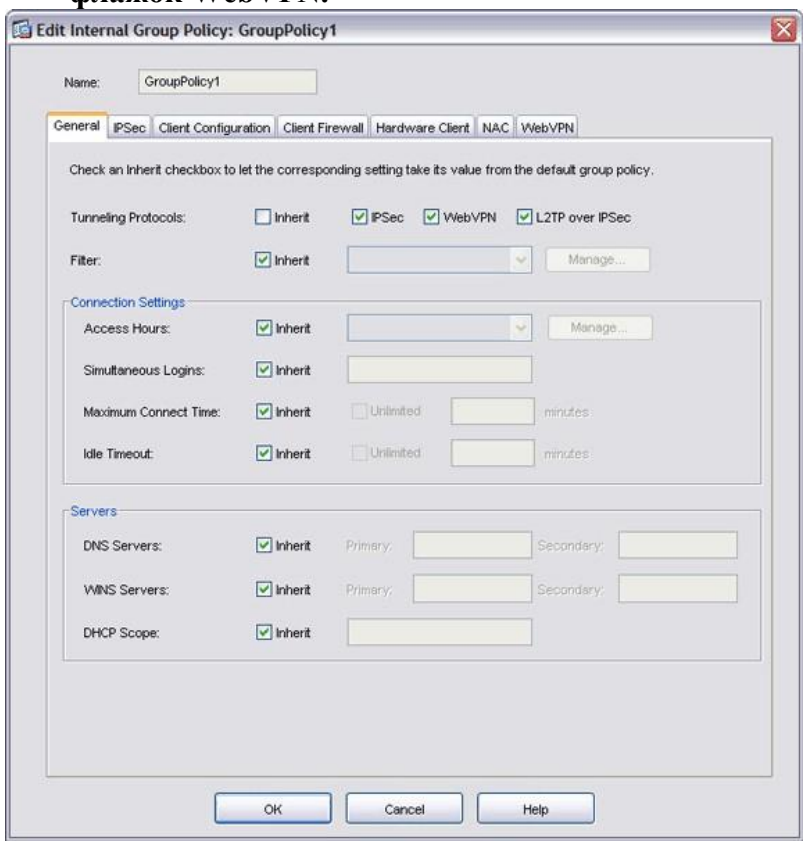
Шаг 4. Включение параметра смены ключа

Для включения повторно вводят параметры:

1. **В навигационной панели разверните General и выберите Group Policy.**
2. **Выберите политику, которую необходимо применить к этой группе клиентов и нажмите Edit.**



3. **На вкладке "General" снимите флажок Tunneling Protocols Inherit и установите флажок WebVPN.**



4. **Щелкните вкладку WebVPN, затем вкладку SSL VPN Client и выберите следующие параметры:**
   a. **В разделе "Use SSL VPN Client" снимите флажок Inherit и установите переключатель в положение Optional.**

Такой выбор позволит удаленному клиенту самому решать, следует ли загружать SVC. Выбор Always гарантирует, что SVC будет загружаться на удаленную рабочую станцию во время каждого подключения SSL VPN.

b. **В разделе "Keep Installer on Client System" снимите флажок Inherit и установите переключатель в положение Yes.**

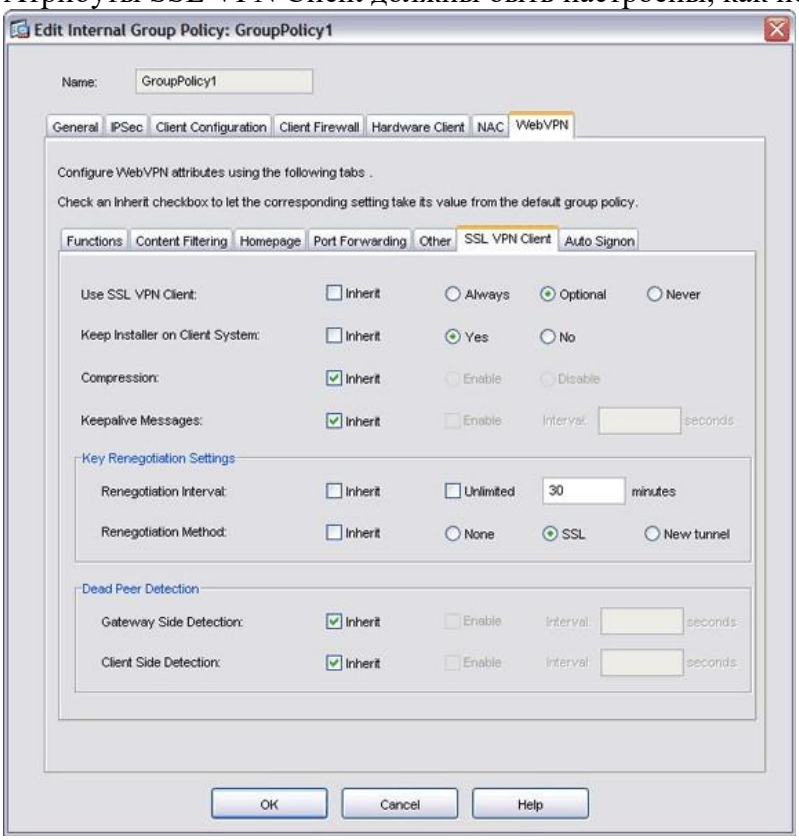
Это позволит ПО SVC оставаться на клиентской машине. Таким образом, модулю ASA не потребуется загружать ПО SVC на клиент во время каждого установления соединения. Такой выбор оптимален для удаленных пользователей, которые часто обращаются к корпоративной сети.

c. **В разделе "Renegotiation Interval" снимите флажки Inherit и Unlimited, после чего укажите время до смены ключа в минутах.**

Задание лимита времени, в течение которого действителен ключ, повышает безопасность.

d. **В разделе "Renegotiation Method" снимите флажок Inherit и установите переключатель в положение SSL.** При повторном согласовании может использоваться имеющийся туннель SSL или новый туннель, созданный специально для повторного согласования.

Атрибуты SSL VPN Client должны быть настроены, как показано на рисунке:



5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Нажмите Save и Yes, чтобы принять изменения.**

Результаты

ASDM создает следующие конфигурации командных строк:

cisco ASA

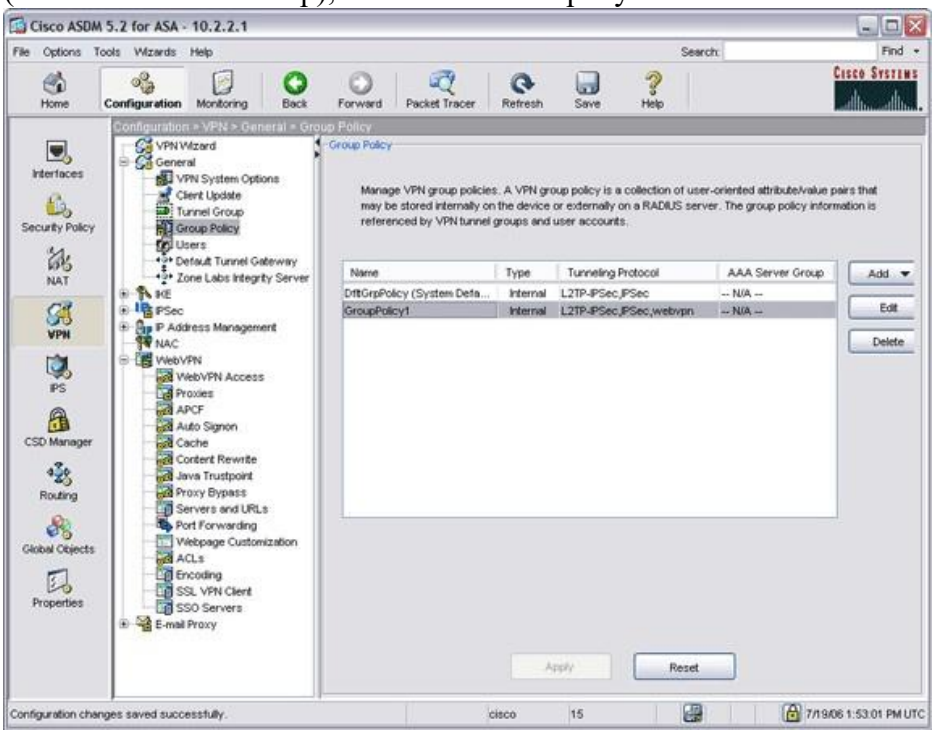
ciscoasa(config)#**show run** ASA Version 7.2(1)
! hostname ciscoasa domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names dns-guard
!
interface Ethernet0/0 nameif outside security-level 0
ip address 172.22.1.160 255.255.255.0
! interface Ethernet0/1
nameif inside

security-level 100 ip address 10.2.2.1 255.255.255.0 passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name cisco.com
no pager logging enable logging asdm informational mtu outside 1500 mtu inside 1500 mtu DMZ1 1500 mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside asdm image disk0:/asdm521.bin no asdm history enable arp timeout 14400
global (outside) 1 interface nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute ! *!--- Group Policy Statements*
group-policy GroupPolicy1 internal group-policy GroupPolicy1 attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn *!--- Enable the SVC for WebVPN*
webvpn svc enable
 svc keep-installer installed svc rekey time 30 svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable http 10.2.2.0 255.255.255.0 inside
! no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart *!--- Tunnel Group and Group Policy using the defaults here*
tunnel-group DefaultWEBVPNGroup general-attributes
address-pool CorporateNet default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa no vpn-addr-assign dhcp
! telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5 console timeout 0
! class-map inspection_default match default-inspection-traffic
! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map
 inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp

```
 inspect sip  inspect netbios  inspect tftp
! service-policy global_policy global !--- Enable webvpn and the select the
SVC client
webvpn enable outside
svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !--- Provide list
for access to resources
url-list ServerList "E-Commerce Server1" http://10.2.2.2 1 url-list ServerList
"BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable
prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

Настройка конфигурации

Процедуры, описанные в разделе Настройка SSL VPN Client на базе ASA, используют имена ASA по умолчанию для групповой политики (GroupPolicy1) и туннельной группы (DefaultWebVPNGroup), как показано на рисунке:



Эта процедура описывает создание собственных групповых политик и туннельных групп и связывание их в соответствии с политикой безопасности организации.

Чтобы настроить конфигурацию, выполните следующие действия:

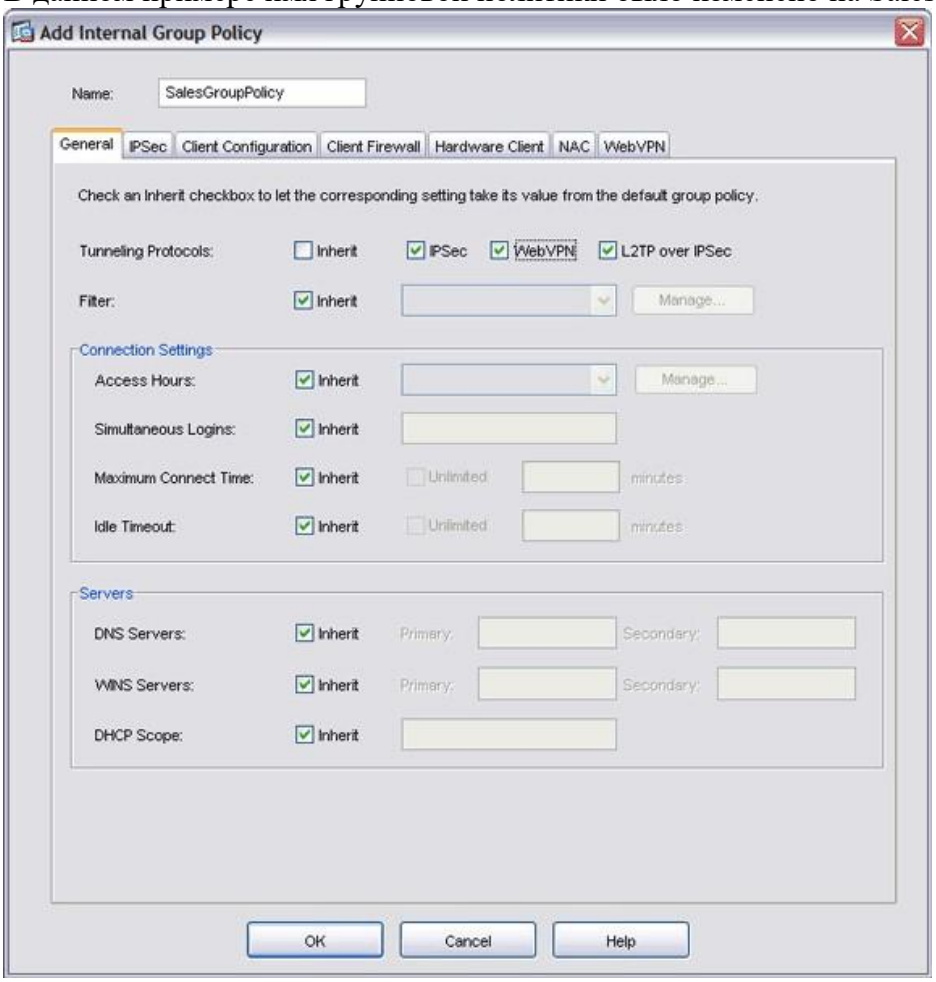
1. Создайте пользовательскую групповую политику
2. Создайте специальную туннельную группу
3. Создайте пользователя и добавьте что пользователь к вашей пользовательской групповой политике

Шаг 1. Создание специальной групповой политики

Чтобы создать специальную групповую политику, выполните следующие действия:

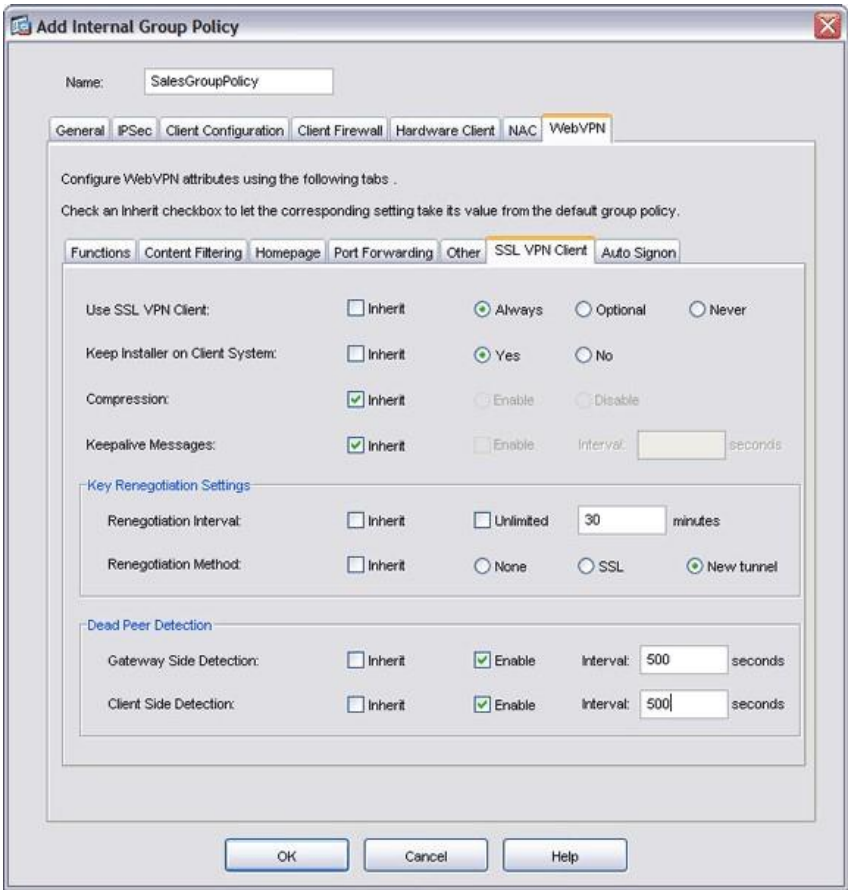
1. **Нажмите Configuration, затем VPN.**
2. **Разверните раздел General (Общее) и выберите Group Policy (Групповая политика).**
3. **Нажмите кнопку Add (Добавить) и выберите Internal Group Policy (Внутренняя групповая политика).**
4. В поле "Name" введите имя групповой политики.

В данном примере имя групповой политики было изменено на SalesGroupPolicy.



5. **На вкладке "General" снимите флажок Tunneling Protocols Inherit и установите флажок WebVPN.**
6. **Щелкните вкладку WebVPN, а затем вкладку SSLVPN Client.**

В этом диалоговом окне можно также настроить режим работы SSL VPN Client.

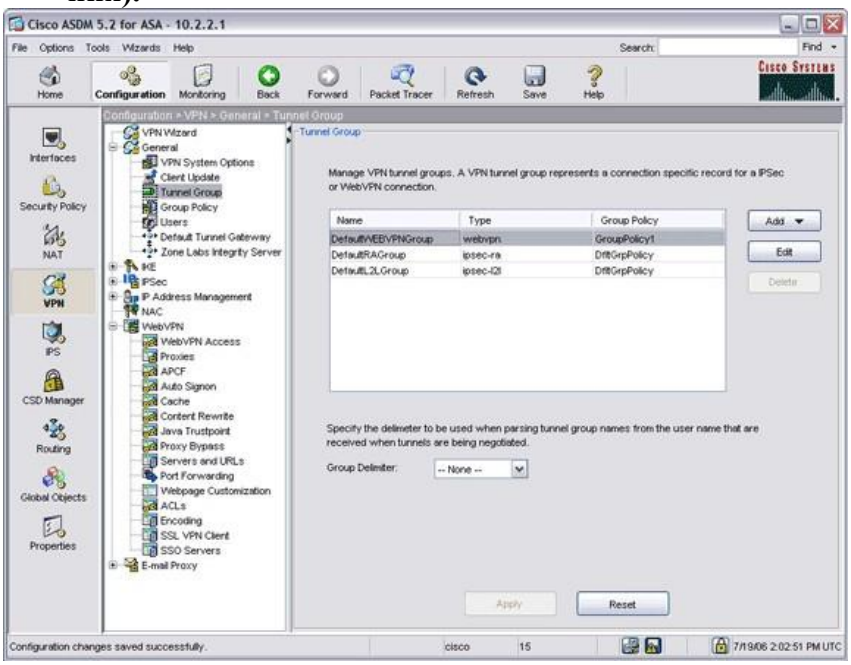


7. **Нажмите кнопку OK, а затем нажмите Apply.**
8. **Нажмите Save и Yes, чтобы принять изменения.**

Шаг 2. Создание специальной туннельной группы

Чтобы создать специальную туннельную группу, выполните следующие действия:

1. **Нажмите Configuration, затем VPN.**
2. **Разверните раздел General (Общее) и выберите Tunnel Group (Группа туннелирования).**

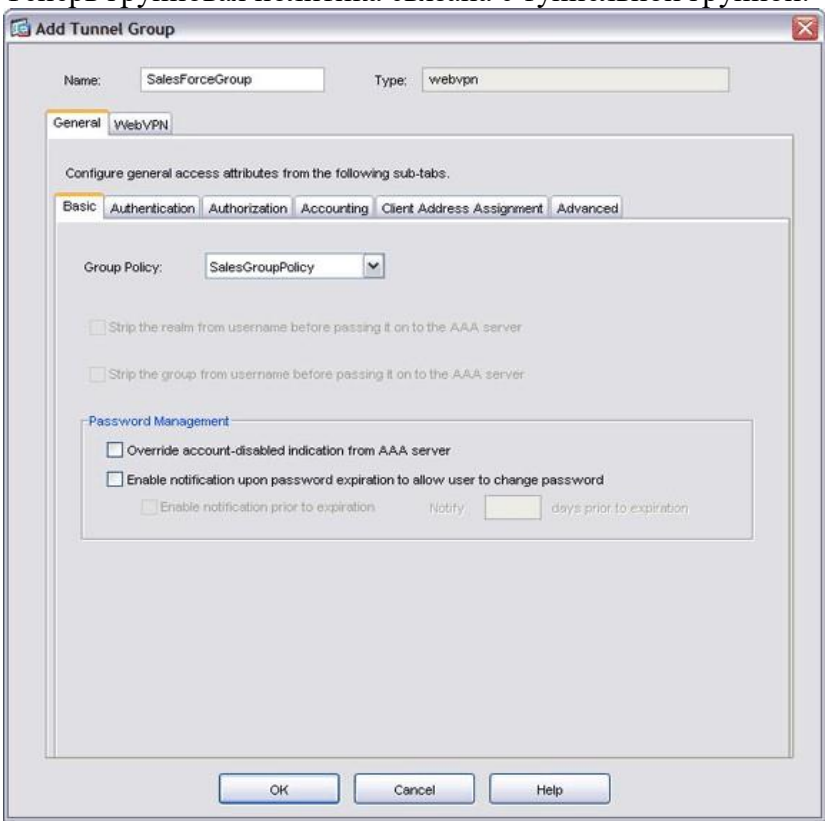


3. **Нажмите кнопку Add (Добавить) и выберите WebVPN Access (Доступ WebVPN).**
4. В поле "Name" введите имя туннельной группы.

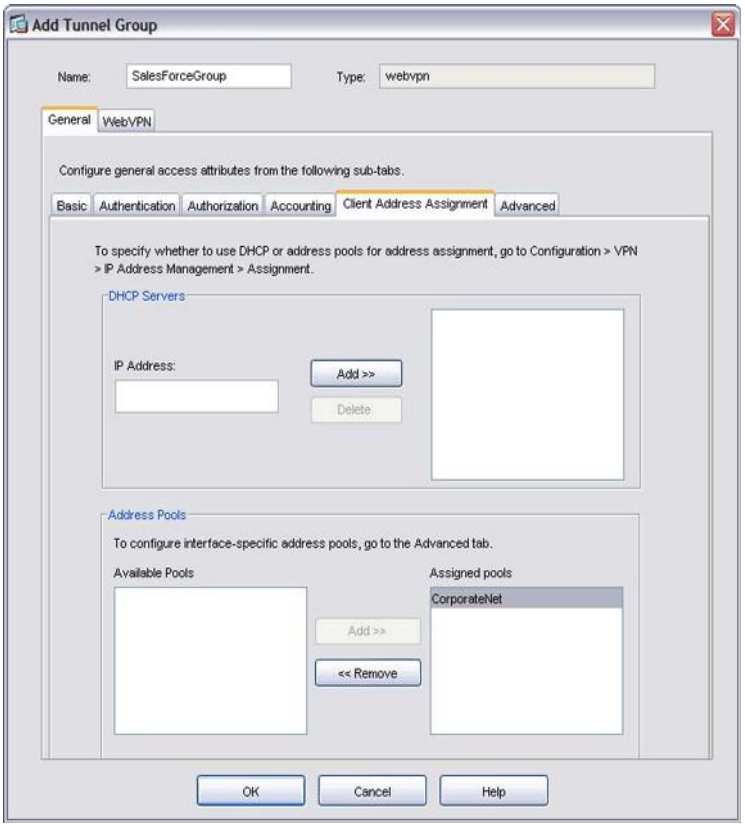
В этом примере имя туннельной группы было изменено на SalesForceGroup.

5. **Нажмите стрелку раскрывающегося списка Group Policy и выберите созданную групповую политику.**

Теперь групповая политика связана с туннельной группой.



6. **Щелкните вкладку Client Address Assignment и введите информацию о сервере DHCP или выберите созданный локально IP-пул.**

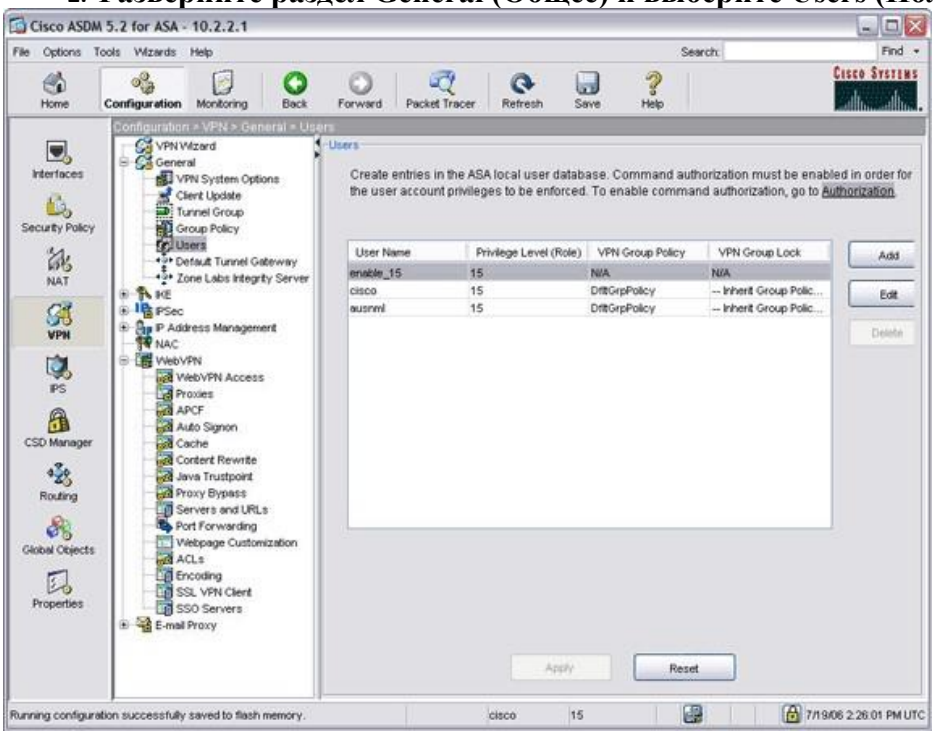


7. **Нажмите кнопку OK, а затем нажмите Apply.**
8. **Нажмите Save и Yes, чтобы принять изменения.**

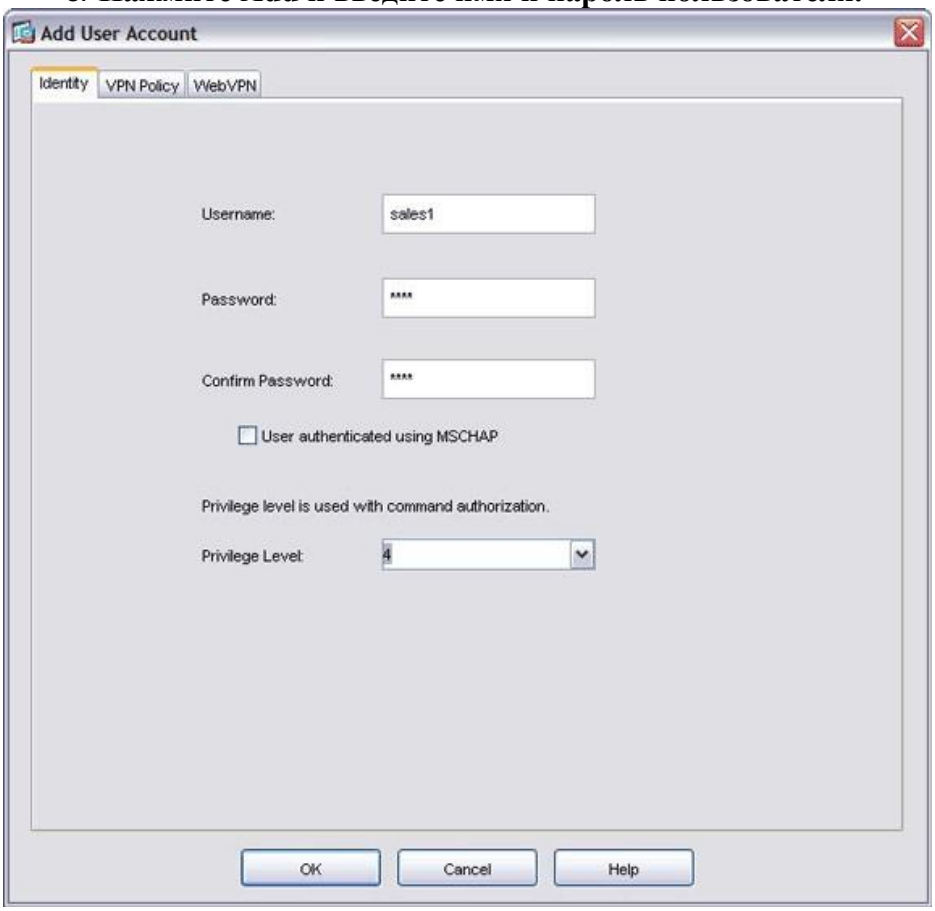
Шаг 3. Создание пользователя и добавление его в специальную групповую политику

Чтобы создать пользователя и добавить что пользователь к вашей пользовательской групповой политике, выполните эти шаги:

1. **Нажмите Configuration, затем VPN.**
2. **Разверните раздел General (Общее) и выберите Users (Пользователи).**

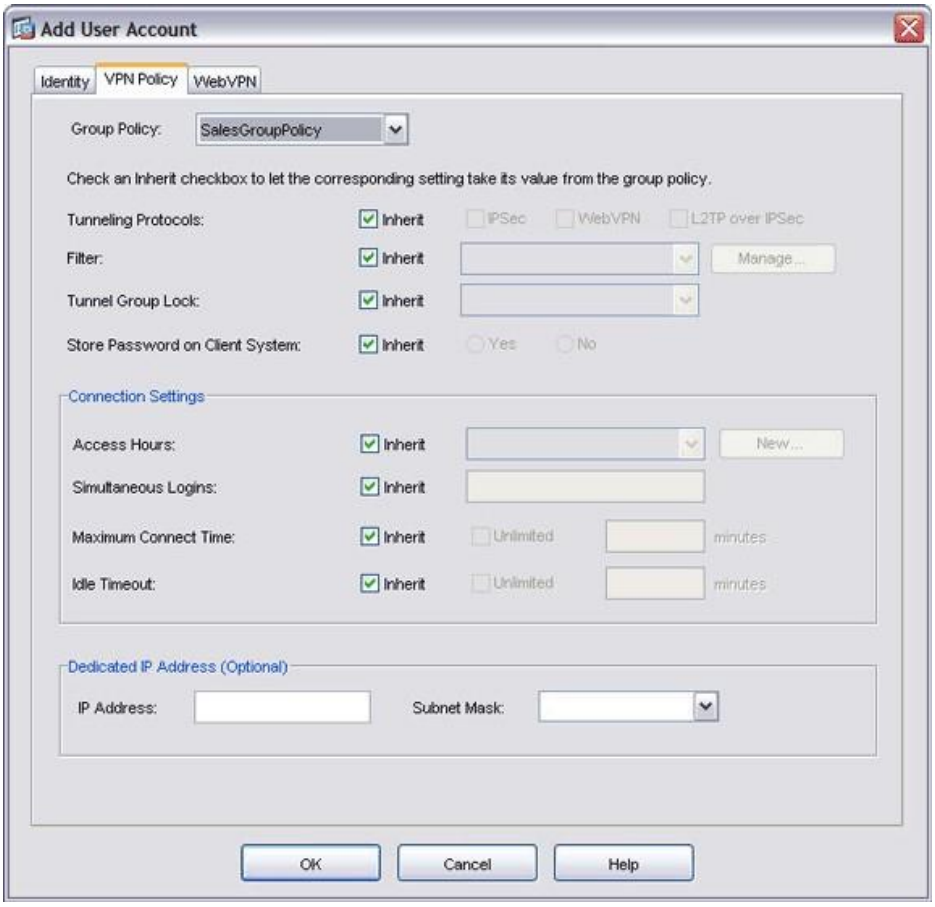


3. **Нажмите Add и введите имя и пароль пользователя.**



4. **Щелкните вкладку VPN Policy.** Убедитесь, что созданная групповая политика отображается в поле "Group Policy".

Пользователь наследует все характеристики новой групповой политики.



5. **Нажмите кнопку OK, а затем нажмите Apply.**
6. **Нажмите Save и Yes, чтобы принять изменения.**

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Аутентификация

Аутентификация для VPN-клиентов SSL (SVC) выполнена с помощью одного из этих методов:

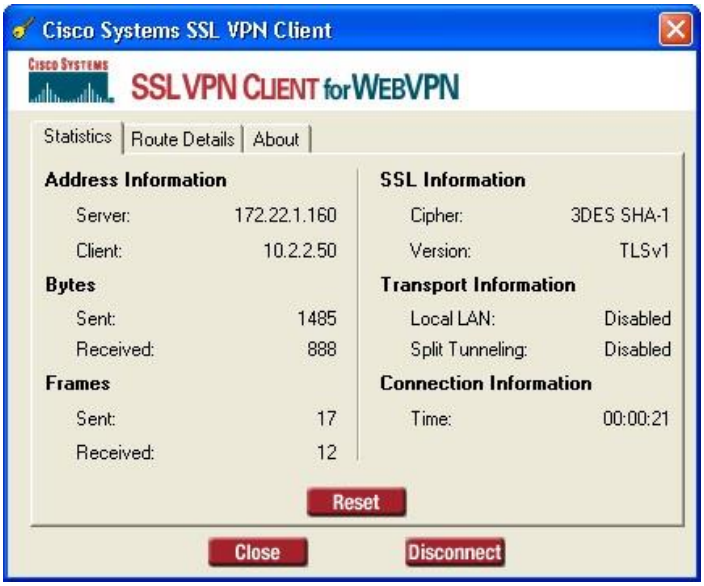
- Сервер Cisco Secure ACS (радиус)
- Домен NT
- Active Directory Разовые пароли
- Цифровые сертификаты
- Смарт-карты
- Локальная аутентификация AAA

Эта документация использует локальную учетную запись, созданную на устройстве ASA.

Примечание: Если Устройство адаптивной безопасности имеет множественные точки доверия, которые совместно используют тот же CA, только одна из этих точек доверия, которые совместно используют CA, может использоваться для проверки сертификатов пользователя.

!--- конфигурацию

Для соединения с ASA с удаленным клиентом введите **https://ASA_outside_address** в поле адреса поддерживающего SSL Webбраузера. Внешний_адрес_ASA — это внешний IP-адрес модуля ASA. Если настройка выполнена успешно, появляется окно "Cisco Systems SSL VPN Client".



Примечание: Окно Cisco Systems SSL VPN Client появляется только после принятия сертификата от ASA и после того, как VPNклиент SSL (SVC) загружен к удаленной станции. Если окно не появилось, проверьте, не свернуто ли оно.

Команды

Некоторые команды show связаны с WebVPN. Эти команды можно выполнить в интерфейсе командной строки (CLI) для отображения статистики и другой информации. Для получения дальнейшей информации о **командах показа**, обратитесь к Проверке конфигураций WebVPN.

Примечание: Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Ошибка SVC

Проблема

Вы могли бы получить это сообщение об ошибках во время аутентификации:
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires re-authentication and must be restarted manually. Close all sensitive networked applications."

Решение

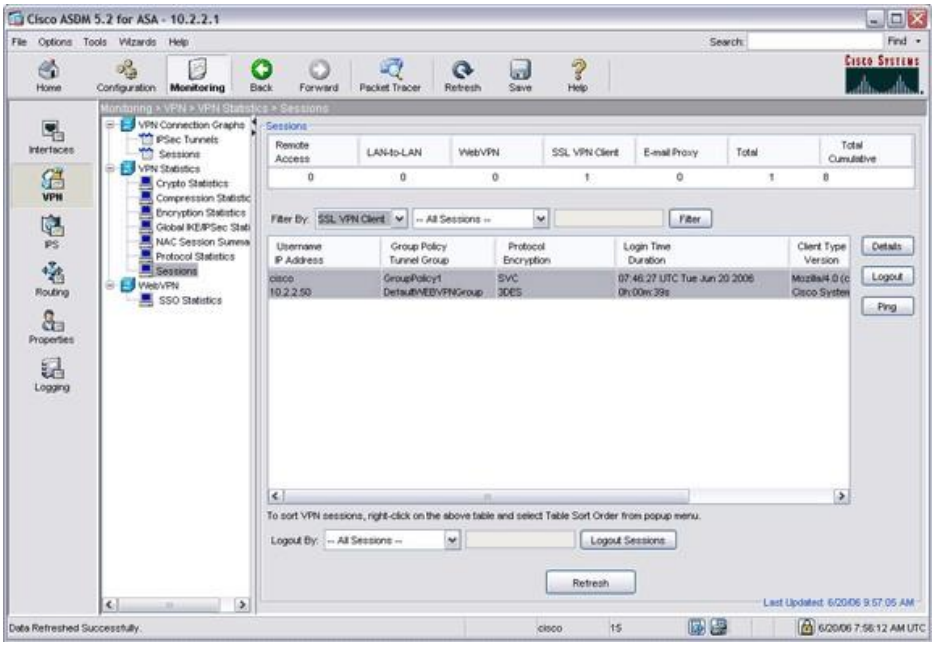
Если сервис межсетевого экрана работает на вашем ПК, он может разрушить аутентификацию. Остановите сервис и воссоедините клиента.

Установил ли клиент SVC защищенный сеанс связи с ASA?

Чтобы проверить, установлен ли защищенный сеанс связи между SSL VPN Client и ASA:

1. **Нажмите Monitoring.**
2. **Разверните VPN Statistics и выберите Sessions.**
3. **В раскрывающемся меню "Filter By" выберите SSL VPN Client и нажмите Filter.**

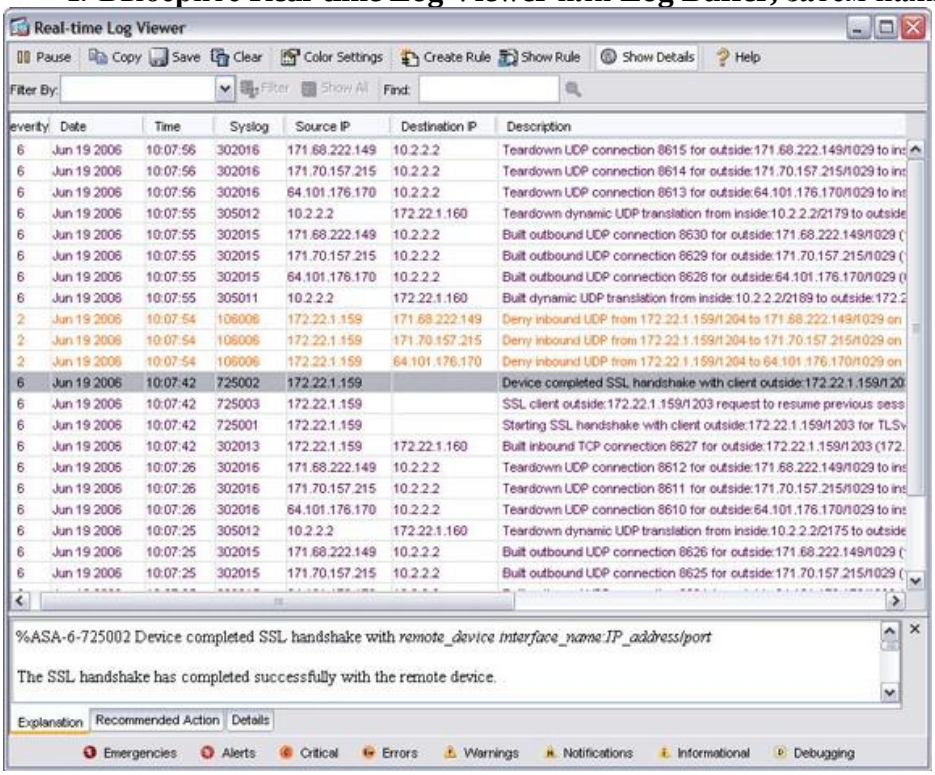
Конфигурация должна отобразиться в списке сеансов.



Успешно ли устанавливаются и завершаются защищенные сеансы?

Чтобы убедиться, что сеансы создаются и завершаются успешно, просмотрите журналы реального времени. Чтобы просмотреть журналы сеансов, выполните следующие действия:

1. **Нажмите Monitoring, а затем Logging.**
2. **Выберите Real-time Log Viewer или Log Buffer, затем нажмите View.**



Примечание: Для отображения только сеансов от точного адреса фильтруйте адресом.

Проверьте пул IP в профиле WebVPN

%ASA-3-722020: Group group User user-name IP IP_address No address available for SVC connection

Никакие адреса не доступны для присвоения на соединение SVC. Поэтому назначьте адрес пула IP в профиле.

Если вы создаете профиль нового соединения, то настраиваете псевдоним или URL группы для доступа к этому профилю подключения. В противном случае все попытки SSL поразят профиль подключения WebVPN по умолчанию, которому не связали пул IP с ним. Настройте это, чтобы использовать профиль подключения по умолчанию и поместить пул IP на него.

Советы

- Удостоверьтесь направив, работает должным образом с пулом IP-адреса, который вы назначаете на своих удаленных клиентов. Пул IP-адресов должен располагаться в подсети имеющейся локальной сети. Для назначения IP-адресов можно также использовать сервер DHCP или сервер аутентификации.
- ASA создает туннельную группу по умолчанию (DefaultWebVPNGroup) и групповую политику по умолчанию (GroupPolicy1). При создании новых групп и политики убедитесь, что применяемые значения находятся в согласии с политиками безопасности сети.
- Если вы хотите включить просмотр файлов Windows через CIFS, введите WINS (NBNS) сервер под

Конфигурацией> VPN> WebVPN> Серверы и URL. Эта технология использует выделение CIFS.

Практическая работа № 21
«Установка системы обнаружения и предотвращения вторжения Snort»

Задание:

1. Сначала необходимо установить всё необходимое программное обеспечение, чтобы облачный сервер был готов:

```
sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev \
libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev \
bison flex libdnet autoconf libtool
```

вставить скриншот с результатом.

2. Установка состоит из нескольких шагов:

Загрузка кода, его настройка, компиляция кода, установка его в соответствующих каталог и настройка правил обнаружения.

Создадим временную папку для загрузки:

```
mkdir ~/snort_src && cd ~/snort_src
```

3. Snort использует библиотеку сбора данных DAQ. Загрузите последний пакет с веб-сайта с помощью команды wget:

```
wget https://www.snort.org/downloads/snort/daq-2.0.7.tar.gz
```

4. Загрузка займёт несколько секунд. По завершении исходный код нужно извлечь из архива и перейти в новый каталог:

```
tar -xvzf daq-2.0.7.tar.gz
cd daq-2.0.7
```

вставить скриншот с результатом.

5. Последняя версия требует дополнительного шага для автоматической перенастройки DAQ перед запуском конфигурации:

```
autoreconf -f -i
```

6. После этого запустите скрипт конфигурации и скомпилируйте программу с помощью команды:

```
./configure && make && sudo make install
```

7. С установленным DAQ можно начинатать работать и вернуться в папку загрузки:

```
cd ~/snort_src
```

вставить скриншот с результатом.

8. Далее загрузите исходный код Snort с помощью wget. Перед этим зайдите на сайт, в случае наличия более поздней версии замените версию в команде загрузки:
wget https://www.snort.org/downloads/snort/snort-2.9.16.tar.gz
9. После завершения загрузки извлеките исходный код и перейдите в каталог:
tar -xvzf snort-2.9.16.tar.gz
cd snort-2.9.16
вставить скриншот с результатом.
10. Затем настройте установку с включённым sourcefire:
./configure --enable-sourcefire && make && sudo make install
11. Далее необходимо настроить Snort для системы. Для этого нужно отредактировать некоторые файлы конфигурации, загрузку правил и пробный запуск. Начнём с обновления общих библиотек:
sudo ldconfig
12. Snort устанавливается в /usr/local/bin/snort директорию, рекомендуется создать ссылку на /usr/sbin/snort.
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
вставить скриншот с результатом.
13. Для безопасного запуска Snort без доступа root нужно создать нового непривилегированного пользователя и новую группу пользователей для запуска демона
sudo groupadd snort
sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
14. Затем создайте папки для размещения конфигураций Snort:
sudo mkdir -p /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules
15. Установите разрешения для новых папок:
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
16. Создайте новые файлы для белых и чёрных списков и локальные правила:
sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules
17. Затем скопируйте конфигурационный файл из папки загрузки:
sudo cp ~/snort_src/snort-2.9.16/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-2.9.16/etc/*.map /etc/snort
вставить скриншот с результатом.
Затем нужно загрузить правила обнаружения, которыми Snort будет следовать для выявления потенциальных угроз. Snort предоставляет три уровня набора правил:
- ✓ Community rules are freely available although slightly limited.
- ✓ By registering for free on their website you get access to your Oink code, which lets you download the registered users rule sets.
- ✓ Lastly, subscriber rules are just that, available to users with an active subscription to Snort services.

18. Для быстрого тестирования Snort можно скачать правила:
wget https://www.snort.org/rules/community -O ~/community.tar.gz
19. Извлекаем правила и копируем в конфигурационную папку:
sudo tar -xvf ~/community.tar.gz -C ~/
sudo cp ~/community-rules/* /etc/snort/rules
вставить скриншот с результатом.

20. По умолчанию Snort ожидает некоторые правила, которые не включены в файл правил. С помощью следующей команды можно закомментировать ненужные строки в файле правил:
sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf
21. Далее вам нужно зарегистрироваться на сайте Snort, зайти на него под своим аккаунтом, открыть данные своего аккаунта, перейти в Oinkcode, скопировать данный код и в следующую команду его вставить:
wget https://www.snort.org/rules/snortrules-snapshot-29160.tar.gz?oinkcode=oinkcode -O ~/registered.tar.gz
вставить скриншот с результатом.
22. Регистрация нужна для загрузки правил. Далее распаковываем в папку:
sudo tar -xvf ~/registered.tar.gz -C /etc/snort
23. После установки отредактируем конфигурационный файл:
sudo nano /etc/snort/snort.conf
24. Найдите разделы, которые указаны ниже и измените параметры по образцу:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.2.15/24
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules
```

25. В шестом разделе измените следующее:
unified2
Recommended for most installs
output unified2: filename snort.log, limit 128
вставить скриншот с результатом.
26. Далее найдите список включённых наборов правил. Раскомментируйте следующую строку для возможности загружать пользовательские правила:
include $RULE_PATH/local.rules
27. Также можно добавить строку:
include $RULE_PATH/community.rules
28. Сохраните и выйдите.
вставить скриншот с результатом.
29. Проверьте конфигурацию:
sudo snort -T -c /etc/snort/snort.conf
30. После запуска проверки должен появиться текст похожий на:

```
--== Initialization Complete ==--
,,_     -*> Snort! <*-
o"  )~   Version 2.9.16 GRE (Build 118)
""    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2020 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.8.1
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.2.11
Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1
Preprocessor Object: SF_DCERPC2  Version 1.0
Preprocessor Object: SF_SSH  Version 1.1
Preprocessor Object: SF_FTPTELNET  Version 1.2
```

```
Preprocessor Object: SF_SDF  Version 1.1
Preprocessor Object: SF_DNP3  Version 1.1
Preprocessor Object: SF_REPUTATION  Version 1.1
Preprocessor Object: SF_IMAP  Version 1.0
Preprocessor Object: SF_SMTP  Version 1.1
Preprocessor Object: SF_GTP  Version 1.1
Preprocessor Object: appid  Version 1.1
Preprocessor Object: SF_MODBUS  Version 1.1
Preprocessor Object: SF_POP  Version 1.0
Preprocessor Object: SF_DNS  Version 1.1
Preprocessor Object: SF_SSLPP  Version 1.1
Preprocessor Object: SF_SIP  Version 1.1
```

В случае возникновения ошибок читаем ошибки, ищем где и исправляем. Чаще всего это отсутствие папок/файлов.

вставить скриншот с результатом.

Практическая работа № 22
«Настройка системы обнаружения и предотвращения вторжения Snort»

Задание:

1. Для проверки Snort на регистрацию предупреждений добавьте предупреждение:
2. sudo nano /etc/snort/rules/local.rules
3. Следующую строку в файл:
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:10000001; rev:001;)
вставить скриншот с результатом.
4. Правило состоит из следующих частей:
   - ✓ action for traffic matching the rule, alert in this case
   - ✓ traffic protocol like TCP, UDP or ICMP like here
   - ✓ the source address and port, simply marked as any to include all addresses and ports
   - ✓ the destination address and port, $HOME_NET as declared in the configuration and any for port
   - ✓ some additional bits
   - ✓ log message
   - ✓ unique rule identifier (sid) which for local rules needs to be 1000001 or higher
   - ✓ rule version number.

Сохраните, выйдите.
5. Запустите Snort с опциями печати предупреждений. Нужно будет правильно выбрать сетевой интерфейс.
sudo snort -A console -i eth0 -u snort -g snort -c /etc/snort/snort.conf
Для проверки интерфейса можно воспользоваться командой:
ip addr
С включённым Snort при пинге вашего сервера вы должны увидеть уведомление для каждого ICMP-вызова в терминале.
07/12-11:20:33.501624 [**] [1:10000001:1] ICMP test [**] [Priority: 0] {ICMP} 83.136.252.119 -> 80.69.173.202
После появления предупреждений вы можете остановить их Ctrl+C. Все предупреждения записываются в журнал /var/log/snort/snort.log.timestamp.
6. Прочитать логи можно с помощью команды внизу:
snort -r /var/log/snort/snort.log.
вставить скриншот с результатом.
7. Для запуска snort в фоновом режиме в качестве службы нужно отредактировать следующий файл:

```
sudo nano /lib/systemd/system/snort.service
Введите следующее:
[Unit]
Description=Snort NIDS Daemon
After=syslog.target network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/snort -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

[Install]
WantedBy=multi-user.target
```

Следующей командой перезагрузите демон systemctl:
sudo systemctl daemon-reload

8. Затем выполните старт snort:
sudo systemctl start snort
9. Увидеть статус можно следующей командой:
sudo systemctl status snort
вставить скриншот с результатом.
Система обнаружения вторжений установлена и протестирована.
Задание 2:
Ответьте на следующие вопросы:
- ✓ Из каких частей состоит правило (п.33)?
- ✓ Какие три условия предоставляет Snort для создания правил?

Ответы:

Практическая работа № 23
«Установка MySQL для работы со Snort»

Задание:

1. Установите зависимости для Barnyard:
Сначала нужно установить некоторые библиотеки и приложения, от которых зависит Barnyard2.
ubuntu> sudo apt-get install -y mysql-server libmysqlclient-dev mysql-client autoconf libtool

```
@ubuntu:~$ sudo apt-get install -y mysql-server libmysqlclient-dev mysql-cl
ient autoconf libtool
```

ubuntu> sudo apt-get install libpcap-dev libmysql-dev libprelude-dev

```
@ubuntu:/$ sudo apt-get install libpcap-dev libmysql-dev libprelude-dev
```

вставить скриншот с результатом.

2. Установите Git:
Мы скачаем и установим последнюю версию Barnyard2 с GitHub. Если у вас еще нет git в вашей системе, то вам нужно будет установить его сейчас.
ubuntu> sudo apt-get update
ubuntu> sudo apt-get install git

Вставьте скриншот с результатом установки.
3. Редактирование конфигурационного файла Snort:
Чтобы направлять наши предупреждения в базу данных, нам нужно отредактировать файл snort.conf. Откройте его с помощью любого текстового редактора и перейдите в раздел вывода (раздел #6). Там мы скажем Snort использовать нашу базу данных MySQL (которую мы создадим позже в этой статье с указанием имени пользователя и пароля, которые вы выберете).
В этом примере мы выбрали простые названия для имени базы данных, пользователя и пароля — все snort.

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output
Modules
##################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp,
mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

output database log,mysql, user=snort password=snort dbname=snort
host=localhost
```

вставить скриншот с результатом.

Практическая работа № 24
«Запись предупреждений о вторжениях в MySQL»

Задание:

1. Скачайте Barnyard2:

Barnyard2 — это диспетчер очереди печати, который уменьшает потребление ресурсов демоном Snort. Он позволяет Snort записывать все предупреждения в более эффективном бинарном виде, а затем Barnyard2 берет эти бинарные файлы и преобразует их в удобную для человека форму. Наконец, он записывает их в базу данных MySQL для последующего анализа.

ubuntu> git clone git://github.com/firnsy/barnyard2.git

```
    @ubuntu:~$ git clone git://github.com/firnsy/barnyard2.git
Cloning into 'barnyard2'...
remote: Counting objects: 1246, done.
remote: Total 1246 (delta 0), reused 0 (delta 0), pack-reused 1246
Receiving objects: 100% (1246/1246), 1.16 MiB | 642.00 KiB/s, done.
Resolving deltas: 100% (835/835), done.
Checking connectivity... done.
keith@ubuntu:~$
```

Теперь проверим, скачался и установился ли он, выполнив следующую команду в этом каталоге

ubuntu> ls -l

```
drwxrwxr-x 10          4096 Apr 12 13:23 barnyard2
drwxr-xr-x 17          4096 Mar  2 15:45 Desktop
drwxr-xr-x  2          4096 Jan  5 10:16 Documents
drwxr-xr-x  6          4096 Feb 24 14:48 Downloads
-rw-r--r--  1          8980 Jan  5 09:55 examples.desktop
drwxr-xr-x  2          4096 Jan  5 10:16 Music
drwxr-xr-x  2          4096 Jan  5 10:16 Pictures
drwxr-xr-x  2          4096 Jan  5 10:16 Public
drwxr-xr-x  2          4096 Jan  5 10:16 Templates
drwxr-xr-x  2          4096 Jan  5 10:16 Videos
```

Вставьте скриншот с командами.

Как вы можете видеть, он создал каталог с именем barnyard2. Перейдем в него и посмотрим на его содержимое.

ubuntu> cd barnyard2

ubuntu> ls -l

```
-rwxrwxr-x 1           471 Apr 12 13:23 autogen.sh
-rw-rw-r-- 1         34200 Apr 12 13:23 configure.ac
-rw-rw-r-- 1         20997 Apr 12 13:23 COPYING
drwxrwxr-x 2          4096 Apr 12 13:23 doc
drwxrwxr-x 2          4096 Apr 12 13:23 etc
-rw-rw-r-- 1         17987 Apr 12 13:23 LICENSE
drwxrwxr-x 2          4096 Apr 12 13:23 m4
-rw-rw-r-- 1           212 Apr 12 13:23 Makefile.am
-rw-rw-r-- 1          7266 Apr 12 13:23 README
-rw-rw-r-- 1         13144 Apr 12 13:23 RELEASE.NOTES
drwxrwxr-x 2          4096 Apr 12 13:23 rpm
drwxrwxr-x 2          4096 Apr 12 13:23 schemas
drwxrwxr-x 5          4096 Apr 12 13:23 src
drwxrwxr-x 2          4096 Apr 12 13:23 tools
```

Обратите внимание на первый файл с именем autogen.sh. Выполним этот скрипт

ubuntu> ./autogen.sh

```
     @ubuntu:~/barnyard2$ ./autogen.sh
Found libtoolize
libtoolize: putting auxiliary files in `.'.
libtoolize: copying file `./ltmain.sh'
libtoolize: putting macros in AC_CONFIG_MACRO_DIR, `m4'.
libtoolize: copying file `m4/libtool.m4'
libtoolize: copying file `m4/ltoptions.m4'
libtoolize: copying file `m4/ltsugar.m4'
libtoolize: copying file `m4/ltversion.m4'
libtoolize: copying file `m4/lt~obsolete.m4'
autoreconf: Entering directory `.'
autoreconf: configure.ac: not using Gettext
autoreconf: running: aclocal --force -I m4
```

Вставьте скриншот с командами.

Затем введите в консоли следующую строку
ubuntu> CFLAGS = '-lpthread'
Затем запустите соответствующую команду configure для вашей системы.
Если вы используете 64-битную архитектуру, то команда configure будет выглядеть следующим образом:
ubuntu> ./configure --with-mysql-libraries=/usr/lib/x86_64-linux-gnu --prefix=$HOME/barnyard2-install
Если вы используете 32-битную архитектуру, то команда configure немного изменится на такую:
ubuntu > ./configure --with-mysql-libraries=/usr/lib/i386-linux-gnu --prefix=$HOME/barnyard2-install

```
keith@ubuntu:~/barnyard2$ ./configure --with-mysql-libraries=/usr/lib/x86_64-lin
ux-gnu --prefix=$HOME/barnyard2-install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for style of include used by make... GNU
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
```

Есть еще одна библиотека, которая нужна Ubuntu для запуска Barnyard2, она называется libdumbnet-dev. Давайте возьмем ее из репозиториев.
sudo apt-get install libdumbnet-dev
Поскольку скрипт make для Barnyard2 ожидает, что у нас есть файл зависимости с именем dnet.h, нам нужно создать символическую ссылку на dumbnet.h, которую мы назовем dnet.h (с момента написания скрипта имена файлов были изменены).
ubuntu> ln -s /usr/include/dumbnet.h /usr/include/dnet.h
Затем обновите библиотеки.
ubuntu> sudo ldconfig
Теперь мы можем выполнить команду make для Barnyard2.
ubuntu> make

```
keith@ubuntu:/snort_source/barnyard2$ make
make  all-recursive
make[1]: Entering directory `/snort_source/barnyard2'
Making all in src
make[2]: Entering directory `/snort_source/barnyard2/src'
Making all in sfutil
make[3]: Entering directory `/snort_source/barnyard2/src/sfutil'
make[3]: Nothing to be done for `all'.
make[3]: Leaving directory `/snort_source/barnyard2/src/sfutil'
Making all in output-plugins
```

Наконец, нам нужно выполнить команды make и install.
ubuntu> sudo make install

Вставьте скриншот с командами.

2. Конфигурирование Barnyard2:

Нам нужно сделать базовую конфигурацию Barnyard2, чтобы убедиться, что он работает правильно. Сначала скопируем файл конфигурации Barnyard2 в директорию /etc/snort
ubuntu > sudo cp /snort_source /etc/barnyard2.conf /etc/snort
Теперь создадим файл, который будет нужен Barnyard2 в каталоге /var/log. Это файл закладок
ubuntu > touch /var/log/snort/barnyard2.waldo

```
@ubuntu:/etc$ sudo cp /snort_source/barnyard2/etc/barnyard2.conf /etc/snort
@ubuntu:/etc$ touch /var/log/snort/barnyard2.waldo
```

Вставьте скриншот с командами.

3. Установка MySQL:

Теперь, когда Barnyard2 установлен, скомпилирован и настроен, нужно установить MySQL, куда будут записываться все предупреждения. Для этого нам необходимо:

- ✓ создать базу данных
- ✓ создать схему базы данных для предупреждений
- ✓ создать пользователя
- ✓ предоставить пользователю соответствующие права

Начнем с входа в систему базы данных MySQL
ubuntu> sudo mysql -u root -p
При запросе пароля введите snort.

```
    @ubuntu:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 48
Server version: 5.5.47-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2015, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Вы находитесь в системе MySQL и должны видеть приглашение командной строки MySQL. Создадим базу данных для использования системы Snort.
mysql > create database snort;

(Обратите внимание, что snort здесь просто имя базы данных, в которой мы будем хранить полученные предупреждения. Ее можно назвать как угодно, но давайте назовем ее так, чтобы было просто запомнить).
Теперь скажем системе, что хотим использовать эту базу данных.
mysql > use snort;

```
mysql> create database snort
    -> ;
Query OK, 1 row affected (7.18 sec)

mysql> use snort;
Database changed
mysql>
```

Вставьте скриншот с командами.

Barnyard2 поставляется вместе со скриптом для создания схемы базы данных для Snort. Он находится в /snort_source/barnyard2/schemas/create_mysql. Мы можем запустить этот скрипт, набрав:
mysql > /snort_source/barnyard2/schemas/create_mysql

```
mysql> source /snort_source/barnyard2/schemas/create_mysql
Query OK, 0 rows affected (1.21 sec)

Query OK, 1 row affected (0.16 sec)

Query OK, 0 rows affected (0.21 sec)

Query OK, 0 rows affected (0.19 sec)

Query OK, 0 rows affected (0.15 sec)

Query OK, 0 rows affected (0.22 sec)

Query OK, 0 rows affected (0.15 sec)

Query OK, 0 rows affected (0.19 sec)

Query OK, 0 rows affected (0.08 sec)

Query OK, 0 rows affected (0.14 sec)

Query OK, 0 rows affected (0.17 sec)
```

Затем нам нужно создать в MySQL пользователя базы данных snort.
mysql > CREATE USER 'snort'@'localhost' IDENTIFIED BY 'snort';
Эта команда создает пользователя snort на сервере localhost, который использует пароль snort. Имя пользователя и пароль могут отличаться, но они должны соответствовать тому, что вы ввели в файле snort.conf на шаге 3 (выше).
Теперь, нужно предоставить этому пользователю необходимые права
mysql > grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';
Это дает пользователю snort права на создание (create) объектов, вставку (insert) данных, выбор (select) данных, удаление (delete) данных и обновление (update) данных в базе данных snort на локальном сервере (localhost).

```
mysql> CREATE USER 'snort'@'localhost' IDENTIFIED BY 'snort'
    -> ;
Query OK, 0 rows affected (0.40 sec)

mysql> grant create,insert,select,delete, update on snort.* to 'snort'@'localhos
t';
Query OK, 0 rows affected (0.04 sec)

mysql>
```

Вставьте скриншот с командами.

Практическая работа № 25
«Установка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort»

Задание:

1. Обновим список пакетов и обновим установленные пакеты:
sudo apt update
sudo apt upgrade –y
Вставьте скриншот об успешном обновлении.
Вставьте скриншот с командами.
2. Import the GPG key and add the PPA repository:
sudo apt -y install lsb-release apt-transport-https ca-certificates
sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
3. Then add repository
echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list
4. Проверьте версию php:
php –v
Вставьте скриншот с версией php
Вставьте скриншот с командами.
5. Установить пакет:
sudo apt-get install -y php-pear
Затем:
sudo pear install -f --alldeps Image_Graph
Для установки других расширений php:
sudo apt-get install php7.4-{cli,json,imap,bcmath,bz2,intl,gd,mbstring,mysql,zip}
вставить скриншот с успешной установкой.
6. Загружаем библиотеку ADODB:
wget https://sourceforge.net/projects/adodb/files/adodb-php5-only/adodb-520-for-php5/adodb-5.20.8.tar.gz
tar -xvzf adodb-5.20.8.tar.gz
sudo mv adodb5 /var/adodb
sudo chmod -R 755 /var/adodb
Вставьте скриншот с командами.

Практическая работа № 26
«Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort»

Задание:

1. Загружаем BASE:
wget http://sourceforge.net/projects/secureideas/files/BASE/base-1.4.5/base-1.4.5.tar.gz
tar xzvf base-1.4.5.tar.gz
sudo mv base-1.4.5 /var/www/html/base/
Вставьте скриншот с командами.
2. Копируем конфигурационный файл:
cd /var/www/html/base
sudo cp base_conf.php.dist base_conf.php
3. И приводим некоторые строки в файле /var/www/html/base/base_conf.php к образцам:
$BASE_urlpath = '/base';

$DBlib_path   = '/var/adodb/';
$alert_dbname   = 'snort';
$alert_host   = 'localhost';
$alert_port   = '';
$alert_user   = 'snort';
$alert_password = 'snortpass';
4. необходимо изменить права, чтобы никто не увидел пароль в файле:
sudo chown -R www-data:www-data /var/www/html/base
sudo chown -R www-data:www-data /var/www/html/base
5. Перезапуск apache2:
/etc/init.d/apache2 restart
вставьте скриншот.
6. Запустите браузер. Вставьте в него:
http://localhost/base/base_main.php
Вставьте скриншот с входом в веб-интерфейс.

Практическая работа № 27
Использование стандартных правил для Snort

Задание:

Создать следующие правила, показанные в примерах:
1. gid
Ключевое слово gid (generator id) используется для идентификации того, какая часть Snort генерирует событие, когда срабатывает конкретное правило. Например, gid равный 1 ассоциируется с подсистемой правил, а различные gid свыше 100 предназначены для определённых препроцессоров и декодеров. Опция gid является необязательной, и если она не определена в правиле, то по умолчанию она устанавливается равной 1, и правило будет являться частью общей подсистемы правил. Чтобы избежать потенциальных конфликтов с gid, определёнными в Snort, рекомендуется использовать значения начиная с 1000000. Для общих правил не рекомендуется использовать ключевое слово gid. Данная опция должна быть использована с опцией sid. Файл “etc/gen-msg.map” содержит больше информации о gid препроцессоров и декодеров.
Синтаксис: gid:<generator id>;
Примеры:
alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

Вставить скриншот с созданным правилом.
2. sid
Ключевое слово sid (Snort id или иногда упоминается как signature id) используется для уникальной идентификации правил Snort. По значению его аргумента можно легко идентифицировать правило. Данное ключевое слово должно использоваться вместе с ключевым словом rev. Файл “sid-msg.map” содержит соответствие предупреждающих сообщений и идентификаторов правил Snort. Значения аргумента:
< 100 зарезервировано разработчиками 100 - 999.999 использованы в правилах, уже включенных в дистрибутив Snort
= 1.000.000 можно использовать для собственных правил
Синтаксис: sid:<snort rules id>;
Примеры:
alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Вставить скриншот с созданным правилом.
3. rev
Указывает значение версии правила. С помощью REV интерпретатор правил Snort определяет версию написанного правила. Этот параметр используется в паре с SID.
Синтаксис: rev:<revision integer>;
Примеры:
alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;)

Вставить скриншот с созданным правилом.
4. classtype
Используется для присвоения категории атаки, к которой необходимо отнести правило, являющееся частью более общего класса атак. Snort предоставляет набор классов, которые используются предоставляемыми правилами по умолчанию. Классификация атак позволяет лучше организовать события, производимые Snort. Классификация атак представлена в файле “classification.conf”. В файле используется следующий синтаксис для каждой записи:
config classification: <имя класса>,<описание класса>,<приоритет по умолчанию>
Приоритет 1 (high) является наиболее высоким, а 4 (very low) - самым низким. Также классификация типов атак представлена в таблице:

Тип класса	Описание	Приоритет

Тип класса	Описание	Приоритет
attempted-admin	Попытка получения прав администратора	high
attempted-user	Попытка получения прав пользователя	high
inappropriate-content	Обнаружено неприемлемое (несоответствующее) содержание	high
policy-violation	Потенциальное нарушение корпоративной конфиденциальности	high
shellcode-detect	Обнаружен исполняемый код	high
successful-admin	Успешное получение прав администратора (повышение привилегий)	high
successful-user	Успешное получение прав пользователя (повышение привилегий)	high
trojan-activity	Обнаружена активность сетевой троянской программы	high
unsuccessful-user	Неудачная попытка получения прав пользователя	high
web-application-attack	Атака на Web-приложение	high
attempted-dos	Предпринята попытка атаки отказ в обслуживании (DoS)	medium
attempted-recon	Попытка утечки информации (разведка)	medium
bad-unknown	Потенциально нежелательный траффик	medium
default-login-attempt	Попытка входа с помощью стандартного логина/пароля	medium
denial-of-service	Обнаружена атака отказ в обслуживании (DoS)	medium
misc-attack	Прочие атаки	medium
non-standard-protocol	Обнаружено использование нестандартного протокола или нестандартное событие	medium
rpc-portmap-decode	Decode of an RPC Query (Декодирован удалённый вызов процедуры (RPC)) (Обнаружен запрос RPC)	medium
successful-dos	Успешная DOS-атака	medium
successful-recon-largescale	Крупномасштабная утечка информации	medium

Тип класса	Описание	Приоритет
successful-recon-limited	Утечка информации	medium
suspicious-filename-detect	Обнаружено подозрительное имя файла	medium
suspicious-login	Обнаружена попытка входа с подозрительным логином	medium
system-call-detect	Обнаружено обращение к ядру системы (system call) (Обнаружен системный вызов)	medium
unusual-client-port-connection	Клиент использует нестандартный порт	medium
web-application-activity	Доступ к потенциально уязвимому Web-приложению	medium
icmp-event	Общее событие ICMP	low
misc-activity	Прочая активность	low
network-scan	Обнаружена попытка сканирования сети	low
not-suspicious	Не являющийся подозрительным траффик	low
protocol-command-decode	Generic Protocol Command Decode (Обнаружена попытка шифрования) (Обнаружена обычная команда протокола)	low
string-detect	Обнаружена подозрительная строка	low
unknown	Неизвестный траффик	low
tcp-connection	Обнаружено TCP соединение	very low

Синтаксис: classtype:<class name>;
Примеры:
alert tcp any any -> any 25 (msg:"SMTP expn root"; flags:A+; content:"expn root"; nocase; classtype:attempted-recon;)
Предупреждения:
Опция classtype может иметь только те значения для классификации, которые определены в snort.conf с помощью config classification. Snort предоставляет стандартный набор классификации в файле classification.config, который используется в поставляемых наборах правил.

Вставить скриншот с созданным правилом.
5. priority
Задаёт правилам уровень важности. Возможно использовать параметр priority вместе с classtype, при этом изменится уровень приоритета параметра classtype.
Синтаксис: priority:<priority integer>;
Примеры:
alert tcp any any -> any 80 (msg:"WEB-MISC phf attempt"; flags:A+; content:"/cgi-bin/phf"; priority:10;)

alert tcp any any -> any 80 (msg:"EXPLOIT ntpdx overflow"; dsize:>128; classtype:attempted-admin; priority:10;)

Вставить скриншот с созданным правилом.

6. metadata

Позволяет автору правил включать дополнительную информацию о правиле, как правило, в формате “ключ-значение”. Ключи и значения тега metadata перечислены в таблице ниже:

Ключ	Описание	Формат значения
engine	Указывает правило библиотеки общего пользования (Indicate a Shared Library Rule)	"shared"
soid	GID и SID правила библиотеки общего пользования (Shared Library Rule Generator and SID)	sid
service	Идентификатор сервиса на основе цели (Target-Based Service Identifier)	"http"

Отличные от указанных в таблице ключи Snort фактически игнорирует, поэтому они могут быть записаны в свободной форме в формате “ключ-значение”. Несколько ключей подряд разделяются запятыми, а ключи и значения отделяются между собой пробелом.

Синтаксис:

metadata:key1 value1;
metadata:key1 value1, key2 value2;

Примеры:

alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; metadata:engine shared; metadata:soid 3|12345;)
alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; metadata:engine shared, soid 3|12345;)
alert tcp any any -> any 80 (msg:"HTTP Service Rule Example"; metadata:service http;)

Вставить скриншот с созданным правилом.

7. content

Позволяет устанавливать условие в правила, которые ищут определённое содержание (контент) в полезной нагрузке пакетов. Условия могут содержать как двоичные данные, так и текстовые. Двоичные данные должны быть заключены между вертикальными чертами “|” в виде байт-кода. Байт-код представляет двоичные данные в виде шестнадцатеричных чисел. В одном правиле может быть указано несколько content-условий. “!” - модификатор отрицания. Если правилу предшествует модификатор отрицания, то правило срабатывает на пакетах, которые не содержат заданный контент.

Ключевое слово content имеет ряд модификаторов, которые изменяют поведение ранее указанного content. Список модификаторов:

nocase
rawbytes
depth
offset
distance
within
http_client_body
http_client_body
http_cookie
http_raw_cookie
http_header
http_raw_header

http_method
http_uri
http_raw_uri
http_stat_code
http_stat_msg
fast_pattern
Синтаксис: content:[!]"<content string>";
Примеры:
```
alert tcp any any -> any 139 (content:"|5c 00|P|00|I|00|P|00|E|00 5c|";)
alert tcp any any -> any 80 (content:!"GET";)
```
Предупреждения:
Необходимо экранировать следующие символы:
; \ "

Вставить скриншот с созданным правилом.

8. protected_content

Имеет схожую функциональность с content, однако работает несклько иным образом. Основное преимущество ключевого слова protected_content над content в том, что оно позволяет скрыть целевой контент, раскрывая только хэш-сумму (дайджест) указанного контента. Как и в случае content, основная цель - сопоставить строки определённых байтов. Поиск осуществляется путём хэширования частей входящих сообщений и сравнения полученных результатов с предоставляемой в условии хэш-суммой. Из-за чего проделывается очень большой объём вычислений.

На данный момент с ключевым словом protected_content возможно использование алгоритмов хэширования MD5, SHA256, и SHA512. Алгоритм хэширования должен быть указан в правиле с использованием ключевого слова hash, если он не задан по умолчанию в конфигурации Snort. Кроме того, вместе с protected_content обязательно должен быть указан модификатор length, чтобы указать длину исходных данных.

Как и в случае content, в правиле возможно использование нескольких условий protected_content. В правиле допускается совместное использование content и protected_content. Также в protected_content можно использовать модификатор отрицания “!”.

Ключевое слово protected_content имеет те же модификаторы, что и content, за исключением следующих:
nocase
fast_pattern
depth
within
Синтаксис: protected_content:[!]"<content hash>", length:orig_len[, hash:md5|sha256|sha512];
Примеры:
Следующие правила срабатывают на строке “HTTP”.
```
alert tcp any any <> any 80 (msg:"MD5 Alert";
protected_content:"293C9EA246FF9985DC6F62A650F78986"; hash:md5; offset:0; length:4;)
alert tcp any any <> any 80 (msg:"SHA256 Alert";
protected_content:"56D6F32151AD8474F40D7B939C2161EE2BBF10023F4AF1DBB3E13260EBDC6342";
hash:sha256; offset:0; length:4;)
```

Вставить скриншот с созданным правилом.

9. nocase

Является модификатором для располагающегося до него ключевого слова content, указывая ему сравнивать содержание без учета регистра символов.
Синтаксис: nocase;
Примеры:
```
alert tcp any any -> any 21 (msg:"FTP ROOT"; content:"USER root"; nocase;)
```

Вставить скриншот с созданным правилом.

10. rawbytes

Ключевое слово rawbytes является модификатором для располагающегося до него ключевого слова content, позволяя работать с необработанными данными пакета, игнорируя любое декодирование, произведённое с помощью препроцессоров.

HTTP Inspect имеет набор ключевых слов http_raw_cookie, http_raw_header, http_raw_uri и др. для работы с необработанными данными, которые сопоставляют определённые части HTTP запросов и ответов. С данными ключевыми словами использовать rawbytes не нужно, так как эти условия по умолчанию работают с необработанными данными.

Большинство других препроцессоров по умолчанию используют декодированные/нормализованные данные для сопоставления с образцом. Поэтому для сопоставления с произвольными необработанными данными из пакета необходимо указывать ключевое слово rawbytes.

Синтаксис: rawbytes;

Примеры:

```
alert tcp any any -> any 21 (msg:"Telnet NOP"; content:"|FF F1|"; rawbytes;)
```

Вставить скриншот с созданным правилом.

11. http_client_body

Ключевое слово http_client_body ограничивает поиск по телу запроса HTTP-клиента. Ключевое слово http_client_body является модификатором для располагающегося до него ключевого слова content. Размер области данных, по которым производится поиск, зависит от опции post_depth в HttpInspect. Паттерн с данным ключевым словом не будет работать, если post_depth в установлена “-1”.

Синтаксис: http_client_body;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_client_body;)
```

Вставить скриншот с созданным правилом.

12. http_header

Ключевое слово http_header ограничивает поиск по извлечённым полям заголовка запроса HTTP-клиента или ответа HTTP-сервера (определяется в конфигурации HttpInspect). Ключевое слово http_method является модификатором для располагающегося до него ключевого слова content. Извлечённые поля заголовка можно нормализовать, определив это в конфигурации HttpInspect.

Синтаксис: http_header;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_header;)
```

Вставить скриншот с созданным правилом.

13. http_method

Ключевое слово http_method ограничивает поиск по извлечённому методу из запроса HTTP-клиента. Ключевое слово http_method является модификатором для располагающегося до него ключевого слова content.

Синтаксис: http_method;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"GET"; http_method;)
```

Вставить скриншот с созданным правилом.

14. http_uri

Ключевое слово http_uri ограничивает поиск по нормализованному полю URI запроса. Ключевое слово http_uri является модификатором для располагающегося до него ключевого слова content. Использование опции http_uri после content эквивалентно опции uricontent.

Синтаксис: http_uri;

Примеры:

```
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_uri;)
```

Вставить скриншот с созданным правилом.

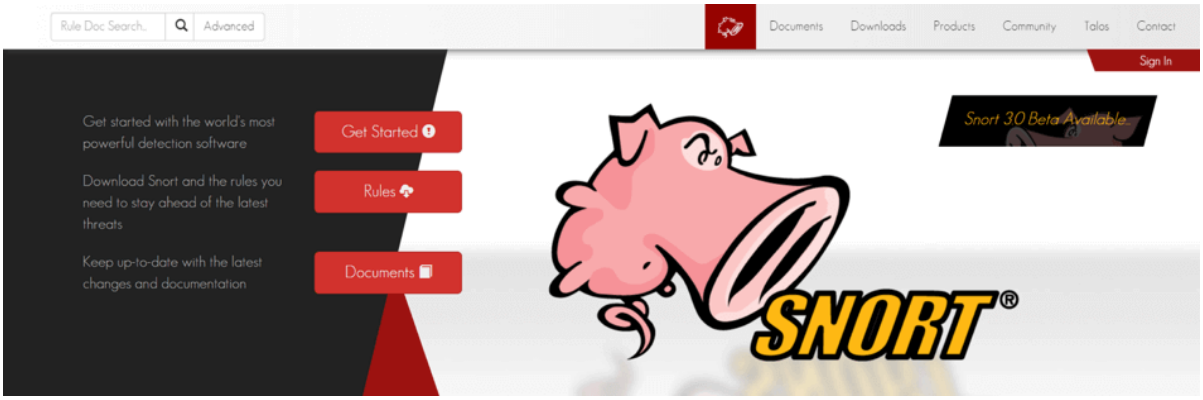
15. http_raw_uri
Ключевое слово http_raw_uri ограничивает поиск по ненормализованному полю URI запроса. Ключевое слово http_raw_uri является модификатором для располагающегося до него ключевого слова content.
Синтаксис: http_raw_uri;
Примеры:
alert tcp any any -> any 80 (content:"ABC"; content:"EFG"; http_raw_uri;)
Вставить скриншот с созданным правилом.
16. http_stat_code
Ключевое слово http_stat_code ограничивает поиск по извлечённому полю пояснения к статус коду ответа HTTP-сервера. Ключевое слово http_stat_code является модификатором для располагающегося до него ключевого слова content. Поле пояснения к статус коду будет извлечено, если только задана опция extended_response_inspection в HttpInspect.
Синтаксис: http_stat_code;
Примеры:
alert tcp any any -> any 80 (content:"ABC"; content:"200"; http_stat_code;)
http_stat_msg

Вставить скриншот с созданным правилом.

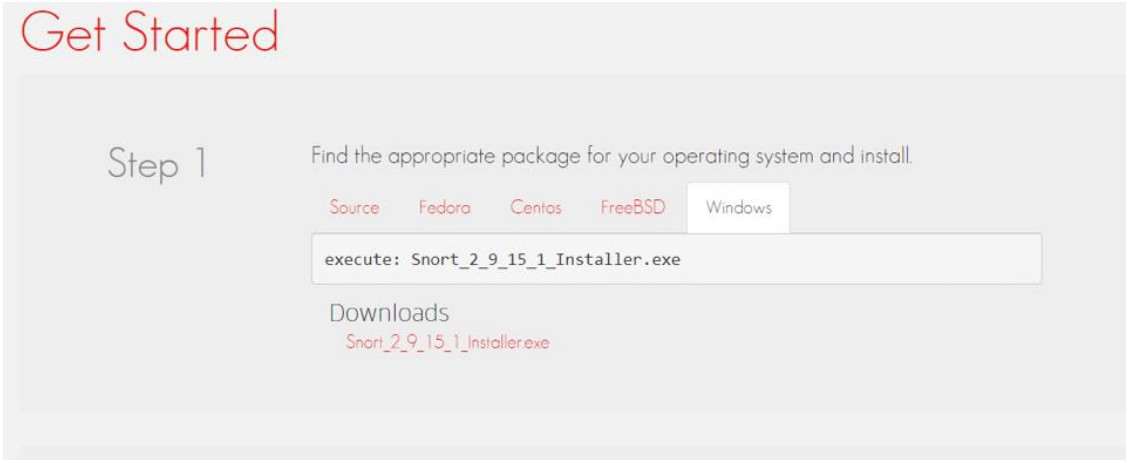
Практическая работа № 28
Создание собственных правил для Snort. Синтаксис правил

Задание:

Установить Snort на операционную систему Winwows.
Открываем любую виртуальную машину с Winwows.
1. Переходим на официальный сайт разработчика Snort.org. Поскольку программа является полностью бесплатной, то никаких проблем с лицензией, пробной версией не появляется
Нажимаем Get Started.



Открывается окно с текстовыми командами, там выбираем в верхних вкладках нашу операционную систему (в данном случае Windows) и загружаем файл загрузчика (Installer.exe).

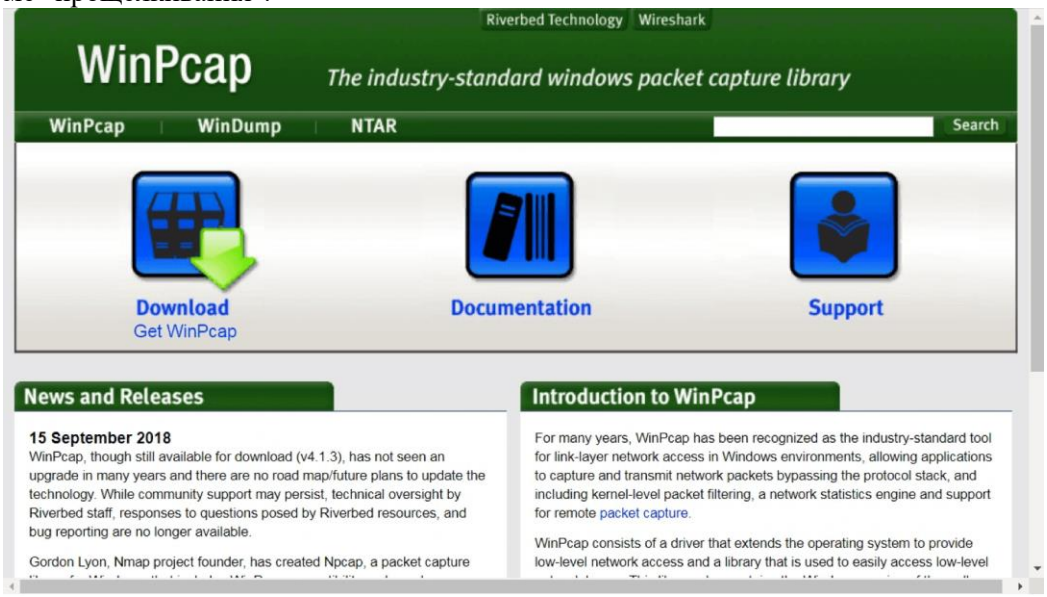


Устанавливаем его в режиме "прощелкивания", то есть, ни снимая никакие флажки, поставленные разработчиком по умолчанию.
вставить скриншот с результатом.

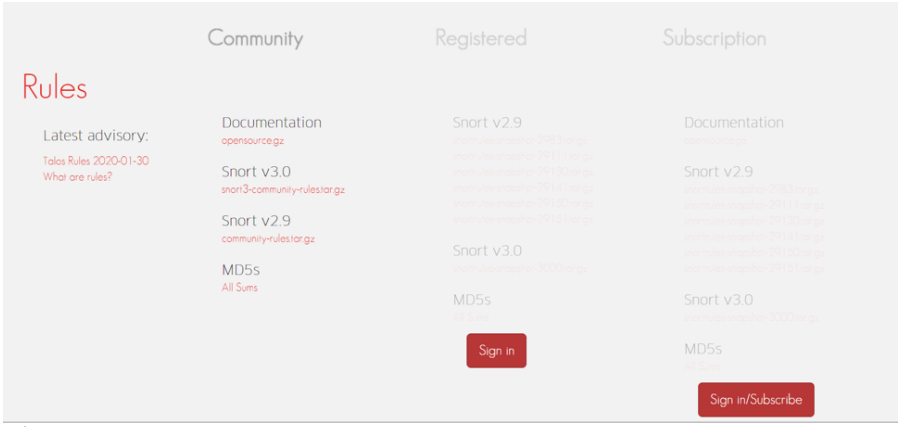
2. Установка вспомогательных утилит

✓ После установки Snort никаких изменений на компьютере не произошло и работать с программой нет возможности, потому что не установлены специальные утилиты и драйвера, которые обеспечат запуск приложения.

✓ В завершающем окне Snort для Windows попросит вас установить хорошо известную сетевым администраторам утилиту Winpcap. Это драйвер, который позволит вашей сетевой карте перейти в мониторный режим, то есть передавать и получать пакеты, обходя стеки протоколов. Данная утилита тоже бесплатная, поэтому ее скачиваем с сайта разработчика www.winpcap.org и также устанавливаем в режиме "прощелкивания".



Вторая вспомогательная утилита - специальный архиватор с высокой степенью сжатия, который нужен, чтобы распаковать файлы. Скачиваем и устанавливаем архиватор 7-Zip с официального сайта 7-zip.org. Итак, установщик загружен и установлен, вспомогательные утилиты тоже поставлены. Но поскольку, графической оболочки нет, нам надо загрузить специальные правила, по которым Snort будет работать. Возвращаемся на официальный сайт Snort.org и нажимаем на кнопку "Rules" (правила). Из открывшегося списка берем файл, список правил (rules), соответствующий нашей версии (они рассортированы по версиям Snort, а не по операционным системам). На начало 2020 г. для Windows актуальна версия 2.9.15.1, которую мы инсталлируем и настроим в качестве примера.



✓ Скачанный файл правил (называется community-rules.tar.gz) находим в папке и открываем с помощью только что установленного архиватора 7-zip. Интерфейс этого архиватора очень похож на WinRar или WinZip.

✓ Все файлы разархивируем, копируем и переносим в папку Snort, которую создал наш установщик. В дальнейшем, это значительно упростит указание путей.

✓ Теперь находим и открываем файл snort.conf (параметры конфигурации для запуска приложения) в NotePad++ или другом текстовом редакторе.

✓ Где-то на 103 строчке (она может немного отличаться по мере того, как разработчик вносит изменения в обновления) находим, установленную разработчиком по умолчанию строчку, указатель пути: c:\snort\rules. Она совпадает с расположением файла на нашей машине. Если у вас путь другой, то припишите именно его. Там, где надо редактировать пути, разработчик ставит две точки.

✓ Теперь нам надо указать путь для папки Log-файлов, куда наш Snort будет записывать все логи, доступные для просмотра и изучения. Редактируем пути к лог-файлам.

✓ В папке C:/snort уже есть папка log, для этого предназначенная, поэтому мы прописываем путь C:\snort\log.

✓ На строчке 182 прописываем в config logdir: c:\snort\log, причем первая часть config logdir уже есть и строку можно найти по ней. Незабываем удалить символ "#", который выбрасывает строки из исполняемого файла, превращая их в комментарий. Результат:

```
177 # config bpf_file:
178 #
179
180 # Configure default log direc
181 #
182 config logdir: c:\snort\log
183
184
185 ##############################
186 # Step #3: Configure the base
```

Вставить скриншот.

✓ Дальнейшее редактирование файла конфигурации проводим по списку по ссылке. Ищем по первой части строк и прописываем правильные пути:

path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
path to dynamic rules libraries
#dynamicdetection directory c:\Snort\lib\snort_dynamicrules

Продолжаем редактирование. Теперь комментируем, добавляя знаки комментария "#" к строкам 259-265. В отредактированном варианте это выглядит так:

Inline packet normalization. For more information, see README.normalize
Does nothing in IDS mode
#preprocessor normalize_ip4
#preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
#preprocessor normalize_icmp4

#preprocessor normalize_ip6
#preprocessor

Практическая работа №29
Настройка виртуальной машины для эмуляции угроз ИБ

Задание:

Запускаем рабочую станцию на Kali Linux.
1. Пробуем провести DoS-атаку на наш Apache. Так как BASE работает по HTTP, легкий способ его «положить» — это атака Slowloris. Поэтому скачиваем на Kali соответствующий скрипт и запускаем атаку:
sudo pip3 install slowloris
slowloris example.com
git clone https://github.com/gkbrk/slowloris.git
cd slowloris
python3 slowloris.py example.com

```
root@kali:~/x# git clone https://github.com/gkbrk/slowloris.git
Клонирование в «slowloris»…
remote: Enumerating objects: 6, done.
remote: Counting objects: 100% (6/6), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 78 (delta 0), reused 3 (delta 0), pack-reused 72
Распаковка объектов: 100% (78/78), готово.
root@kali:~/x# cd slowloris/
root@kali:~/x/slowloris# python3 slowloris.py 192.168.1.20
[02-11-2018 22:06:26] Attacking 192.168.1.20 with 150 sockets.
[02-11-2018 22:06:26] Creating sockets...
[02-11-2018 22:06:30] Sending keep-alive headers... Socket count: 150
[02-11-2018 22:06:45] Sending keep-alive headers... Socket count: 150
[02-11-2018 22:07:00] Sending keep-alive headers... Socket count: 150
^C
Stopping Slowloris...
```

вставить скриншоты с установленным скриптом и запуском атаки на Apache, лог из Snort.
2. Запустим sql-инъекцию с kali на машину с установленным snort:(http://sqlmap.org/)
Команда для скачивания: git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git sqlmap-dev
Запустите sqlmap на BASE по запросу http://ip-адрес snort/base/base_stat_alerts.php?sensor=1
Результатов не будет, потому что snort не настроен для обнаружения данной атаки.
вставьте скриншот.
Создайте следующее правило:
alert tcp any any -> any any (msg: "SQL Injection"; content: "GET"; http_method; uricontent: "and 1=1"; nocase; sid:3000001; rev:1;)
Снова запустите атаку и посмотрите результаты.

Вставьте скриншот с результатами.

Практическая работа № 30
Отслеживание действий в сети и создание своих правил

Задание:

Редактирум пути к правилам правил Snort
such as: c:\snort\rules
var RULE_PATH c:\Snort\rules
var SO_RULE_PATH c:\Snort\so_rules

var PREPROC_RULE_PATH c:\Snort\preproc_rules
If you are using reputation preprocessor set these
var WHITE_LIST_PATH c:\Snort\rules
var BLACK_LIST_PATH c:\Snort\rules
Вставить скриншот.

✓ Прописываем путь к папке лог
config logdir: c:\Snort\log
✓ Редактируем пути для libraries
path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\Snort\lib\snort_dynamicpreprocessor
path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll
path to dynamic rules libraries
#dynamicdetection directory c:\Snort\lib\snort_dynamicrules
✓ Комментируем
Inline packet normalization. For more information, see README.normalize
Does nothing in IDS mode
preprocessor normalize_ip4
preprocessor normalize_tcp: block, rsv, pad, urp, req_urg, req_pay, req_urp, ips, ecn stream
preprocessor normalize_icmp4
preprocessor normalize_ip6
preprocessor normalize_icmp6
Back Orifice detection.
preprocessor bo
Portscan detection. For more information, see README.sfportscan
preprocessor sfportscan: proto { all } memcap { 10000000 } sense_level { low }
whitelist $WHITE_LIST_PATH\white.list, \
blacklist $BLACK_LIST_PATH\black.list
Вставить скриншот.

✓ Исправляем пути правил
✓ Определяем сетевую карту snort -W
✓ Тестируем конфиг snort -T -c c:\snort\etc\snort.conf -l c:\snort\log -i 2 ключ -T указывает, что нужно протестировать текущую конфигурацию Snort ключ -c означает, что включен режим IDS
✓ Далее следует путь к конфигурационному файлу snort.conf
ключ -l включает режим записи на жесткий диск с указанием пути к файлу
ключ -A показывает что все предупрежления(alerts) будут дублтроваться выводом на консоль
ключ -i указывает на порядковый номер(index) интересующего нас интерфейса
✓ Чтобы узнать поддерживаемые интерфейсы необходимо выполнить команду: snort -W
✓ Добавляем нужные вам правила
✓ Запускаем Режим IDS: snort -A console -c c:\snort\etc\snort.conf -l c:\snort\log -i 2
Вставить скриншот.