Министерство образования и науки Российской Федерации

Московский Государственный Технический Университет
им. Н.Э. Баумана

Факультет «Информатика и системы управления»
Кафедра «Компьютерные системы и сети»

Сурков Л.В.

Методические указания
к лабораторной работе по дисциплине
Корпоративные сети

Раздел
Построение защищенных сетей с использованием брандмауэров

Виртуальные частные сети.
IPSec-туннель

.

2011

Виртуальные частные сети
IPSec-туннель

Теоретические основы

Перед выполнением практической части работы рекомендуется внимательно прочитать:

1. Раздел «Основы протокола IPSec» лабораторной работы «Защита сетевого трафика с использованием IPSec и сертификатов».
2. Раздел «Теоретические основы VPN» лабораторной работы «Построение виртуальных частных сетей VPN в сетевой среде Windows Server 2008/2003»

Сведения по конфигурированию брандмауэра Cisco ASA 5500

Режимы работы ASA 5500

Cisco ASA 5505 может работать в двух режимах.

- Маршрутизирущий режим. ASA работает в этом режиме по умолчанию и выполняет фильтрацию трафика в соответствии с правилами межсетевого экрана как обычный узел сети.
- Прозрачный (Transparent) режим. . ASA осуществляет только фильтрацию трафика 2 уровня, но не маршрутизирует его, а только лишь перенаправляет с порта *inside* на порт *outside*. Пакеты уровня 2 пропускаются только для следующих MAC-адресов:
  - широковещательный адрес (FFFF.FFFF.FFFF);
  - групповые адреса IPv4 (0100.5E00.0000-0100.5EFE.FFFF);
  - групповые адреса IPv6 (3333.0000.0000-3333.FFFF.FFFF);
  - адрес групповой рассылки BPDU (0100.0CCC.CCCD).

При смене режимов ASA очищает текущую конфигурацию, не изменяя загрузочную
Пакеты уровня 3 фильтруются в соответствии с параметром «security» интерфейсов. Пакеты ARP пропускаются без ограничений.
IP-адрес назначается устройству в целом, а не конкретному интерфейсу, и используется в качестве адреса отправителя в пакетах, отправленных с ASA. Адрес должен принадлежать сети, к которой подключен интерфейс.

Для настройки интерфейса управления выполните команду:
(config)# interface management0/0

В этом режиме не поддерживается терминация VPN, протоколы динамической маршрутизации (как и сама маршрутизация) и процедуры QoS.

Чтобы включить прозрачный режим, выполните следующую команду:
(config)# firewall transparent

Чтобы выключить прозрачный режим (и включить маршрутизирующий), выполните следующую команду: (config)# no firewall transparent

Базовые настройки ASA 5500 Series

Пароль для Telnet/SSH-соединений (по умолчанию «cisco»):
(config)# password <пароль>

Пароль для переходя в привилегированный режим («enable»):
(config)# enable password <пароль>

Имя устройства (hostname):
(config)# hostname <имя_узла>

Имя домена: (config)# domain-name <имя_домена>

Дата и время:
(config)# clock set <часы>:<минуты>:<секунды> <день> <месяц> <год>

Месяц вводится словом: january, etc.

Интерфейсы ASA 5500 Series

Cisco ASA 5505 имеет 8 Ethernet-портов, которые могут работать в 2 режимах:

- порты коммутатора 2 уровня;
- порты, образующие VLAN:

◦ в маршрутизирующем режиме происходит маршрутизация трафика между VLAN с учетом политик межсетевого экрана и VPN;
◦ в прозрачном режиме происходит перенаправление трафика между VLAN одной подсети в соответствии с политиками межсетевого экрана.

При перенаправлении трафика между портами, входящими в одну VLAN, политики МСЭ не применяются. В прозрачном режиме разрешено создать не более 2 VLAN, в маршрутизирующем — не более 3, причем одна из них (VLAN для построения демилитаризованной зоны, DMZ) сможет инициировать обмен трафиком только в одну из двух других VLAN. Создать тегирующий порт нельзя, то есть невозможно построение магистральных линий связи между устройствами, обслуживающими более одной VLAN.

Для каждого интерфейса должен быть задан параметр *security* в границах от 0 до 100. Это параметр, определяющий базовую возможность взаимодействия между портами: порт с большим значением *security* всегда может инициировать соединения на порт с меньшим значением *security*, при этом порт с меньшим значением *security* не может инициировать соединения на порт с большим значением *security*. Порты с равным значением *security* могут свободно взаимодействовать между собой.

Обычно *security*=100 задают для порта, присоединенного к локальной сети, *security*=0 для порта, присоединенного к внешней сети, а порту, присоединенному к DMZ, присваивается промежуточное значение. Дальнейшее ограничение доступа осуществляется с помощью списков контроля доступа (Access Control Lists, ACL). Также по этим значениям определяется тип соединения — входящее (с порта с меньшим security на порт с большим *security*) или исходящее (с порта с большим *security* на порт с меньшим *security*). По умолчанию интерфейсу присваивается *security*=0. Если интерфейс *inside*, то для него по умолчанию *security*=100.

Перейти в режим настройки VLAN:
(config)# interface vlan <vlan_id>
vlan_id может иметь значение от 0 до 4090.

Настроить «DMZ VLAN» (VLAN, из которой могут устанавливаться соединения только в одну из двух других VLAN):
(config-if)# no forward interface vlan <vlan_id>

Здесь vlan_id — номер VLAN, в которую запрещено устанавливать соединения. «DMZ VLAN» должна быть настроена до создания третьей VLAN.

Включить порт в VLAN:
(config)# interface <имя>
(config-if)# switchport access vlan <vlan_id>

Запретить взаимодействие с другими защищ□нными портами в VLAN:
(config-if)# switchport protected

Если вы настраиваете VLAN, то следующие параметры надо назначать интерфейсу VLAN, а не каждому физическому интерфейсу.

Задать интерфейсу имя:
(config-if)# nameif <символьное_имя>
Символьное имя должно быть не длиннее 48 символов, регистр не имеет значения.

Задать интерфейсу значение security:

(config-if)# security-level <значение>

Задать интерфейсу IP-адрес: (config-if)# ip address <адрес> <маска>

Включить получение IP-адреса по DHCP:
(config-if)# ip address dhcp [setroute]

Ключ setroute разрешает использование маршрута по умолчанию, получаемого от DHCP-сервера.

Настроить интерфейс как интерфейс управления:
(config-if)# management-only

По умолчанию все интерфейсы административно отключены. Чтобы включить их, выполните команду no shutdown в режиме настройки интерфейса.

Вывести настройки всех интерфейсов:
show interface

Вывести краткие настройки IP-интерфейсов:
show interface ip brief

Списки контроля доступа (ACL) ASA 5500 Series

Список контроля доступа — инструмент для фильтрации трафика. Каждый список доступа состоит из нескольких записей контроля доступа (Access Control Entry, ACE). Каждая такая запись разрешает или запрещает перенаправление попадающего под правила этой записи пакета. Каждая новая ACE по умолчанию добавляется в конец списка. ACE применяются по порядку их появления в списке.

Существует два типа списков доступа:

- Стандартные (standard) — применяются для контроля адресов направлений в маршрутах OSPF. Не могут быть назначены интерфейсам для фильтрации трафика. В конец всегда добавляется правило, запрещающее весь трафик.

- Расширенные (extended) — определяют адреса отправителя и получателя, протокол, порты (для TCP и UDP) и типы сообщений ICMP.

Создание стандартного списка доступа
(config)# access-list <имя_ACL> standard {deny | permit} {any | <IP-адрес> <маска>}

Создание расширенного списка доступа
Для IP-трафика, без указания портов:
(config)# access-list <имя_ACL> [line <номер_строки>] extended {deny|permit} <протокол> <адрес_отправителя> <маска> <адрес_получателя> <маска>

Протокол может быть задан по имени или по номеру. Список протоколов с именами и номерами можно посмотреть в файле */etc/protocols* на компьютерах.

Для трафика UDP и TCP:

(config)# access-list <имя_ACL> [line <номер_строки>] extended {deny | permit} {tcp|udp} <адрес_отправителя> <маска> [<оператор> <порт>] <адрес_получателя> <маска> [<оператор> <порт>]

Оператор может принимать все значения, которые он может принимать в маршрутизаторах и коммутаторах Cisco.

Для трафика ICMP:
(config)# access-list <имя_ACL> [line <номер_строки>] extended {deny | permit} icmp <адрес_отправителя> <маска> <адрес_получателя> <маска> [<тип_ICMP>]

Для полей «адрес отправителя», «адрес получателя» и «маска» действуют модификаторы any и host. Маска вводится в прямой форме.

Для каждого порта можно контролировать два потока трафика:

- Inbound (входящий) — поток, проходящий от внешних узлов через порт в ASA;
- Outbound (исходящий) — поток, выходящий через порт ASA к внешним узлам.

Таким образом, один пакет может быть подвергнут как входной, так и выходной фильтрации.

Список контроля входящего потока может применяться к отдельному порту или ко всему устройству в целом. При этом глобальный список контроля доступа не перекрывает интерфейсные списки, они применяются последовательно: сначала интерфейсный, затем глобальный.

Для протоколов TCP и UDP ASA создает запись о двунаправленном соединении и, соответственно, разрешает обратный трафик, относящийся к этому соединению. Для протокола ICMP ASA создает запись об однонаправленном соединении, поэтому требуется разрешать обратный ICMP-трафик отдельно.

Применить список контроля доступа к интерфейсу:
(config)# access-group <имя_ACL> {in | out} interface <имя_интерфейса>

Network Address Translation (NAT) ASA 5500 Series

! Настройка интерфейса inside

(config)# interface Vlan 1
(config-if)# nameif inside
(config-if)# security-level 100

(config-if)# ip address <адрес> <маска>
(config-if)# no shutdown
(config-if)# exit

! Настройка интерфейса outside

(config)# interface Vlan 2
(config-if)# nameif outside
(config-if)# security-level 0
(config-if)# ip address <адрес> <маска>
(config-if)# no shutdown
(config-if)# exit

! Добавление порта к интерфейсу inside

(config)# interface <имя>
(config-if)# switchport access vlan 1
(config-if)# no shutdown (config-if)# exit

! Добавление порта к интерфейсу outside

(config)# interface <имя>
(config-if)# switchport access vlan 2
(config-if)# no shutdown (config-if)# exit

! Включение NAT (PAT)

! Имена интерфейсов должны записываться в круглых скобках

! Создание пула адресов, состоящего из одного адреса

! Указываем, что адрес надо брать с интерфейса

(config)# global (outside) <номер_NAT> interface

! Создание правила NAT

(config)# nat (inside) <номер_NAT> 0.0.0.0 0.0.0.0

! Добавление маршрута по умолчанию к провадеру

(config)# route outside 0.0.0.0 0.0.0.0 <IP-адрес_шлюза> <метрика>

Настройка туннеля IPSec ASA 5500 Series

! Настройка ISAKMP (фаза 1)

! Выбор шифрования

(config-if)# crypto isakmp policy <приоритет> encryption (aes|aes-192|aes-256 |des| 3des)

! Выбор хеша

(config)# crypto isakmp policy <приоритет> hash (md5 | sha)

! Выбор метода аутентификации с общим ключом

(config)# crypto isakmp policy <приоритет> authentication pre-share

! Выбор группы Диффи-Хеллмана

(config)# crypto isakmp policy <приоритет> group (1 | 2 | 5)

! Задание времени жизни объединения безопасности

! (в секундах от 120 до 2147483647)

(config)# crypto isakmp policy <приоритет> lifetime <время>

! Включение ISAKMP на интерфейсе outside

(config)# crypto isakmp enable outside

! Выбор метода идентификации сторон

! address – по IP-адресу

! hostname – по FQDN

! key-id – по общему ключу

! auto – (для аутентификации с общим ключом) по IP-адресу

(config)# crypto isakmp identity (address | hostname | key-id <ключ> | auto)

! Настройка IPSec (фаза 2)

! Создание расширенного списка доступа для определения шифруемого трафика

(config)# access-list <номер_ACL> permit ip <адрес_отправителя> <маска_адреса_отправителя> <адрес_получателя> <маска_адреса_получателя>

! Создание набора алгоритмов для туннеля

(config)# crypto ipsec transform-set <имя> <алгоритм> [<алгоритм> …]

! Создание криптосвязи

! Задание ACL для выбора шифруемого трафика

(config)# crypto map <имя> <индекс> match address <номер_ACL>

! Задание адреса соседа по туннелю

(config)# crypto map <имя> <индекс> set peer <IP-адрес_соседа>

! Задание набора алгоритмов (config)# crypto map <имя> <индекс> set transform-set <имя>

! Задание времени жизни объединения безопасности

(config)# crypto map <имя> <индекс> set security-association lifetime (seconds <время_в_секундах> | kilobytes <объем_трафика_в_килобайтах>)

! Назначение криптосвязи на интерфейс

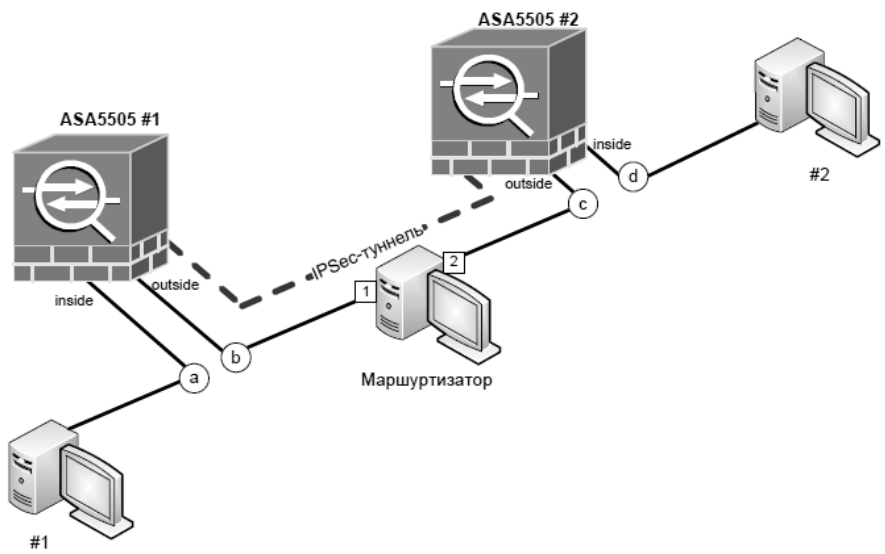
(config)# crypto map <имя_криптосвязи> interface <имя_интерфейса>

Практическая часть

Цель работы:
Изучение протокола IPSec и способа его настройки в ОС Linux и на брандмауэре ASA5505.

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке.



Рисунок

2. Настройте рабочие станции и брандмауэры таким образом, чтобы создать четыре различных IP-подсети: a, b, c и d (в соответствие с рисунком).

3. Настройте IPSec-туннель, как это показано на рисунке.

4. Проверьте работоспособность сети, обратившись с машины #1 на машину #2.

Литература

1. James Boney, Cisco IOS in a Nutshell, 2-nd Ed., O`Reilly, 2008

2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2008

3. НПП «Учтех-Профи», ОС Arch Linux, Лабораторный практикум, Челябинск, 2010

4. Сурков Л.В. Защита сетевого трафика с использованием IPSec и сертификатов. МГТУ им. Н.Э.Баумана, каф. ИУ6, 2010

5. Сурков Л.В. Построение виртуальных частных сетей VPN в сетевой среде Windows Server 2008/2003. МГТУ им. Н.Э.Баумана, каф. ИУ6, 2010