Практическая работа № 9

Исследование основных функций межсетевого экрана CISCO ASA 5505

Цель работы: изучить основные функциональные особенности оборудования Cisco ASA 5505, освоить принципы использования оборудования Cisco ASA 5505, а так же освоить принципы конфигурирования оборудования Cisco ASA 5505.

Используемые средства и оборудование: IBM/PC совместимый компьютер с пакетом Cisco Packet Tracer; лабораторный стенд Cisco.

Краткая теория

Межсетевой экран или сетевой экран — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации

Существует три фундаментальные технологии, на основе которых фаерволы выполняют свою работу:

— Статическая пакетная фильтрация (packet filtering) - пакеты фильтруются на основе статической информации в заголовке сетевых пакетов

— Прокси-фаервол (proxy firewall) - устройство находится между клиентом и внешней сетью и все запросы, и соединения клиента с внешними хостами осуществляются от имени прокси сервера

— Динамическая пакетная фильтрация (stateful packet filtering) - сочетает в себе лучшее первых двух.

Статическая пакетная фильтрация (packet filtering)

Это наиболее древняя и широко применяемая технология. Статическая пакетная фильтрация используется для фильтрации пакетов, входящих в сеть, а также пакетов, проходящих между разными сегментами сети. Пакетный фаервол инспектирует входящий трафик, анализируя информацию сетевого и транспортного уровней модели OSI.

Фаервол анализирует IP пакет и сравнивает его с заданным набором правил, аксес листом (ACL - Access Control List). ACLs задаются администратором вручную. Анализируются только следующие элементы:

— Адрес источника

— Порт источника

— Адрес назначения

— Порт назначения

— Протокол

Некоторые фаерволы также могут анализировать информацию из заголовка пакета, проверяя, является ли пакет частью нового либо установленного соединения.

Если пакет, не удовлетворяет правилам, заданным в ACL , по которым он может быть пропущен в защищенную сеть, пакет отбрасывается. Преимущество статической пакетной фильтрации в ее быстродействии.

У статической пакетной фильтрации есть следующие недостатки:

— Произвольный пакет будет пропущен в сеть, если он удовлетворяет правилам ACL (например, спуфинг).

— Пакеты, которые должны быть отфильтрованы, могут попасть в сеть, если они фрагментированы.

— В процессе задания правил ACL могут формироваться очень большие списки, которыми сложно управлять.

— Ряд сервисов не может контролироваться пакетной фильтрацией. Это, например, приложения мультимедиа, где соединения динамически устанавливаются на произвольных портах, номера которых будут известны только после установки соединения.

Статическая пакетная фильтрация часто используется на маршрутизаторах. Устройства защиты Cisco также могут использовать такую фильтрацию.

Прокси-фаервол (proxy-firewall)

Прокси-фаервол, называемый также прокси-сервером - это обычно прикладная программа, устанавливаемая на сервер, имеющий доступ в защищенную и внешнюю сеть.

Все соединения хостов защищенной сети с хостами внешней сети осуществляются от имени прокси-фаервола, как если бы прокси-фаервол сам устанавливал эти соединения. Хосты защищенной сети никогда сами не устанавливают соединений с внешним миром. Для установки связи, хосты внутренней сети посылают запросы прокси-фаерволу, запросы сравниваются с базой правил.

Если запрос соответствует правилу в базе и разрешен, прокси-фаервол посылает запрос внешнему хосту и затем «форвардит» ответ внутреннему хо сту.

Прокси-фаерволы работают на верхних уровнях модели OSI. Соединения устанавливаются между сетевым и транспортным уровнем, однако прокси-фаервол анализирует запрос вплоть до седьмого уровня на предмет соответствия набору правил, если все удовлетворяет, он устанавливает соединение.

Анализ пакетов до седьмого уровня является большим преимуществом прокси-фаерволов. Но имеются и следующие недостатки:

Если прокси-фаервол будет взломан, доступ ко всей внутренней сети будет открыт

— Прокси-сервер - это программа, работающая под управлением определенной операционной системы, поэтому прокси-сервер будет настолько безопасным, насколько безопасна сама эта система

— Значительная процессорная нагрузка для осуществления прокси сервисов, что сказывается на производительности, при увеличении числа запросов на соединение. Это самая медленная технология

Динамическая пакетная фильтрация (stateful packet filtering)

Данная технология обеспечивает лучшую комбинацию безопасности и производительности. Используется не только ACL, но также анализируется состояние сессии, записываемое в базу, которую называют таблицей состояния (state table). Эту технологию Cisco преимущественно использует в своих устройствах защиты.

После того как соединение установлено, все данные сессии сравниваются с таблицей состояния. Если данные сессии не соответствуют информации в таблице состояния для этой сессии, соединение сбрасывается.

В этой технологии сохраняется состояние каждой открытой сессии. Каждый раз, когда устанавливается разрешенное внешнее либо внутреннее TCP или UDP соединение, информация об этом соединении запоминается в таблице состояния сессий. В таблицу заносится адрес источника и назначения, номера портов, порядковые номера TCP сессии (sequence numbers), также дополнительные флаги.

Зачем это необходимо? Для анализа возвращаемых пакетов в каждой конкретной сессии на предмет их легитимности (те же порты, правильные порядковые номера сессии, флаги и т.д.). То есть теперь все входящие и исходящие пакеты сравниваются с информацией в таблице состояния.

То есть в общем смысл работы динамической фильтрации заключается в следующем - если соединение, запрашиваемое хостом, разрешено Cisco фаерволом, то он запоминает это и помещает информацию о соединении в таблицу состояний (state table) и при возвращении трафика, то есть при ответе другого хоста на запрос, пакеты разрешаются, если они соответствуют тому, что ожидает устройство защиты, то есть соответствуют информации, хранящейся в state table.

Этот метод эффективен по трем причинам:

— Он работает и с пакетами и с соединениями.

— Производительность выше, чем у прокси-фаерволов.

— Сохраняется информация каждого соединения, что позволяет определить является ли пакет частью этого соединения.

Принципы использования оборудования сетевых экранов рассмотрим на примере оборудования Cisco ASA 5505.

Cisco ASA 5505 — многофункциональное устройство защиты ресурсов сети от внутренних и внешних атак для небольших офисов.

Особенности Cisco ASA 5505:

— Производительность МСЭ: до 150 Мбит/сек;

— Производительность МСЭ и отражения атак: недоступно;

— Производительность VPN: до 100 Мбит/сек;

— Количество одновременно поддерживаемых сессий: 10 000/25 000

— Число IPSec VPN-туннелей:10/25

— Число SSL VPN-туннелей: 2/25

— «Виртуальные» МСЭ: 0;

— Кластеризация и балансировка VPN: Нет;

— Поддерживаемые физические интерфейсы: 8-ми портовый коммутатор 10/100, 2 интерфейса поддерживают PoE;

— Поддержка дополнительного четырехпортового модуля Gigabit Ethernet: Нет;

— Поддерживаемые логические интерфейсы VLAN 802.1:3 (без транковых интерфейсов)/20 (с транковыми интерфейсами)

Технические характеристики ASA 5505:

— Предназначение - небольшие, домашние офисы;

— Количество защищаемых узлов: 10, 50, не ограничено

— Производительность межсетевого экрана, Мб/с: 150;

— Производительность шифрования 3DES/AES, Мб/с: 100;

— Максимальное количество IPSEC VPN сессий: 10, 25

— Максимальное количество SSL VPN сессий: 2/

— Максимальное количество контролируемых соединений: 10 000, 25000 (в зависимости от типа лицензий);

— Максимальное количество новых сессий в 1 секунду: 3000;

— Максимальная скорость обработки пакетов (64 байт) пакетов в секунду: 85000;

— Объем оперативной памяти : 256;

— Минимальный объем флэш памяти: 64;

— Количество интегрированных портов: 8x10/100 включая 2 PoE;

— Количество виртуальных сетей (VLAN): 3/20 (с использованием транков);

— Поддержка аппаратных модулей SSC/SSM : нет;

— Количество контекстов включено/максимум: 0.

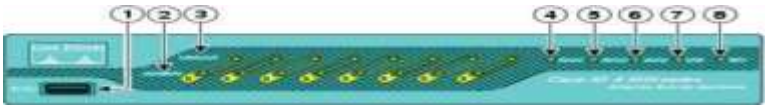


Рис.1. Вид передней панели

Таблица 9.1

Порт/ Индикация	Цвет	Статус	Описание
USB Port	—	—	Резервный USB порт для применения в будущем.
Speed Indicators	—	—	Скорость сети 10 Mbps.
	Зеленый	Горит	Скорость сети 100 Mbps.
Link Activity Indicators	Зеленый	Горит	Физическое соеденение установлено
	Зеленый	Мигает	Обмен даными в сети
Power	Зеленый	Горит	Устройство включено
	—	—	Устройство выключено

Status	Зеленый	Мигает	Диагностика и загрузка системы
		Горит	Система работает
	Желтый	Горит	Система не работает, в следствии ошибок
Active	Зеленый	Горит	Система в работе
	Желтый	Горит	Система в резерве
VPN	Зеленый	Горит	VPN тунель установлен.
		Мигает	Система устанавливает VPN тунель.
	Желтый	Горит	Тунель разорван
SSC	—	—	Наличие SSC.

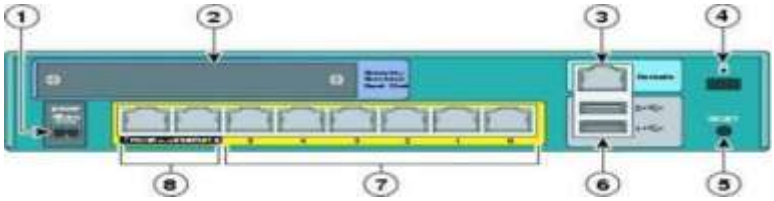


Рисунок 2 - Вид задней панели

	Порт/ Индикация	Описание
	Power connector	Порт подключения питания
	Security service card slot	Резервный слот для применения в будущем.
	Serial console port	Порт управления (консоль)
	Lock device	Разъем установления ключа
	RESET button	Перезапуск устройства
	Two USB v2.0 ports	Два резервный USB порта для применения в будушем.
	Ethernet switch ports 0-7	Ethernet порты имеюшие гибкие настройки VLAN
	PoE8 switch ports 6-7	Два порта для подключения PoE устройств (например, IP телефон)

Межсетевой экран ASA 5505 имеет возможность управления через Telnet. Так же как и коммутатор Catalyst 2960 экран первоначально не имеет никаких настроек. Первоначальная настройка производится через интерфейс консоль

Рассмотрим базовые команды устройств защиты Cisco ASA, необходимые для работоспособности данного устройства. Минимальные команды, которые необходимы для начала работы это: hostname, interface, nameif, security-level, ip address.

При первом включении необходимо войти в режим конфигураций.

```
ciscoasa> enable
ciscoasa# config terminal
ciscoasa (config)#
```

Hostname - индивидуальное имя устройства. Имя может иметь до 63 буквенно-числовых символов в верхнем и нижнем регистрах.

```
ciscoasa(config)#hostname    ASA5505
ASA5505 (config)#
```

Interface - определяет интерфейс и его расположение (слот). Для входа в конфигурацию интерфейса, необходимо указать его тип, слот и порт. Например, GigabitEthernet0/0 либо Management0/0. После чего мы можем задать необходимые параметры.

Надо помнить, что по умолчанию интерфейсы выключены, поэтому не забываем их включать командой no shutdown.

```
ciscoasa (config)# interface vlan1
ciscoasa (config-if)#
```

Nameif - команда дает имя интерфейсу на устройстве защиты. По умолчанию первые два интерфейса имеют имена inside и outside.

```
ciscoasa (config)# interface vlan1
ciscoasa (config-if)# nameif inside
```

Любому из интерфейсов устройства защиты вы можете присвоить ip адрес. Командой clear configure ip сбрасываются ip адреса на всех интерфейсах. Командой ip address также задается резервный адрес в конфигурации файловера (failover).

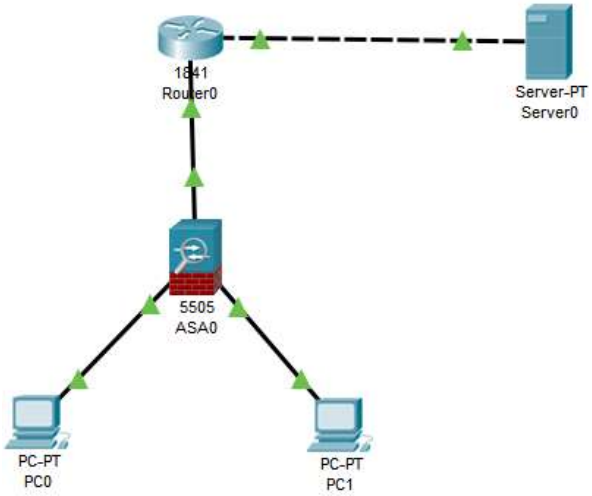
```
ciscoasa (config)# interface vlan1
ciscoasa (config-if)# nameif inside
ciscoasa (config-if)# ip address 192.168.1.1 255.255.255.0
```

Security level - по умолчанию, когда вы включите Cisco ASA, вы увидите, что внутреннему (inside) и внешнему (outside) интерфейсам уже присвоены уровни безопасности. 100 - внутреннему, 0 - внешнему. При задании имени другим интерфейсам, устройство защиты автоматически назначает им уровень безопасности 0, который вы должны будете изменить в соответствии с вашим дизайном сети.

```
ciscoasa (config)# interface vlan1
ciscoasa (config-if)# nameif inside
ciscoasa (config-if)# ip address 192.168.1.1 255.255.255.0 ciscoasa (config-if)# security-level 100
```

Ход работы

При выполнении практической работы промоделировала сеть



Вошла в управляющую программу сетевого экрана через HyperTerminal

```
ciscoasa>en
Password:
ciscoasa#
```

Вошла в режим конфигурации;

```
ciscoasa#show run
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
<--- More --->
```

По умолчанию на CISCOASA 5505 работает DHCP-сервер, поэтому подключенные к нему компьютеры автоматически получают IP-адреса.

Для обеспечения безопасного входа на устройство задала пароль для входа в привилегированный режим и пользовательское имя и пароль.

```
ciscoasa(config)#
ciscoasa(config)#enable password lab9
ciscoasa(config)#username admin password cisco
ciscoasa(config)#
```

Пароли для enable и пользователя сразу зашифрованы.

```
hostname ciscoasa
enable password jHDLkGRAqGzO2xMw encrypted

username admin password 4IncP7vTjpaba2aF encrypted
```

С помощью команды show ip address узнала параметры VLAN (должно быть настроено две VLAN: внутренняя и внешняя сети);

```
ciscoasa#conf t
ciscoasa(config)#show ip address
System IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP

Current IP Addresses:
Interface              Name                IP address      Subnet mask     Method
Vlan1                  inside              192.168.1.1     255.255.255.0   CONFIG
Vlan2                  outside             unassigned      unassigned      DHCP
```

Установила имя устройства, для повышения безопасности устройства, настроила протокол удаленного доступа SSH для этого указываем сеть, из которой будет возможен доступ (внутренняя сеть) и интерфейс, с которого будет осуществляться доступ:

```
ciscoasa(config)#hostname asa5505
asa5505(config)#ssh 192.168.1.0 255.255.255.0 inside
asa5505(config)#aaa authentication ssh console local
asa5505(config)#
```

Изменила Security-level и присвоила адрес внешнему интерфейсу, для этого выполнила следующие команды:

```
asa5505(config)#int vlan 1
asa5505(config-if)#security-level 95
asa5505(config-if)#exit
asa5505(config)#int vlan 2
asa5505(config-if)#security-level 5
asa5505(config-if)#ip add 210.210.0.2 255.255.255.252
asa5505(config-if)#no sh
asa5505(config-if)#exit
asa5505(config)#
```

Перешла к настройке маршрутизатора.

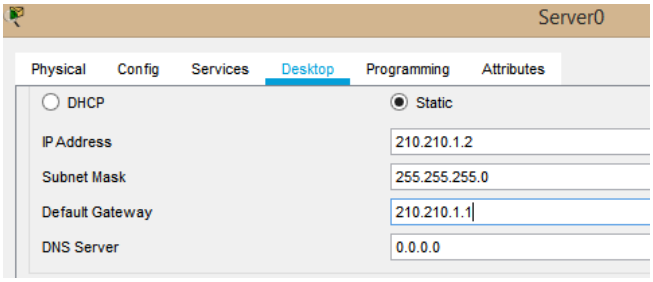
```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# int fa0/0
Router(config-if)#ip addr 210.210.0.1  255.255.255.252
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

Router(config-if)#exit
Router(config)#int fa0/1
Router(config-if)#ip addr 210.210.1.1 255.255.255.0
Router(config-if)#no sh
```

Перешла к настройке Сервера.



Прописала маршрут по умолчанию для роутера во внутреннюю сеть и для ASA во внешнюю.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip route 192.168.1.0 255.255.255.0 210.210.0.2
Router(config)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#wr mem
Building configuration...
[OK]
Router#
```

```
asa5505(config)#route outside 0.0.0.0 0.0.0.0 210.210.0.1
asa5505(config)#end
asa5505#
```

Организовала связь между компьютерами, для этого прописала на маршрутизаторе маршрут в локальную сеть и организовала инспектирование трафика на межсетевом экране, а также инспектирование HTTP-трафика.

```
asa5505(config)#class-map inspection-default
asa5505(config-cmap)#match default-inspection-traffic
asa5505(config-cmap)#exit
asa5505(config)#policy-map golbal-policy
asa5505(config-pmap)#class inspection-default
asa5505(config-pmap-c)#inspect icmp
asa5505(config-pmap-c)#exit
asa5505(config)#service-policy global-policy global
ERROR: Policy map global-policy does not exist
asa5505(config)#policy-map global-policy
asa5505(config-pmap)#class inspection-default
asa5505(config-pmap-c)#inspect http
asa5505(config-pmap-c)#end
```

Настроила автоматический NAT на устройстве ASA.

```
asa5505(config)#object network FOR-NAT
asa5505(config-network-object)#subnet 192.168.1.0 255.255.255.0
asa5505(config-network-object)#nat(inside?
% Unrecognized command
asa5505(config-network-object)#nat(inside,outside) dynamic interface
                                  ^
% Invalid input detected at '^' marker.

asa5505(config-network-object)#nat (inside,outside) dynamic interfac
asa5505(config-network-object)#end
asa5505#wr men
         ^
% Invalid input detected at '^' marker.

asa5505#wr mem
Building configuration...
Cryptochecksum: 75db19b9 2084419d 278d63f9 4f6827cf

1246  bytes copied in 2.551 secs (488 bytes/sec)
[OK]
asa5505#
```

Проверила видимость устройств во внутренней сети.

```
C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time<1ms TTL=128
Reply from 192.168.1.6: bytes=32 time=4ms TTL=128
Reply from 192.168.1.6: bytes=32 time=1ms TTL=128
Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=20ms TTL=128
Reply from 192.168.1.5: bytes=32 time<1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=8ms TTL=128
Reply from 192.168.1.5: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 20ms, Average = 8ms
```

Контрольные вопросы

1. Для чего предназначен packet filtering?
2. Для чего предназначен proxy-firewall?
3. Для чего предназначен stateful packet filtering?
4. С помощью, какой команды можно присвоить интерфейсу устройства защиты IP адрес?