Packet Tracer. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI)

Топология

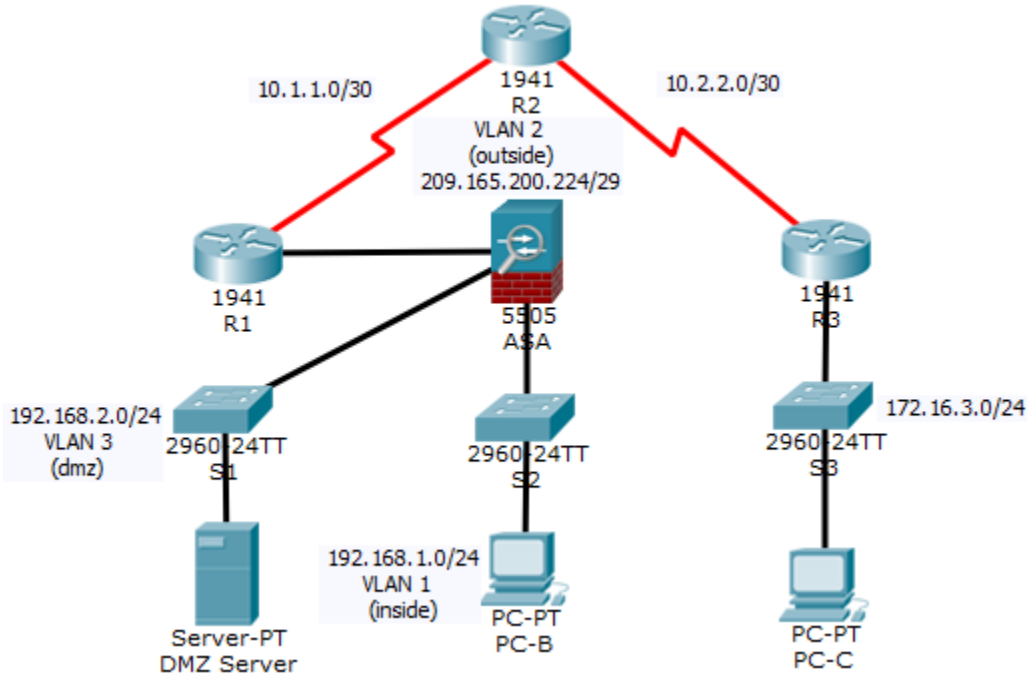

Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	209.165.200.225	255.255.255.248	Н/П
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П
	S0/0/1	10.2.2.1	255.255.255.252	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П
Сервер DMZ	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Задачи

- Проверка связи и знакомство с ASA
- Настройка основных параметров ASA и уровней безопасности интерфейса с помощью интерфейса командной строки
- Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки
- Настройка DHCP, AAA и SSH
- Настройка DMZ, статического преобразования сетевых адресов (NAT) и списков контроля доступа (ACL)

Сценарий

В вашей компании есть один пункт, подключенный к ISP. Маршрутизатор R1 представляет собой конечное устройство (CPE) под управлением ISP. R2 – это промежуточный интернет-маршрутизатор. R3 – это поставщик ISP, подключающий компьютер администратора из компании управления сетью, который был нанят на работу для дистанционного управления вашей сетью. ASA – это граничное устройство безопасности, подключающее внутрикорпоративную сеть и DMZ к ISP и одновременно предоставляющее сервисы NAT и DHCP внутренним хостам. Устройство ASA необходимо сконфигурировать для управления администратором во внутренней сети, а также удаленным администратором. Интерфейсы VLAN 3-го уровня обеспечивают доступ к трем зонам, созданным в этом задании: внутренней, внешней и DMZ. ISP назначил пространство общедоступных IP-адресов 209.165.200.224/29, которое будет использовано для преобразования адресов на ASA.

На всех маршрутизаторах и коммутаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль консоли: **ciscoconpa55**
- Имя пользователя и пароль администратора: **admin/adminpa55**

Примечание. Данное задание с Packet Tracer не заменяет лабораторные работы по ASA. Оно позволяет учащимся получить дополнительную практику и моделирует большинство конфигураций ASA 5505. По сравнению с реальным устройством ASA 5505 возможны незначительные отличия в выходных данных и командах, которые пока не поддерживаются в Packet Tracer.

Часть 1: Проверка связи и знакомство с ASA

Примечание. Это задание с Packet Tracer начинается, когда 20% оценочных вопросов отмечены как выполненные. Это сделано для того, чтобы вы случайно не изменили некоторые значения по умолчанию для ASA. Например, имя внутреннего интерфейса по умолчанию – inside, и его не следует изменять. Нажмите **Check Results** (Проверить результаты), чтобы посмотреть, какие пункты проверочной работы уже оценены как правильные.

Шаг 1: Проверка связи.

В настоящий момент устройство ASA не настроено. Однако все маршрутизаторы, компьютеры и сервер DMZ настроены. Убедитесь, что компьютер PC-C может успешно отправлять эхо-запросы на любой интерфейс маршрутизатора. Компьютер PC-C не может отправлять эхо-запросы устройству ASA, компьютеру PC-B или серверу DMZ.

Шаг 2: Определение версии, интерфейсов и лицензии для ASA.

С помощью команды **show version** определите различные аспекты этого устройства ASA.

Шаг 3: Определение файловой системы и содержимого флеш-памяти.

a. Перейдите в привилегированный режим. Пароль не задан. При появлении запроса пароля нажмите **Enter**.

b. С помощью команды **show file system** отобразите файловую систему ASA и определите поддерживаемые префиксы.

c. С помощью команды **show flash:** или **show disk0:** отобразите содержимое флеш-памяти.

Часть 2: Настройка параметров ASA и защиты интерфейса с помощью интерфейса командной строки

Совет. Многие команды интерфейса командной строки для ASA и для Cisco IOS схожи или идентичны. Кроме того, процесс перехода между режимами и подрежимами настройки практически одинаковый.

Шаг 1: Настройка имени хоста и доменного имени.

a. Установите имя хоста ASA – **CCNAS-ASA**.

b. Установите доменное имя – **ccnasecurity.com**.

Шаг 2: Установка пароля для режима привилегированного доступа.

Используйте команду **enable password** для смены пароля привилегированного режима на **ciscoenpa55**.

Шаг 3: Установка даты и времени.

С помощью команды **clock set** настройте вручную дату и время (этот шаг не оценивается).

Шаг 4: Настройка внутреннего и внешнего интерфейсов.

Сейчас вы настроите только интерфейсы VLAN 1 (внутренний) и VLAN 2 (внешний). Интерфейс VLAN 3 (dmz) будет настроен в пятой части задания.

a. Создайте логический интерфейс VLAN 1 для внутренней сети (192.168.1.0/24) и задайте наивысший уровень безопасности 100.

```
CCNAS-ASA(config)# interface vlan 1
CCNAS-ASA(config-if)# nameif inside
CCNAS-ASA(config-if)# ip address 192.168.1.1 255.255.255.0
CCNAS-ASA(config-if)# security-level 100
```

b. Создайте логический интерфейс VLAN 2 для внешней сети (209.165.200.224/29), задайте самый низкий уровень безопасности 0 и включите интерфейс VLAN 2.

```
CCNAS-ASA(config-if)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
```



```
CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# security-level 0
```

c. Используйте следующие команды для проверки настроек.

1) Используйте команду **show interface ip brief** для отображения состояния всех интерфейсов ASA. **Примечание.** Эта команда отличается от команды IOS **show ip interface brief**. Если какие-либо ранее настроенные физические или логические интерфейсы не находятся в состоянии up/up, устраните неполадки, прежде чем продолжить.

Совет. Большинство команд ASA **show**, включая **ping, copy** и другие, можно выполнить из командной строки любого режима настройки, не используя команду **do**.

2) Отобразите информацию по интерфейсам VLAN 3-го уровня, используя команду **show ip address**.

3) С помощью команды **show switch vlan** отобразите внутренние и внешние сети VLAN, настроенные на ASA, и назначенные порты.

Шаг 5: Проверка связи с ASA.

a. Вы должны отправить эхо-запрос с компьютера PC-B по адресу внутреннего интерфейса ASA (192.168.1.1). Если эхо-запрос завершился неудачно, исправьте ошибки в конфигурации.

b. С компьютера PC-B отправьте эхо-запрос на интерфейс VLAN 2 (внешний) по IP-адресу 209.165.200.226. Эхо-запрос по этому адресу должен завершиться ошибкой.

Часть 3: Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки

Шаг 1: Настройка статического маршрута по умолчанию для ASA.

Настройте на внешнем интерфейсе ASA статический маршрут по умолчанию, чтобы устройство ASA могло получать доступ к внешним сетям.

a. Создайте маршрут по умолчанию «из четырех нулей» с помощью команды **route**, свяжите его с внешним интерфейсом ASA и укажите IP-адрес (209.165.200.225) интерфейса G0/0 маршрутизатора R1 в качестве последнего шлюза.

```
CCNAS-ASA(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

b. С помощью команды **show route** убедитесь, что статический маршрут по умолчанию присутствует в таблице маршрутизации ASA.

c. Убедитесь, что ASA может успешно отправлять эхо-запрос по IP-адресу (10.1.1.1) интерфейса S0/0/0 маршрутизатора R1. Если отправить эхо-запрос не удается, устраните неполадки.

Шаг 2: Настройка преобразования адресов с помощью PAT и сетевых объектов.

a. Создайте сетевой объект **inside-net** и назначьте ему атрибуты с помощью команд **subnet** и **nat**.

```
CCNAS-ASA(config)# object network inside-net
CCNAS-ASA(config-network-object)# subnet 192.168.1.0 255.255.255.0
CCNAS-ASA(config-network-object)# nat (inside,outside) dynamic interface
CCNAS-ASA(config-network-object)# end
```

b. ASA разделяет конфигурацию на объектную часть, которая определяет преобразуемую сеть, и фактические параметры команды **nat**. Эти части находятся в двух разных местах текущей конфигурации. Отобразите конфигурацию объектов NAT с помощью команды **show run**.

c. Отправьте эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу 209.165.200.225. Эхо-запросы должны завершиться ошибкой.

d. Отправьте команду **show nat** на ASA для просмотра преобразованных и непреобразованных элементов. Обратите внимание, что среди эхо-запросов с компьютера PC-B четыре были преобразованы, а четыре – нет. Исходящие эхо-запросы были преобразованы и отправлены по назначению. Эхо-ответы были заблокированы

политикой межсетевого экрана. Вы настроите политику инспектирования по умолчанию, разрешающую протокол ICMP на шаге 3 данной части задания.

Шаг 3: Изменение глобальной политики инспектирования приложений MPF по умолчанию.

Для инспектирования уровня приложений и выполнения других сложных задач на устройствах ASA имеется инфраструктура Cisco MPF.

В Packet Tracer на устройстве ASA по умолчанию нет карты политик MPF. В качестве модификации можно создать карту политик по умолчанию для проверки трафика, направляющегося из внутренней сети во внешнюю. При правильной настройке только трафик, исходящий из внутренней сети, будет пропускаться обратно во внешний интерфейс. Вам потребуется добавить протокол ICMP в список инспектирования.

a. Создайте карту классов, карту политик и политику обслуживания. Добавьте инспектирование трафика ICMP в список карт политик с помощью следующих команд.

```
CCNAS-ASA(config)# class-map inspection_default
CCNAS-ASA(config-cmap)# match default-inspection-traffic
CCNAS-ASA(config-cmap)# exit
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
CCNAS-ASA(config-pmap-c)# exit
CCNAS-ASA(config)# service-policy global_policy global
```

b. Отправьте эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу 209.165.200.225. Эхо-запросы должны быть выполнены успешно, так как трафик ICMP теперь проверяется и легитимный обратный трафик разрешен. Если эхо-запросы завершились неудачно, исправьте ошибки в конфигурациях.

Часть 4: Настройка DHCP, AAA и SSH

Шаг 1: Настройка ASA в качестве DHCP-сервера.

a. Настройте пул адресов DHCP и включите его на внутреннем интерфейсе ASA.

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
```

b. (Необязательно) Укажите IP-адрес DNS-сервера, который нужно сообщить клиентам.

```
CCNAS-ASA(config)# dhcpd dns 209.165.201.2 interface inside
```

c. Включите демон DHCP в ASA для прослушивания запросов DHCP-клиентов на включенном интерфейсе (внутреннем).

```
CCNAS-ASA(config)# dhcpd enable inside
```

d. На компьютере PC-B замените статический IP-адрес на адрес DHCP-клиента и убедитесь, что он получает сведения об IP-адресах. При необходимости устраните неполадки.

Шаг 2: Настройка AAA на использование локальной базы данных для аутентификации.

a. Определите локального пользователя **admin** с помощью команды **username**. Задайте пароль **adminpa55**.

```
CCNAS-ASA(config)# username admin password adminpa55
```

b. Настройте AAA на использование локальной базы данных ASA для аутентификации пользователей по протоколу SSH.

```
CCNAS-ASA(config)# aaa authentication ssh console LOCAL
```


Шаг 3: Настройка удаленного доступа к ASA.

Устройство ASA можно настроить так, чтобы оно принимало подключения с одного или нескольких хостов во внутренней или внешней сети. На этом шаге хосты из внешней сети могут использовать для связи с ASA только протокол SSH. Устройства внутренней сети могут получать доступ к ASA с помощью SSH-сеансов.

a. Создайте пару ключей RSA, которая требуется для поддержки подключений SSH. Поскольку на устройстве ASA уже имеются ключи RSA, в качестве ответа введите **no**, когда будет предложено их заменить.

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.

Do you really want to replace them? [yes/no]: no
ERROR: Failed to create new RSA keys named <Default-RSA-Key>
```

b. Настройте на ASA разрешение SSH-подключений с любого хоста во внутренней сети (192.168.1.0/24) и с удаленного управляющего хоста в филиале (172.16.3.3) во внешней сети. Задайте время ожидания SSH равным 10 мин (по умолчанию – 5 мин).

```
CCNAS-ASA(config)# ssh 192.168.1.0 255.255.255.0 inside
CCNAS-ASA(config)# ssh 172.16.3.3 255.255.255.255 outside
CCNAS-ASA(config)# ssh timeout 10
```

c. Установите SSH-сеанс связи компьютера PC-C с ASA (209.165.200.226). Устраните неполадки, если они возникнут.

```
PC> ssh -l admin 209.165.200.226
```

d. Установите SSH-сеанс связи компьютера PC-B с ASA (192.168.1.1). Устраните неполадки, если они возникнут.

```
PC> ssh -l admin 192.168.1.1
```

Часть 5: Настройка DMZ, статического преобразования сетевых адресов (NAT) и списков контроля доступа (ACL)

Интерфейс G0/0 маршрутизатора R1 и внешний интерфейс ASA уже используют адреса 209.165.200.225 и .226 соответственно. Вы будете использовать общедоступный адрес 209.165.200.227 и статическое преобразование NAT для предоставления к серверу доступа с преобразованием адресов.

Шаг 1: Настройка интерфейса DMZ VLAN 3 на ASA.

a. Настройте DMZ VLAN 3, где будет располагаться веб-сервер с открытым доступом. Назначьте этой сети IP-адрес **192.168.2.1/24**, присвойте ей имя **dmz** и уровень безопасности **70**. Поскольку сервер DMZ не нуждается в связи с внутренними пользователями, отключите отправку сообщений на интерфейс VLAN 1.

```
CCNAS-ASA(config)# interface vlan 3
CCNAS-ASA(config-if)# ip address 192.168.2.1 255.255.255.0
CCNAS-ASA(config-if)# no forward interface vlan 1
CCNAS-ASA(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
CCNAS-ASA(config-if)# security-level 70
```

b. Назначьте физический интерфейс E0/2 в ASA для DMZ VLAN 3 и включите интерфейс.

```
CCNAS-ASA(config-if)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
```

c. Используйте следующие команды для проверки настроек.

1) Используйте команду **show interface ip brief** для отображения состояния всех интерфейсов ASA.

2) Отобразите информацию по интерфейсам VLAN 3-го уровня, используя команду **show ip address**.

3) С помощью команды **show switch vlan** отобразите внутренние и внешние сети VLAN, настроенные на ASA, и назначенные порты.

Шаг 2: Настройка статического преобразования NAT на сервере DMZ с помощью сетевого объекта.

Создайте сетевой объект с именем **dmz-server** и назначьте ему статический IP-адрес сервера DMZ (192.168.2.3). В режиме определения объекта введите команду **nat**, указывающую, что данный объект используется для преобразования адреса DMZ во внешний адрес с помощью статического алгоритма NAT, и введите общедоступный преобразованный адрес 209.165.200.227.

```
CCNAS-ASA(config)# object network dmz-server
CCNAS-ASA(config-network-object)# host 192.168.2.3
CCNAS-ASA(config-network-object)# nat (dmz,outside) static 209.165.200.227
CCNAS-ASA(config-network-object)# exit
```

Шаг 3: Настройка списка ACL, разрешающего доступ к серверу DMZ через Интернет.

Создайте именованный список доступа **OUTSIDE-DMZ**, разрешающий TCP-соединение на порте 80 с любого внешнего хоста к внутреннему IP-адресу сервера DMZ. Примените список контроля доступа к внешнему интерфейсу ASA во входящем направлении (IN).

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit icmp any host 192.168.2.3
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit tcp any host 192.168.2.3 eq 80
CCNAS-ASA(config)# access-group OUTSIDE-DMZ in interface outside
```

Примечание. В отличие от списков ACL в IOS, оператор permit списка ACL для ASA должен разрешать доступ к внутреннему частному адресу DMZ. Внешние хосты обращаются к серверу по его общедоступному адресу статического NAT, который ASA преобразует во внутренний IP-адрес хоста, а затем применяет список ACL.

Шаг 4: Проверка доступа к серверу DMZ.

На момент создания этого задания на Packet Tracer возможность проверки внешнего доступа к веб-серверу DMZ не была реализована, поэтому успешное выполнение этого задания не требуется.

Шаг 5: Проверка результатов.

Вы полностью выполнили задание. Нажмите **Check Results (Проверить результаты)** для просмотра отзыва и проверки завершенных обязательных компонентов.

