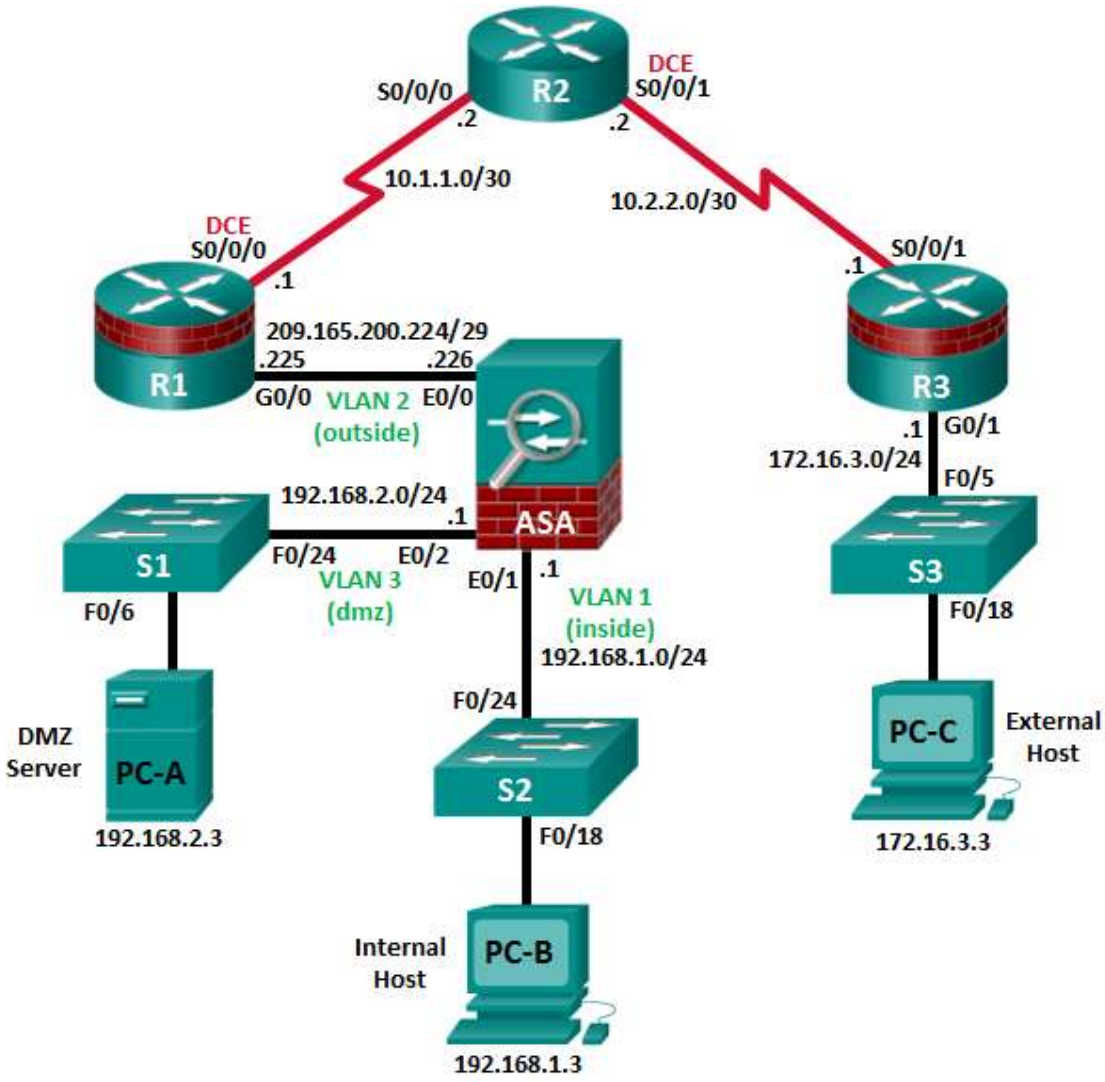
CCNA Security

Глава 9. Лабораторная работа A. Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI)

Топология



Примечание. Устройства ISR G2 используют интерфейсы FastEthernet вместо GigabitEthernet.

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
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
ASA	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

Задачи

Часть 1. Базовая настройка маршрутизатора/коммутатора/ПК

- Подключение сетевых кабелей, как показано на топологической схеме
- Настройка имен хостов и IP-адресов интерфейсов для маршрутизаторов, коммутаторов и ПК
- Настройка статических маршрутов на маршрутизаторах R1, R2 и R3
- Включение на маршрутизаторе R1 доступа по SSH и HTTP
- Конфигурирование параметров IP для хостов
- Проверка связи между хостами, коммутаторами и маршрутизаторами
- Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора

Часть 2. Доступ к консоли ASA и конфигурирование базовых параметров с помощью режима настройки CLI

- Получение доступа к консоли ASA. Проверка параметров аппаратного обеспечения, программного обеспечения и конфигурации
- Определение версии, интерфейсов и лицензии для ASA
- Определение файловой системы и содержимого флеш-памяти
- Конфигурирование базовых параметров (имен хостов, паролей, часов и т. д.) с помощью режима настройки CLI

Часть 3. Настройка основных параметров ASA и уровней безопасности интерфейса с помощью интерфейса командной строки

- Настройка имени хоста и доменного имени
- Конфигурирование пароля для входа в систему и пароля привилегированного доступа
- Установка даты и времени
- Настройка внутреннего и внешнего интерфейсов
- Проверка связи с ASA
- Настройка доступа к ASA по SSH
- Настройка на ASA доступа по HTTPS для ASDM

Часть 4. Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки

- Настройка статического маршрута по умолчанию для ASA
- Настройка PAT и сетевых объектов
- Изменение глобальной политики инспектирования приложений MPF

Часть 5. Настройка DHCP, AAA и SSH

- Настройка ASA в качестве DHCP-сервера или клиента
- Настройка локальной аутентификации пользователей AAA
- Настройка удаленного доступа к ASA по SSH

Часть 6. Настройка DMZ, статического преобразования NAT и ACL-списков

- Настройка интерфейса DMZ VLAN 3 на ASA
- Настройка статического преобразования NAT для сервера DMZ с помощью сетевого объекта
- Настройка списка ACL, разрешающего доступ к серверу DMZ через Интернет
- Проверка доступа к серверу DMZ для внешних и внутренних пользователей

Исходные данные/сценарий

Многофункциональное устройство безопасности ASA Cisco (Adaptive Security Appliance; ASA) – это усовершенствованное устройство сетевой безопасности, включающее в себя межсетевой экран с сохранением состояния, VPN и другие возможности. В данной лабораторной работе для создания межсетевого экрана и защиты внутренней корпоративной сети от внешнего проникновения, а также организации доступа в Интернет для внутренних пользователей используется ASA 5505. ASA создает три интерфейса безопасности: внешний, внутренний и DMZ. Данное устройство предоставляет внешним пользователям ограниченный доступ к DMZ и блокирует им доступ к внутренним ресурсам. Внутренние пользователи имеют доступ к DMZ и внешним ресурсам.

Основной упор в данной лабораторной работе делается на настройке ASA в качестве основного межсетевого экрана. На других устройствах необходимо выполнить минимальную настройку для поддержки работы ASA. Для конфигурирования основных параметров устройства и безопасности в лабораторной работе используется интерфейс ASA GIU, схожий с IOS CLI.

В части 1 данной лабораторной работы будет необходимо сконфигурировать топологию и устройства, отличные от ASA. В частях 2, 3 и 4 будет необходимо сконфигурировать основные параметры ASA и межсетевой экран между внутренней и внешней сетями. В части 5 будет необходимо настроить ASA для дополнительных сервисов, таких как DHCP, AAA и SSH. В части 6 будет необходимо настроить DMZ на ASA и предоставить доступ к серверу в DMZ.

В вашей компании есть одна зона, подключенная к ISP. Маршрутизатор R1 представляет собой конечное устройство (CPE), работой которого управляет 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 предоставляют доступ к трем зонам, созданным в ходе лабораторной работы: внутренней, внешней и DMZ. ISP назначил пространство общедоступных IP-адресов 209.165.200.224/29, которое будет использоваться для преобразования адресов на ASA.

Примечание. В данной лабораторной работе используются команды и выходные данные маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. В конце этой лабораторной работы приведена сводная таблица по интерфейсам маршрутизаторов, с помощью которой можно определить идентификаторы 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.

ASA, применяемое в данной лабораторной работе, представляет собой модель Cisco 5505 с интегрированным коммутатором на восемь портов, с операционной системой версии 9.2(3) и диспетчером Adaptive Security Device Manager (ASDM) версии 7.4(1) и имеет базовую лицензию, поддерживающую максимум 3 сети VLAN.

Примечание. 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)
- 3 коммутатора (Cisco 2960 с образом IOS с криптографией для поддержки SSH – Release 15.0(2)SE7 или аналогичная)
- Одно устройство ASA 5505 (версия ОС 9.2 (3), ASDM версии 7.4(1), базовая или сопоставимая лицензия)
- 3 ПК (Windows 7 или 8, с установленным SSH-клиентом)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Базовая настройка маршрутизатора/коммутатора/ПК

В части 1 этой лабораторной работы необходимо определить топологию сети и сконфигурировать основные параметры на маршрутизаторах, такие как IP-адреса интерфейсов и статическая маршрутизация.

Примечание. На данном этапе не конфигурируйте параметры ASA.

Шаг 1: Подключите сетевые кабели и сбросьте предыдущие настройки 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: Сконфигурируйте основные параметры 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 DCE-кабеля, подключенного к последовательному интерфейсу каждого из них. 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 настройки коммутаторов можно оставить по умолчанию. IP-адрес для управления сетью VLAN для коммутаторов задавать необязательно.

Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.

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

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R3(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/1
```

b. Настройте статический маршрут из маршрутизатора R2 в подсеть G0/0 маршрутизатора R1 (подключенную к интерфейсу E0/0 в ASA) и статический маршрут из маршрутизатора R2 в LAN маршрутизатора R3.

```
R2(config)# ip route 209.165.200.224 255.255.255.248 Serial0/0/0
R2(config)# ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```


Шаг 4: Включите HTTP-сервер, настройте учетную запись пользователя, зашифрованные пароли и криптографические ключи для SSH.

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

a. С помощью команды **ip http server** в режиме глобальной настройки откройте доступ по HTTP к маршрутизатору R1. Установите пароли для линий консоли и VTY – cisco. Это позволит установить веб- и SSH-цели для тестирования в будущем.

```
R1(config)# ip http server
```

b. Задайте минимальную длину пароля в 10 символов, используя команду **security passwords.**

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

c. Настройте доменное имя.

```
R1(config)# ip domain-name ccnasecurity.com
```

d. Настройте криптографические ключи для SSH.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

e. Создайте учетную запись пользователя admin01, используя algorithm-type scrypt для шифрования и пароль cisco12345.

```
R1(config)# username admin01 algorithm-type scrypt secret cisco12345
```

f. Настройте линию 0 консоли на использование локальной базы данных пользователей для входа в систему. 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)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
```

g. Настройте линию vty 0 4 на использование локальной базы данных пользователей для входа в систему и разрешите доступ только для соединений по SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
```

h. Настройте пароль привилегированного доступа с надежным шифрованием.

```
R1(config)# enable algorithm-type scrypt secret class12345
```

Шаг 5: Настройте параметры 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: Проверьте связь.

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 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 статическая маршрутизация настроена и работает исправно.

Шаг 7: Сохраните основную текущую конфигурацию для каждого маршрутизатора и коммутатора.

Часть 2: Доступ к консоли ASA и конфигурирование базовых параметров с помощью режима настройки CLI

В части 2 этой лабораторной работы вы будете обращаться к ASA через консоль и использовать различные команды **show** для определения настроек аппаратного обеспечения, программного обеспечения и конфигурации. Необходимо сбросить текущую конфигурацию и использовать утилиту интерактивной настройки CLI для конфигурирования основных параметров ASA.

Примечание. На данном этапе не конфигурируйте параметры ASA.

Шаг 1: Получите доступ к консоли ASA.

a. 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.

b. Используйте эмулятор терминала, например TeraTerm или PuTTy, для доступа к CLI. Установите следующие настройки последовательного порта: 9600 бод, 8 бит данных, без проверки четности, 1 стоповый бит, без управления потоком.

c. Войдите в привилегированный режим при помощи команды **enable** и пароля (если установлен). По умолчанию пароль пустой. Нажмите **Enter**. Если пароль был изменен на указанный в данной работе, введите слово **class.** Имя хоста ASA по умолчанию и приглашение – ciscoasa>.

```
ciscoasa> enable
Password: class (or press Enter if none set)
```

Шаг 2: Определите версию, интерфейсы и лицензии для ASA.

Комплект поставки ASA 5505 включает в себя коммутатор с восемью интегрированными портами Ethernet. Порты с E0/0 по E0/5 – обычные порты Fast Ethernet, а порты E0/6 и E0/7 – порты PoE, предназначенные для использования устройств PoE, например IP-телефонов или сетевых камер.

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

```
ciscoasa# show version

Cisco Adaptive Security Appliance Software Version 9.2(3)
Device Manager Version 7.4(1)

Compiled on Mon 15-Dec-14 18:17 by builders
System image file is "disk0:/asa923-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 23 hours 0 mins

Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB

Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode        : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode     : CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode       : CNlite-MC-IPSECm-MAIN-2.06
                             Number of accelerators: 1
```



```
 0: Int: Internal-Data0/0    : address is 0007.7dbf.5645, irq 11
 1: Ext: Ethernet0/0         : address is 0007.7dbf.563d, irq 255
 2: Ext: Ethernet0/1         : address is 0007.7dbf.563e, irq 255

<output omitted>
```

Какую версию программного обеспечения использует это ASA?

_____

Какое имя имеет файл образа системы? Откуда этот файл загружен?

_____

_____

Для управления устройством ASA можно использовать встроенный GUI, который называется диспетчером ASDM. Какую версию ASDM использует это ASA?

_____

Какой объем оперативной памяти имеет ASA?

_____

Какой объем флеш-памяти имеет ASA?

_____

Сколько портов Ethernet имеет ASA?

_____

Какой тип лицензии используется для ASA?

_____

Сколько сетей VLAN можно создать с такой лицензией?

_____

Шаг 3: Определите файловую систему и содержимое флеш-памяти.

a. С помощью команды **show file system** отобразите файловую систему ASA. Определите поддерживаемые префиксы.

```
ciscoasa# show file system

File Systems:

     Size(b)     Free(b)      Type      Flags  Prefixes
* 128573440     55664640      disk      rw      disk0: flash:
              -            -  network   rw      tftp:
              -            -  opaque    rw      system:
              -            -  network   ro      http:
              -            -  network   ro      https:
              -            -  network   rw      ftp:
              -            -  network   rw      smb:
```

Как по-другому называется flash:?_____

b. С помощью одной из команд **show flash**, **show disk0**, **dir flash:** или **dir disk0:** отобразите содержимое флеш-памяти.

```
ciscoasa# show flash
--#--  --length--  -----date/time------  path
  168  25159680    Aug 29 2011 13:00:52  asa923-k8.bin
  122  0           Aug 29 2011 13:09:32  nat_ident_migrate
   13  2048        Aug 29 2011 13:02:14  coredumpinfo
   14  59          Aug 29 2011 13:02:14  coredumpinfo/coredump.cfg
  169  16280544    Aug 29 2011 13:02:58  asdm-741.bin
    3  2048        Aug 29 2011 13:04:42  log
    6  2048        Aug 29 2011 13:05:00  crypto_archive
  171  34816       Jan 01 1980 00:00:00  FSCK0000.REC
  173  36864       Jan 01 1980 00:00:00  FSCK0001.REC
  174  12998641    Aug 29 2011 13:09:22  csd_3.5.2008-k9.pkg
  175  2048        Aug 29 2011 13:09:24  sdesktop
  211  0           Aug 29 2011 13:09:24  sdesktop/data.xml
  176  6487517     Aug 29 2011 13:09:26  anyconnect-macosx-i386-2.5.2014-k9.pkg
  177  6689498     Aug 29 2011 13:09:30  anyconnect-linux-2.5.2014-k9.pkg
  178  4678691     Aug 29 2011 13:09:32  anyconnect-win-2.5.2014-k9.pkg
  <output omitted>
```

c. Как называется файл ASDM во flash:? _____

Шаг 4: Определите текущую конфигурацию.

ASA 5505 обычно используется как граничное устройство безопасности, обеспечивающее подключение малого или домашнего офиса к устройству ISP, например к DSL или кабельному модему, для доступа в Интернет. Ниже указаны заводские настройки по умолчанию для ASA 5505.

- Сконфигурирован внутренний интерфейс VLAN 1, то есть порты коммутатора Ethernet 0/1 – 0/7. IP-адрес и маска подсети VLAN 1 – 192.168.1.1 и 255.255.255.0.
- Сконфигурирован внешний интерфейс VLAN 2, то есть порт коммутатора Ethernet 0/0. VLAN 2 получает IP-адрес от ISP, используя протокол DHCP по умолчанию.
- Маршрут по умолчанию основан на шлюзе DHCP по умолчанию.
- Все внутренние IP-адреса преобразуются при доступе к внешней среде с помощью PAT на интерфейсе VLAN 2.
- По умолчанию внутренние пользователи могут получить доступ к внешней среде с помощью списка доступа, но внешние пользователи не могут получить доступ внутрь системы.
- DHCP-сервер включен на устройстве безопасности, поэтому ПК, подключенный к интерфейсу VLAN 1, получает адрес в диапазоне 192.168.1.5–192.168.1.36 (при использовании базовой лицензии), хотя фактический диапазон адресов может быть другим.
- Сервер HTTP включен для ASDM и доступен пользователям в сети 192.168.1.0/24.
- Пароли консоли и привилегированного доступа не требуются, а имя хоста по умолчанию – ciscoasa.

Примечание. В данной лабораторной работе вы вручную настроите параметры, похожие на указанные выше, а также некоторые дополнительные параметры с помощью ASA CLI.

a. Отобразите текущую конфигурацию с помощью команды **show running-config**.

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.2(3)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2

<output omitted>
```

Примечание. Для остановки выходных данных команды с помощью CLI нажмите **Q.**

Если вы видите сети VLAN 1 и 2, а также другие параметры, настроенные так же, как описано выше, то, скорее всего, на устройстве применяется заводская конфигурация по умолчанию. Вы также можете видеть другие функции безопасности, например глобальную политику для инспектирования выбранного трафика приложений, который устройство ASA вставляет по умолчанию, если была удалена исходная конфигурация запуска. Фактические выходные данные зависят от модели ASA, его версии и состояния конфигурации.

b. Для восстановления заводской конфигурации ASA по умолчанию используйте команду **configure factory-default.**

```
ciscoasa# conf t
ciscoasa(config)# configure factory-default

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed
Executing command: interface Ethernet 0/0
Executing command: switchport access vlan 2
Executing command: no shutdown
Executing command: exit
Executing command: interface Ethernet 0/1
Executing command: switchport access vlan 1
Executing command: no shutdown
Executing command: exit

<output omitted>
```


c. Просмотрите эти выходные данные и обратите особое внимание на интерфейсы VLAN, а также разделы, относящиеся к NAT и DHCP. Они будут настроены в дальнейшем в этой лабораторной работе при помощи CLI.

d. При необходимости, заводскую конфигурацию можно скопировать и распечатать. Для копирования такой конфигурации из ASA и ее вставки в текстовый документ используйте программу эмуляции терминала. Затем, если нужно, вы сможете отредактировать данный файл, чтобы оставить в нем только необходимые команды. Чтобы активировать нужные интерфейсы, удалите команды для паролей и введите команду **no shut**.

Шаг 5: Сбросьте предыдущие настройки конфигурации ASA.

a. 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 в ASA.

b. Используйте команду **reload** для перезагрузки ASA. При этом ASA загрузится в режиме настройки CLI. При получении запроса на сохранение измененных настроек введите **N**, а затем нажмите **Enter,** чтобы продолжить перезагрузку.

```
ciscoasa# reload
Proceed with reload? [confirm]
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 6: Настройте основные параметры с помощью интерактивного режима настройки CLI.

После перезагрузки устройство ASA 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 5. Кроме того, вы можете ввести команду **setup** в режиме глобальной настройки, но сначала необходимо создать интерфейс VLAN (VLAN 1), назначить имя для управления VLAN (с помощью команды **nameif**), а также назначить для VLAN IP-адрес.

Примечание. Режим интерактивного запроса не позволяет установить на ASA заводские настройки, как описано на шаге 4. Этот режим может быть использован для настройки минимально необходимых базовых параметров, таких как имя хоста, время и пароли. Кроме того, вы можете перейти непосредственно в CLI для настройки параметров ASA, как описано в части 3.

a. После перезагрузки ASA введите следующие ответы на интерактивные запросы программы установки:

```
Pre-configure Firewall now through interactive prompts [yes]? <Enter>
Firewall Mode [Routed]: <Enter>
Enable password [<use current password>]: class
Allow password recovery [yes]? <Enter>
Clock (UTC):
  Year [2015]: <Enter>
  Month [Apr]: <Enter>
  Day [19]: <Enter>
  Time [23:32:19]: <Enter>
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com
IP address of host running Device Manager: <Enter>

The following configuration will be used:
Enable password: cisco
Allow password recovery: yes
Clock (UTC): 23:32:19 Apr 19 2015
Firewall Mode: Routed
Management IP address: 192.168.1.1
Management network mask: 255.255.255.0
Host name: ASA-Init
Domain name: generic.com


Use this configuration and save to flash? [yes] yes
INFO: Security level for "management" set to 0 by default.
Cryptochecksum: c8a535f0 e273d49e 5bddfd19 e12566b1

2070 bytes copied in 0.940 secs
Type help or '?' for a list of available commands.
ASA-Init>
```

Примечание. В описанной выше конфигурации IP-адрес хоста, на котором выполняется ASDM, оставлен пустым. На хосте установка диспетчера ASDM не является обязательной. Его можно запускать из флеш-памяти устройства ASA, используя браузер хоста.

Примечание. Введенные ответы на запросы автоматически сохраняются в текущей конфигурации (running config) и конфигурации запуска (startup-config). Однако дополнительные команды, относящиеся к безопасности, например глобальная политика инспектирования по умолчанию, вставляются в текущую конфигурацию операционной системой ASA.

b. Войдите в привилегированный режим при помощи команды **enable**. Введите пароль – **class.**

c. Введите команду **show run**, чтобы просмотреть дополнительные команды настроек по безопасности, введенные устройством ASA.

d. Введите команду **copy run start** для извлечения дополнительных команд по безопасности в файле startup-config.

Часть 3: Настройка параметров ASA и защиты интерфейса с помощью интерфейса командной строки

В части 3 необходимо настроить основные параметры с помощью ASA CLI, несмотря на то что часть из них уже была настроена с помощью интерактивных запросов режима настройки в части 2. В этой части вы начнете с параметров, настроенных в части 2, а затем добавите их или измените, чтобы создать полную базовую конфигурацию.

Совет. Многие команды интерфейса командной строки для ASA и для Cisco IOS схожи или идентичны. Кроме того, процесс перехода между режимами и подрежимами настройки по сути один и тот же.

Примечание. Прежде чем приступить к части 3, необходимо выполнить часть 2.

Шаг 1: Настройте имя хоста и доменное имя.

a. 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.

```
ASA-Init# config t
ASA-Init(config)#

***************************** NOTICE *****************************

Help to improve the ASA platform by enabling anonymous reporting,
which allows Cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall

Would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: n

In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".

Please remember to save your configuration.
```

b. Настройте имя хоста ASA с помощью команды **hostname.**

```
ASA-Init(config)# hostname CCNAS-ASA
```

c. Настройте доменное имя с помощью команды **domain-name.**

```
CCNAS-ASA(config)# domain-name ccnasecurity.com
```

Шаг 2: Установите логин и пароль для режима привилегированного доступа.

a. Пароль для входа в систему используется для соединений Telnet (а также SSH для версий ASA до 8.4). Пароль по умолчанию – cisco, но так как конфигурация запуска по умолчанию была сброшена, вы можете установить пароль с помощью команды **passwd** или **password.** Эта команда не является обязательной, так как в ходе дальнейшего выполнения лабораторной работы вы настроите ASA для доступа по SSH, а не Telnet.

```
CCNAS-ASA(config)# passwd cisco
```

b. С помощью команды **enable password** установите пароль для привилегированного режима.

```
CCNAS-ASA(config)# enable password class
```


Шаг 3: Установите дату и время.

С помощью команды **clock set** можно вручную установить дату и время. Синтаксис команды **clock set**: **clock set** *hh:mm:ss {month day | day month} year*. В следующем примере показано, как установить время и дату в 24-часовом формате:

```
CCNAS-ASA(config)# clock set 19:09:00 april 19 2015
```

Шаг 4: Настройте внутренний и внешний интерфейсы.

Примечания по интерфейсу в ASA 5505.

Модель 5505 отличается от других моделей ASA серии 5500. На других моделях ASA физическому порту можно непосредственно назначить IP-адрес третьего уровня так же, как и на маршрутизаторе Cisco. 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. Изначально все восемь портов назначены сети VLAN 1, за исключением случаев, когда присутствует заводская конфигурация по умолчанию: тогда порт E0/0 назначен сети VLAN 2. На данном шаге необходимо создать внешние и внутренние интерфейсы VLAN, именовать их, назначить им IP-адреса и установить уровень безопасности интерфейса.

Если вы выполняли процесс установки начальной конфигурации через утилиту настройки, интерфейс VLAN 1 настроен в качестве управляющей сети VLAN с IP-адресом 192.168.1.1. Вы настроите его в качестве внутреннего интерфейса в данной лабораторной работе. Сейчас вы настроите только интерфейсы VLAN 1 (внутренний) и VLAN 2 (внешний). Интерфейс VLAN 3 (dmz) будет настроен в части 6 лабораторной работы.

a. Сконфигурируйте 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 получите доступ к интерфейсу VLAN 2.

```
CCNAS-ASA(config-if)# interface vlan 2
CCNAS-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.

CCNAS-ASA(config-if)# ip address 209.165.200.226 255.255.255.248
CCNAS-ASA(config-if)# no shutdown
```

Примечания по уровням безопасности интерфейсов.

Вы можете получить сообщение о том, что уровень безопасности внутреннего интерфейса автоматически установлен на 100, а внешнего интерфейса – на 0. В ASA используется диапазон уровней безопасности от 0 до 100 для принудительного применения политики безопасности. Уровень безопасности 100 (внутренний) является наиболее безопасным, а уровень 0 (внешний) – наименее безопасным.

По умолчанию ASA применяет политику, при которой трафик из интерфейса с более высоким уровнем безопасности на интерфейс с более низким уровнем безопасности разрешен, а трафик с интерфейса с более низким уровнем безопасности на интерфейс с более высоким уровнем безопасности запрещен. Политика безопасности по умолчанию в ASA разрешает исходящий трафик, который по умолчанию не инспектируется. Возвратный трафик разрешается вследствие инспектирования пакетов с сохранением состояния. Поведение устройства ASA в качестве межсетевого экрана по умолчанию в «маршрутизируемом режиме» позволяет маршрутизировать пакеты из внутренней сети во внешнюю, но не наоборот. В части 4 данной лабораторной работы вы настроите функцию NAT для улучшения защиты межсетевого экрана.

c. С помощью команды **show interface** убедитесь, что оба порта второго уровня ASA – E0/0 (для VLAN 2) и E0/1 (для VLAN 1) – активны (up). Ниже приведен пример для E0/0. Если какой-то порт отображается как down/down, проверьте физическое соединение. Если какой-то порт административно выключен (administratively down), включите его с помощью команды **no shutdown.**

```
CCNAS-ASA# show interface e0/0
Interface Ethernet0/0 "", is administratively down, line protocol is up
  Hardware is 88E6095, BW 100 Mbps, DLY 100 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
<output omitted>
```

d. Назначьте порт ASA уровня 2 E0/1 сети VLAN 1, а порт E0/0 – сети VLAN 2. С помощью команды **no shutdown** убедитесь, что они активны.

```
CCNAS-ASA(config)# interface e0/1
CCNAS-ASA(config-if)# switchport access vlan 1
CCNAS-ASA(config-if)# no shutdown
CCNAS-ASA(config-if)# interface e0/0
CCNAS-ASA(config-if)# switchport access vlan 2
CCNAS-ASA(config-if)# no shutdown
```

Примечание. Хотя интерфейс E0/1 находится во VLAN 1 по умолчанию, команды приведены выше.

e. 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**, а также **ping, copy** и проч. можно вводить в командной строке в любом режиме настройки, не используя команду **do,** которая требуется в IOS.

```
CCNAS-ASA(config)# show interface ip brief
Interface                  IP-Address      OK? Method Status            Protocol
Ethernet0/0                unassigned      YES unset  up                up
Ethernet0/1                unassigned      YES unset  up                up
Ethernet0/2                unassigned      YES unset  up                up
Ethernet0/3                unassigned      YES unset  down              down
Ethernet0/4                unassigned      YES unset  down              down
Ethernet0/5                unassigned      YES unset  down              down
Ethernet0/6                unassigned      YES unset  down              down
Ethernet0/7                unassigned      YES unset  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
Vlan2                      209.165.200.226 YES manual up                up
Virtual0                   127.0.0.1       YES unset  up                up
```

f. Отобразите информацию по интерфейсам VLAN третьего уровня, используя команду **show ip address**.

```
CCNAS-ASA(config)# show ip address
System IP Addresses:
Interface          Name          IP address        Subnet mask      Method
Vlan1              inside        192.168.1.1       255.255.255.0    manual
Vlan2              outside       209.165.200.226   255.255.255.248  manual
```



```
Current IP Addresses:
Interface          Name           IP address        Subnet mask      Method
Vlan1              inside         192.168.1.1       255.255.255.0    manual
Vlan2              outside        209.165.200.226   255.255.255.248  manual
```

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

```
CCNAS-ASA# show switch vlan
VLAN Name                            Status    Ports
---- --------------------------------- --------- -----------------------------
1    inside                            up        Et0/1, Et0/2, Et0/3, Et0/4
                                                 Et0/5, Et0/6, Et0/7
2    outside                           up        Et0/0
```

h. Вы также можете использовать команду **show running-config interface type/number** для отображения конфигурации конкретного интерфейса из текущей конфигурации.

```
CCNAS-ASA# show run interface vlan 1
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

Шаг 5: Проверьте связь с ASA.

a. Убедитесь, что компьютер PC-B имеет статический IP-адрес 192.168.1.3 с маской подсети 255.255.255.0 и шлюз по умолчанию 192.168.1.1 (IP-адрес внутреннего интерфейса ASA VLAN 1).

b. Эхо-запросы с компьютера PC-B по адресу внутреннего интерфейса ASA, а также с ASA на PC-B, должны быть выполнены успешно. Если они завершились неудачно, исправьте ошибки в конфигурации.

```
CCNAS-ASA# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

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

Шаг 6: Настройте доступ к ASA через ASDM.

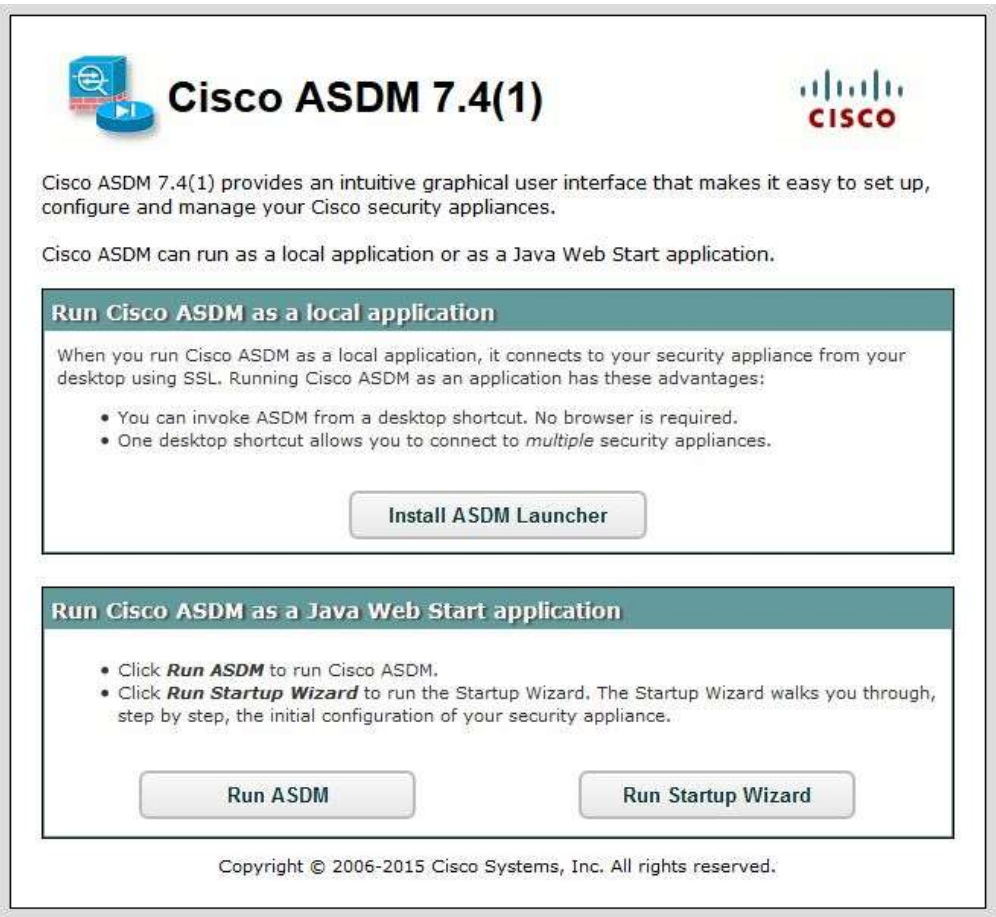
a. Вы можете настроить ASA на прием соединений HTTPS при помощи команды **http**. Это позволяет получить доступ к ASA GUI (ASDM). Настройте на ASA разрешение HTTPS-подключений с любого хоста во внутренней сети (192.168.1.0/24).

```
CCNAS-ASA(config)# http server enable
CCNAS-ASA(config)# http 192.168.1.0 255.255.255.0 inside
```

b. Откройте браузер на компьютере PC-B и проверьте HTTPS-доступ к ASA, введя адрес **https://192.168.1.1.** Вы получите предупреждение о сертификате безопасности. Нажмите **Continue**. На все другие предупреждения системы безопасности нажимайте **Yes.** Вы должны увидеть экран Cisco ASDM Welcome, на котором можно выполнить следующее: установить ASDM Launcher и запустить ASDM, просто запустить ASDM или запустить мастер запуска (Startup Wizard).

Примечание. Если вы не смогли запустить ASDM, в список IP-адресов Java нужно добавить IP-адрес.

1) Перейдите на панель управления Windows и нажмите **Java**.
2) На панели управления Java перейдите на вкладку **Security.** Нажмите **Edit Site List.**
3) В списке Exception Site нажмите **Add**. В поле Location введите **https://192.168.1.1**.
4) Нажмите **OK**, чтобы добавить IP-адрес.
5) Убедитесь, что IP-адрес добавлен. Нажмите **OK**, чтобы подтвердить изменения.



c. Закройте браузер. В следующей лабораторной работе вы будете активно использовать ASDM для конфигурирования ASA. Сейчас цель – не использование экранов конфигурирования ASDM, а проверка связи с ASA через HTTP/ASDM. Если получить доступ к ASDM не удается, проверьте настройки. Если все настройки корректны, обратитесь за помощью к инструктору.

Часть 4: Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки

В части 4 данной лабораторной работы вы настроите для ASA маршрут по умолчанию для доступа к внешним сетям. Также вы настроите преобразование адресов с помощью сетевых объектов для повышения безопасности межсетевого экрана. Затем вы измените политику инспектирования приложений по умолчанию, чтобы разрешить трафик определенного типа.

Примечание. Прежде чем приступить к части 4, необходимо выполнить часть 3.

Шаг 1: Настройте статический маршрут по умолчанию для ASA.

В части 3 вы настроили внешний интерфейс ASA со статическим IP-адресом и маской подсети. Однако для ASA не определен шлюз последней надежды (gateway of last resort). Вы настроите на внешнем интерфейсе ASA статический маршрут по умолчанию, чтобы устройство ASA могло получать доступ к внешним сетям.

Примечание. Если внешний интерфейс ASA настроен как DHCP-клиент, он может получить IP-адрес шлюза по умолчанию из ISP. Однако в рамках данной лабораторной работы внешний интерфейс сконфигурирован со статическим адресом.

a. Отправьте эхо-запрос с ASA на интерфейс G0/0 маршрутизатора R1 по IP-адресу 209.165.200.225. Эхо-запрос выполнен успешно?

_____

_____

b. Отправьте эхо-запрос с ASA на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу 10.1.1.1. Эхо-запрос выполнен успешно?

_____

_____

c. 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 шлюза последней надежды. Административная дальность по умолчанию равна единице.

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

d. С помощью команды **show route** отобразите таблицу маршрутизации ASA и только что созданный статический маршрут по умолчанию.

```
CCNAS-ASA# show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 209.165.200.225 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 209.165.200.225, outside
C        192.168.1.0 255.255.255.0 is directly connected, inside
L        192.168.1.1 255.255.255.255 is directly connected, inside
C        209.165.200.224 255.255.255.248 is directly connected, outside
L        209.165.200.226 255.255.255.255 is directly connected, outside
```

e. Отправьте эхо-запрос с ASA на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу 10.1.1.1. Эхо-запрос выполнен успешно?

_____

_____

Шаг 2: Настройте преобразование адресов с помощью PAT и сетевых объектов.

Примечание. Начиная с ASA версии 8.3, для настройки любых форм NAT используются сетевые объекты. Создается сетевой объект, и внутри него настраивается NAT. На шаге 2a сетевой объект **INSIDE-NET** используется для преобразования внутренних сетевых адресов (192.168.10.0/24) в глобальный адрес внешнего интерфейса ASA. Данный тип конфигурации объектов называется Auto-NAT.

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 команд **show run object** и **show run nat.**

```
CCNAS-ASA# show run object
object network INSIDE-NET
 subnet 192.168.1.0 255.255.255.0

CCNAS-ASA# show run nat
!
object network INSIDE-NET
 nat (inside,outside) dynamic interface
```

c. Отправьте эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу **209.165.200.225**. Эхо-запрос завершился успешно? _____.

d. Введите 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, потому что протокол ICMP не проверяется в соответствии с глобальной политикой инспектирования. Исходящие эхо-запросы были преобразованы, а обратные эхо-ответы были заблокированы политикой межсетевого экрана. Вы настроите политику инспектирования по умолчанию, разрешающую протокол ICMP, на следующем шаге. **Примечание.** В зависимости от процессов и демонов, выполняемых на компьютере, используемом как PC-B, вы можете получить большее количество преобразованных и непреобразованных элементов, чем четыре эхо-запроса и эхо-ответа.

```
CCNAS-ASA# show nat

Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic INSIDE-NET interface
    translate_hits = 4, untranslate_hits = 4
```

e. Отправьте эхо-запрос с компьютера PC-B на маршрутизатор R1 снова и быстро введите команду **show xlate,** чтобы увидеть преобразуемые адреса.

```
CCNAS-ASA# show xlate
1 in use, 28 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice

ICMP PAT from inside:192.168.1.3/512 to outside:209.165.200.226/21469 flags ri idle 0:00:03
timeout 0:00:30
```

Примечание. Флаги (r и i) показывают, что преобразование основано на карте портов (r) и оно выполнено динамически (i).

f. На компьютере PC-B откройте браузер и введите IP-адрес интерфейса G0/0 маршрутизатора R1 (209.165.200.225). Во всплывающем окне должно быть сообщение о том, что на маршрутизаторе R1 требуется аутентификация. Политика инспектирования межсетевого экрана по умолчанию разрешает основанный на TCP HTTP-трафик.

g. На ASA снова введите команды **show nat** и **show xlate**, чтобы увидеть элементы и адреса, преобразуемые для HTTP-соединения.

Шаг 3: Измените глобальную политику инспектирования приложений MPF по умолчанию.

Для инспектирования уровня приложений и выполнения других сложных задач на устройствах ASA имеется инфраструктура Cisco MPF. В Cisco MPF используются три объекта конфигурации для определения модульной, объектно-ориентированной и иерархической политик.

- **Карты классов** (class map) – определяют критерии соответствия.
- **Карты политик** (policy map) – связывают действия с критериями соответствия.
- **Сервисные политики** (service policy) – прикрепляют карту политик к интерфейсу или глобально ко всем интерфейсам устройства.

a. Отобразите карту политик MPF по умолчанию, которая инспектирует трафик, направляющийся из внутренней сети во внешнюю. Только трафик, исходящий из внутренней сети, будет пропускаться обратно во внешний интерфейс. Обратите внимание, что протокол ICMP отсутствует.

```
CCNAS-ASA# show run | begin class
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  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 ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
<output omitted>
```

b. Добавьте инспектирование трафика ICMP в список карт политик с помощью следующих команд.

```
CCNAS-ASA(config)# policy-map global_policy
CCNAS-ASA(config-pmap)# class inspection_default
CCNAS-ASA(config-pmap-c)# inspect icmp
```


c. Отобразите карту политик MPF по умолчанию и убедитесь, что теперь ICMP указан в правилах инспектирования.

CCNAS-ASA(config-pmap-c)# **show run policy-map**

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  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 ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
```

d. Отправьте эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу 209.165.200.225. Эхо-запрос должен быть выполнен успешно, так как трафик ICMP теперь инспектируется и легитимный обратный трафик разрешен.

Часть 5: Настройка DHCP, AAA и SSH

В части 5 необходимо настроить функции ASA, такие как DHCP и расширенная защита входа, с помощью AAA и SSH.

Примечание. Прежде чем приступить к части 5, необходимо выполнить часть 4.

Шаг 1: Настройте ASA в качестве DHCP-сервера.

ASA может быть как DHCP-сервером, так и DHCP-клиентом. На данном шаге необходимо настроить ASA как DHCP-сервер для динамического назначения IP-адресов для DHCP-клиентов во внутренней сети.

a. Настройте пул адресов DHCP и включите его на внутреннем интерфейсе ASA. Это будет диапазон адресов, назначаемых внутренним DHCP-клиентам. Попытайтесь установить диапазон адресов с 192.168.1.5 до 192.168.1.100.

```
CCNAS-ASA(config)# dhcpd address 192.168.1.5-192.168.1.100 inside
Warning, DHCP pool range is limited to 32 addresses, set address range as: 192.168.1.5-
192.168.1.36
```

Вам удалось выполнить это действие на ASA?

_____

_____

b. Повторите команду **dhcpd** и укажите пул как **192.168.1.5-192.168.1.36.**

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

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

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

Примечание. Также можно указать для клиентов другие параметры, такие как сервер WINS, длительность аренды и доменное имя. По умолчанию ASA устанавливает свой IP-адрес в качестве шлюза DHCP по умолчанию, поэтому настраивать его нет необходимости. Тем не менее для ручной настройки шлюза по умолчанию или установки для него IP-адреса другого сетевого устройства используйте следующую команду:

```
CCNAS-ASA(config)# dhcpd option 3 ip 192.168.1.1
```

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

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

e. Проверьте настройки демона DHCP с помощью команды **show run dhcpd.**

```
CCNAS-ASA(config)# show run dhcpd
dhcpd dns 209.165.201.2
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
```

f. Откройте Network Connection IP Properties для компьютера PC-B, вместо статического IP-адреса укажите DHCP-клиент, чтобы PC-B автоматически получал IP-адрес с DHCP-сервера на устройстве ASA. Данная процедура зависит от операционной системы этого компьютера. Возможно, потребуется ввести на компьютере PC-B команду **ipconfig /renew**, чтобы он принудительно получал новый IP-адрес из ASA.

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

a. Определите локального пользователя **admin** с помощью команды **username**. Задайте пароль **cisco12345.**

```
CCNAS-ASA(config)# username admin password cisco12345
```

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

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

Примечание. Начиная с версии ASA 8.4(2), для большей безопасности настройте аутентификацию AAA для поддержки соединений SSH. Вход по умолчанию по Telnet/SSH не поддерживается. Вы больше не сможете подключиться по SSH к ASA, используя для входа имя пользователя и пароль по умолчанию.

Шаг 3: Настройте удаленный доступ к ASA по SSH.

Устройство ASA можно настроить так, чтобы оно принимало соединения SSH с одного или нескольких хостов во внутренней или внешней сети.

a. Создайте пару ключей **RSA**, которая требуется для поддержки подключений SSH. Размер модуля (в битах) может быть 512, 768, 1024 или 2048. Чем больший размер модуля ключа вы укажете, тем дольше будет генерироваться RSA. Укажите размер модуля **1024** с помощью команды **crypto key.**

```
CCNAS-ASA(config)# crypto key generate rsa modulus 1024
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Примечание. Вы можете получить сообщение, что пара ключей RSA уже определена. Чтобы заменить пару ключей RSA, ответьте **yes**.

b. Сохраните ключи RSA во флеш-память с помощью команды **copy run start** или **write mem.**

```
CCNAS-ASA# write mem
Building configuration...
Cryptochecksum: 3c845d0f b6b8839a f9e43be0 33feb4ef
3270 bytes copied in 0.890 secs
[OK]
```

c. 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
```

d. На компьютере PC-C используйте клиент SSH, например PuTTY, и попытайтесь подключиться к внешнему интерфейсу ASA по адресу **209.165.200.226**. При первом соединении вы можете получить запрос от SSH-клиента на приемку ключа RSA хоста SSH-сервера ASA. Войдите в систему как пользователь **admin** с паролем **cisco12345.** Вы также можете подключиться к внутреннему интерфейсу ASA по IP-адресу **192.168.1.1** с клиента SSH на PC-B.

Часть 6: Настройка DMZ, статического преобразования NAT и ACL-списков

Ранее вы настроили маршрутизацию для внутренней сети при помощи PAT. В этой части необходимо создать DMZ на ASA, настроить на сервере DMZ статическое преобразование NAT, а затем применить списки ACL для контроля доступа к серверу.

Для обеспечения 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 внешний интерфейс ASA уже используют 209.165.200.225 и .226. Вы будете использовать общедоступный адрес 209.165.200.227 и статическое преобразование NAT для предоставления серверу доступа с преобразованием адресов.

Шаг 1: Настройте интерфейс DMZ VLAN 3 на ASA.

a. Настройте DMZ VLAN **3**, где будет располагаться веб-сервер с открытым доступом. Назначьте сети VLAN 3 IP-адрес **192.168.2.1/24**, присвойте ей имя **dmz**, и уровень безопасности **70**.

Примечание. Если вы работаете на ASA 5505 с базовой лицензией, вы увидите сообщение об ошибке, показанное в выходных данных ниже. Базовая лицензия ASA 5505 позволяет создать до 3 именованных интерфейсов VLAN. Однако вам придется отключить связь между третьим интерфейсом и одним из двух других, используя команду **no forward**. Эта проблема не возникает с лицензией ASA Security Plus, которая допускает создание до 20 именованных сетей VLAN.

Так как сервер не нуждается в установке связи с внутренними пользователями, отключите пересылку 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)# nameif dmz
ERROR: This license does not allow configuring more than 2 interfaces with
nameif and without a "no forward" command on this interface or on 1 interface(s)
with nameif already configured.
```



```
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
CCNAS-ASA(config-if)# no shut
```

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

```
CCNAS-ASA(config-if)# interface Ethernet0/2
CCNAS-ASA(config-if)# switchport access vlan 3
CCNAS-ASA(config-if)# no shut
```

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

```
CCNAS-ASA # show interface ip brief
Interface                  IP-Address      OK? Method Status            Protocol
Ethernet0/0                unassigned      YES unset  up                up
Ethernet0/1                unassigned      YES unset  up                up
Ethernet0/2                unassigned      YES unset  up                up
Ethernet0/3                unassigned      YES unset  down              down
Ethernet0/4                unassigned      YES unset  down              down
Ethernet0/5                unassigned      YES unset  down              down
Ethernet0/6                unassigned      YES unset  down              down
Ethernet0/7                unassigned      YES unset  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
Vlan2                      209.165.200.226 YES manual up                up
Vlan3                      192.168.2.1     YES manual up                up
Virtual0                   127.0.0.1       YES unset  up                up
```

d. Отобразите информацию по интерфейсам VLAN третьего уровня, используя команду **show ip address**.

```
CCNAS-ASA # show ip address
System IP Addresses:
Interface          Name            IP address        Subnet mask       Method
Vlan1              inside          192.168.1.1       255.255.255.0     manual
Vlan2              outside         209.165.200.226   255.255.255.248   manual
Vlan3              dmz             192.168.2.1       255.255.255.0     manual
<output omitted>
```

e. Отобразите сети VLAN и назначенные порты на устройстве ASA, используя команду **show switch vlan**.

```
CCNAS-ASA(config)# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    inside                           up        Et0/1, Et0/3, Et0/4, Et0/5
                                                Et0/6, Et0/7
2    outside                          up        Et0/0
3    dmz                              up        Et0/2
```


Шаг 2: Настройте статическое преобразование 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
```

Шаг 3: Настройте список ACL, разрешающий доступ к серверу DMZ через Интернет.

Создайте именованный список доступа (**OUTSIDE-DMZ**), разрешающий любое IP-соединение с любого внешнего хоста с внутренним IP-адресом сервера DMZ. Примените список контроля доступа к внешнему интерфейсу ASA в направлении **IN**.

```
CCNAS-ASA(config)# access-list OUTSIDE-DMZ permit ip any host 192.168.2.3
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.

Данный список ACL можно изменить, чтобы открыть внешним хостам только нужные сервисы, например веб (HTTP) или FTP.

Шаг 4: Проверьте доступ к серверу DMZ.

a. Создайте интерфейс loopback 0 на маршрутизаторе R2, представляющем собой внешний хост. Назначьте для **Lo0** IP-адрес **172.30.1.1** и маску подсети **255.255.255.0**. Отправьте эхо-запрос с маршрутизатора R2 на общедоступный адрес сервера DMZ, используя интерфейс loopback в качестве источника такого запроса. Эхо-запрос должен быть выполнен успешно.

```
R2(config-if)# interface lo0
R2(config-if)# ip address 172.30.1.1 255.255.255.0
R2(config-if)# end
R2# ping 209.165.200.227 source lo0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.227, timeout is 2 seconds:
Packet sent with a source address of 172.30.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

b. Сбросьте счетчики NAT с помощью команды **clear nat counters**.

```
CCNAS-ASA# clear nat counters
```

c. Отправьте эхо-запрос с PC-C на сервер DMZ по общедоступному адресу **209.165.200.227**. Эхо-запрос должен быть выполнен успешно.

d. Чтобы увидеть эффект эхо-запроса, введите на ASA команды **show nat** и **show xlate.** Показаны политики PAT (из внутренней сети во внешнюю) и статического NAT (из DMZ во внешнюю сеть).


```
CCNAS-ASA# show nat

Auto NAT Policies (Section 2)
1 (dmz) to (outside) source static dmz-server 209.165.200.227
    translate_hits = 0, untranslate_hits = 4

2 (inside) to (outside) source dynamic INSIDE-NET interface
    translate_hits = 4, untranslate_hits = 0
```

Примечание. Эхо-запросы из внутренней сети во внешнюю являются преобразованными элементами. Эхо-запросы с внешнего хоста PC-C в DMZ не являются преобразованными элементами.

```
CCNAS-ASA# show xlate
1 in use, 3 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
NAT from dmz:192.168.2.3 to outside:209.165.200.227
    flags s idle 0:22:58 timeout 0:00:00
```

Примечание. На этот раз указан флаг **s**, что означает статическое преобразование.

e. Вы также можете получить доступ к серверу DMZ с хоста во внутренней сети, так как на внутреннем интерфейсе ASA (VLAN 1) установлен уровень безопасности 100 (самый высокий), а на интерфейсе DMZ (VLAN 3) – 70. ASA выполняет роль маршрутизатора 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, а также тому факту, что протокол ICMP проверяется на внутреннем интерфейсе глобальной политикой инспектирования. Эхо-запросы из PC-B в PC-A не будут влиять на число преобразований NAT, потому что эти компьютеры находятся за межсетевым экраном и преобразование не выполняется.

f. Сервер DMZ не может отправить эхо-запрос на компьютер PC-B, так как уровень безопасности интерфейса VLAN 3 сервера DMZ ниже, а также потому, что была указана команда **no forward** при создании интерфейса VLAN 3. Попытайтесь отправить эхо-запрос с PC-A сервера DMZ на PC-B по IP-адресу **192.168.1.3.** Запрос должен быть выполнен с ошибкой.

g. Используйте команду **show run** для отображения конфигурации для VLAN 3.

```
CCNAS-ASA# show run interface vlan 3
!
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 70
 ip address 192.168.2.1 255.255.255.0
```

Примечание. Список доступа может быть применен к внутреннему интерфейсу, чтобы контролировать тип доступа (разрешить или отклонить) к DMZ-серверу для внутренних хостов.

Вопросы для повторения

1. Чем конфигурации межсетевого экрана ASA и ISR отличаются друг от друга?

_____

_____

_____

_____

2. Что использует ASA для определения преобразования адресов и в чем преимущества данного способа?

   _____

   _____

   _____

   _____

3. Как ASA 5505 использует логические и физические интерфейсы для управления безопасностью и в чем отличия от других моделей ASA?

   _____

   _____

   _____

   _____

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.

