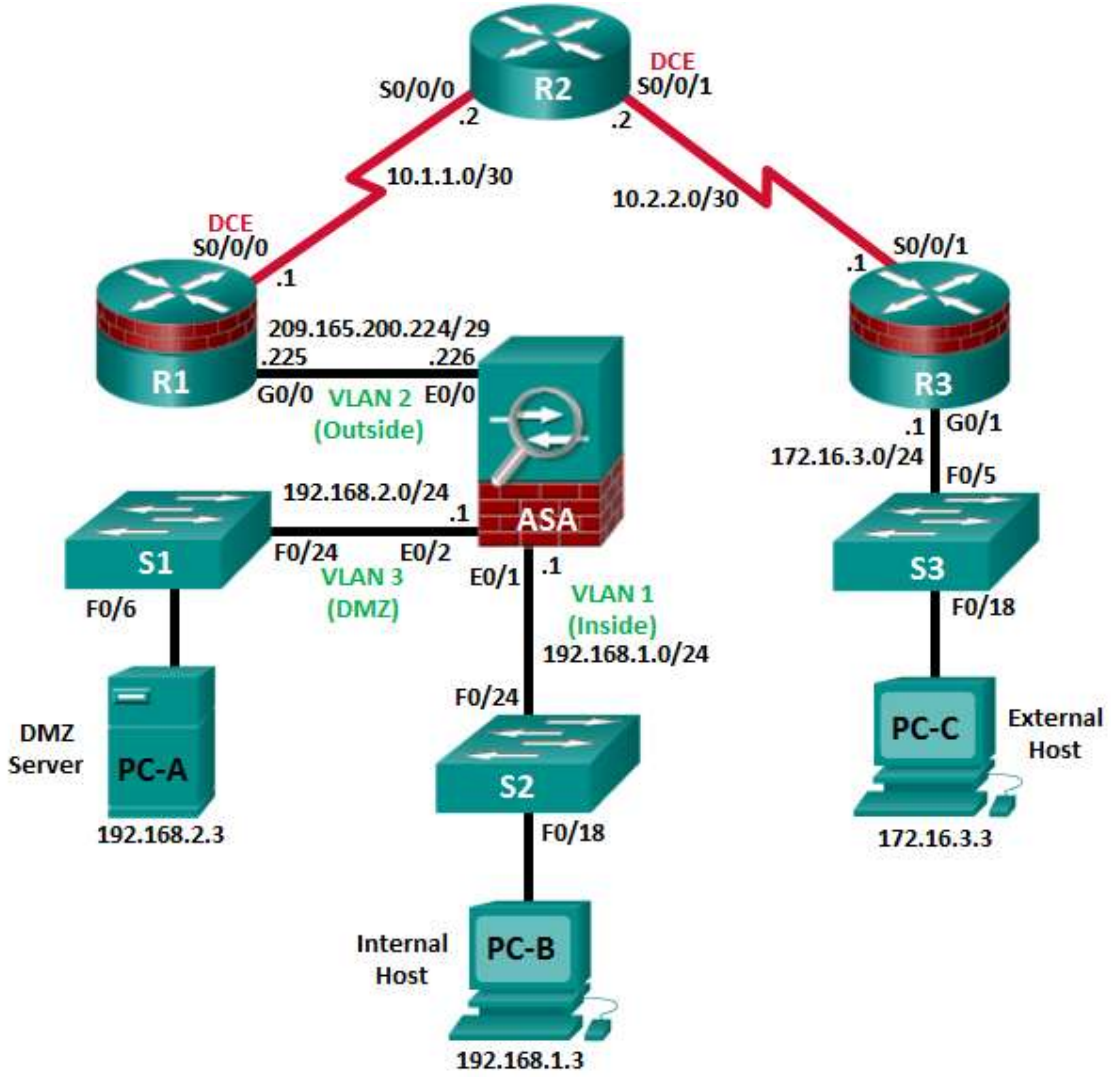
CCNA Security

Глава 10. Настройка основных параметров ASA и межсетевого экрана с помощью ASDM

Топология



Примечание. В устройствах ISR G1 используются 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
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

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

Часть 2. Организация доступа к консоли ASA и ASDM

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

Часть 3. Настройка ASA и межсетевого экрана с использованием мастера запуска ASDM

- Войдите в меню конфигурации и запустите мастер запуска.
- Установите имя хоста, доменное имя и пароль привилегированного доступа.
- Настройте внутренние и внешние интерфейсы VLAN.
- Настройте DHCP, преобразование адресов и административный доступ.
- Проверьте краткую информацию и отправьте команды на ASA.
- Проверьте доступ к внешнему веб-сайту с компьютера PC-B.
- Проверьте доступ к внешнему веб-сайту с использованием утилиты ASDM Packet Tracer.

Часть 4. Настройка параметров ASA в меню конфигурации ASDM

- Установите дату и время на ASA.
- Настройте статический маршрут по умолчанию для ASA.
- Настройте аутентификацию пользователей AAA с использованием локальной базы данных ASA.
- Проверьте доступ к ASA по SSH.
- Проверьте связь с использованием команд ASDM Ping и Traceroute.
- Измените политику инспектирования приложений в MPF.

Часть 5. Настройка DMZ, статического преобразования NAT и ACL-списков

- Настройте интерфейс ASA DMZ VLAN 3.
- Настройте сервер DMZ и статическое преобразование NAT.
- Проверьте правило доступа к DMZ, сгенерированное приложением ASDM.
- Проверьте доступ к серверу DMZ из внешней сети.

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 приложение ASDM графического интерфейса пользователя (GUI) в ASA.

В части 1 этой лабораторной работы необходимо сконфигурировать топологию и устройства, отличные от ASA. В части 2 необходимо подготовить ASA к доступу через ASDM. В третьей части с помощью мастера запуска ASDM необходимо будет сконфигурировать основные параметры ASA и межсетевой экран между внутренней и внешней сетями. В четвертой части будет необходимо сконфигурировать дополнительные параметры через меню конфигурации ASDM. В пятой части будет необходимо сконфигурировать DMZ на устройстве ASA и предоставить доступ к серверу в DMZ.

В вашей компании есть одна зона, подключенная к ISP. Маршрутизатор R1 – это клиентское устройство (CPE), которым управляет поставщик ISP. R2 – это промежуточный интернет-маршрутизатор. Маршрутизатор R3 подключает компьютер администратора из компании управления сетью, который был нанят 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. 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 для маршрутизатора Cisco 1941 с ПО Cisco IOS Release 15.4(3)M2 (с лицензией Security Technology Package). Допускается использование других маршрутизаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. В зависимости от модели маршрутизатора и версии Cisco IOS, доступные команды и выходные данные могут отличаться от указанных в данной лабораторной работе.

ASA в данной лабораторной работе представляет собой модель Cisco 5505 с встроенным 8-портовым коммутатором, с ОС версии 9.2(3) и ASDM версии 7.4(1) и имеет базовую лицензию, поддерживающую максимум три сети VLAN.

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

Необходимые ресурсы

- Одно устройство ASA 5505 (версия ОС 9.2 (3), ASDM версии 7.4(1), базовая или сопоставимая лицензия)
- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 3 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 3 ПК (Windows 7 или 8.1, с установленным SSH-клиентом и WinRadius)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

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

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

Шаг 2: Конфигурирование основных параметров для маршрутизаторов и коммутаторов.

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

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

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

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

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

Шаг 3: Настройка статической маршрутизации на маршрутизаторах.

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

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

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

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

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


Шаг 4: Конфигурирование и шифрование паролей на маршрутизаторе R1.

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

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

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

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

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

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

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

Шаг 5: Конфигурирование параметров IP для хостов.

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

Шаг 6: Проверка связи.

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

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

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

Часть 2: Доступ к консоли ASA и ASDM

В части 2 вы будете обращаться к ASA через консоль и использовать различные команды **show** для определения настроек аппаратного обеспечения, программного обеспечения и конфигурации. Необходимо будет подготовить ASA к доступу через ASDM, изучить экраны ASDM, а также его параметры.

Шаг 1: 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 для доступа к CLI. Установите следующие настройки последовательного порта: 9600 бод, 8 бит данных, без проверки четности, 1 стоповый бит, без управления потоком.

c. При получении запроса на вход в режим интерактивной настройки межсетевого экрана (режим установки) ответьте **no**.

d. Войдите в привилегированный режим при помощи команды **enable** и пароля (если установлен). По умолчанию пароль пустой, поэтому просто нажмите **Enter.** Если пароль был изменен на указанный в данной лабораторной работе, введите пароль **cisco12345.** Имя хоста ASA по умолчанию и приглашение – **ciscoasa>**.

```
ciscoasa> enable
Password: cisco12345 (or press Enter if no password is set)
```


Шаг 2: Сброс предыдущих настроек конфигурации ASA.

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 на ASA.

b. Используйте команду **reload** для перезагрузки ASA. При этом ASA загрузится в режиме настройки CLI. Если вы получите сообщение: “`System config has been modified. Save? [Y]es/[N]o:`”, введите **n** и нажмите **Enter.**

```
ciscoasa# reload
Proceed with reload? [confirm] <Enter>
ciscoasa#
***
*** --- START GRACEFUL SHUTDOWN ---
Shutting down isakmp
Shutting down File system
***
*** --- SHUTDOWN NOW ---
Process shutdown finished
Rebooting.....
CISCO SYSTEMS
Embedded BIOS Version 1.0(12)13 08/28/08 15:50:37.45
<output omitted>
```

Шаг 3: Пропуск режима настройки и конфигурирование интерфейсов ASDM VLAN.

После перезагрузки ASA оно должно определить, что не хватает файла **startup-config**, и выполнить серию интерактивных запросов для конфигурирования основных параметров ASA. Если переход в данный режим не выполняется, повторите шаг 2.

a. При запросе на предварительную настройку межсетевого экрана с помощью интерактивных запросов (режим установки) ответьте **no.**

```
Pre-configure Firewall now through interactive prompts [yes]? no
```

b. Войдите в привилегированный режим при помощи команды **enable**. На данном этапе пароль должен быть пустым (отсутствовать).

c. 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.**

d. Настройте внутренний интерфейс VLAN 1 для подготовки к доступу через ASDM. Уровень безопасности должен быть автоматически установлен на наивысший уровень **100.** Логический интерфейс VLAN 1 будет использоваться компьютером PC-B для доступа к ASDM на физическом интерфейсе E0/1 устройства ASA.

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
INFO: Уровень безопасности для внутреннего интерфейса inside установлен на значение 100
по умолчанию.
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# exit
```

Компьютер PC-B подключен к коммутатору S2. Коммутатор S2 подключен к порту E0/1 на ASA. Почему не нужно добавлять физический интерфейс E0/1 к этой VLAN?

_____

_____

Примечания по интерфейсу в ASA 5505.

Модель 5505 отличается от других моделей ASA серии 5500. На других устройствах ASA, к примеру на маршрутизаторе Cisco, физическому порту можно непосредственно назначить IP-адрес 3-го уровня. ASA 5505 имеет 8 встроенных портов коммутатора, являющихся портами уровня 2. Для назначения параметров уровня 3 необходимо создать виртуальный интерфейс коммутатора (SVI) или логический интерфейс VLAN и затем назначить ему один или несколько физических портов уровня 2.

По умолчанию все физические интерфейсы ASA административно отключены (down), за исключением случаев, когда была запущена утилита установки (Setup) или были сброшены заводские настройки. Так как никакие физические интерфейсы в сети VLAN 1 не включены, VLAN 1 находится в состоянии down/down. Чтобы в этом убедиться, используйте команду **show interface ip brief.**

```
ciscoasa(config)# show interface ip brief
Interface        IP-Address    OK? Method Status                Protocol
Ethernet0/0      unassigned    YES unset  administratively down up
Ethernet0/1      unassigned    YES unset  administratively down up
Ethernet0/2      unassigned    YES unset  administratively down up
Ethernet0/3      unassigned    YES unset  administratively down up
Ethernet0/4      unassigned    YES unset  administratively down down
Ethernet0/5      unassigned    YES unset  administratively down down
Ethernet0/6      unassigned    YES unset  administratively down down
Ethernet0/7      unassigned    YES unset  administratively down down
Internal-Data0/0 unassigned    YES unset  up                   up
Internal-Data0/1 unassigned    YES unset  up                   up
Vlan1            192.168.1.1   YES manual down                 down
Virtual0         127.0.0.1     YES unset  up                   up
```

e. Включите интерфейс E0/1 с помощью команды **no shutdown** и проверьте состояние интерфейсов E0/1 и VLAN 1. Состояние и протокол для интерфейсов E0/1 и VLAN 1 должны быть up/up.

```
ciscoasa(config)# interface e0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# exit

ciscoasa(config)# show interface ip brief
Interface        IP-Address    OK? Method Status                Protocol
Ethernet0/0      unassigned    YES unset  administratively down up
Ethernet0/1      unassigned    YES unset  up                   up
Ethernet0/2      unassigned    YES unset  administratively down up
```



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

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

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

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

Шаг 4: Настройка ASDM и проверка доступа к ASA.

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

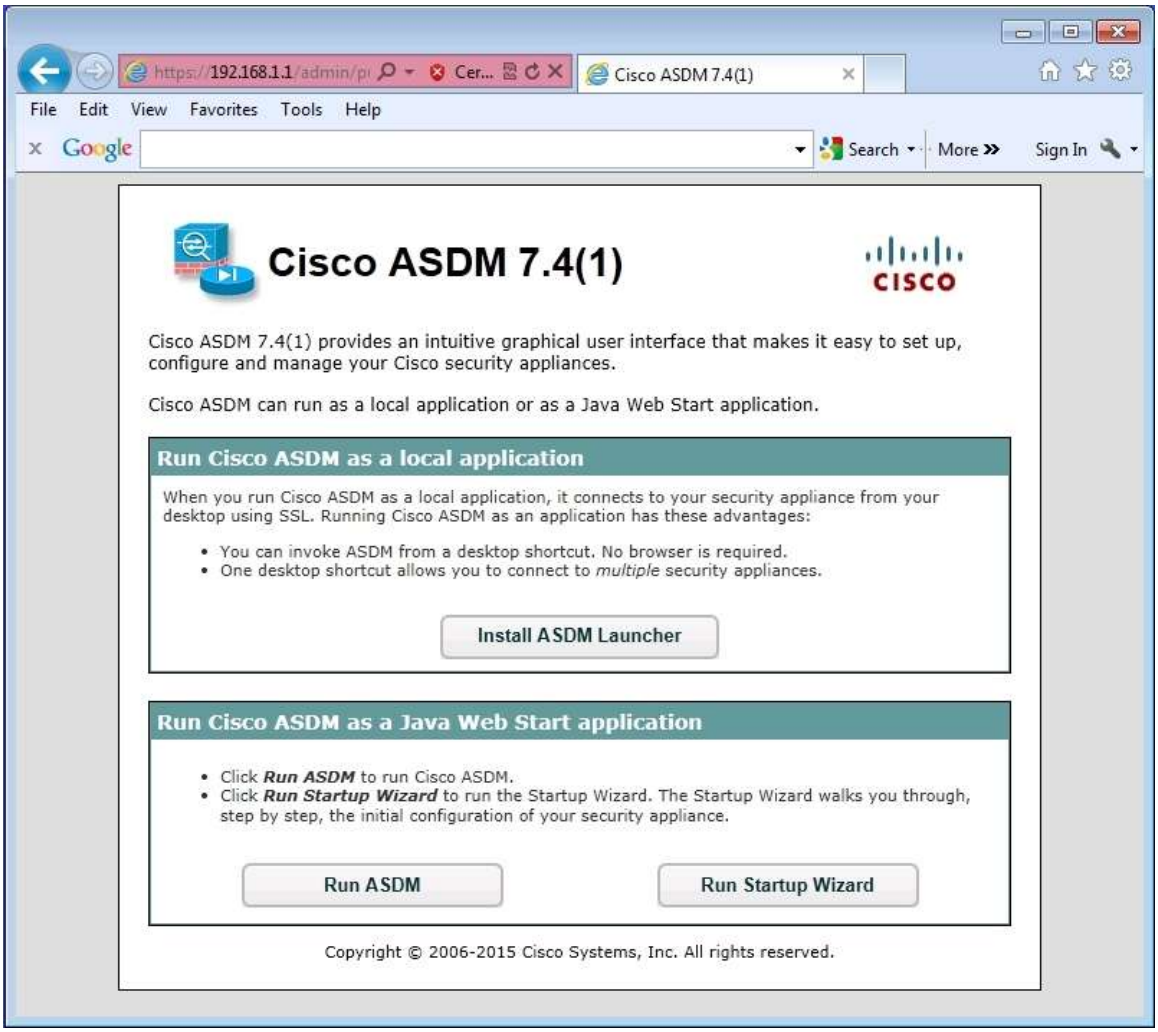
```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.1.0 255.255.255.0 inside
```

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

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

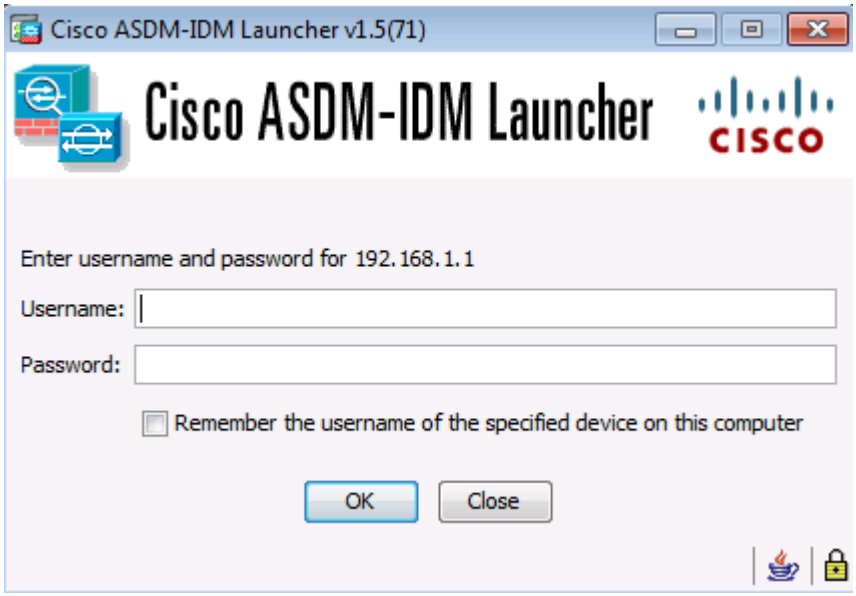
Шаг 5: Доступ к ASDM и изучение GUI.

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



b. Нажмите **Run ASDM**.

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

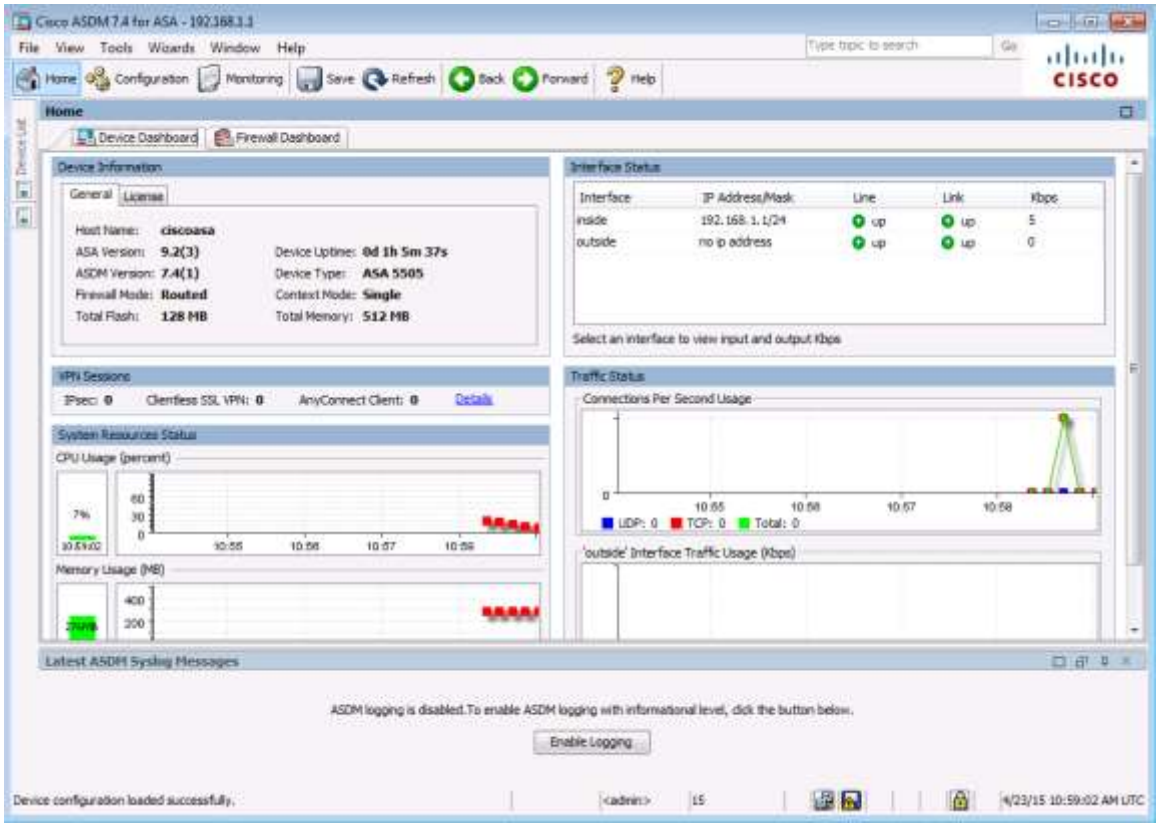


d. Для продолжения щелкните **OK**. ASDM загрузит текущую конфигурацию в GUI.

e. Появляется начальный экран GUI, содержащий различные области и параметры. Меню в верхней левой части экрана содержит три основных раздела:: Home, Configuration и Monitoring. Раздел Home является разделом по умолчанию и состоит из двух информационных панелей: Device и Firewall. Экраном по умолчанию является информационная панель Device, на которой отображается информация об устройстве, например тип (ASA 5505), версии ASA и ASDM, объем памяти и режим межсетевого экрана (routed). На информационной панели Device имеются пять зон:

- Device Information
- Interface Status
- VPN Sessions
- System Resources Status
- Traffic Status

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



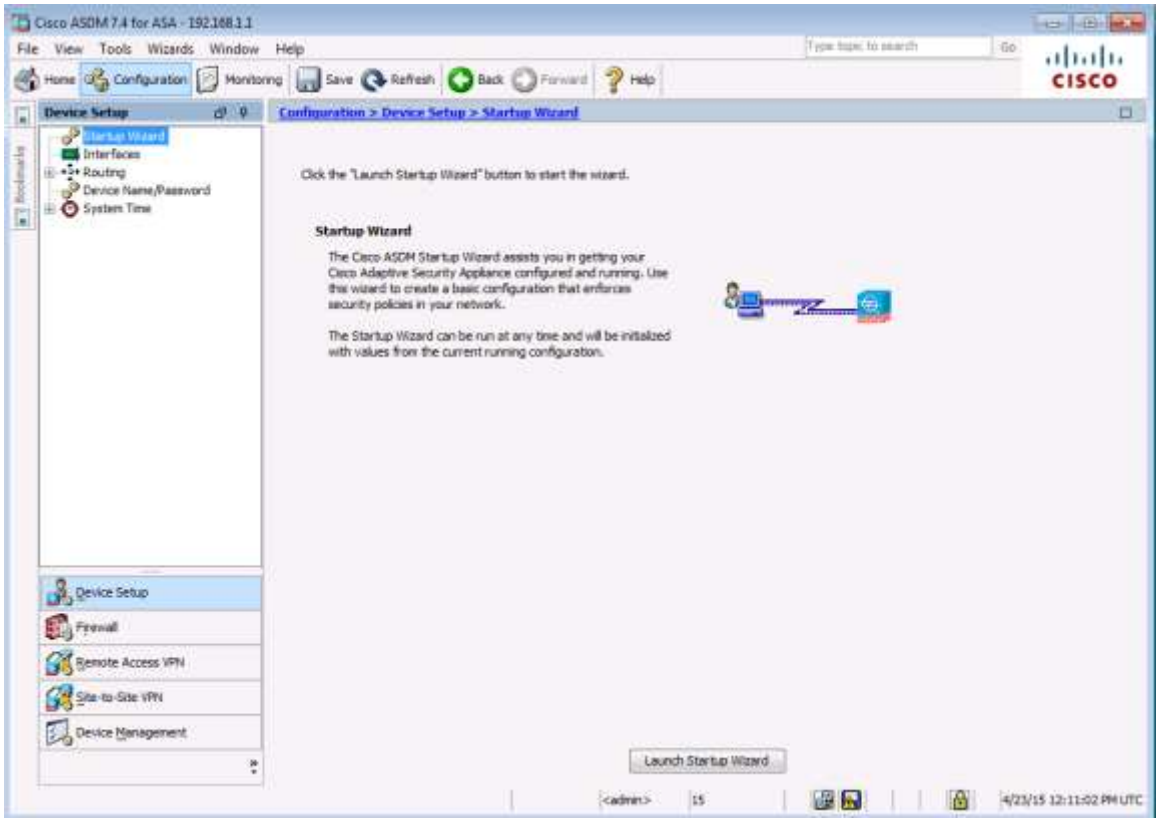
f. Нажмите кнопки **Configuration** и **Monitoring,** чтобы познакомиться с их расположением и увидеть доступные опции.

Часть 3: Настройка основных параметров ASA и межсетевого экрана с помощью мастера запуска ASDM

Шаг 1: Вход в меню конфигурации и запуск Startup Wizard.

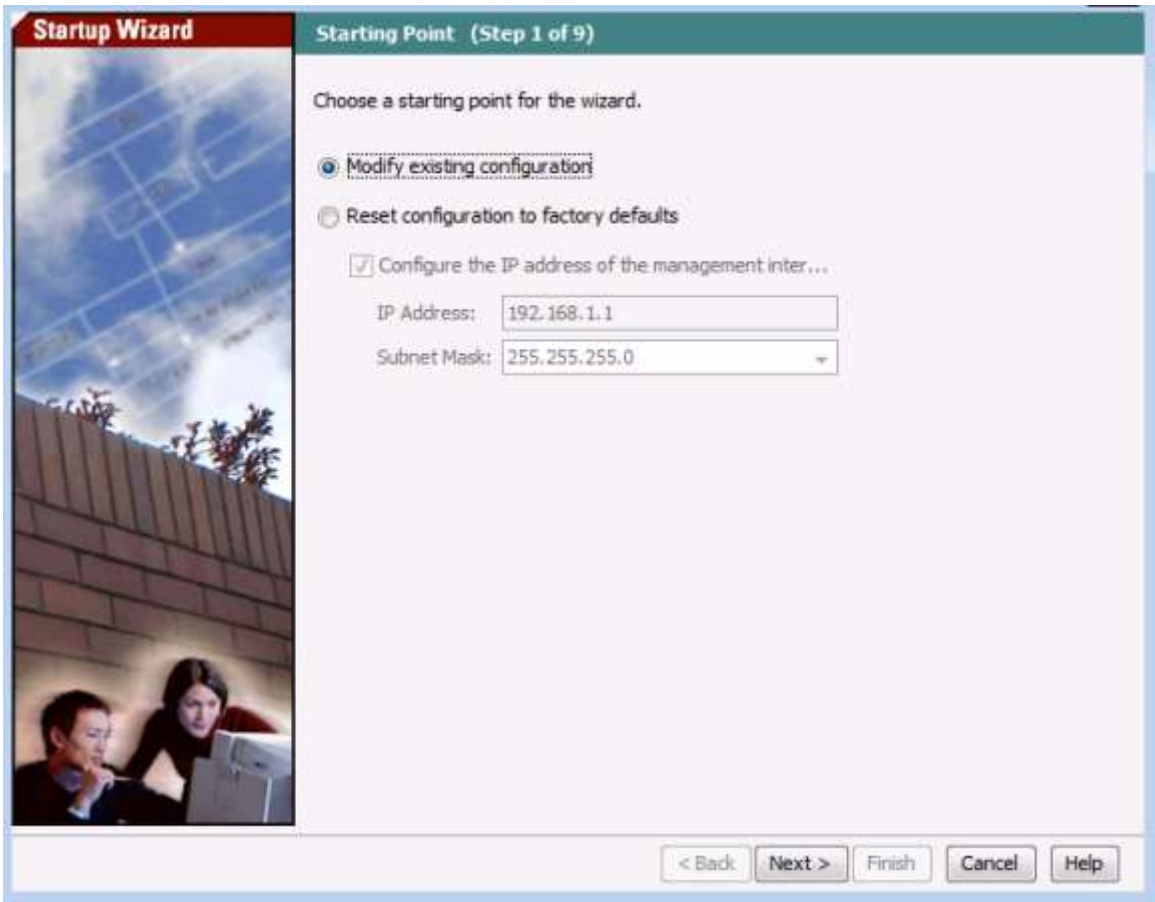
a. В строке меню нажмите **Configuration.** Есть 5 основных зон конфигурирования:
   - Device Setup
   - Firewall
   - Remote Access VPN
   - Site-to-Site VPN
   - Device Management

b. Мастер Device Setup Startup – первая доступная опция, которая отображается по умолчанию. Ознакомьтесь с текстом на экране, описывающим мастер запуска, а затем щелкните **Launch Startup Wizard.**

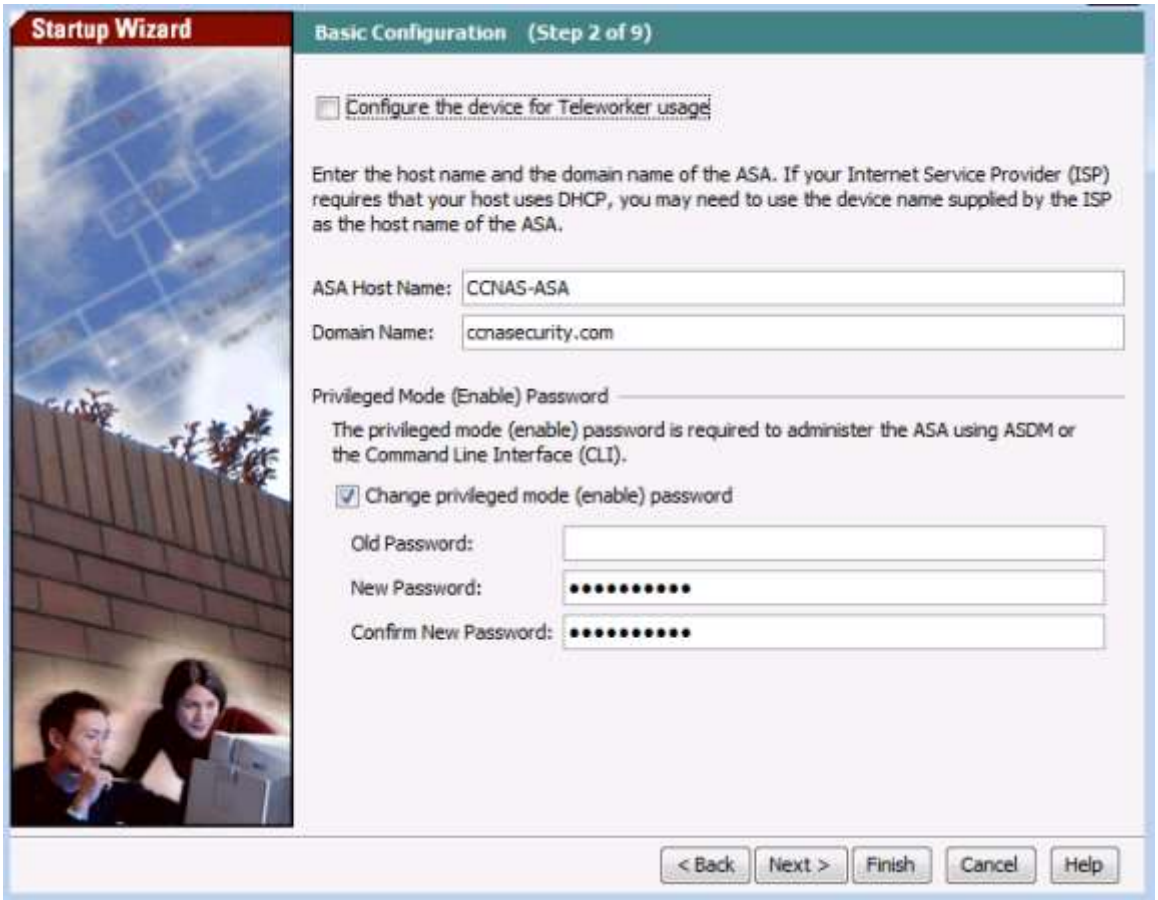


Шаг 2: Настройка имени хоста, доменного имени и пароля привилегированного доступа.

a. На стартовом экране мастера Startup Wizard измените существующую конфигурацию или верните заводские настройки для ASA. Убедитесь, что выбрана опция **Modify Existing Configuration**, и нажмите **Next**, чтобы продолжить.

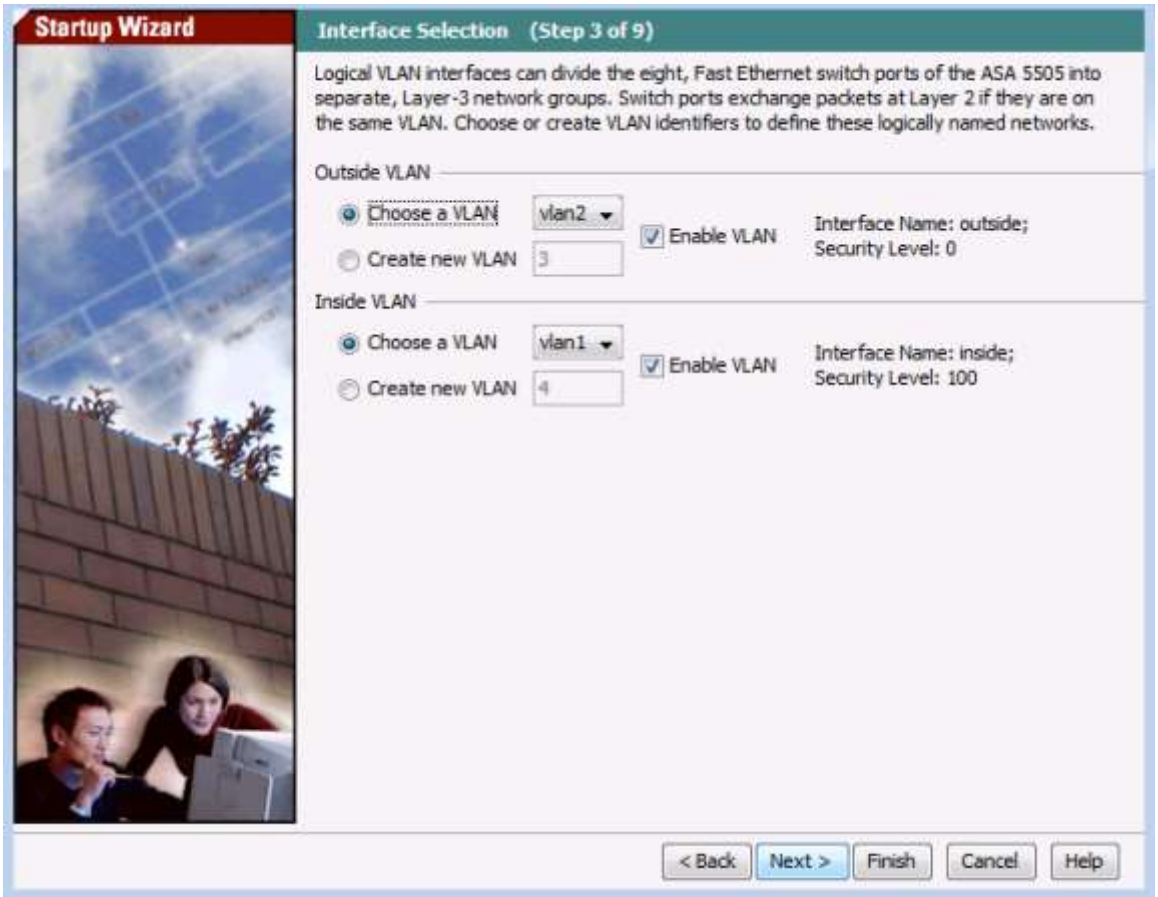


b. На экране Startup Wizard Step 2 установите имя хоста ASA **CCNAS-ASA** и доменное имя **ccnasecurity.com**. Установите флажок для изменения пароля привилегированного режима, измените его с пустого на **cisco12345,** затем повторно введите его для подтверждения. После ввода всех значений нажмите **Next,** чтобы продолжить.

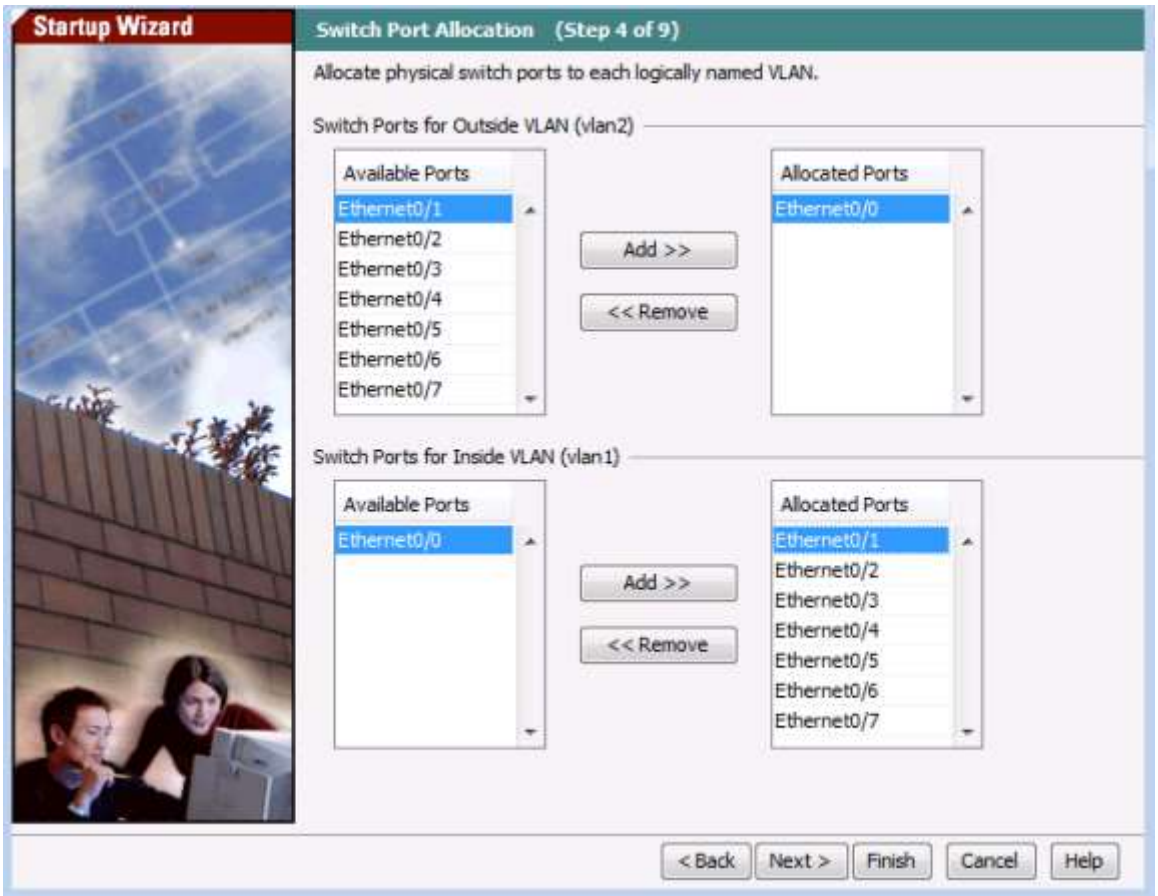


Шаг 3: Настройка внешних и внутренних интерфейсов VLAN.

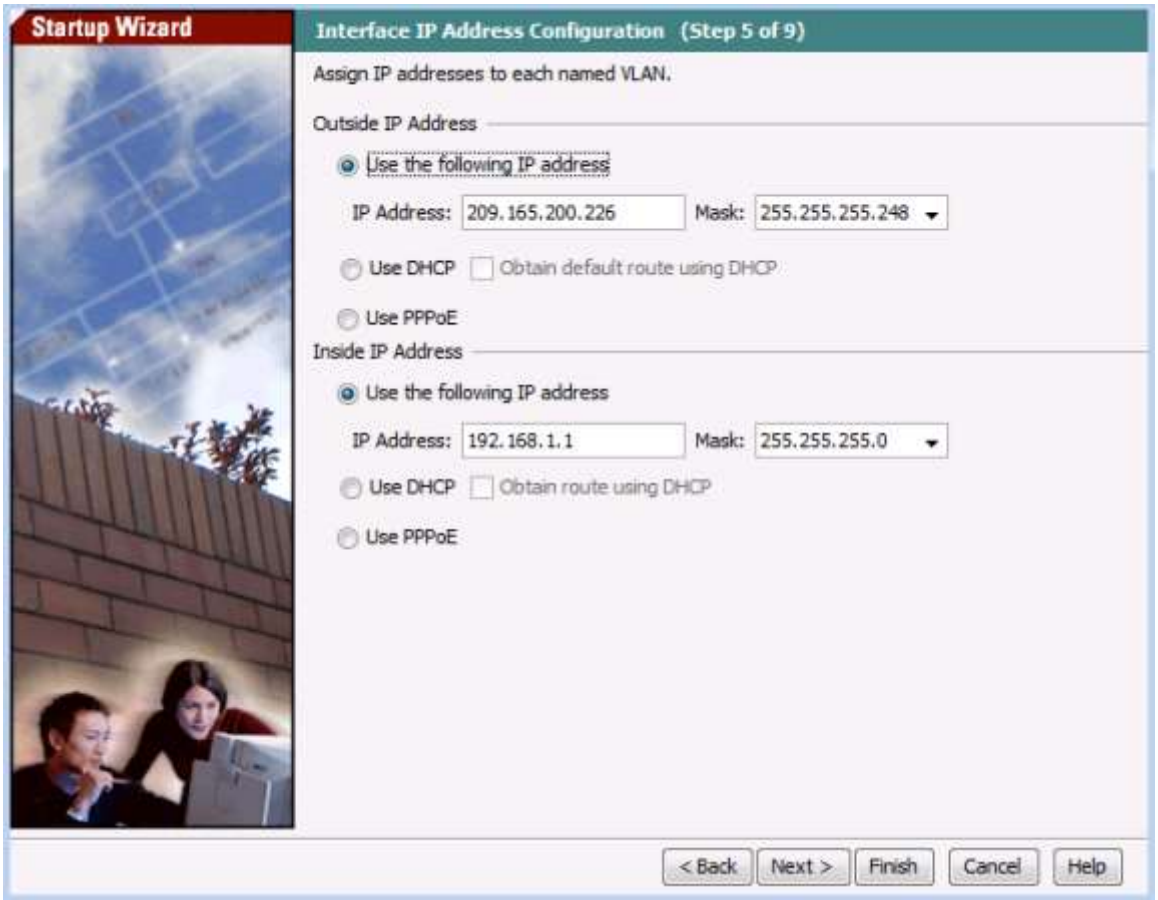
a. На экране Startup Wizard Step 3 производится настройка внешних и внутренних сетей VLAN. Не изменяйте текущие настройки, так как они уже были определены с помощью CLI. Внутренняя сеть VLAN имеет имя **inside**, а для уровня безопасности установлено значение 100 (наивысший). Интерфейс внешней сети VLAN называется **outside,** а для уровня безопасности установлено значение 0 (наименьший). Нажмите **Next**, чтобы продолжить.



b. На экране Startup Wizard Step 4 (Switch Port Allocation) убедитесь, что порт **Ethernet0/1** выделен для внутренней VLAN 1, а порт **Ethernet0/0 –** для внешней VLAN 2. Нажмите **Next**, чтобы продолжить.



c. На экране Startup Wizard Step 5 (Interface IP Address Configuration) введите внешний IP-адрес **209.165.200.226** и маску **255.255.255.248**. Для выбора маски можно использовать раскрывающееся меню. Оставьте IP-адрес внутреннего интерфейса **192.168.1.1** с маской **255.255.255.0**. Нажмите **Next**, чтобы продолжить.

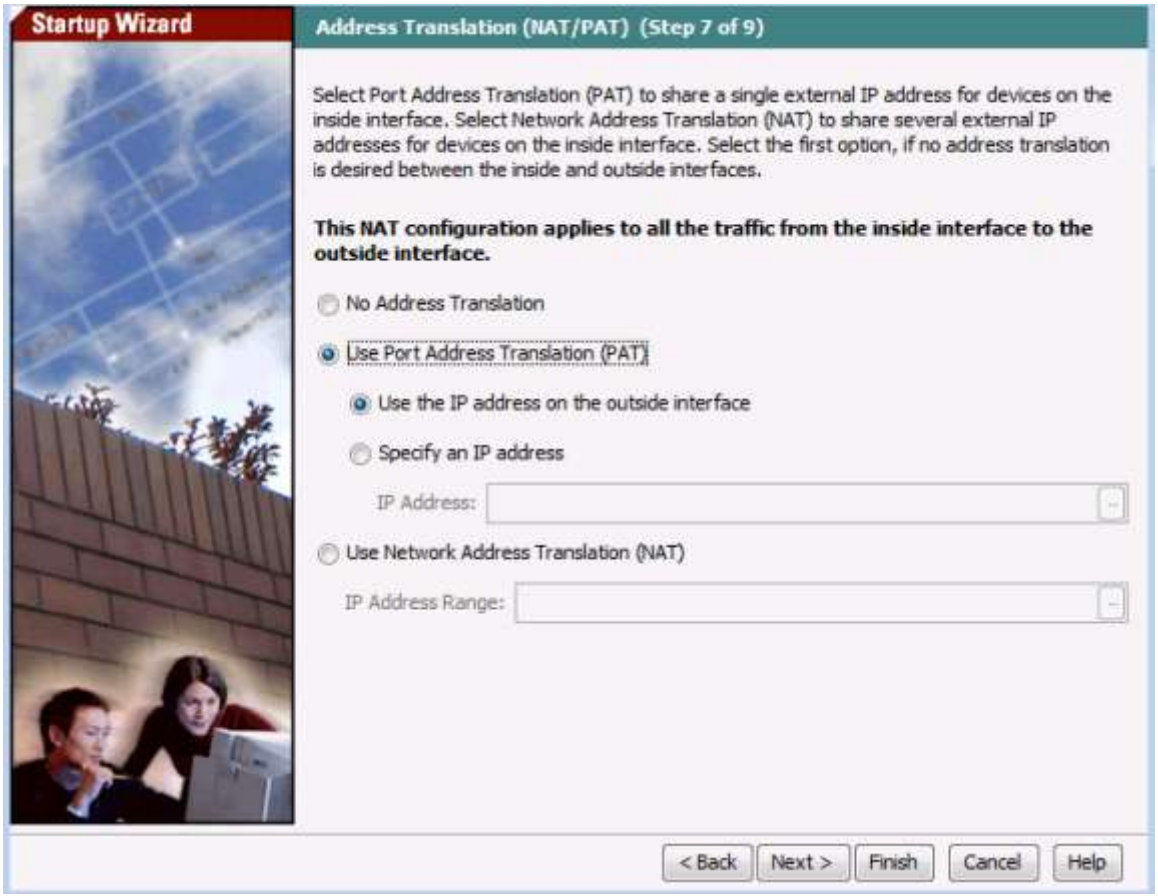


Шаг 4: Настройка DHCP, преобразования адресов и административного доступа.

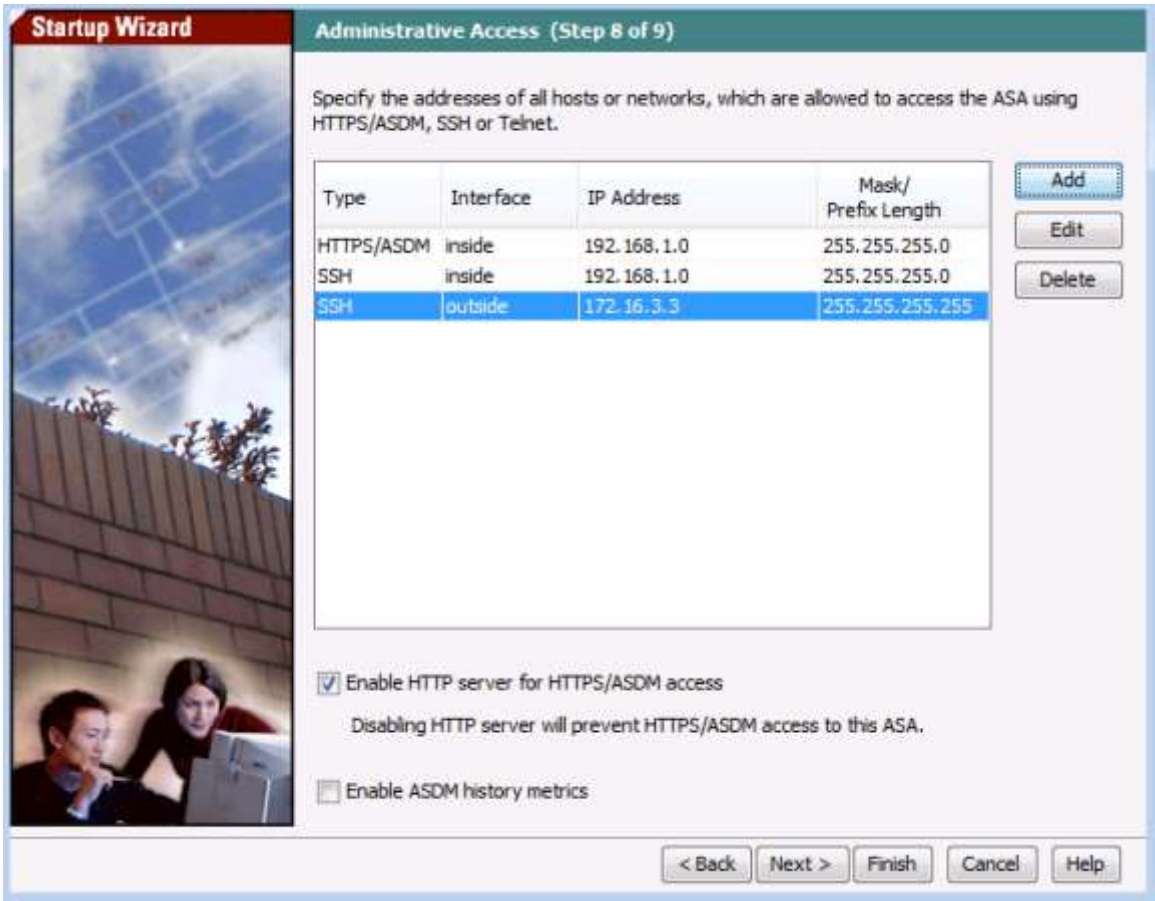
a. На экране Startup Wizard Step 6 (DHCP Server) установите флажок **Enable DHCP server on the inside interface.** Введите начальный IP-адрес **192.168.1.31** и конечный IP-адрес **192.168.1.39**. Введите адрес сервера DNS 1 **10.20.30.40** и доменное имя **ccnasecurity.com**. **НЕ** устанавливайте флажок Enable auto-configuration from interface. Нажмите **Next**, чтобы продолжить.

b. На экране Startup Wizard Step 7 (Address Translation (NAT/PAT) нажмите **Use Port Address Translation (PAT).** По умолчанию используется IP-адрес внешнего интерфейса.

Примечание. Вы также можете назначить конкретный IP-адрес для PAT или диапазон адресов для NAT. Нажмите **Next**, чтобы продолжить.



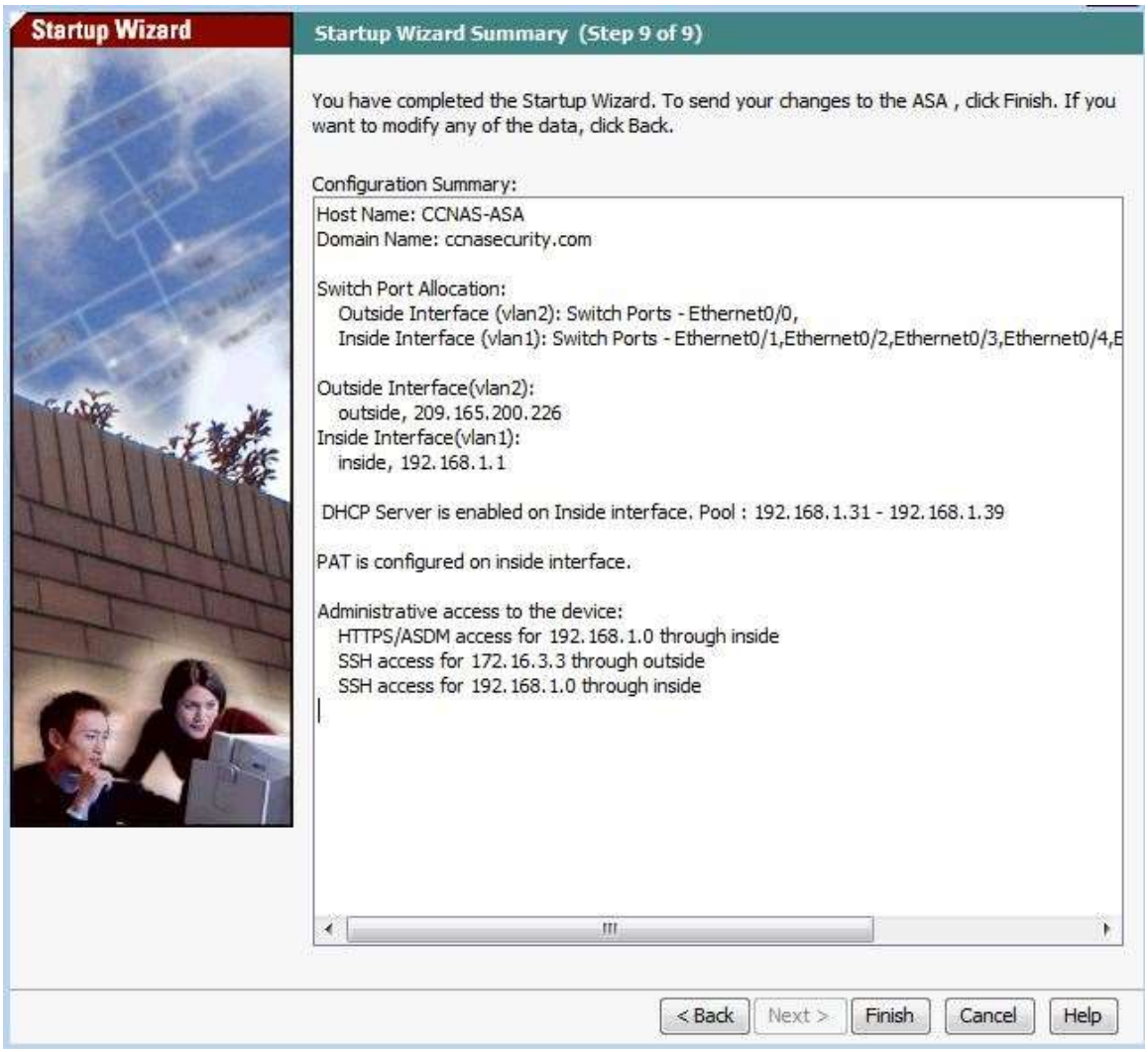
c. На экране Startup Wizard Step 8 (Administrative Access) доступ HTTPS/ASDM настроен в настоящее время для хостов во внутренней сети 192.168.1.0/24. Добавьте доступ по **SSH** к ASA из внутренней сети **192.168.1.0** с маской подсети **255.255.255.0**. Добавьте доступ по **SSH** к ASA из хоста **172.16.3.3** во внешней сети. Убедитесь, что установлен флажок **Enable HTTP server for HTTPS/ASDM access.** Нажмите **Next**, чтобы продолжить.



Шаг 5: Проверка сводной информации и отправка команд на ASA.

a. На экране Startup Wizard Step 9 (Startup Wizard Summary) просмотрите сводную информацию по конфигурации (**Configuration Summary**) и нажмите **Finish.** ASDM передаст команды на устройство ASA, а затем перезагрузит измененную конфигурацию.

Примечание. Если во время перезагрузки диалоговое окно интерфейса GUI перестанет реагировать, закройте его, выйдите из ASDM и перезапустите браузер и ASDM. При получении запроса на сохранение конфигурации во флеш-память ответьте **Yes.** Даже если вам кажется, что ASDM не перезагрузил конфигурацию, следует иметь в виду, что команды были отправлены. Если во время передачи команд из ASDM произошли ошибки, будет выведен список команд, выполненных успешно, а также с ошибкой.



b. Перезапустите ASDM и установите новый пароль привилегированного доступа **cisco12345** (имя пользователя не вводите). Вернитесь на информационную панель Device и проверьте информацию в окне Interface Status. Там должны быть перечислены внутренние и внешние интерфейсы со своими IP-адресами и состоянием. Для внутреннего интерфейса должна быть показана скорость передачи в кбит/с. В окне Traffic Status может отображаться доступ ASDM как всплеск трафика TCP.

Шаг 6: Проверка доступа к внешнему веб-сайту с компьютера PC-B.

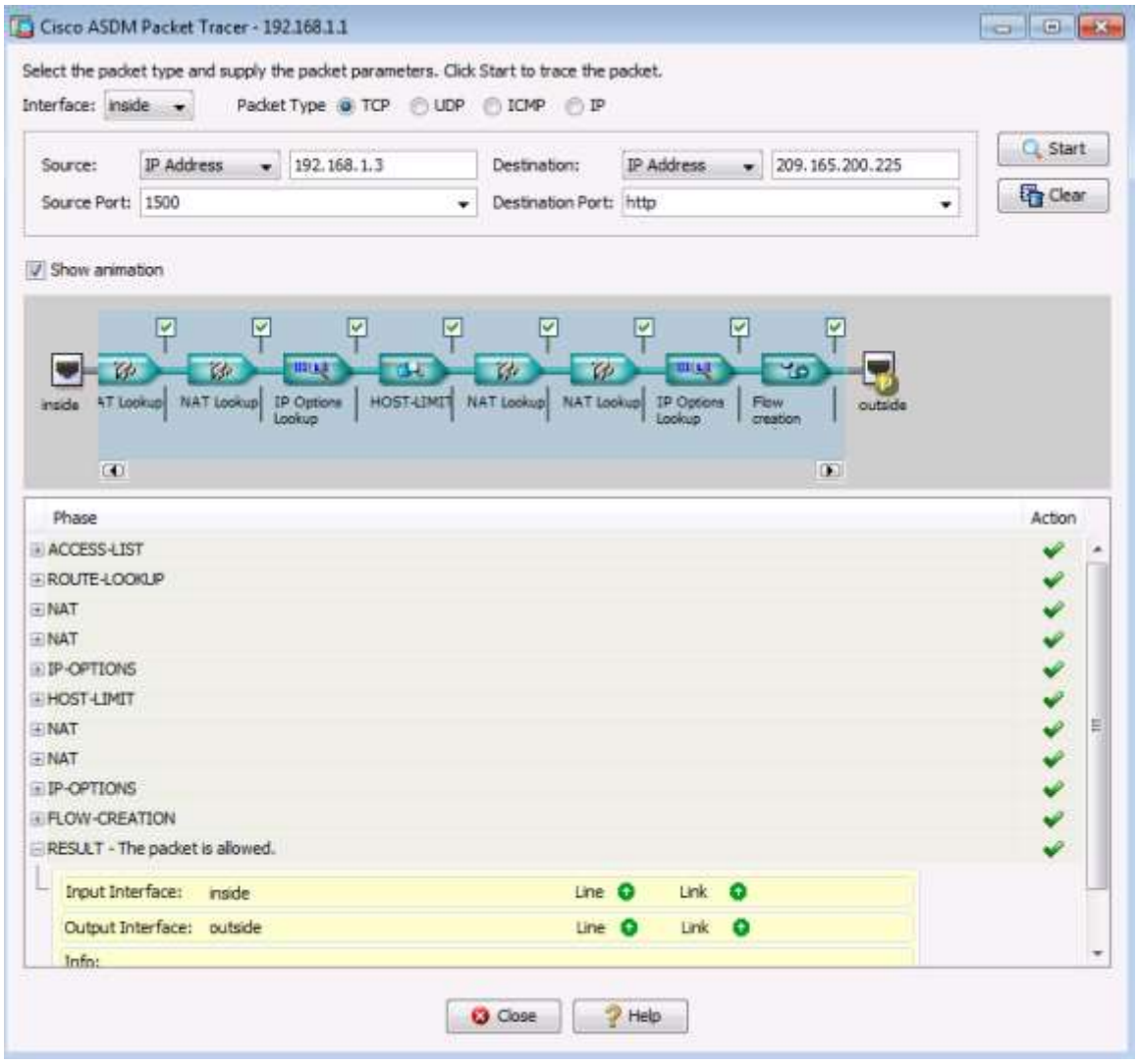
a. На компьютере PC-B откройте браузер и введите IP-адрес интерфейса G0/0 маршрутизатора R1 (**209.165.200.225**) для имитации доступа к внешнему веб-сайту.

b. HTTP-сервер на маршрутизаторе R1 был включен в части 1. Вы должны получить запрос на аутентификацию пользователя из диспетчера устройств R1 GUI. Введите имя пользователя **admin01** и пароль **admin01pass**. Закройте браузер. Вы должны видеть активность TCP на информационной панели ASDM Device в окне Traffic Status на главной странице.

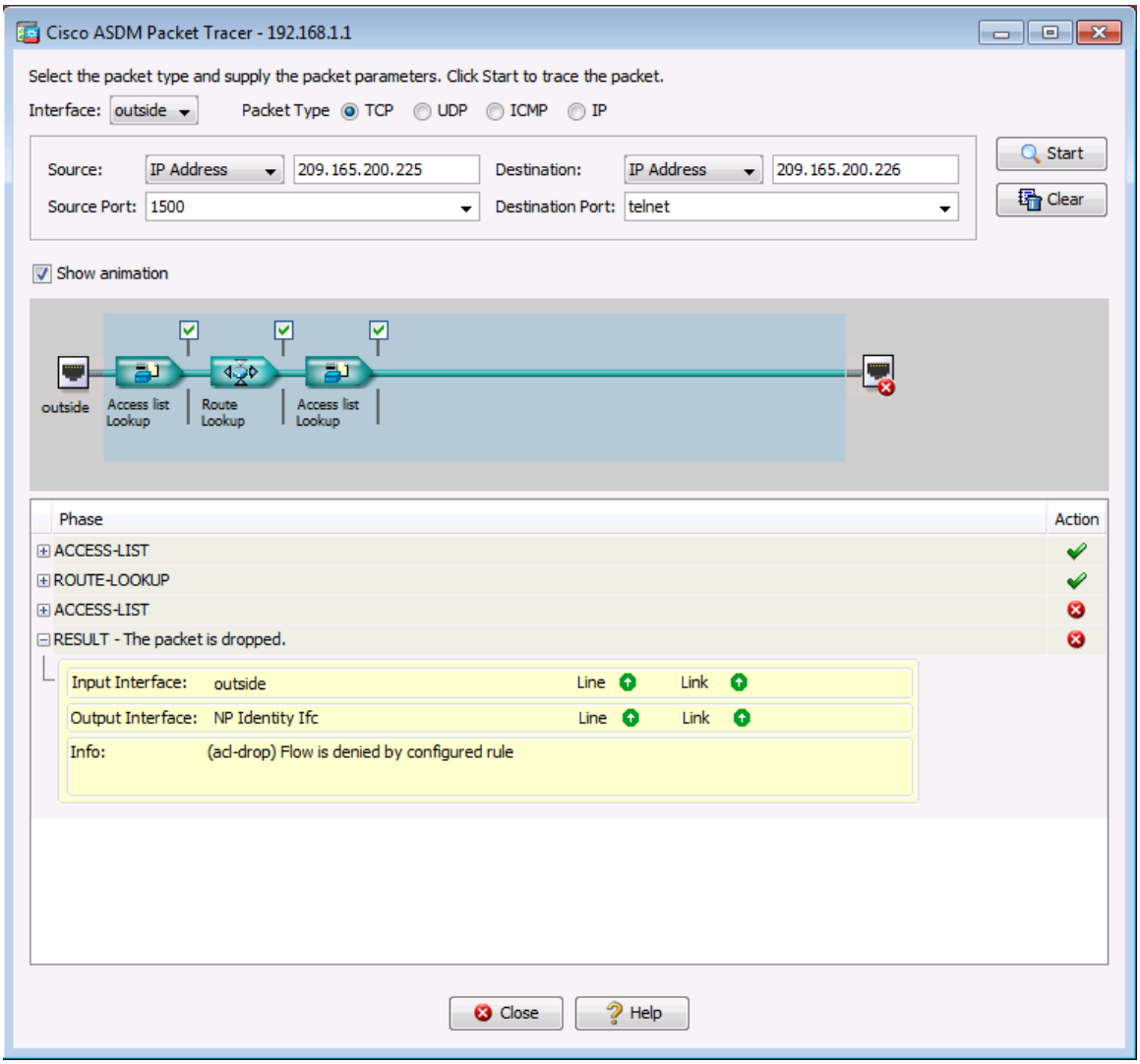
Шаг 7: Проверка доступа к внешнему веб-сайту с использованием утилиты ASDM Packet Tracer.

a. Выберите **Tools** > **Packet Tracer.**

b. Выберите интерфейс **inside** в раскрывающемся меню Interface и **TCP** в области Packet Type. В раскрывающемся меню Source выберите **IP Address** и введите адрес **192.168.1.3** (PC-B). Для Source Port введите значение **1500**. В раскрывающемся меню Destination выберите **IP Address** и введите **209.165.200.225** (R1 Fa0/0). Для Destination Port введите значение **HTTP**. Нажмите **Start** для запуска сеанса трассировки пакета. Пакет должен быть разрешен.



c. Нажмите **Clear** для сброса введенных данных. Настройте другой сеанс трассировки: выберите в раскрывающемся меню **Interface** пункт **outside**, оставьте **TCP** в качестве типа пакета. В раскрывающемся меню **Sources** выберите **IP Address,** введите адрес **209.165.200.225** (R1 G0/0). Для Source Port введите значение 1500. В раскрывающемся меню **Destination** выберите **IP Address,** введите **209.165.200.226** (внешний интерфейс ASA). Для Destination Port введите значение **telnet**. Нажмите **Start** для запуска сеанса трассировки пакета. Пакет должен быть отброшен. Нажмите **Close** для продолжения.



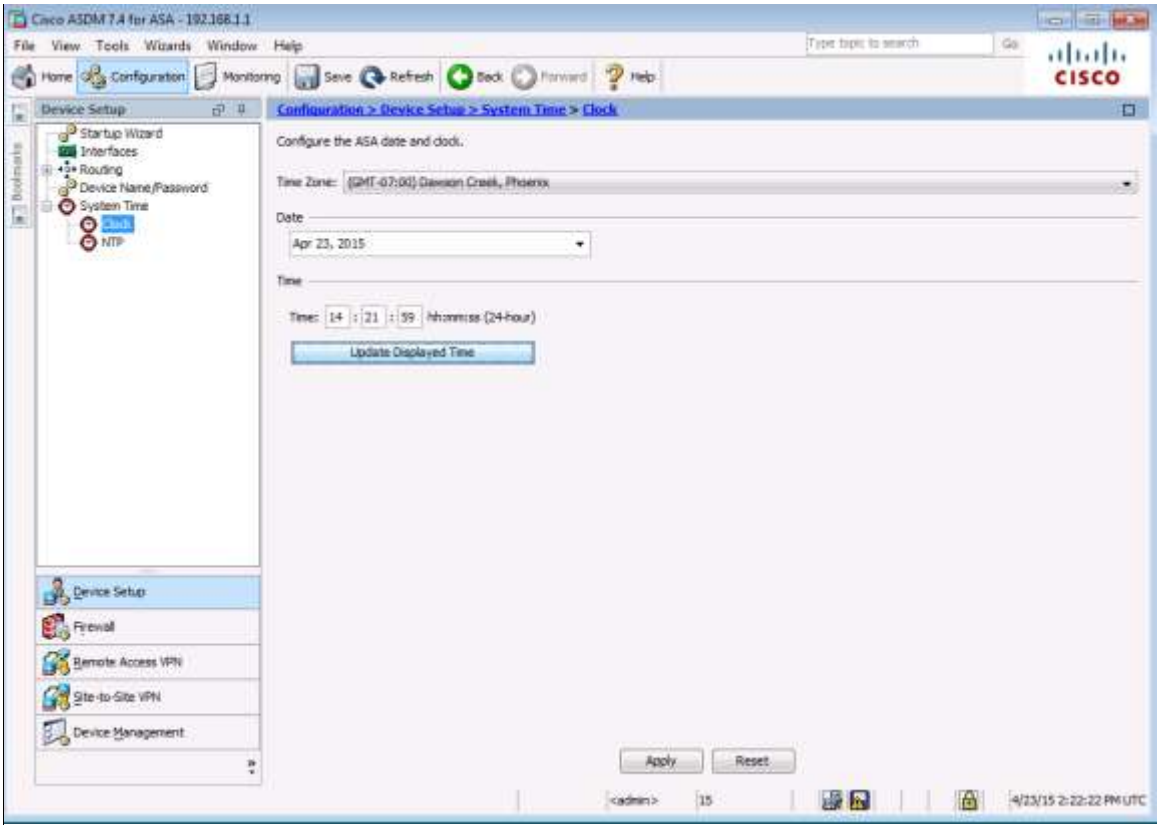
Часть 4: Настройка параметров ASA в меню конфигурации ASDM

В четвертой части необходимо установить время на ASA, настроить маршрут по умолчанию, проверить связь с помощью команд ASDM ping и traceroute, настроить локальную аутентификацию пользователей AAA, проверить доступ по SSH и изменить политику инспектирования применения MPF.

Шаг 1: Установка даты и времени на ASA.

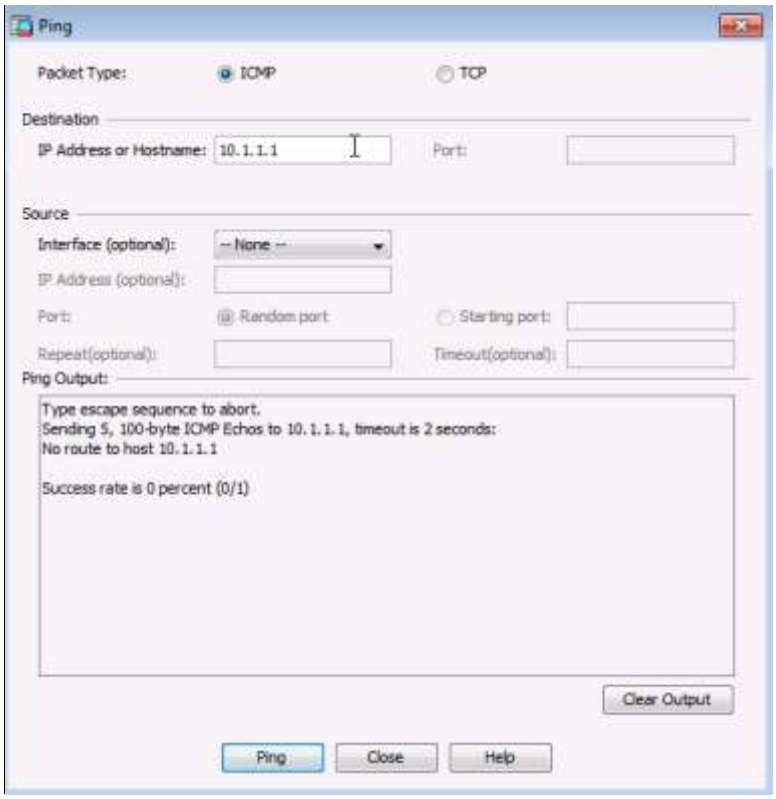
a. На экране **Configuration** откройте меню **Device Setup** и выберите **System Time** > **Clock**.

b. Выберите свою временную зону (**Time Zone)** в раскрывающемся списке и введите в соответствующие поля текущую дату и время. (Используется 24-часовой формат времени.) Нажмите **Apply** для отправки команд на ASA.



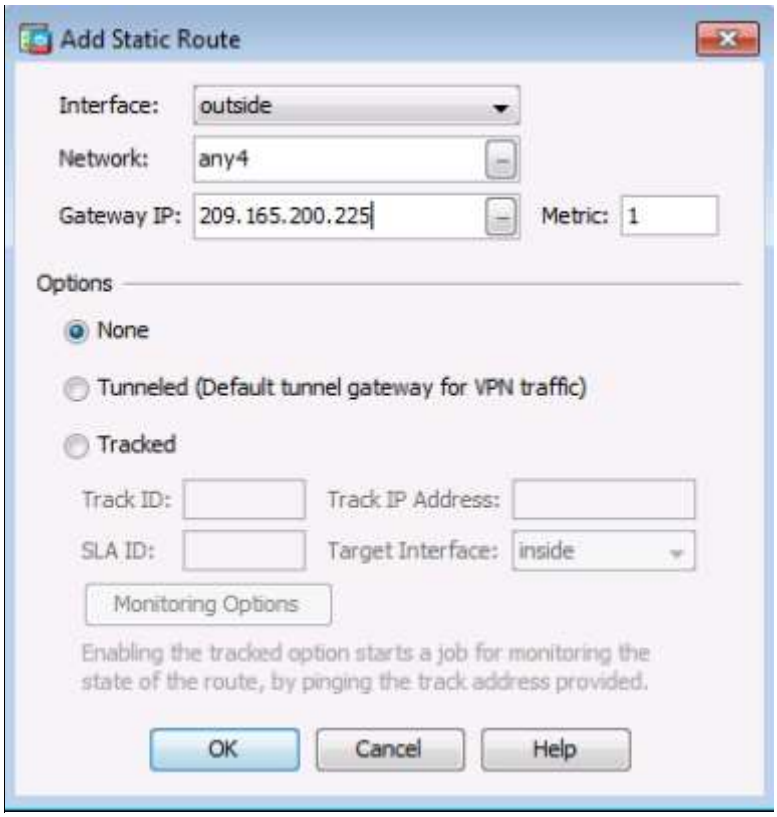
Шаг 2: Настройка статического маршрута по умолчанию для ASA.

a. В меню **ASDM Tools** выберите **Ping** и введите IP-адрес интерфейса S0/0/0 маршрутизатора R1 (**10.1.1.1**). В ASA нет маршрута по умолчанию к неизвестным внешним сетям. Эхо-запрос (ping) должен завершиться сбоем, так как у ASA нет маршрута к 10.1.1.1. Нажмите **Close** для продолжения.

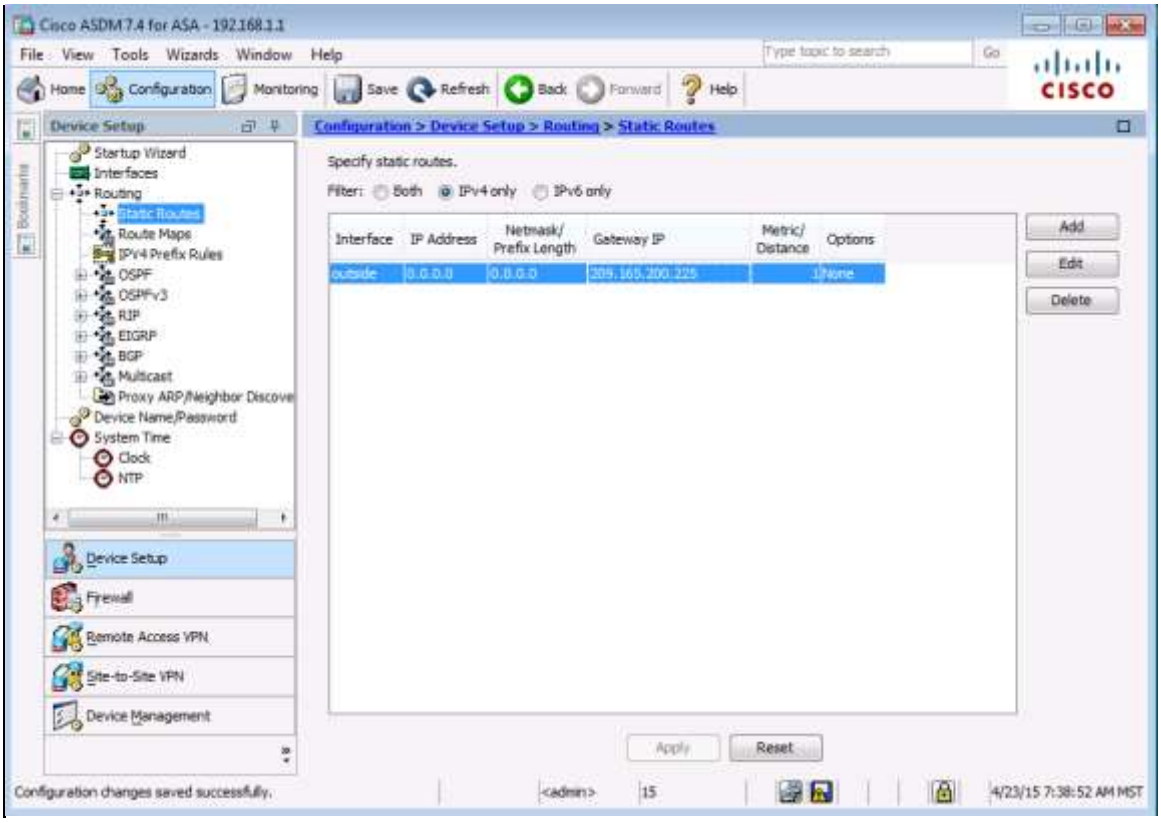


b. На экране **Configuration** откройте меню **Device Setup** и выберите **Routing** > **Static Routes.** Щелкните **IPv4 Only** и нажмите **Add**, чтобы добавить новый статический маршрут.

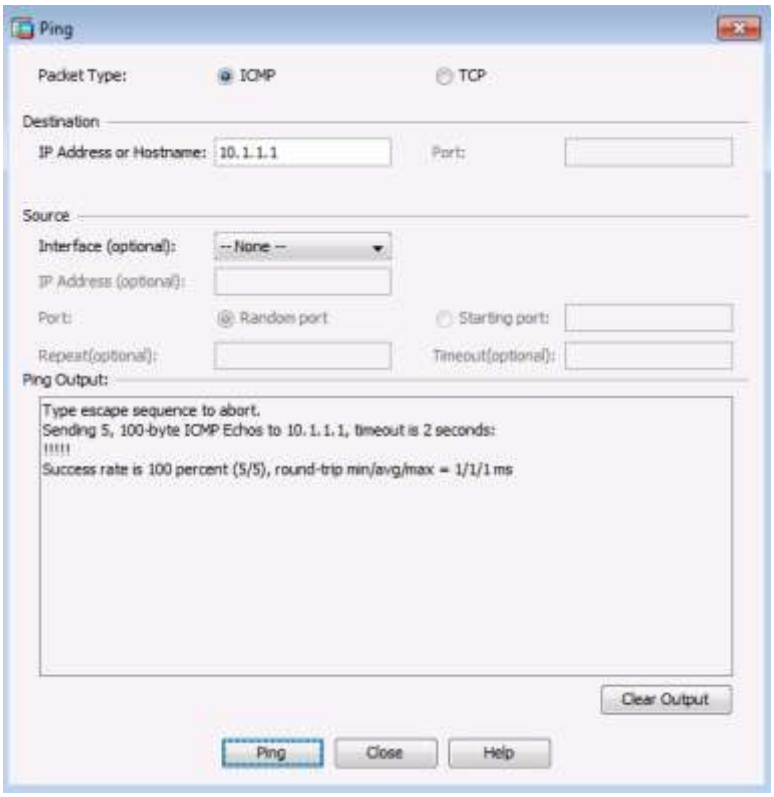
c. В диалоговом окне Add Static Route выберите интерфейс **outside** в раскрывающемся списке. Нажмите кнопку выбора справа от **Network**, выберите **any4** в списке сетевых объектов и нажмите **OK.** При выборе **any4** выполняется преобразование в маршрут из «четырех нулей». В поле Gateway IP введите **209.165.200.225** (интерфейс G0/0 маршрутизатора R1).



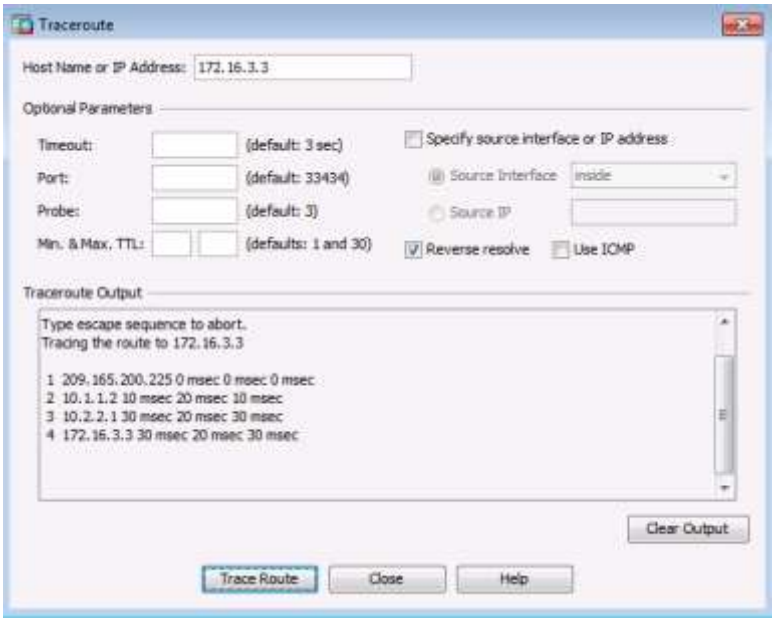
d. Нажмите **OK** > **Apply** для отправки команд на ASA.



e. В меню **ASDM Tools** выберите **Ping** и введите IP-адрес интерфейса S0/0/0 маршрутизатора R1 (**10.1.1.1**). На этот раз эхо-запрос должен быть выполнен успешно. Нажмите **Close** для продолжения.



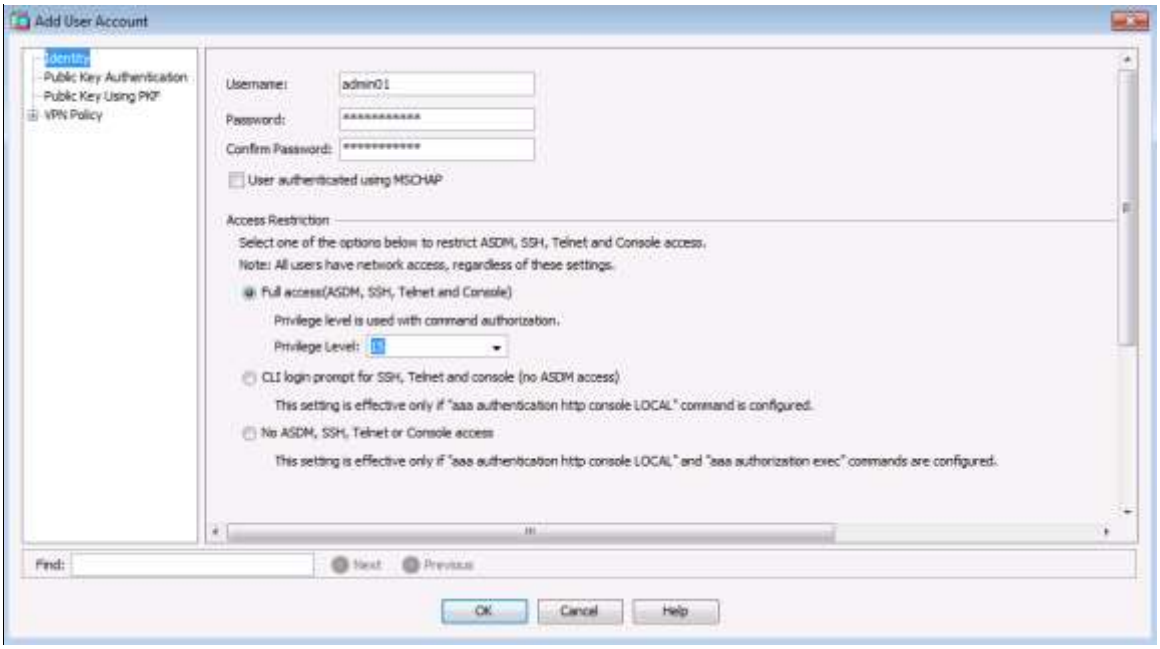
f. В меню **ASDM Tools** выберите **Traceroute** и введите IP-адрес внешнего хоста PC-C (**172.16.3.3**). Нажмите **Trace Route**. Команда трассировки маршрута должна быть успешно выполнена и показать переходы от ASA через маршрутизаторы R1, R2 и R3 к хосту PC-C. Нажмите **Close** для продолжения.



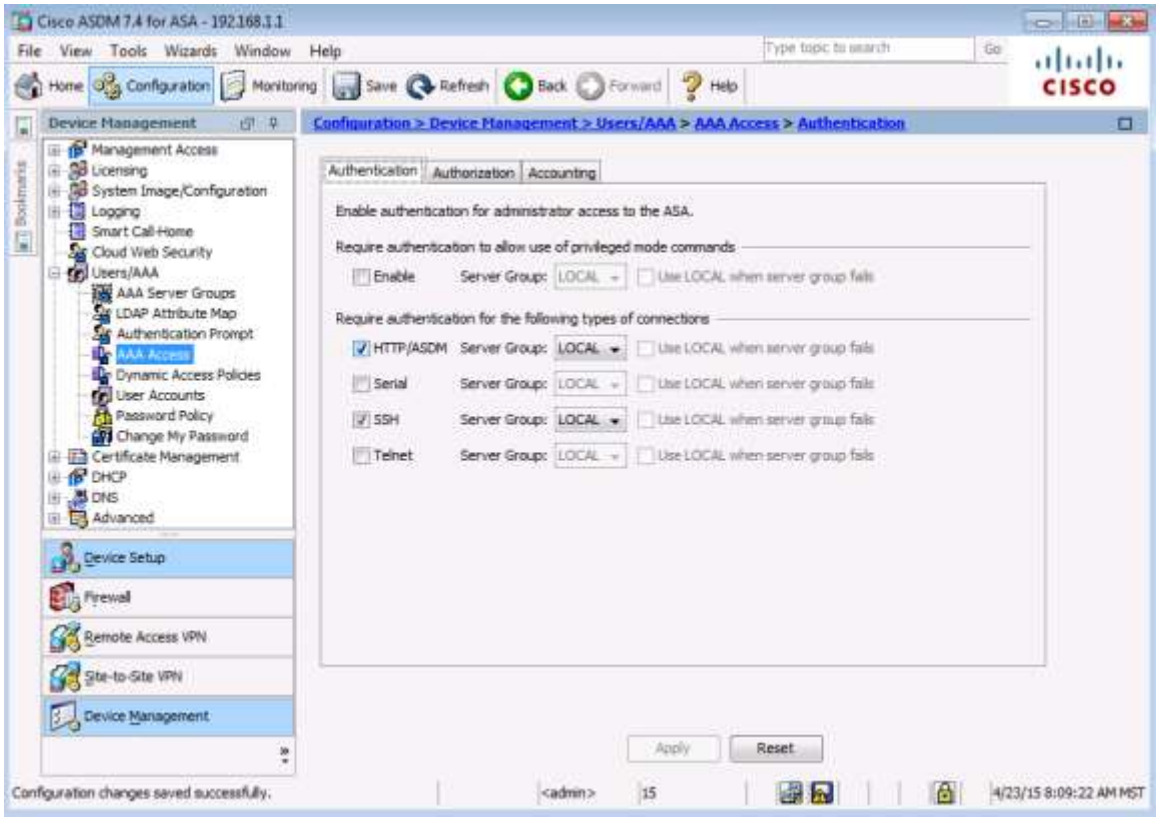
Шаг 3: Настройка аутентификации пользователей AAA с использованием локальной базы данных ASA.

Включите функцию аутентификации пользователей AAA для доступа к ASA по SSH. Вы разрешили доступ к ASA по SSH из внутренней сети и с внешнего хоста PC-C при запуске мастера **Startup Wizard.** Чтобы разрешить администратору доступ к ASA по SSH, необходимо создать пользователя в локальной базе данных.

a. На экране **Configuration** в области **Device Management** нажмите **Users/AAA.** Выберите **User Accounts** > **Add**. Создайте нового пользователя с именем **admin01** и паролем **admin01pass.** Для подтверждения пароля введите его повторно. Предоставьте этому пользователю полный доступ – **Full access** (ASDM, SSH, Telnet и консоль) – и присвойте ему уровень привилегий **15**. Нажмите **OK**, чтобы добавить пользователя, а затем **Apply** для отправки команды на ASA.



b. На экране **Configuration** в области **Device Management** нажмите **Users/AAA.** Нажмите **AAA Access**. На вкладке **Authentication** установите флажок, чтобы требовать аутентификацию для подключений по **HTTP/ASDM** и **SSH**, и укажите группу серверов **LOCAL** для каждого типа подключения. Нажмите **Apply** для отправки команд на ASA.



Примечание. Перед выполнением следующих действий в ADSM необходимо войти в систему под учетной записью **admin01** с паролем **admin01pass.**

Шаг 4: Проверка доступа к ASA по SSH.

a. На компьютере PC-B откройте клиент SSH, например PuTTY, и подключитесь к внутреннему интерфейсу ASA по IP-адресу **192.168.1.1**. Получив запрос на вход в систему, введите имя пользователя **admin01** и пароль **admin01pass**.

b. На компьютере **PC-C** откройте клиент SSH, например PuTTY, и попытайтесь подключиться к внешнему интерфейсу ASA по адресу **209.165.200.226**. Получив запрос на вход в систему, введите имя пользователя **admin01** и пароль **admin01pass**.

c. После входа в ASA при помощи SSH введите команду **enable** и пароль **cisco12345.** Введите команду **show run**, чтобы показать текущую конфигурацию, созданную при помощи ASDM.

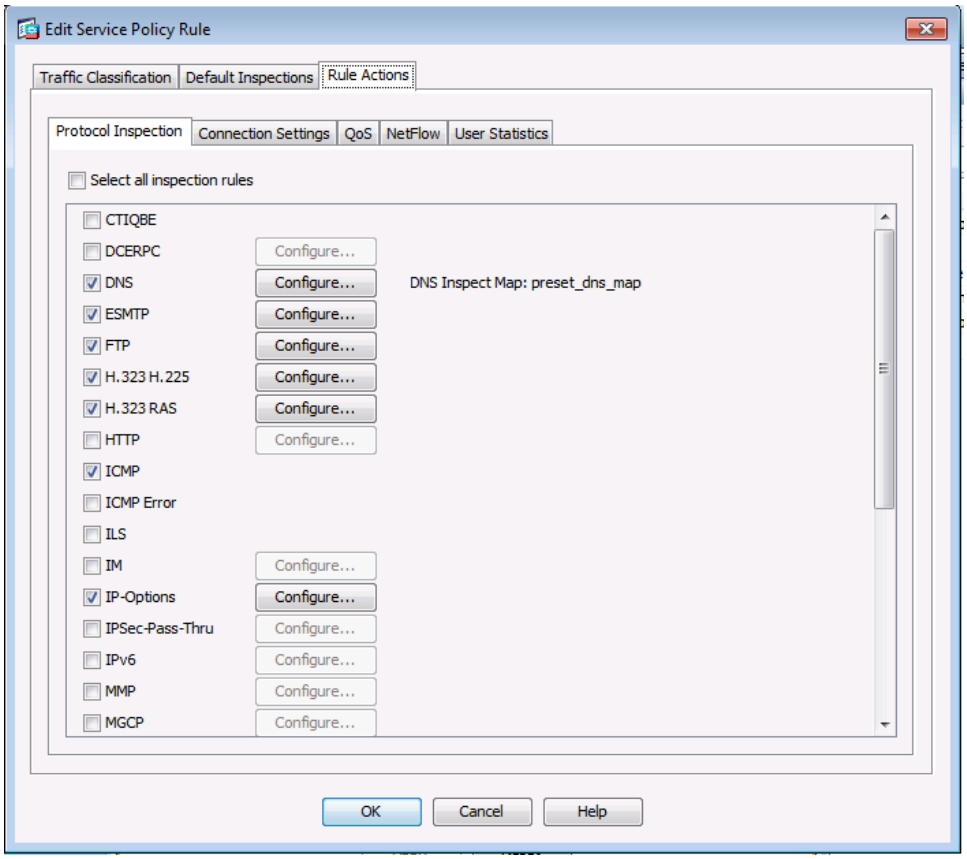
Примечание. Период бездействия (idle timeout) для SSH можно изменить. Чтобы изменить значение этого параметра, используйте команду CLI **logging synchronous** или выберите ASDM **Device Management** > **Management Access** > **ASDM/HTTP/Telnet/SSH**.

Шаг 5: Изменение политики инспектирования применения MPF.

Для инспектирования уровня приложений и выполнения других сложных задач на устройствах ASA имеется Cisco Modular Policy Framework (MPF).

a. Глобальная политика инспектирования по умолчанию не проверяет ICMP. Чтобы хосты во внутренней сети могли отправлять эхо-запросы на внешние хосты и получать от них ответы, необходимо инспектировать трафик ICMP. На экране **Configuration** в меню в области **Firewall** выберите **Service Policy Rules.**

b. Чтобы изменить правила инспектирования по умолчанию, выберите политику **inspection_default** и нажмите **Edit.** В окне Edit Service Policy Rule перейдите на вкладку **Rule Actions** и установите флажок **ICMP.** Не изменяйте другие протоколы по умолчанию, которые отмечены флажком. Нажмите **OK** > **Apply** для отправки команд на ASA. При получении запроса выполните вход как **admin01** и введите пароль **admin01pass.**



c. С компьютера PC-B отправьте эхо-запрос (**ping**) на внешний интерфейс S0/0/0 маршрутизатора R1 (**10.1.1.1**). Эхо-запрос должен быть выполнен успешно.

Часть 5: Настройка DMZ, статического преобразования NAT и ACL-списков

В третьей части вы настроили преобразование адресов с помощью PAT для внутренней сети. В этой части необходимо создать DMZ на ASA, настроить на сервере DMZ статическое преобразование NAT, а затем применить ACL для контроля доступа к серверу.

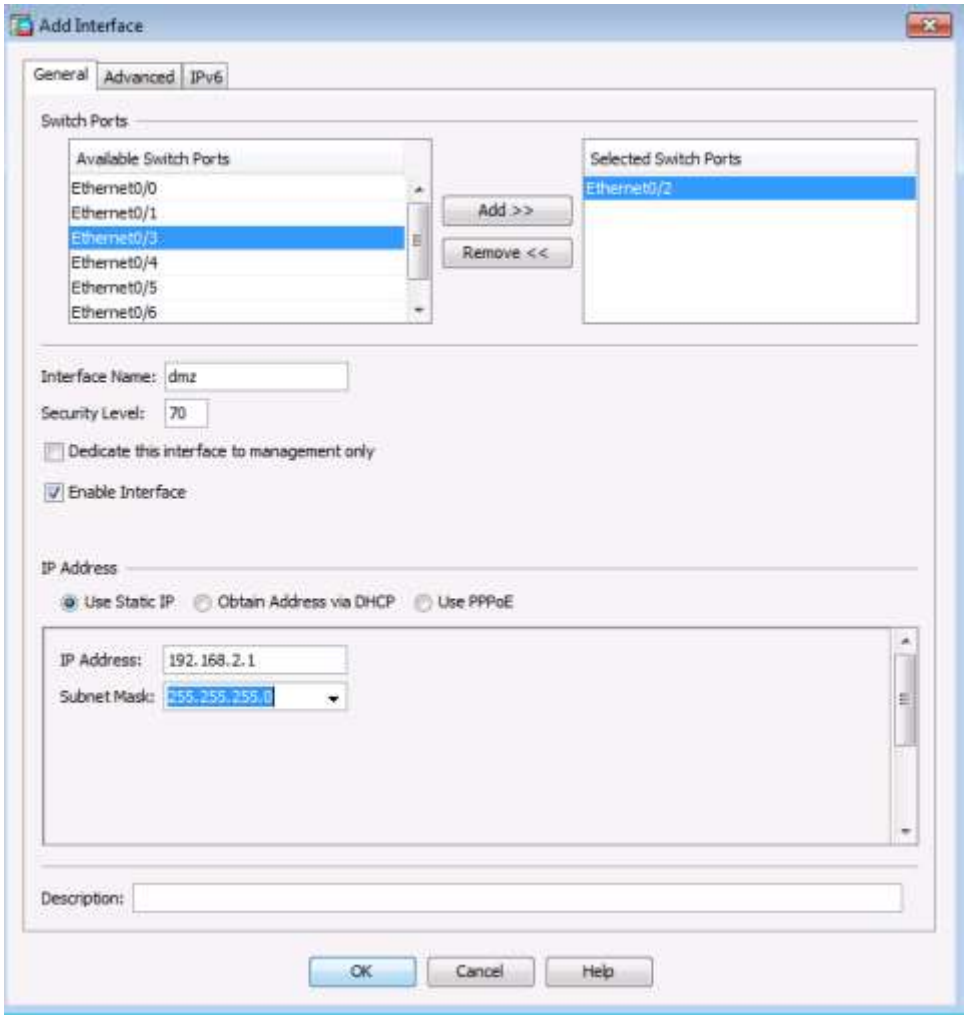
Шаг 1: Настройка интерфейса ASA DMZ VLAN 3.

На данном шаге необходимо создать новый интерфейс VLAN 3 с именем **dmz,** назначить физический интерфейс E0/2 для сети VLAN, установить уровень безопасности **70** и ограничить передачу данных из этого интерфейса на внутренний (VLAN1) интерфейс.

a. На экране **Configuration** в меню **Device Setup** нажмите **Interfaces.** По умолчанию отображается вкладка Interface, на которой указываются внутренние (VLAN 1, E0/1) и внешние (VLAN 2, E0/0) интерфейсы. Нажмите **Add** для создания нового интерфейса.

b. В диалоговом окне Add Interface выберите порт **Ethernet0/2** и нажмите **Add**. Вы получите запрос на изменение интерфейса из внутренней сети. Нажмите **OK** в этом сообщении, чтобы удалить порт из внутреннего интерфейса и добавить его в новый интерфейс. В окне Interface Name введите для интерфейса имя **dmz**, назначьте ему уровень безопасности 70 и убедитесь, что установлен флажок **Enable Interface.**

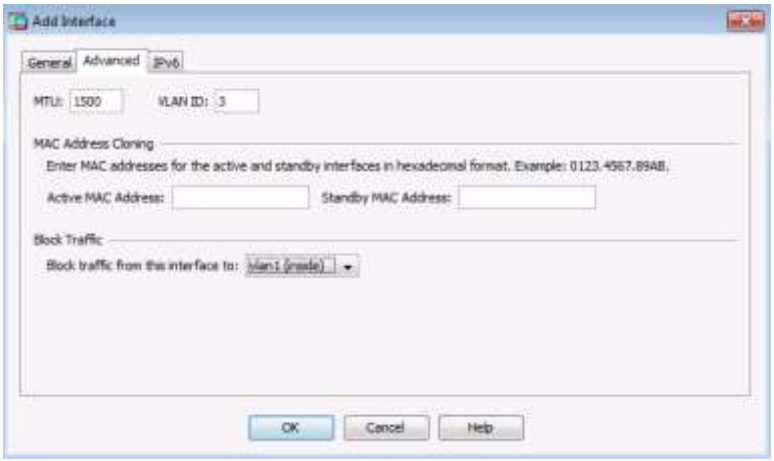
c. Убедитесь, что выбрана опция **Use Static IP**, введите IP-адрес **192.168.2.1** и маску подсети **255.255.255.0**. Пока НЕ нажимайте кнопку **OK.**



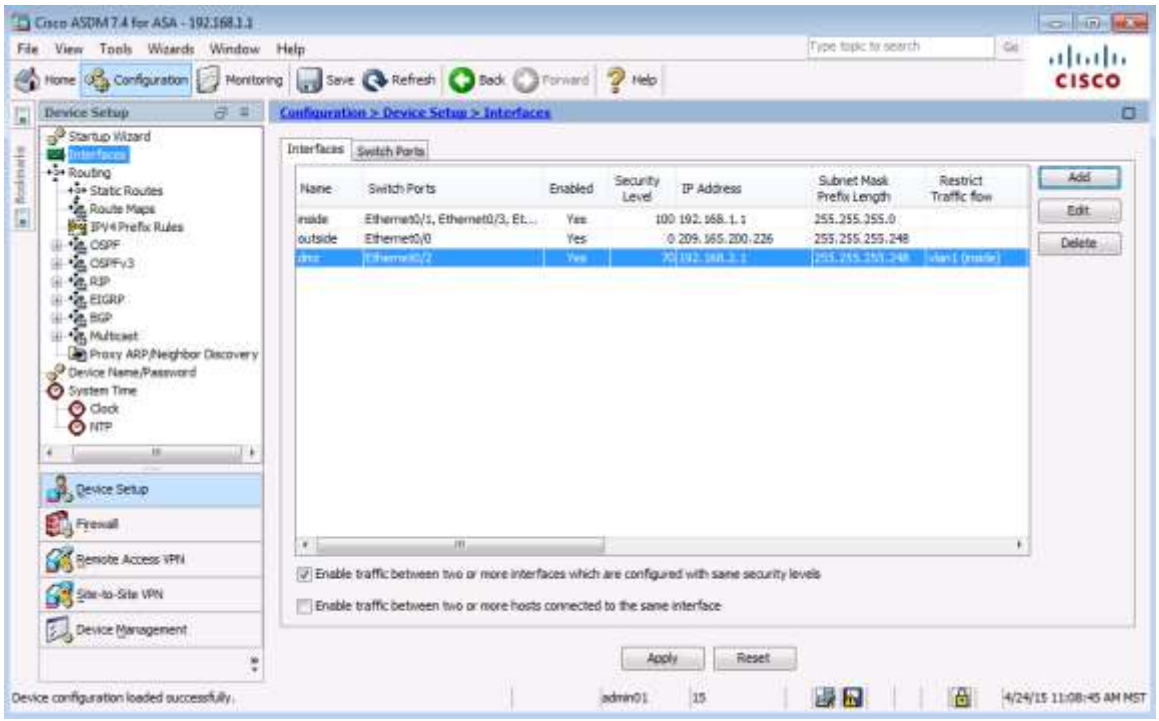
d. ASDM по умолчанию настроит этот интерфейс как VLAN ID 12. Перейдите на вкладку **Advanced** и определите этот интерфейс как VLAN ID **3,** после чего нажмите кнопку **OK,** чтобы добавить интерфейс.

Примечание. Если вы работаете с базовой лицензией на ASA 5505, вы можете создать максимум три именованных интерфейса. Однако вам придется отключить связь между третьим интерфейсом и одним из других интерфейсов. Так как серверу DMZ не нужно инициировать связь с внутренними пользователями, вы можете отключить передачу данных на интерфейсы VLAN 1.

e. На вкладке Advanced нужно заблокировать трафик, передаваемый из данного интерфейса VLAN 3 (dmz) в интерфейс VLAN 1 (внутренний). В области Block Traffic выберите **vlan1 (inside)** в раскрывающемся меню. Нажмите **OK** для возврата в окно Interfaces.



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



Примечание. Если при применении конфигурации интерфейса dmz на ASA появится окно **Error in sending command**, нужно будет вручную отправить команду **security-level 70** на VLAN 3 на ASA. Закройте окно **Error in sending command.** С помощью ASA CLI отправьте команду **security-level 70** на VLAN 3.

```
CCNA-ASA(config)# interface vlan 3
CCNA-ASA(config-if)# security-level 70
CCNA-ASA(config-if)# exit
```

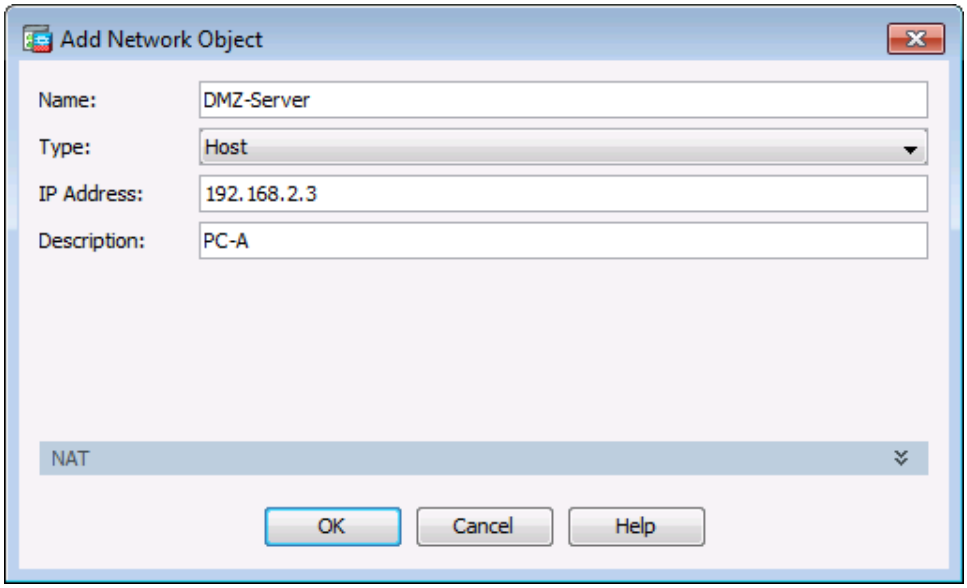
После ввода команд CLI диспетчер ASDM предложит обновить экран. После обновления в столбце Security Level для интерфейса dmz должно появиться значение **70.**

Шаг 2: Настройка сервера DMZ и статического преобразования NAT.

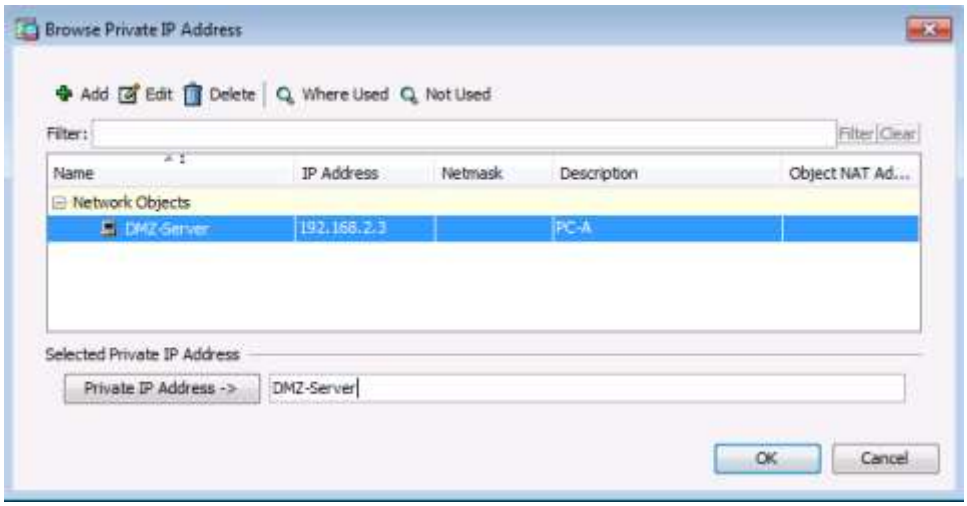
Для согласования добавления сервера DMZ и веб-сервера нужно будет использовать другой адрес из назначенного диапазона адресов ISP 209.165.200.224/29 (.224-.231). Интерфейс G0/0 маршрутизатора R1 и интерфейс ASA уже используют адреса 209.165.200.225 и 226. Для доступа к серверу с преобразованием адресов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

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

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

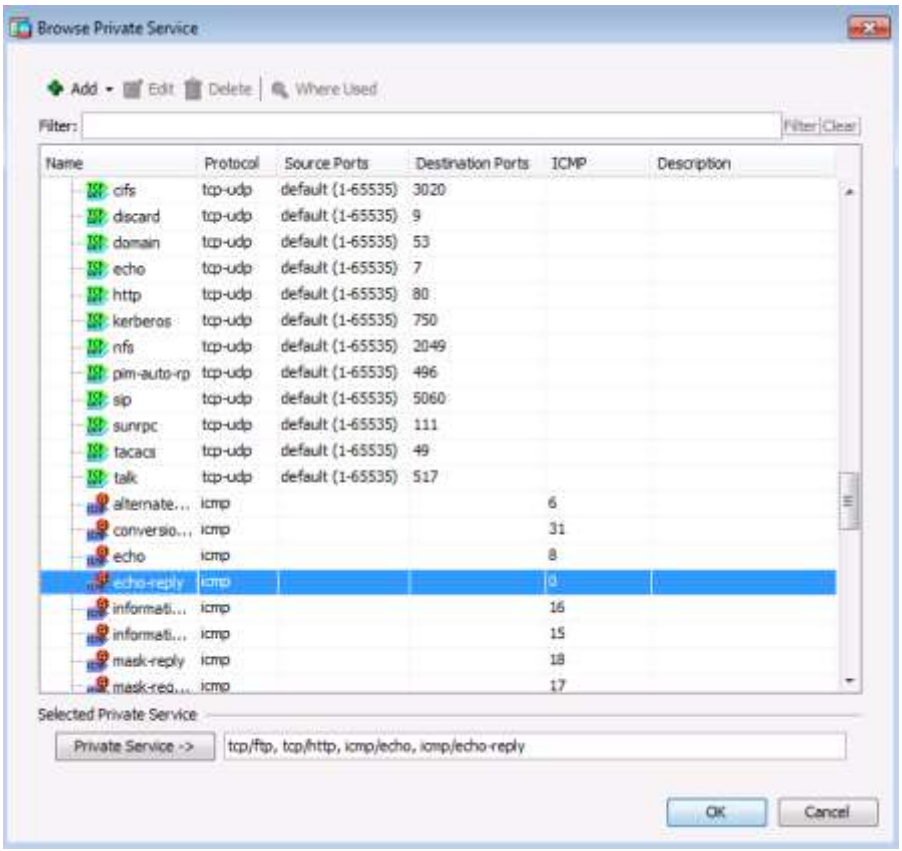


c. В окне Browse Private IP Address убедитесь, что в поле Selected Private IP Address отображается DMZ-Server, и нажмите **OK.** Вы вернетесь в диалоговое окно Add Public Server.

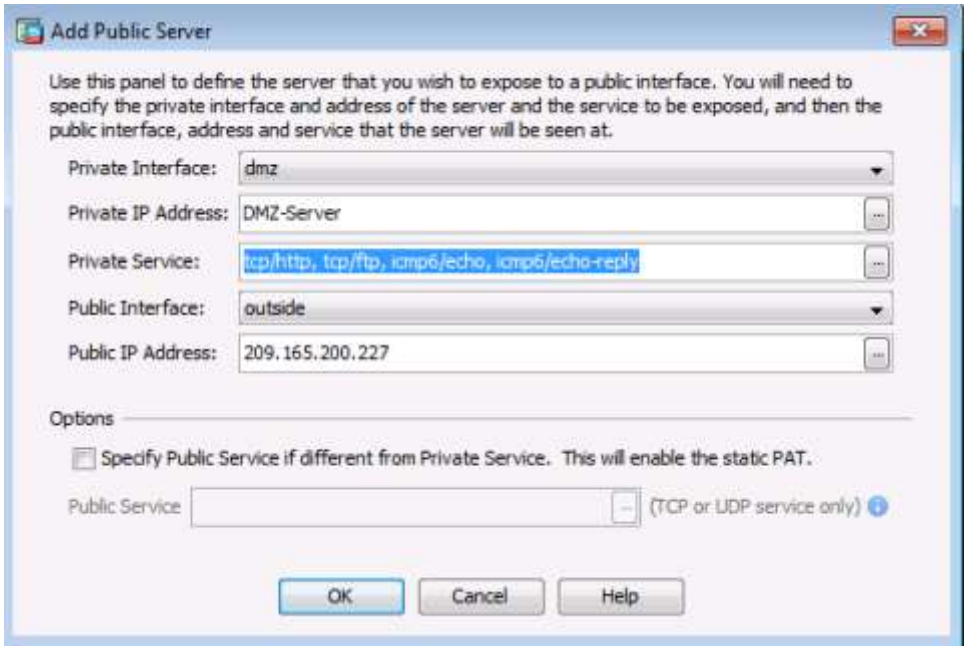


d. В диалоговом окне Add Public Server нажмите кнопку выбора, расположенную справа от поля Private Service. В окне Browse Private Service дважды щелкните следующие сервисы: **tcp/ftp**, **tcp/http**, **icmp/echo**, и **icmp/echo-reply** (чтобы увидеть все сервисы, используйте полосу прокрутки). Нажмите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

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



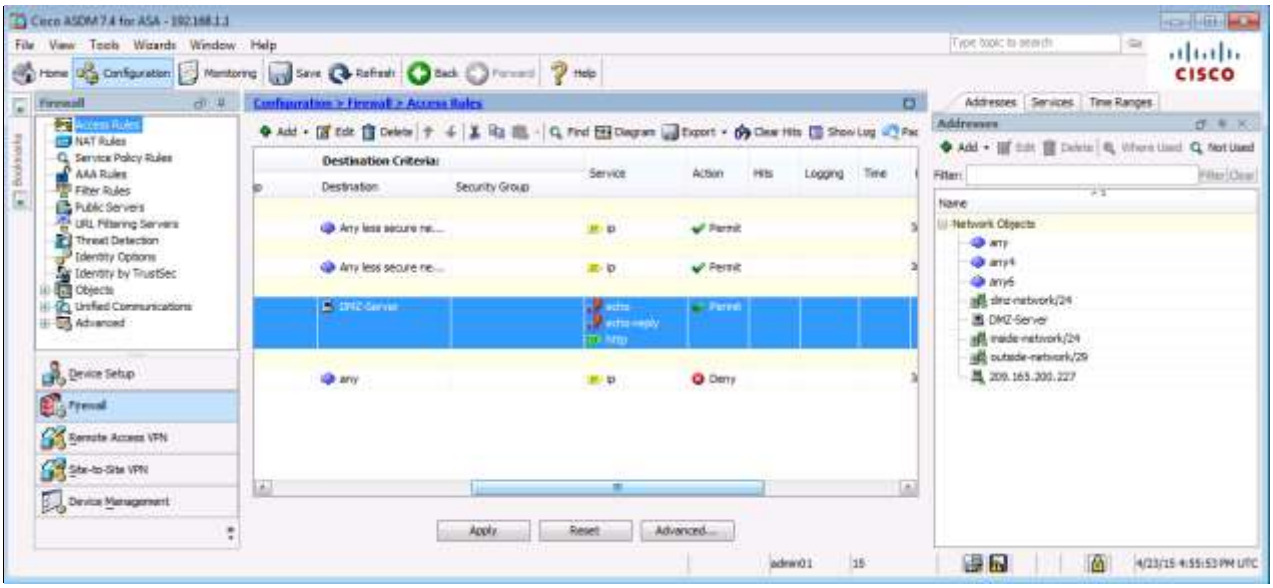
e. После ввода всей информации в диалоговом окне Add Public Server оно должно выглядеть примерно так, как показано ниже. Нажмите **OK**, чтобы добавить сервер. На экране Public Servers нажмите **Apply**, чтобы отправить команды на ASA.



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

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

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



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

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

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

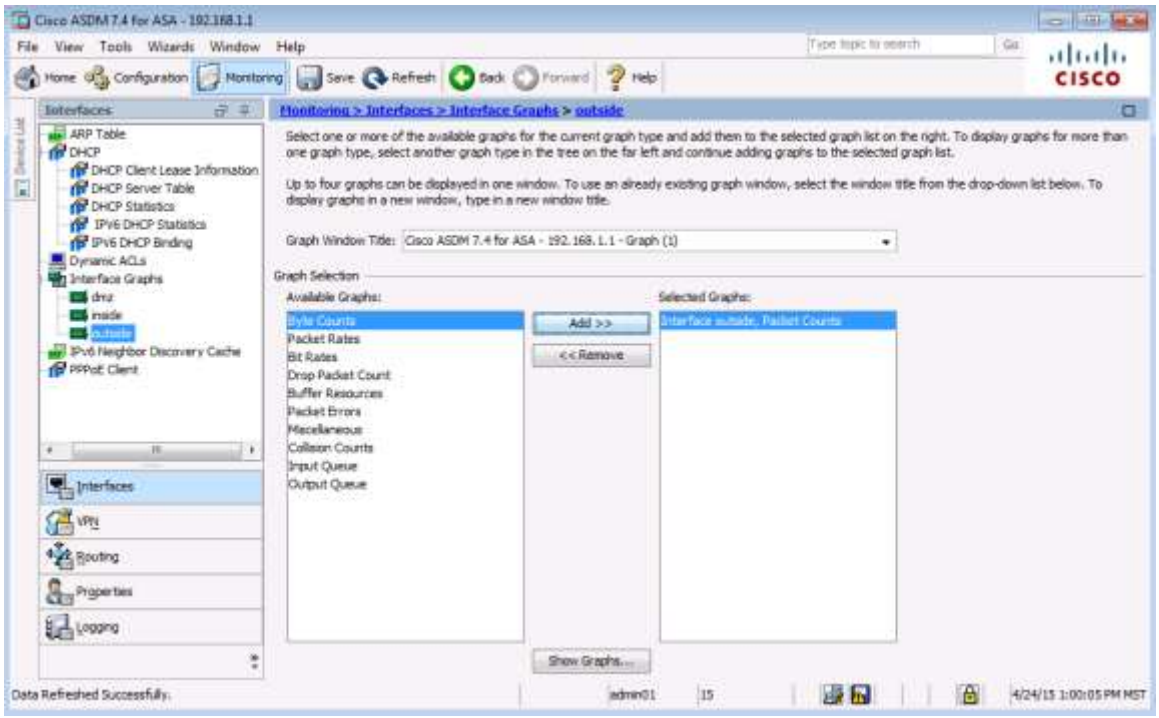
b. Так как уровень безопасности внутреннего интерфейса VLAN 1 ASA равен 100 (наивысший), а интерфейса DMZ (VLAN 3) – 70, вы также можете получить доступ к серверу DMZ с хоста из внутренней сети. ASA функционирует как маршрутизатор между двумя сетями. Отправьте эхо-запрос с хоста PC-B (192.168.1.X) внутренней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

c. Сервер DMZ не может выполнять эхо-запрос компьютера PC-B во внутренней сети. Это объясняется тем, что интерфейс DMZ VLAN 3 имеет более низкий уровень безопасности, и тем фактом, что во время создания интерфейса VLAN 3 было необходимо задать команду **no forward.** Попытайтесь отправить эхо-запрос с сервера DMZ на PC-A на компьютер PC-B по IP-адресу 192.168.1.X. Эти запросы должны завершаться ошибкой.

Шаг 5: Использование мониторинга ASDM для отслеживания активности пакетов.

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

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



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

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

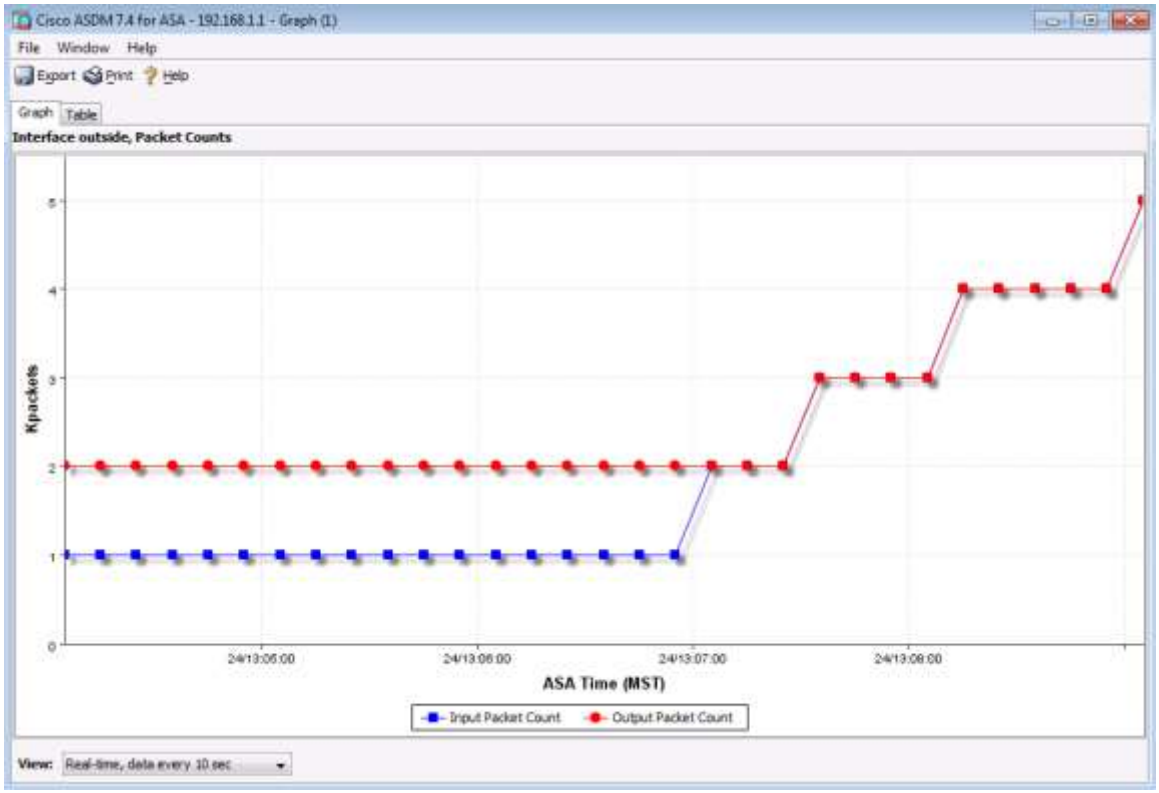
```
R2# ping 209.165.200.227 repeat 1000

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

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

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

```
C:>\ ping 10.1.1.1 -n 100
```

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



Вопросы для повторения

1. Перечислите некоторые преимущества использования ASDM по сравнению с CLI.

_____
_____
_____
_____
_____
_____

2. Перечислите некоторые преимущества использования CLI по сравнению с ASDM.

_____
_____
_____
_____
_____
_____

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.				

