CCNA Security

Глава 11. Комплексная лабораторная работа по курсу CCNA Security

Топология

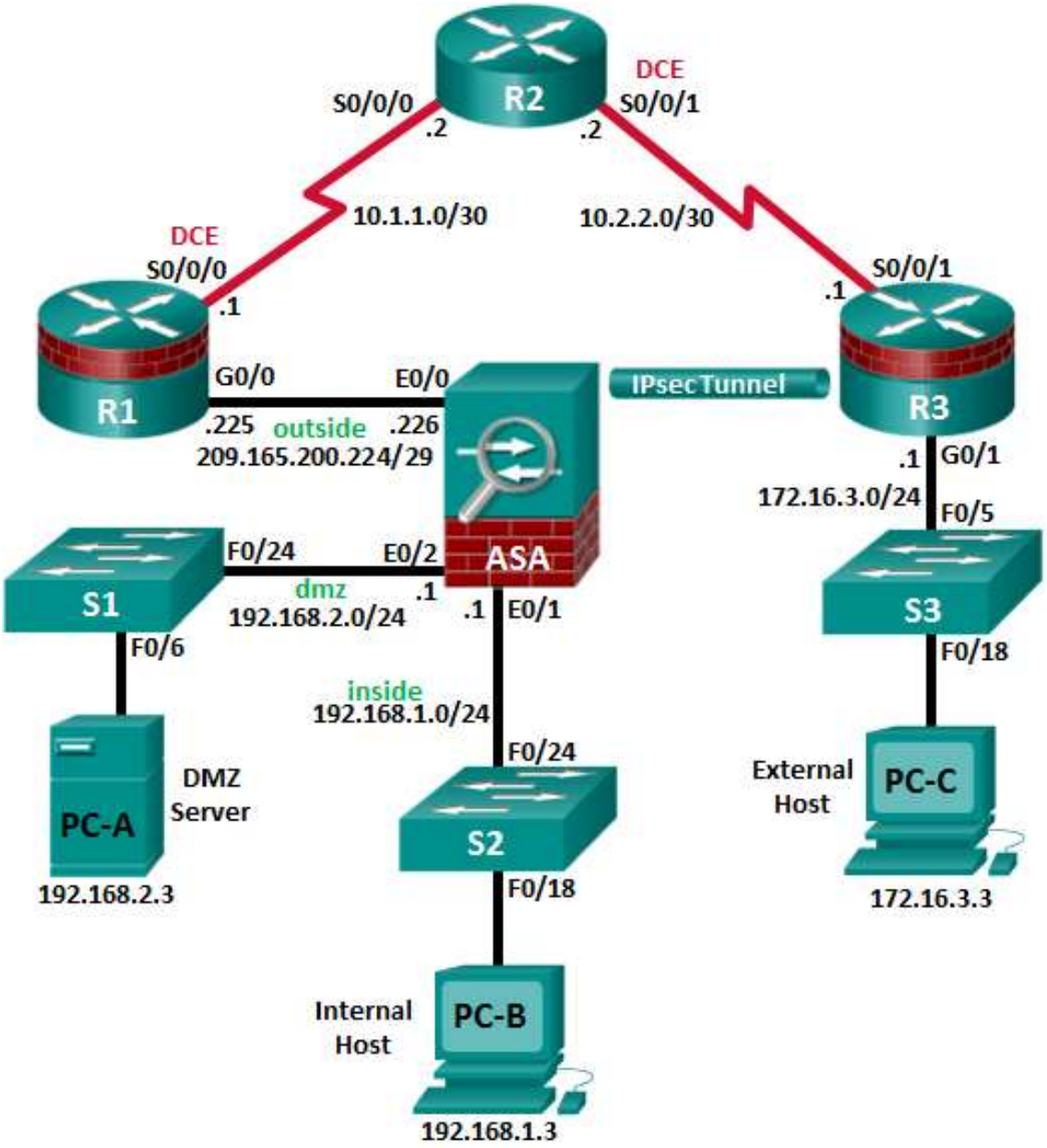

Таблица IP-адресов

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
	Loopback 1	172.20.1.1	255.255.255.0	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
S1	VLAN 1	192.168.2.11	255.255.255.0	192.168.2.1	Н/П
S2	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1	Н/П
S3	VLAN 1	172.16.1.11	255.255.255.0	172.30.3.1	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 2 (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. Создание базовой технической политики безопасности

Часть 2. Настройка основных параметров устройства

Часть 3. Настройка защищенного административного доступа к маршрутизатору

- Настройка зашифрованных паролей и баннера при входе в систему
- Настройка времени ожидания для привилегированного режима на линиях консоли и VTY
- Настройка частоты ошибок при входе в систему и расширений для входа в систему для VTY
- Настройка доступа по протоколу Secure Shell (SSH) и отключение Telnet
- Настройка локальной аутентификации пользователей по протоколу аутентификации, авторизации и учета (AAA)
- Защита маршрутизатора от атак методом подбора учетных данных, защита образа IOS и файла конфигурации
- Настройка NTP-клиентов и NTP-сервера на маршрутизаторе
- Настройка отчетности системного журнала маршрутизатора syslog и сервера syslog на локальном хосте

Часть 4. Настройка зонального межсетевого экрана и системы предотвращения вторжений

- Настройка зонального межсетевого экрана (ZPF) на ISR с помощью командной строки (CLI)
- Настройка системы предотвращения вторжений (IPS) на ISR с помощью командной строки (CLI)

Часть 5. Защита сетевых коммутаторов

- Настройка паролей и баннера при входе в систему

- Настройка доступа управляющей сети VLAN
- Защита портов доступа
- Защита от атак на Spanning Tree Protocol (STP)
- Настройка безопасности портов и отключение неиспользуемых портов

Часть 6. Настройка основных параметров ASA и межсетевого экрана

- Настройка основных параметров, паролей, даты и времени
- Настройка внешних и внутренних интерфейсов VLAN
- Настройка преобразования адресов портов (PAT) для внутренней сети
- Настройка сервера Dynamic Host Configuration Protocol (DHCP) для внутренней сети
- Настройка административного доступа по протоколам Telnet и SSH
- Настройка статического маршрута по умолчанию для многофункционального устройства безопасности (ASA)
- Настройка локальной аутентификации пользователей AAA
- Настройка DMZ со статическим NAT и списком ACL
- Проверка преобразования адресов и функций межсетевого экрана

Часть 7. Настройка DMZ, статического NAT и списков контроля доступа (ACL) на ASA

Часть 8. Настройка в ASA сети SSL VPN удаленного доступа без использования клиента с помощью ASDM

- Настройка сети SSL VPN удаленного доступа с помощью диспетчера Adaptive Security Device Manager (ASDM)
- Проверка доступа к порталу по сети SSL VPN

Часть 9. Настройка сети Site-to-Site VPN между ASA и ISR

- Настройка сети IPsec site-to-site VPN между ASA и маршрутизатором R3 с помощью ASDM и CLI
- Активация и проверка туннеля IPsec site-to-site VPN между ASA и маршрутизатором R3

Исходные данные/сценарий

Эта комплексная лабораторная работа состоит из девяти частей. Части следует выполнять по порядку. В части 1 вы создадите базовую техническую политику обеспечения безопасности. В части 2 вы настроите базовые параметры устройства. В части 3 с помощью интерфейса командной строки (CLI) вы настроите функции IOS, включая AAA и SSH, для защиты сетевого маршрутизатора. В части 4 вы настроите ZPF и IPS на ISR. В части 5 вы настроите сетевой коммутатор с помощью CLI. В частях 7 и 8 вы настроите функции межсетевого экрана ASA и удаленный доступ по сети SSL VPN без использования клиента. В части 9 вы настроите сеть site-to-site VPN между ASA и маршрутизатором R3.

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). Команды коммутатора и выходные данные соответствуют коммутаторам Cisco WS-C2960-24TT-L с ОС Cisco IOS Release 15.0(2)SE4 (образ C2960-LANBASEK9-M). Допускается использование других маршрутизаторов, коммутаторов 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 или коммутатора 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. 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: Создание базовой политики технической безопасности (главы 1 и 11)

В части 1 вы создадите документ «Руководство по безопасности сетевых устройств», который послужит частью комплексной политики обеспечения сетевой безопасности. В данном документе приведены меры по обеспечению безопасности для конкретных маршрутизаторов и коммутаторов, а также описаны требования безопасности для внедрения на оборудовании инфраструктуры.

Задача 1: Указание возможных разделов базовой политики сетевой безопасности

Политика сетевой безопасности должна включать в себя несколько ключевых разделов, рассматривающих возможные вопросы касательно пользователей, сетевого доступа, доступа к устройствам и прочих областей. Перечислите некоторые из ключевых разделов, которые, по вашему мнению, могли бы быть частью базовой политики обеспечения безопасности.

_____

_____

_____

_____

Задача 2: Создание документа «Руководство по обеспечению безопасности сетевых устройств» в качестве дополнения к базовой политике обеспечения безопасности

Шаг 1: Просмотрите задачи из предыдущих лабораторных работ по CCNA Security.

a. Откройте каждую из лабораторных работ, выполненных в главах 1–9, и просмотрите задачи, приведенные в каждой из них.

b. Скопируйте задачи в отдельный документ и используйте его как начальный пункт. Сфокусируйтесь на задачах, связанных с обеспечением безопасности и настройками оборудования.

Шаг 2: Создайте документ «Руководство по безопасности сетевых устройств» для обеспечения безопасности маршрутизатора и коммутатора.

Создайте высокоуровневый список задач для обеспечения сетевой безопасности и безопасности устройств. Этот документ предназначен для того, чтобы укрепить и дополнить информацию, представленную в базовой политике обеспечения безопасности. Он будет основан на содержимом предыдущих лабораторных работ по CCNA Security и сетевых устройствах, присутствующих в топологии лабораторных работ курса.

Примечание. Документ «Руководство по безопасности сетевых устройств» должен содержать не более двух страниц, и он будет основой для настройки оборудования в остальных частях лабораторной работы.

Шаг 3: Отправьте документ «Руководство по безопасности сетевых устройств» своему инструктору.

Предоставьте документ «Руководство по безопасности сетевых устройств» своему инструктору на проверку перед тем, как приступить к части 2 данной лабораторной работы. Вы можете отправить документ как вложение по электронной почте или скопировать на съемный носитель, например на флеш-карту.

Часть 2: Настройка основных параметров устройства (главы 2 и 6)

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Установите основные параметры для всех маршрутизаторов.

a. Задайте имена хостов, как показано на топологической схеме.

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

c. Установите для всех маршрутизаторов частоту DCE последовательного интерфейса **128000**, если используются маршрутизаторы, не указанные в данной лабораторной работе.

d. Отключите поиск DNS на всех маршрутизаторах.

Шаг 3: Настройте статические маршруты по умолчанию на маршрутизаторах R1 и R3.

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

b. Настройте статические маршруты из маршрутизатора R2 к симулируемой локальной сети R1 (Loopback 1), подсети Fa0/0-to-ASA маршрутизатора R1 и локальной сети маршрутизатора R3.

Шаг 4: Настройте основные параметры для каждого коммутатора.

a. Задайте имена хостов, как показано на топологической схеме.

b. Настройте адрес для управления интерфейсом VLAN 1 на каждом коммутаторе, как показано в таблице IP-адресов.

c. Настройте шлюз IP по умолчанию для каждого из трех коммутаторов.

d. Отключите поиск DNS на всех коммутаторах.

Шаг 5: Установите параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для каждого ПК, как показано в таблице IP-адресов.

Шаг 6: Проверьте связь между компьютером PC-C и интерфейсом G0/0 маршрутизатора R1.

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

Часть 3: Настройка защищенного административного доступа к маршрутизатору (главы 2 и 3)

С помощью CLI вы настроите пароли и ограничения доступа к устройству.

Задача 1: Настройка параметров для маршрутизаторов R1 и R3

Шаг 1: Задайте минимальную длину пароля в 10 символов.

Шаг 2: Зашифруйте пароли, заданные в виде открытого текста.

Шаг 3: Настройте предупреждающий баннер при входе в систему.

Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD), выводящего следующий текст: **Unauthorized access strictly prohibited and prosecuted to the full extent of the law!** (**Несанкционированный доступ строго запрещен и преследуется по всей строгости закона!**)

Шаг 4: Настройте пароль привилегированного доступа.

В качестве пароля привилегированного доступа (**enable secret**) задайте **cisco12345**. Используйте самый стойкий тип шифрования из доступных.

Шаг 5: Настройте локальную базу данных пользователей.

Создайте локальную учетную запись пользователя **Admin01** с паролем привилегированного доступа **Admin01pa55** и уровнем привилегий **15**. Используйте самый стойкий тип шифрования из доступных.

Шаг 6: Включите сервисы AAA.

Шаг 7: Разверните сервисы AAA с помощью локальной базы данных.

Создайте список методов аутентификации учетных данных по умолчанию. Используйте в качестве первого варианта локальную аутентификацию с учетом регистра, а также пароль привилегированного доступа в качестве резервного варианта, используемого в случае ошибки локальной аутентификации.

Шаг 8: Настройте линию консоли.

Настройте линию консоли для уровня привилегий 15 при входе в систему. Установите автоматический выход из системы после 15 минут бездействия посредством параметра **exec-timeout**. Предотвратите прерывание ввода команд сообщениями консоли.

Шаг 9: Настройте линии VTY.

Настройте для линий VTY доступ при входе в систему с уровнем привилегий 15. Установите автоматическое завершение сеанса после **15** минут бездействия посредством параметра **exec-timeout**. Разрешите удаленный доступ только по протоколу SSH.

Шаг 10: Настройте запись в журнал входа в систему на маршрутизаторе.

a. Настройте на маршрутизаторе запись системных сообщений в журнал об успешных и неудачных попытках входа в систему. Настройте запись в журнал всех удачных входов в систему на маршрутизаторе. Настройте запись в журнал всех вторых неудачных попыток входа в систему на маршрутизаторе.

b. Введите команду **show login**. Какая дополнительная информация отображается?

_____

_____

Шаг 11: Включите доступ по протоколу HTTP.

a. Включите HTTP-сервер на маршрутизаторе R1 для моделирования интернет-цели для последующего тестирования.

b. Настройте HTTP-аутентификацию на использование локальной базы данных пользователя на маршрутизаторе R1.

Задача 2: Настройка SSH-сервера на маршрутизаторах R1 и R3

Шаг 1: Настройте доменное имя.

Настройте доменное имя **ccnasecurity.com**.

Шаг 2: Сгенерируйте пару ключей RSA-шифрования.

Задайте количество битов модуля для RSA-ключей, равное **1024**.

Шаг 3: Настройте версию SSH.

Настройте маршрутизатор на прием соединений только по протоколу **SSH версии 2**.

Шаг 4: Настройте время ожидания SSH и параметры аутентификации.

Значения времени ожидания и параметров аутентификации SSH по умолчанию можно изменить на более ограничительные. Задайте время ожидания SSH **90** секунд и количество попыток аутентификации **2**.

Шаг 5: Проверьте связь с маршрутизатором R1 с компьютера PC-C.

a. Запустите SSH-клиент на компьютере PC-C, введите IP-адрес интерфейса S0/0/0 маршрутизатора R1 (**10.1.1.1**), и войдите в систему под именем **Admin01** и паролем **Admin01pa55**. Если появится предупреждение системы безопасности от SSH-клиента касательно ключа хоста сервера, нажмите кнопку **Yes**.

b. В сеансе SSH введите на компьютере PC-C команду **show run**. При этом на экране должны появиться настройки для маршрутизатора R1.

Задача 3: Защита от атак методом подбора учетных данных и защита образа IOS и файла конфигурации на маршрутизаторе R1

Шаг 1: Настройте расширенную защиту входа в систему.

Если пользователь совершает две неудачные попытки входа в систему за временной промежуток в **30** секунд, необходимо отключить возможность входа на **1** минуту. Регистрируйте в журнале все неудачные попытки входа в систему.

Шаг 2: Защитите файл образа Cisco IOS и заархивируйте копию текущей конфигурации.

a. Команда **secure boot-image** обеспечивает защиту образа Cisco IOS, позволяя не указывать файл в выходных данных для команд **dir** и **show**. Данный файл нельзя просматривать, копировать, изменять или удалять с помощью команд привилегированного режима. (Его можно просматривать в режиме ROMMON.)

b. Команда **secure boot-config** делает снимок состояния текущей конфигурации маршрутизатора и надежно архивирует его в постоянной памяти (флеш-памяти).

Шаг 3: Проверьте защищенность образа и конфигурации.

a. Для показа имени архивированного файла вы можете использовать только команду **show secure bootset**. Отобразите состояние защиты конфигурации и имя первичного загрузочного файла.

Какое имя у файла архива текущей конфигурации и на чем оно основано?

_____

_____

b. Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.

Шаг 4: Восстановите файлы IOS и конфигурации в состояние по умолчанию.

Вы проверили настройки защиты файлов IOS и конфигурации. Теперь с помощью команд **no secure boot-image** и **no secure boot config** восстановите настройки по умолчанию для этих файлов.

Задача 4: Настройка источника синхронизированного времени с использованием NTP

Маршрутизатор R2 будет главным источником сигналов времени для маршрутизаторов R1 и R3.

Шаг 1: Настройте главный NTP-узел с использованием команд Cisco IOS.

Маршрутизатор R2 является главным NTP-сервером в данной лабораторной работе. Все остальные маршрутизаторы и коммутаторы с его помощью настраивают время как напрямую, так и косвенно. Поэтому убедитесь, что на маршрутизаторе R2 установлено правильное время в соответствии с UTC.

a. Используйте команду **show clock** для показа текущего времени, заданного в маршрутизаторе.

b. Используйте команду в формате **clock set** *time,* чтобы задать время на маршрутизаторе.

c. Настройте аутентификацию NTP, задав номер ключа аутентификации **1**, тип хеширования **md5** и пароль **NTPpassword**. Пароль чувствителен к регистру.

d. Настройте доверенный ключ, который будет использоваться для аутентификации на маршрутизаторе R2.

e. Включите функцию аутентификации NTP на маршрутизаторе R2.

f. Настройте маршрутизатор R2 как главный NTP-узел, используя команду в формате **ntp master** *stratum-number* в режиме глобальной настройки. Номер слоя указывает на расстояние от источника. В данной лабораторной работе используйте номер слоя **3** на маршрутизаторе R2. Когда устройство узнает время из источника NTP, его номер слоя становится на 1 больше, чем номер слоя его источника.

Шаг 2: Настройте маршрутизаторы R1 и R3 в качестве клиентов NTP с использованием командной строки.

a. Настройте аутентификацию NTP, задав номер ключа аутентификации **1**, тип хеширования **md5** и пароль **NTPpassword**.

b. Настройте доверенный ключ, который будет использоваться для аутентификации. Данная команда защищает устройство от случайной синхронизации с недоверенным источником времени.

c. Включите функцию аутентификации NTP.

d. Маршрутизаторы R1 и R3 станут NTP-клиентами маршрутизатора R2. Используйте команду режима глобальной настройки в формате **ntp server** *hostname*. В качестве имени хоста используйте последовательный IP-адрес маршрутизатора R2. Введите команду **ntp update-calendar** на маршрутизаторах R1 и R3 для периодического обновления календаря в соответствии со временем NTP.

e. Используйте команду **show ntp associations**, чтобы убедиться, что маршрутизатор R1 установил ассоциацию с R2. Вы также можете использовать более подробную версию команды, добавив аргумент *detail*. Для формирования ассоциации с протоколом NTP может понадобиться некоторое время.

f. Проверьте время на маршрутизаторах R1 и R3 после того, как они создадут ассоциации NTP с R2.

Задача 5: Настройка поддержки системного журнала (syslog) на маршрутизаторе R3 и компьютере PC-C

Шаг 1: Установите сервер syslog на компьютере PC-C.

a. Программа Tftpd32 с сайта jounin.net бесплатна для скачивания и установки. Она включает в себя TFTP-сервер, TFTP-клиент, а также сервер и средство просмотра системного журнала. Если программа Tftpd32 еще не установлена, загрузите ее по ссылке http://tftpd32.jounin.net и установите на компьютер PC-C.

b. Запустите файл **Tftpd32.exe**, нажмите **Settings** и убедитесь, что флажок **syslog server** установлен. На вкладке **SYSLOG** вы можете настроить файл для сохранения сообщений syslog. Закройте окно настроек, затем в главном окне интерфейса Tftpd32 обратите внимание на IP-адрес интерфейса сервера, после чего перейдите на вкладку **Syslog server**, чтобы переместить ее на передний план.

Шаг 2: Настройте маршрутизатор R3 для записи сообщений в журнал на сервере syslog с помощью командной строки.

a. Убедитесь, что у вас есть связь между маршрутизатором R3 и компьютером PC-C, отправив запрос ping на интерфейс G0/1 маршрутизатора R3 по IP-адресу **172.16.3.1**. Если это сделать не удается, устраните проблему перед тем, как продолжить.

b. Протокол NTP был настроен в задаче 2 для синхронизации времени в сети. Очень важно, чтобы в сообщениях syslog отображались правильные дата и время, когда syslog используется для мониторинга сети. Если правильные время и дата сообщений неизвестны, то определить, вследствие чего возникло то или иное сообщение о событии, станет затруднительно.

   Убедитесь, что на маршрутизаторе включен сервис временных меток для ведения журналов, с помощью команды **show run**. Используйте команду **service timestamps log datetime msec**, если сервис временных меток не включен.

c. Настройте сервис syslog на маршрутизаторе для отправки сообщений системного журнала на сервер syslog.

Шаг 3: Настройте уровень критичности ведения журнала на маршрутизаторе R3.

Для журнальных прерываний можно установить поддержку функции ведения журналов. Прерывание – это порог, при котором появляется журнальное сообщение. Уровень журнальных сообщений можно настроить так, чтобы администратор мог определить типы сообщений, которые должны отправляться на сервер syslog. Маршрутизаторы поддерживают различные уровни ведения журналов. Таких уровней восемь: от 0 (авария), который указывает на нестабильность системы, до 7 (отладка), при котором отправляются сообщения, содержащие информацию о маршрутизаторе.

Примечание. Для системного журнала уровень по умолчанию – 6 (информационные сообщения). Консоль и мониторинг по умолчанию имеют уровень 7 (отладка).

a. Используя команду **logging trap**, установите для маршрутизатора R3 уровень критичности 4 **(warnings)**.

b. Используйте команду **show logging** для просмотра текущего типа и уровня ведения журнала.

Часть 4: Настройка зонального межсетевого экрана и системы предотвращения вторжений (главы 4 и 5)

В части 4 с помощью интерфейса командной строки вы настроите ZPF и IPS на маршрутизаторе R3.

Задача 1: Настройка ZPF на маршрутизаторе R3 с помощью командной строки

Шаг 1: Создайте зоны безопасности.

a. Создайте внутренние **(INSIDE)** и внешние **(OUTSIDE)** зоны безопасности.

b. Создайте карту класса инспектирования для сопоставления разрешенного трафика из зоны **INSIDE** в зону **OUTSIDE.** Так как мы доверяем зоне **INSIDE**, мы разрешаем все основные протоколы. Используйте ключевое слово **match-any**, чтобы сообщить маршрутизатору, что следующие операторы протокола **match** будут квалифицироваться как положительное совпадение. При этом будет применена политика. Ищите совпадение для пакетов **TCP**, **UDP** или **ICMP**.

c. Создайте карту политик инспектирования с именем **INSIDE-TO-OUTSIDE**. Привяжите карту классов **INSIDE-PROTOCOLS** к карте политик. Инспектироваться будут все пакеты, отмеченные картой класса **INSIDE-PROTOCOLS**.

d. Создайте пару зон с именем **INSIDE-TO-OUTSIDE**, которая будет разрешать трафик, исходящий из внутренней сети во внешнюю, но запрещать трафик, исходящий из внешней сети во внутреннюю.

e. Примените карту политик к паре зон.

f. Назначьте интерфейс G0/1 маршрутизатора R3 зоне безопасности **INSIDE**, а интерфейс S0/0/1 – зоне безопасности **OUTSIDE**.

g. Проверьте конфигурацию ZPF с помощью команд **show zone-pair security**, **show policy-map type inspect zone-pair** и **show zone security**.

Задача 2: Настройка IPS на маршрутизаторе R3 с помощью командной строки.

Шаг 1: Подготовьте маршрутизатор R3 и TFTP-сервер.

Для настройки Cisco IOS IPS 5.x необходимо, чтобы на ПК с установленным TFTP-сервером были доступны файл пакета сигнатур IOS IPS и файл открытых криптографических ключей. Маршрутизатор R3 использует компьютер PC-C в качестве TFTP-сервера. Если этих файлов на вашем компьютере нет, обратитесь к инструктору.

a. Убедитесь, что файл пакета сигнатур **IOS-Sxxx-CLI.pkg** находится в папке TFTP по умолчанию. Буквами *xxx* в имени файла обозначается номер версии. Это значение зависит от того, какой файл был загружен с сайта Cisco.com.

b. Убедитесь, что имеется файл **realm-cisco.pub.key.txt**, и отметьте его расположение на компьютере PC-C. Это открытый криптографический ключ, используемый системой Cisco IOS IPS.

c. Проверьте или создайте папку IPS (**ipsdir**) во флеш-памяти маршрутизатора R3. С помощью командной строки маршрутизатора R3 отобразите содержимое флеш-памяти и проверьте, существует ли папка **ipsdir**.

d. Если папка **ipsdir** в списке отсутствует, создайте ее в привилегированном режиме, используя команду **mkdir**.

Примечание. Если папка IPSDIR присутствует в списке и в ней находятся файлы, обратитесь к инструктору. Перед настройкой IPS эта папка должна быть пустой. Если файлов в этой папке нет, вы можете перейти к дальнейшей настройке IPS.

Шаг 2: Проверьте расположение пакета сигнатур IOS IPS и установочный файл TFTP-сервера.

a. Используйте команду **ping** для проверки соединения между маршрутизатором R3, компьютером PC-C и TFTP-сервером**.**

b. Запустите Tftpd32 (или другой TFTP-сервер) и задайте по умолчанию папку с пакетом сигнатур IPS. Запишите имя файла, чтобы использовать его на следующем шаге.

Шаг 3: Скопируйте и вставьте файл криптографического ключа в конфигурацию маршрутизатора R3.

В режиме глобальной настройки выберите и скопируйте файл криптографического ключа с именем **realm-cisco.pub.key.txt**. Вставьте содержимое криптографического ключа в запросе режима глобальной настройки.

Примечание. Содержимое файла realm-cisco.pub.key.txt приведено ниже.

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
   17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
   B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
   5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
   FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
   50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
   006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
   2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
   F3020301 0001
  quit
```

Шаг 4: Настройте параметры IPS на маршрутизаторе R3 в интерфейсе командной строки.

a. Создайте правило IPS и назначьте ему имя **IOSIPS**.

b. Задайте расположение хранилища сигнатур IPS в папке **IPSDIR**, которую вы создали во флеш-памяти на шаге 1d.

c. Включите HTTP-сервер и уведомление о событиях IPS SDEE.

d. Настройте систему предотвращения вторжений IOS на использование предварительно заданных категорий сигнатур.

Примечание. При настройке IOS IPS необходимо сначала вывести из использования все сигнатуры в категории all, а затем вернуть в использование выбранные категории сигнатур.

После того как вы выведете из использования все сигнатуры в категории **all**, введите в использование категорию **ios_ips basic**.

e. Примените правило IPS ко входящему трафику интерфейса S0/0/1 маршрутизатора R3.

Шаг 5: Запустите TFTP-сервер на компьютере PC-C и проверьте папку файла IPS.

Убедитесь, что файл пакета сигнатур IPS компьютера PC-C находится в папке на TFTP-сервере. Имя файла обычно имеет формат IOS-S*xxx*-CLI.pkg. Буквы *xxx* обозначают номер версии файла сигнатуры.

Примечание. Если этот файл отсутствует, обратитесь к инструктору перед тем, как продолжить.

Шаг 6: Скопируйте пакет сигнатур с TFTP-сервера на маршрутизатор R3.

a. С помощью команды **copy tftp** получите файл сигнатур и загрузите его в конфигурацию обнаружения вторжений. В конце команды **copy** используйте ключевое слово **idconf**.

Примечание. Компилирование сигнатур начнется сразу после загрузки пакета сигнатур на маршрутизатор. При уровне ведения журнала 6 или выше вы сможете увидеть сообщения на маршрутизаторе.

b. Используйте команду **dir flash** для просмотра содержимого папки **IPSDIR**, которую вы создали ранее в этой лабораторной работе. В ней должно быть шесть файлов, как показано далее.

c. С помощью команды **show ip ips signature count** определите число сигнатур в пакете скомпилированных сигнатур.

```
R3# show ip ips signature count
```


Примечание. Во время компилирования сигнатур вы можете увидеть сообщение об ошибке, например: %IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)». Это значит, что открытый криптографический ключ недействителен. Вернитесь к задаче 3 «Настройка криптографического ключа IPS», чтобы перенастроить открытый криптографический ключ.

d. Используйте команду **show ip ips all**, чтобы просмотреть сводку состояний конфигурации IPS.

Часть 5: Защита сетевых коммутаторов (глава 6)

Примечание. В этой части лабораторной работы будут настроены не все функции безопасности и не на всех коммутаторах. Однако в производственной сети все функции безопасности необходимо настроить на всех коммутаторах.

Шаг 1: Настройте основные параметры безопасности на коммутаторе S1.

a. Доступ к коммутатору по HTTP включен по умолчанию. Предотвратите доступ по HTTP, отключив HTTP- и HTTPS-серверы.

Используйте пароль привилегированного доступа **cisco12345**. Используйте самый стойкий тип шифрования из доступных.

b. Зашифруйте пароли, заданные в виде открытого текста.

c. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD), выводящего текст: **Unauthorized access strictly prohibited!** (Неавторизованный доступ запрещен!).

Шаг 2: Настройте SSH-сервер на коммутаторе S1.

a. Настройте доменное имя.

b. Настройте в локальной базе данных имя пользователя **Admin01** с паролем **Admin01pa55.** Установите для пользователя максимально возможный уровень привилегий. К паролю необходимо применить самый стойкий метод шифрования из возможных.

c. Задайте количество битов модуля для RSA-ключей, равное 1024.

d. Включите протокол SSH версии 2.

e. Установите время ожидания SSH **90** секунд и количество повторных попыток аутентификации **2**.

Шаг 3: Настройте линии консоли и линии VTY.

a. Настройте консоль на использование локальной базы для входа в систему. Если пользователь имеет наивысший уровень привилегий, задайте автоматический вход в привилегированный режим. Установите автоматический выход из системы после пяти минут бездействия посредством параметра **exec-timeout**. Предотвратите прерывание ввода команд сообщениями консоли.

b. Настройте линии VTY на использование локальной базы данных для входа в систему. Если пользователь имеет наивысший уровень привилегий, задайте автоматический вход в привилегированный режим. Установите автоматический выход из системы после пяти минут бездействия посредством параметра **exec-timeout**. Разрешите удаленный доступ по протоколу SSH ко всем линиям VTY.

Шаг 4: Настройте безопасность портов и отключите неиспользуемые порты.

Примечание. Изменения настроек, внесенные на шаге 4 для интерфейса F0/6 в среде NETLAB+, могут отрицательно повлиять на результаты лабораторной работы из-за скрытого управляющего коммутатора между коммутатором S1 и компьютером PC-A. Если вы выполняете эту лабораторную работу в среде NETLAB+, то на этом шаге рекомендуется изменять настройки на интерфейсе F0/7 (активный порт), а не на F0/6.

a. Отключите транкинг в порте F0/6.

b. Включите PortFast на F0/6.

c. Включите функцию BPDU Guard на F0/6.

d. Примените основной уровень безопасности по умолчанию на порте F0/6. Это позволит установить максимальное число MAC-адресов (1) и действие при нарушении (shutdown). Используйте опцию sticky, чтобы защитить MAC-адрес, который динамически определяется на порту для текущей конфигурации коммутатора.

e. Отключите неиспользуемые порты на коммутаторе S1.

Шаг 5: Установите Loop Guard как функцию по умолчанию для всех неназначенных портов на коммутаторе S1.

Шаг 6: Сохраните текущую конфигурацию в конфигурацию запуска каждого коммутатора.

Часть 6: Настройка основных параметров ASA и межсетевого экрана (глава 9)

Задача 1: Подготовка ASA к доступу через ASDM

Шаг 1: Сбросьте предыдущие настройки конфигурации ASA.

a. С помощью команды **write erase** удалите файл **startup-config** из флеш-памяти.

b. Используйте команду **reload** для перезапуска ASA.

Шаг 2: Пропустите режим настройки и настройте интерфейсы ASDM VLAN с помощью интерфейса командной строки.

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

b. Перейдите в привилегированный режим. На данном этапе пароль должен быть пустым (отсутствовать).

c. Войдите в режим глобальной настройки. На запрос включения анонимной отправки отчетов ответьте **no** (нет).

d. Логический интерфейс VLAN 1 будет использоваться компьютером PC-B для доступа к ASDM на физическом интерфейсе E0/1 устройства ASA. Настройте интерфейс **VLAN 1** и назовите его **inside**. Уровень безопасности должен быть автоматически установлен на наивысший уровень 100. Укажите IP-адрес **192.168.1.1** и маску подсети **255.255.255.0**.

e. Включите физический интерфейс **E0/1**.

f. Предварительно настройте интерфейс **VLAN 2**, назовите его **outside**, назначьте IP-адрес **209.165.200.226** и маску подсети **255.255.255.248**. Обратите внимание, что уровень безопасности VLAN автоматически устанавливается на 0.

g. Назначьте **VLAN 2** физическому интерфейсу **E0/0** и включите интерфейс.

h. Настройте сеть VLAN 3, в которой будет находиться веб-сервер с открытым доступом. Назначьте сети IP-адрес **192.168.2.1/24**, присвойте ей имя **dmz** и уровень безопасности **70**.

Примечание. Если вы работаете с устройством 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.

i. Назначьте **VLAN 3** интерфейсу **E0/2** и включите интерфейс.

j. Отобразите состояние всех интерфейсов ASA, используя команду **show interface ip brief**.

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

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

Шаг 3: Настройте и проверьте доступ к устройству ASA из внутренней сети.

a. Отправьте запрос ping с компьютера PC-B на внутренний интерфейс устройства ASA (192.168.1.1). Запрос ping должен быть выполнен успешно.

b. С помощью команды **http** настройте на ASA возможность установления соединений HTTPS и разрешите доступ к ASDM с любого хоста во внутренней сети (192.168.1.0/24).

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

d. На стартовой странице ASDM нажмите **Run ASDM**. При получении запроса на ввод имени пользователя и пароля оставьте поля пустыми и нажмите **OK**.

Задача 2: Настройка основных параметров устройства ASA с использованием мастера ASDM Startup Wizard

Шаг 1: Войдите в меню конфигурации и запустите Startup Wizard.

В верхней левой части экрана выберите **Configuration** > **Launch Startup wizard** (Настройки > Запуск мастера запуска).

Шаг 2: Настройте имя хоста, доменное имя и пароль привилегированного доступа.

a. На начальном экране мастера Startup Wizard выберите опцию **Modify Existing Configuration** (Изменить текущую конфигурацию).

b. На экране Startup Wizard Step 2 введите имя хоста ASA **CCNAS-ASA** и доменное имя **ccnasecurity.com**. Измените пароль привилегированного режима с пустого (отсутствие пароля) на **cisco12345**.

Шаг 3: Проверьте настройки VLAN и интерфейса.

a. На экране Startup Wizard Step 3 не изменяйте текущие настройки, так как они уже были определены с помощью CLI.

b. На экране Startup Wizard Step 4 убедитесь, что порт **Ethernet 0/1** выделен внутренней сети VLAN 1, а порт **Ethernet 0/0 –** внешней сети VLAN 2.

c. На экране Startup Wizard Step 5 убедитесь, что внешний и внутренний IP-адреса настроены правильно. Нажмите **Next**.

Шаг 4: Настройте DHCP, преобразование адресов и административный доступ.

a. На экране Startup Wizard Step 6 – DHCP Server выберите **Enable DHCP server on the inside interface,** укажите начальный IP-адрес **192.168.1.5** и конечный IP-адрес **192.168.1.30**. Введите адрес сервера DNS 1 **10.3.3.3** и доменное имя **ccnasecurity.com**. **НЕ** устанавливайте флажок Enable auto-configuration from interface.

b. На экране Startup Wizard Step 7 – Address Translation (NAT/PAT) установите для устройства ASA опцию **Use Port Address Translation (PAT)** и выберите опцию **Use Port Address Translation (PAT)** (Использовать преобразование адреса и номера порта PAT)**.**

c. На экране Startup Wizard Step 8 – Administrative Access доступ HTTPS/ASDM сейчас настроен для хостов во внутренней сети (192.168.1.0/24). Добавьте доступ по протоколу **SSH** к ASA для внутренней (**inside**) сети (**192.168.1.0**) с маской подсети **255.255.255.0**.

d. Завершите работу мастера запуска и передайте команды на устройство ASA.

Примечание. При повторном запросе на вход в систему оставьте поле **Username** пустым и введите пароль **cisco12345**.

Задача 3: Настройка параметров устройства ASA из меню конфигурации ASDM

Шаг 1: Установите дату и время на ASA.

На экране **Configuration** > **Device Setup** нажмите **System Time** > **Clock** (Системное время > Часы). Установите часовой пояс, текущую дату, время и примените команды на устройстве ASA.

Шаг 2: Настройте статический маршрут по умолчанию для устройства ASA.

a. На экране **Configuration** > **Device Setup** выберите **Routing** > **Static Routes.** Нажмите кнопку **IPv4 only** (Только IPv4), после чего добавьте статический маршрут для интерфейса **outside**. Для Network укажите **any4**, а для Gateway IP введите IP-адрес **209.165.200.225** (интерфейс G0/0 маршрутизатора R1). Примените (**Apply**) настройки статического маршрута на устройстве ASA.

b. В меню **Tools ASDM** выберите **Ping** и введите IP-адрес интерфейса S0/0/0 маршрутизатора R1 (**10.1.1.1**). Запрос ping должен быть выполнен успешно.

Шаг 3: Проверьте доступ к внешнему веб-сайту с компьютера PC-B.

Откройте браузер на компьютере PC-B и введите IP-адрес интерфейса S0/0/0 маршрутизатора R1 (**10.1.1.1**), тем самым смоделировав доступ к внешнему сайту. HTTP-сервер на маршрутизаторе R1 был включен во второй части данной лабораторной работы. Вы должны получить запрос на аутентификацию пользователя из диспетчера устройств R1 GUI. Закройте браузер.

Примечание.: Вам не удастся отправить запрос ping с компьютера PC-B на интерфейс S0/0/0 маршрутизатора R1, так как политика инспектирования трафика прикладного уровня ASA не разрешает ICMP из внешней сети.

Шаг 4: Настройте аутентификацию AAA для клиентского доступа SSH.

a. На экране **Configuration** > **Device Management** выберите **Users/AAA** > **User Accounts** > **Add**. Создайте нового пользователя с именем **Admin01** и паролем **Admin01pa55.** Назначьте этому пользователю полный доступ (**Full access**) (ASDM, SSH, Telnet и консоль) и установите уровень привилегий **15**. Примените команду на устройстве ASA.

b. На экране **Configuration** > **Device Management** выберите **Users/AAA** > **AAA Access**. На вкладке Authentication настройте требование аутентификации для соединений по **HTTP/ASDM** и **SSH,** затем укажите группу серверов **LOCAL** для каждого вида соединения. Нажмите **Apply** для отправки команды на ASA.

Примечание. Перед выполнением следующего действия с ADSM необходимо войти в систему под учетной записью **Admin01** с паролем **Admin01pa55.**

c. На компьютере PC-B откройте клиент SSH и попытайтесь подключиться ко внутреннему интерфейсу ASA по адресу **192.168.1.1**. Установление соединения должно быть возможно. Получив запрос на вход в систему, введите имя пользователя **Admin01** и пароль **Admin01pa55**.

d. После входа в ASA при помощи SSH введите команду **enable** и пароль **cisco12345.** Введите команду **show run**, чтобы отобразить текущую конфигурацию, созданную при помощи ASDM. Закройте SSH-сеанс.

Задача 4: Изменение модульной системы политик по умолчанию с помощью ASDM

Шаг 1: Измените политику инспектирования трафика на прикладном уровне MPF.

Глобальная политика инспектирования трафика по умолчанию не проверяет ICMP. Чтобы хосты во внутренней сети могли посылать запросы ping на внешние хосты и получать от них ответы, необходимо инспектировать трафик ICMP.

a. С компьютера PC-B перейдите к экрану ASDM **Configuration** и выберите меню **Firewall**. Нажмите **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 отмеченные флажками протоколы по умолчанию. Нажмите **OK** > **Apply** для отправки команды на ASA.

Примечание. При получении запроса выполните вход под учетной записью **Admin01** и паролем **Admin01pa55.**

Шаг 2: Убедитесь, что обратный ICMP-трафик разрешен.

Отправьте эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу **209.165.200.225**. Запрос ping должен быть выполнен успешно, так как для ICMP-трафика теперь выполняется инспектирование.

Часть 7: Настройка DMZ, статического преобразования сетевых адресов (NAT) и списков контроля доступа (ACL) (глава 10)

В части 6 данной лабораторной работы вы настроили преобразование адресов при помощи PAT для внутренней сети, используя ASDM. В этой части вы с помощью ASDM настроите DMZ, статическое преобразование NAT и списки контроля доступа (ACL) на устройстве ASA.

Для обеспечения добавления DMZ и веб-сервера вы будете использовать другой адрес из назначенного диапазона адресов ISP (209.165.200.224/29). Интерфейс G0/0 маршрутизатора R1 и внешний интерфейс ASA уже используют адреса 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 статическое преобразование NAT на сервере DMZ с помощью сетевого объекта.

a. С компьютера PC-B перейдите к экрану ASDM **Configuration** и выберите меню **Firewall**. Для определения сервера DMZ и предлагаемых сервисов выберите 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 в поле Public IP address адрес **209.165.200.227**.

b. Нажмите кнопку выбора справа от поля Private IP Address. В окне Browse Private IP Address нажмите **Add**, чтобы определить сервер как сетевой объект (**Network Object**). Введите имя **DMZ-Server**, в поле Type выберите **Host**, введите в поле Private IP Address адрес **192.168.2.3**, в поле Description – **PC-A.**

c. В окне Browse Private IP Address убедитесь, что сервер DMZ отображается в поле Selected Private IP Address, 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 нажмите следующие сервисы: **tcp/ftp**, **tcp/http** и **icmp/echo** (используйте полосу прокрутки, чтобы увидеть все сервисы). Нажмите **OK**, чтобы продолжить и вернуться в диалоговое окно **Add Public Server**.

e. Нажмите **OK**, чтобы добавить сервер. На экране Public Servers нажмите **Apply**, чтобы отправить команды на устройство ASA.

Шаг 2: Просмотрите правило доступа DMZ (ACL), созданное диспетчером ASDM.

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.

Просмотрите это правило доступа в ASDM путем выбора **Configuration** > **Firewall** > **Access Rules** (Настройки > Межсетевой экран > Правила доступа). Оно будет показано в качестве внешнего входящего правила. Вы можете выбрать правило и просмотреть его компоненты с помощью горизонтальной полосы прокрутки.

Шаг 3: Проверьте доступ 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**). Запрос ping должен быть выполнен успешно.

b. Вы также можете получить доступ к серверу DMZ с хоста внутренней сети, так как на внутреннем интерфейсе ASA (VLAN 1) установлен уровень безопасности 100 (самый высокий), а на интерфейсе DMZ (VLAN 3) – 70. ASA играет роль маршрутизатора между двумя сетями. Отправьте команду ping на внутренний адрес сервера DMZ (PC-A) (**192.168.2.3**) с компьютера PC-B. Запрос ping должен быть выполнен успешно благодаря установленному уровню безопасности и тому факту, что глобальная политика инспектирования осуществляет контроль ICMP на внутреннем интерфейсе.

c. Сервер DMZ не может отправить запрос ping на компьютер PC-B, так как уровень безопасности интерфейса VLAN 3 сервера DMZ ниже, а также в связи с необходимостью указания команды **no forward** при создании интерфейса VLAN 3. Попытайтесь отправить запрос ping с сервера DMZ PC-A на компьютер PC-B. Этот запрос пройти не должен.

Часть 8: Настройка в ASA сети SSL VPN удаленного доступа без использования клиента (глава 10)

В части 8 данной лабораторной работы вы настроите на устройстве ASA поддержку сети SSL VPN удаленного доступа без использования клиента с помощью мастера ASDM Clientless SSL VPN. Вы проверите конфигурацию с помощью браузера с компьютера PC-C.

Шаг 1: Запустите мастер VPN.

С помощью ASDM на компьютере PC-B выберите **Wizards** > **VPN Wizards** > **Clientless SSL VPN wizard**. Появится окно Clientless SSL VPN Connection мастера SSL VPN.

Шаг 2: Настройте интерфейс пользователя для SSL VPN.

На экране SSL VPN Interface в поле Connection Profile Name укажите **VPN-PROFILE**, а также компонент **outside** в качестве интерфейса, к которому будут подключаться внешние пользователи.

Шаг 3: Настройте аутентификацию пользователей AAA.

На экране User Authentication нажмите **Authenticate Using the Local User Database**, введите имя пользователя **VPNuser** и пароль **Remotepa55**. Нажмите **Add,** чтобы добавить нового пользователя.

Шаг 4: Настройте групповую политику VPN.

На экране Group Policy создайте новую групповую политику с именем **VPN-GROUP**.

Шаг 5: Настройте список закладок.

a. На экране Clientless Connections Only – Bookmark List нажмите **Manage**, чтобы создать закладку HTTP-сервера в списке закладок. В окне Configure GUI Customization Objects нажмите **Add**, чтобы открыть окно Add Bookmark List. Назовите список **WebServer**.

b. Добавьте новую закладку с заголовком **Web Mail**. Введите IP-адрес сервера назначения **192.168.1.3** (компьютер PC-B моделирует внутренний веб-сервер) в строке URL.

c. Нажмите OK, чтобы завершить работу мастера, и **Apply** для отправки данных в ASA.

Шаг 6: Проверьте доступ к виртуальной частной сети (VPN) с удаленного хоста.

a. Откройте браузер на компьютере PC-C и введите URL-адрес входа для SSL VPN в поле адреса (**https://209.165.200.226**). Используйте защищенный протокол HTTP (HTTPS), так как для подключения к ASA требуется SSL.

Примечание. Примите все предупреждения системы безопасности.

b. Должно появиться окно Login. Введите настроенное ранее имя пользователя **VPNuser,** пароль **Remotepa55** и нажмите кнопку **Logon**, чтобы продолжить.

Шаг 7: Войдите на страницу веб-портала.

После аутентификации пользователя появится веб-страница портала ASA SSL. На ней будут перечислены закладки, назначенные ранее данному профилю. Если закладка указывает на действительный IP-адрес сервера или хоста, на котором установлены и работают веб-сервисы HTTP, внешний пользователь сможет получить доступ к этому серверу через портал ASA.

Примечание. В этой лабораторной работе почтовый веб-сервер на компьютере PC-B не установлен.

Часть 9: Настройка сети Site-to-Site IPsec VPN между устройством ASA и маршрутизатором R3 (главы 8 и 10)

В части 9 этой лабораторной работы вы воспользуетесь интерфейсом командной строки (CLI) для настройки IPSec VPN-туннеля на маршрутизаторе R3, а также настроите другую сторону туннеля IPsec на устройстве ASA с помощью мастера ASDM Site-to-Site Wizard.

Задача 1: Настройка туннеля Site-to-Site IPsec VPN на маршрутизаторе R3

Шаг 1: Включите IKE и настройте параметры политики ISAKMP.

a. Убедитесь, что IKE поддерживается и включен.

b. Создайте политику ISAKMP с номером приоритета **1**. Используйте тип аутентификации **pre-shared key**, алгоритм шифрования **3des,** алгоритм хеширования **sha** и группу Diffie-Hellman **2** для обмена ключами.

c. Настройте общий ключ **Site2SiteKEY1** и направьте его на IP-адрес внешнего интерфейса устройства ASA.

d. Проверьте политику IKE с помощью команды **show crypto isakmp policy**.

Шаг 2: Настройте набор преобразований и время жизни IPsec.

Создайте набор преобразований с тегом **TRNSFRM-SET** и примените преобразование ESP с шифром AES 256 с ESP и хеш-функцией SHA.

Шаг 3: Определите «интересный» трафик.

Настройте список ACL для «интересного» IPSec VPN-трафика. Используйте номер расширенного списка контроля доступа **101**. Исходной сетью должна быть локальная сеть маршрутизатора R3 (172.16.3.0/24), а сетью назначения – локальная сеть устройства ASA (192.168.1.0/24).

Шаг 4: Создайте и примените криптографическую карту.

a. Создайте криптографическую карту на маршрутизаторе R3, назовите ее **CMAP** и укажите 1 в качестве порядкового номера.

b. Используйте команду **match address <access-list>** для указания списка доступа, определяющего трафик, который нужно шифровать.

c. Задайте в качестве адреса другого узла IP-адрес интерфейса удаленного конечного устройства VPN (**209.165.200.226**).

d. Укажите набор преобразований **TRNSFRM-SET**.

e. Примените криптографическую карту к интерфейсу S0/0/1 маршрутизатора R3.

Шаг 5: Проверьте конфигурацию IPsec на маршрутизаторе R3.

Проверьте конфигурацию сети IPsec VPN маршрутизатора R3 с помощью команд **show crypto map** и **show crypto ipsec sa**.

Задача 2: Настройка сети Site-to-Site VPN на устройстве ASA с помощью ASDM

Шаг 1: Используя браузер на компьютере PC-B, установите сеанс связи ASDM с устройством ASA.

a. Установив сеанс с ASDM, используйте мастер **Site-to-Site VPN Wizard** для настройки параметров сети Ipsec site-to-site VPN на устройстве ASA.

b. Укажите IP-адрес (**10.2.2.1**) интерфейса S0/0/1 маршрутизатора R3 в поле Peer IP Address. Убедитесь, что в поле VPN Access Interface выбрано значение **outside**.

c. Укажите трафик, который необходимо защитить. Установите в поле Local Network значение **inside-network/24**, а в поле Remote Network – **172.16.3.0/24**.

d. Настройте общий ключ. Введите в поле Pre-shared Key значение **Site2SiteKEY1**.

e. Включите исключение NAT. Установите флажок **Exempt ASA side host/network from address translation** и убедитесь, что выбран интерфейс **inside**.

Шаг 2: Примените настройки IPsec к устройству ASA.

Нажмите **Finish**, чтобы применить конфигурацию сети типа site-to-site к устройству ASA.

Задача 3: Проверка соединения по сети Site-to-Site IPsec VPN между устройством ASA и маршрутизатором R3

Шаг 1: Отправьте запрос ping на интерфейс LAN маршрутизатора R3 с компьютера PC-B.

При этом должен быть осуществлен доступ к соединению по сети IPsec Site-to-site VPN между устройством ASA и маршрутизатором R3.

Шаг 2: Убедитесь, что сеанс сети IPsec Site-to-site VPN активен.

a. В ASDM на компьютере PC-B выберите меню **Monitoring**>**VPN**. В середине экрана должен отображаться IP-адрес (10.2.2.1) профиля соединения. Нажмите кнопку **Details** для просмотра подробных сведений о сеансе IKE и IPsec.

b. Введите команду **show crypto isakmp sa** и убедитесь, что ассоциация безопасности (SA) IKE активна.

c. Введите команду **tracert 192.168.1.3** на компьютере PC-C. Если туннель site-to-site VPN работает правильно, то вы увидите, что трафик не проходит через маршрутизатор R2 (10.2.2.2).

d. Введите команду **show crypto ipsec sa** на маршрутизаторе R3, чтобы увидеть количество пакетов, которые были инкапсулированы и декапсулированы. Убедитесь в отсутствии ошибок пакетов или ошибок отправки и приема.

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1700	Fast Ethernet 0 (F0)	Fast Ethernet 1 (F1)	Serial 0 (S0)	Serial 1 (S1)
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.