Packet Tracer. Усложненное задание на совокупное использование навыков

Топология

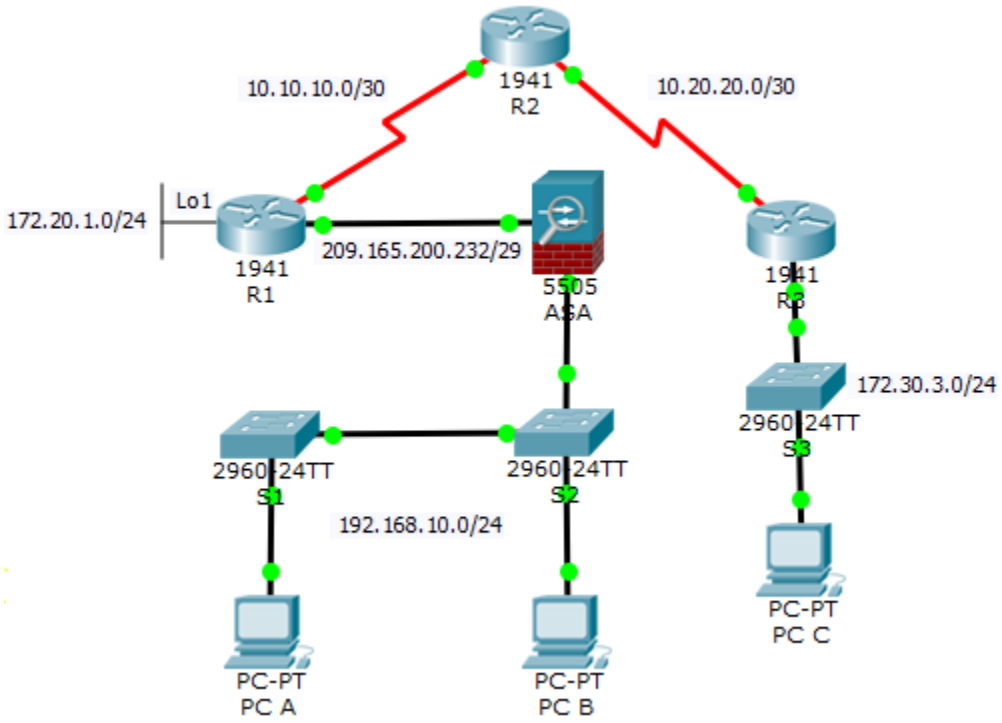

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	209.165.200.233	255.255.255.248	Н/П
	S0/0/0 (DCE)	10.10.10.1	255.255.255.252	Н/П
	Loopback 1	172.20.1.1	255.255.255.0	Н/П
R2	S0/0/0	10.10.10.2	255.255.255.252	Н/П
	S0/0/1 (DCE)	10.20.20.2	255.255.255.252	Н/П
R3	G0/1	172.30.3.1	255.255.255.0	Н/П
	S0/0/1	10.20.20.1	255.255.255.252	Н/П
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN 1	172.30.3.11	255.255.255.0	172.30.3.1
ASA	VLAN 1 (E0/1)	192.168.10.1	255.255.255.0	Н/П
	VLAN 2 (E0/0)	209.165.200.234	255.255.255.248	Н/П
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	172.30.3.3	255.255.255.0	172.30.3.1

Задачи

- Настройка базового уровня безопасности маршрутизатора
- Настройка базового уровня безопасности коммутатора
- Настройка локальной аутентификации AAA
- Настройка SSH
- Защита от атак методом подбора учетных данных
- Настройка сетей site-to-site IPsec VPN
- Настройка параметров межсетевого экрана и системы предотвращения вторжений (IPS)
- Настройка базовых параметров безопасности ASA и межсетевого экрана

Сценарий

Это итоговое задание охватывает многие навыки, которые вы приобрели в ходе данного курса. Для маршрутизаторов и коммутаторов предварительно настроены базовые параметры устройств, такие как IP-адресация и маршрутизация. С помощью интерфейса командной строки (CLI) вы настроите различные функции IOS, связанные с безопасностью, включая AAA, SSH и зональный межсетевой экран (ZPF), для защиты маршрутизаторов. Вы настроите сеть site-to-site VPN (VPN между двумя пунктами) между маршрутизаторами R1 и R3. Вы обеспечите безопасность коммутаторов в сети. Кроме того, вы также настроите функции межсетевого экрана на ASA.

Требования

Примечание. Будут настроены не все функции безопасности и не на всех устройствах, однако они будут присутствовать в производственной сети.

Настройка базового уровня безопасности маршрутизатора

- Настройте маршрутизатор R1 следующим образом.
  - Минимальная длина пароля составляет 10 символов.
  - Зашифруйте пароли, заданные в виде открытого текста.
  - Пароль для привилегированного режима – **ciscoenapa55**.
  - Пароль для линий консоли – **ciscoconpa55**, время ожидания – **15** минут, сообщения консоли не должны прерывать ввод команд.
  - Баннер с сообщением дня (MOTD) должен содержать слово **unauthorized**.
- Настройте маршрутизатор R2 следующим образом.
  - Пароль для привилегированного режима – **ciscoenapa55**.
  - Пароль для линий VTY – **ciscovtypa55**, время ожидания – **15** минут, требуются учетные данные для входа в систему.

Настройка базового уровня безопасности коммутатора

- Настройте коммутатор S1 следующим образом.
  - Зашифруйте пароли, заданные в виде открытого текста.
  - Пароль для привилегированного режима – **ciscoenapa55**.
  - Пароль для линий консоли – **ciscoconpa55**, время ожидания – **5** минут, сообщения консоли не должны прерывать ввод команд.
  - Пароль для линий VTY – **ciscovtypa55**, время ожидания – **5** минут, требуются учетные данные для входа в систему.
  - Баннер с сообщением дня (MOTD) должен содержать слово **unauthorized**.
- Настройте транкинг между коммутаторами S1 и S2 со следующими параметрами.
  - Установите режим **trunk** и назначьте VLAN **99** в качестве нативной (native) VLAN.
  - Отключите генерацию кадров DTP.
- Настройте для коммутатора S1 следующие параметры портов.
  - F0/6 должен разрешать только режим доступа, задайте **PortFast** и включите функцию BPDU Guard.
  - F0/6 использует базовый уровень безопасности порта по умолчанию с динамически получаемыми MAC-адресами, которые добавляются в текущую конфигурацию.
  - Все остальные порты должны быть отключены.

Примечание. Хотя проверяются не все порты, ваш инструктор при желании может захотеть убедиться, что все неиспользуемые порты отключены.

Настройка локальной аутентификации AAA

- Настройте маршрутизатор R1 следующим образом.
  - Создайте учетную запись локального пользователя **Admin01**, секретный пароль **Admin01pa55**, уровень привилегий **15**.
  - Включите сервисы AAA.
  - Разверните сервисы AAA, используя локальную базу данных в качестве первого варианта, а затем пароль **enable** в качестве резервного варианта.

Настройка SSH

- Настройте маршрутизатор R1 следующим образом.
  - Доменное имя – **ccnasecurity.com.**

- Ключ RSA должен содержать 1024 бита.
- Допускается только протокол SSH версии 2.
- На линиях VTY разрешается использовать только протокол SSH.

- Убедитесь, что компьютер PC-C может получить удаленный доступ к маршрутизатору R1 (209.165.200.233) по протоколу SSH.

Защита от атак методом подбора учетных данных

- Настройте маршрутизатор R1 следующим образом.
  - Если пользователю не удается войти в систему дважды за временной промежуток в 30 секунд, необходимо отключить возможность входа на одну минуту.
  - Регистрируйте в журнале все неудачные попытки входа в систему.

Настройка сетей site-to-site IPsec VPN

Примечание. Некоторые конфигурации VPN не оцениваются. Однако у вас должна быть возможность проверить подключение по туннелю VPN IPsec.

- Активируйте лицензию Security Technology Package на маршрутизаторе R1.
  - Сохраните текущую конфигурацию перед перезагрузкой.
- Настройте маршрутизатор R1 следующим образом.
  - Создайте список доступа для выявления «интересного» трафика на маршрутизаторе R1.
  - Настройте список ACL **101** для разрешения трафика из сети R1 Lo1 в локальную сеть R3 G0/1.
- Настройте свойства **crypto isakmp policy 10** для фазы 1 на маршрутизаторе R1 и общий ключ шифрования **ciscovpnpa55**. Используйте следующие параметры.
  - Метод распределения ключей: **ISAKMP**
  - Шифрование: **aes 256**
  - Хеш: **sha**
  - Метод аутентификации: **pre-shared**
  - Обмен ключами: **DH Group 5**
  - Время жизни IKE SA: **3600**
  - Ключ ISAKMP: **ciscovpnpa55**
- Создайте набор преобразований **VPN-SET** для использования **esp-aes 256** и **esp-sha-hmac**. Затем создайте криптографическую карту **CMAP**, связывающую друг с другом все параметры фазы 2. Используйте порядковый номер **10** и определите его как карту **ipsec-isakmp**. Используйте следующие параметры.
  - Набор преобразований: **VPN-SET**
  - Шифрование преобразований: **esp-aes 256**
  - Аутентификация преобразований: **esp-sha-hmac**
  - Perfect Forward Secrecy (PFS): **group5**
  - Имя криптографической карты: **CMAP**
  - Установление SA: **ipsec-isakmp**
  - Привяжите криптографическую карту (**CMAP**) к исходящему интерфейсу.
- Убедитесь, что лицензия Security Technology Package активирована. Повторите базовые настройки для сети site-to-site VPN на маршрутизаторе R3 так, чтобы они точно соответствовали всем параметрам конфигурации маршрутизатора R1.
- Отправьте команду ping на интерфейс Lo1 (172.20.1.1) маршрутизатора R1 с компьютера PC-C. На маршрутизаторе R3 используйте команду **show crypto ipsec sa**, чтобы убедиться, что число пакетов больше 0, что свидетельствует о работоспособности VPN-туннеля IPsec.

Настройка параметров межсетевого экрана и системы предотвращения вторжений (IPS)

- Настройте ZPF на маршрутизаторе R3 в соответствии со следующими требованиями.
  - Создайте зоны с именами **IN-ZONE** и **OUT-ZONE**.
  - Создайте список ACL с номером **110**, определяющий внутренний трафик и разрешающий все IP-протоколы из исходной сети 172.30.3.0/24 с любым (**any**) местом назначения.
- Создайте карту классов с именем **INTERNAL-CLASS-MAP**, которая использует параметр **match-all** и список ACL **110.**
- Создайте карту политик с именем **IN-2-OUT-PMAP**, которая использует карту классов **INTERNAL-CLASS-MAP** для инспектирования (**inspect**) всего соответствующего трафика.
- Создайте пару зон с именем **IN-2-OUT-ZPAIR**, которая определяет **IN-ZONE** как зону источника и **OUT-ZONE** как зону назначения.
  - Укажите, что карта политик **IN-2-OUT-PMAP** должна использоваться для инспектирования (**inspect**) трафика между двумя зонами.
  - Назначьте G0/1 в качестве члена **IN-ZONE**, а S0/0/1 – в качестве члена **OUT-ZONE**.
- Настройте систему защиты от вторжений (IPS) на маршрутизаторе R3, используя следующие требования.

Примечание. В Packet Tracer файлы сигнатур уже импортированы на маршрутизаторы. Это XML-файлы по умолчанию, хранящиеся во флеш-памяти. По этой причине не нужно настраивать открытый криптографический ключ и вручную импортировать файлы сигнатур.

  - Создайте каталог во флеш-памяти с именем **ipsdir** и задайте его в качестве расположения для хранения сигнатур IPS.
  - Создайте правило IPS с именем **IPS-RULE**.
  - Выведите из использования категорию сигнатур **all** с помощью команды **retired true** (все сигнатуры в выпуске сигнатур).
  - Верните в использование категорию **IOS_IPS Basic** с помощью команды **retired false**.
  - Примените правило inbound на интерфейсе S0/0/1.

Настройка базовых параметров безопасности ASA и межсетевого экрана

- Настройте следующие параметры для интерфейсов VLAN.
  - Для интерфейса VLAN 1 настройте использование адресов **192.168.10.1/24.**
  - Для интерфейса VLAN 2 удалите параметр DHCP по умолчанию и настройте использование адресов **209.165.200.234/29**.
- Настройте имя хоста, доменное имя, пароль привилегированного доступа и пароль консоли с помощью следующих параметров.
  - Имя хоста ASA – **CCNAS-ASA**.
  - Доменное имя – **ccnasecurity.com.**
  - Пароль привилегированного доступа – **ciscoenapa55**.
- Создайте пользователя и настройте AAA на использование локальной базы данных для удаленной аутентификации.
  - Настройте учетную запись локального пользователя с именем **admin** и паролем **adminpa55**. Не используйте атрибут **encrypted**.
  - Настройте AAA на использование локальной базы данных ASA для аутентификации пользователя по протоколу SSH.
  - Разрешите SSH-доступ с внешнего хоста **172.30.3.3** со временем ожидания **10** минут.
- Настройте ASA в качестве DHCP-сервера с помощью следующих параметров.
  - Назначьте IP-адреса внутренним клиентам DHCP в диапазоне от 192.168.10.5 до 192.168.10.30.
  - Разрешите для DHCP ожидание запросов клиента DHCP.

- Настройте статическую маршрутизацию и NAT.
    - Создайте статический маршрут по умолчанию по IP-адресу маршрутизатора на следующем транзитном участке (R1).
    - Создайте сетевой объект с именем **inside-net** и назначьте ему атрибуты с помощью команд **subnet** и **nat**.
    - Создайте динамическое преобразование NAT для внешнего интерфейса.
- Измените модульную систему политик Cisco Modular Policy Framework (MPF) на ASA с помощью следующих параметров.
    - Установите для параметра **class-map inspection_default** значение **match default-inspection-traffic** и перейдите в режим глобальной настройки.
    - Настройте список **policy-map** с **global_policy**. Введите **class inspection_default** и введите команду **inspect icmp**. Затем перейдите в режим глобальной настройки.
    - Настройте политику MPF **service-policy**, чтобы политика **global_policy** применялась глобально.

