МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПЕРИМЕТРА ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебно-методическое пособие

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПЕРИМЕТРА ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебно-методическое пособие
по выполнению лабораторных работ по дисциплине
«Безопасность компьютерных сетей»
для студентов дневного и заочного отделения по направлению
09.04.02 – Информационные системы и технологии,
09.04.03 – Прикладная информатика

Севастополь
СевГУ
2024

УДК 004.732:004.056.5(076.5)
ББК 32.973.202я73
М545

Р е ц е н з е н т ы :
К. В. Кротов - д-р техн. наук, доцент кафедры ИС
Т. В. Волкова - канд. техн. наук, доцент кафедры ИТиКС

Ответственный за выпуск:
И. П. Шумейко - заведующий кафедрой «Информационные системы»,
канд. физ.-мат. наук, доцент

Составитель: В. С. Чернега

М545 Методы и средства защиты периметра локальных компьютерных сетей : учебно-методическое пособие по выполнению лабораторных работ по дисциплине «Безопасность компьютерных сетей» для студентов дневного и заочного отделения по направлению 09.04.02 – Информационные системы и технологи, 09.04.03 – Прикладная информатика / Севастопольский государственный университет ; сост. В. С. Чернега. – Севастополь : СевГУ, 2024. – 38 с. – Текст : электронный.

Учебно-методическое пособие предназначено для углубления теоретических знаний и проведения лабораторных работ по дисциплине «Безопасность компьютерных сетей». Целью методических указаний является помощь студентам в изучении методов защиты периметра компьютерных сетей на основе использования аппаратных межсетевых защитных экранов. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

УДК 004.732:004.056.5(076.5)
ББК 32.973.202я73

Рассмотрено и утверждено на методическом семинаре и заседании кафедры «Информационные системы», протокол № 8 от 16 апреля 2024 г.

Рассмотрено и рекомендовано к изданию на заседании Учёного Совета Института информационных технологий, протокол № 5 от 18 апреля 2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для эффективного функционирования предприятия или организации требуется подключение корпоративной локальной компьютерной сети к глобальной сети Интернет. За доступ к ресурсам глобальной сети и предоставление связанные с этим услуг отвечает организация, называемая Интернет-сервис провайдер **ISP** (Internet Service Provider). Точки стыка локальной сети с каналом глобальной называется периметром сети. Защита периметра является частью комплексной защиты в рамках обеспечения защищенности специализированных внутренних сетей предприятий и организаций. Она позволяет предотвратить атаки на ИТ-ресурсы и реализовать безопасный доступ сотрудникам компаний во внешние сети, а авторизованным удаленным пользователям — к корпоративным ресурсам.

Защита периметра считается обязательным элементом системы обеспечения информационной безопасности корпоративной сети и включает в себя шлюзы безопасности, средства межсетевого экранирования (Firewall), организацию виртуальных частных сетей VPN (Virtual Private Network), системы обнаружения и предотвращения вторжений IDS/IPS (Intrusion Detection System/ Intrusion Prevention System).

В настоящем пособии рассматриваются лишь вопросы защиты ресурсов корпоративных локальных компьютерных сетей на основе программно-аппаратных межсетевых защитных экранов (файерволлов).

В процессе изучения раздела дисциплины «Безопасность компьютерных сетей», относящегося защите локальных сетей с помощью файерволлов студенты-магистранты должны изучить уязвимости и угрозы безопасности, ознакомиться с принципами построения и реализации политики безопасности, способами защиты ресурсов компьютерных сетей на основе списков доступа.

Целью настоящего учебно-методического пособия является углубление теоретических знаний в области безопасности компьютерных сетей, а также приобретение практических навыков исследования функционирования локальных проводных и беспроводных компьютерных сетей, выявления слабых мест, разработка сценариев конфигурирования межсетевых защитных экранов для повышения безопасности корпоративных локальных компьютерных сетей.

Выполнение лабораторных работ осуществляется в виртуальной среде эмулирования компьютерных сетей Cisco Packet Tracer (CPT). Интерфейсы конфигурация сетевого оборудования в среде CPT практически не отличаются от интерфейсов конфигурации реального сетевого оборудования.

Выполнение лабораторных работ по дисциплине «Безопасность компьютерных сетей» предполагает знание дисциплины «Инфокоммуникационные системы и сети», которая входит в учебный план подготовки бакалавров по направлениям «Информационные системы и технологии» и «Прикладная информатика». Предполагается, что студенты знакомы с системой Cisco Packet Tracer.

1. ФУНКЦИИ И ХАРАКТЕРИСТИКА МЕЖСЕТЕВЫХ ЗАЩИТНЫХ ЭКРАНОВ

1.1. Функции защитного экрана и схема включения в сети

Одним из способов защиты корпоративных локальных компьютерных сетей от несанкционированного доступа к ее ресурсам является использование межсетевых защитных экранов (они же брандмауэры или файрволлы). Межсетевой защитный экран (МЗЭ) является пограничным устройством, расположенным между корпоративной локальной сетью и публичной сетью Интернет.

В корпоративных компьютерных сетях общедоступные ресурсы обычно отделяют от корпоративных и располагают их на выделенных устройствах (серверах), размещенных в отдельной зоне, называемой демилитаризованной зоной (DMZ). Общедоступные ресурсы (почтовые, DNS и Веб-серверы) должны быть доступны также из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

МЗЭ — это система сетевой безопасности, которая контролирует входящие и исходящие пакеты путем анализа IP-адресов, номеров портов, используемых протоколов и других признаков, запрещая прохождение пакетов в соответствии с политикой безопасности, принятой для конкретной сети. Файрволлы могут быть реализованы, программным и программно-аппаратным способом. Программный МЗЭ функционирует на основе маршрутизатора, а программно-аппаратный выполняется в виде отдельного устройства. Аппаратную реализацию МЗЭ в корпорации Cisco названо адаптивным устройством безопасности, сокращенно **ASA** (*Adaptive Security Appliance*).

Поскольку файрволлы являются сетевыми устройствами, устанавливаемыми на границе между внутренней и внешней сетями, и выполняют функцию сетевого шлюза, то в конструктивном плане они должны иметь как минимум три порта. К одному из этих портов подключается внешняя сеть (Интернет), превращая его во внешний WAN-порт. Ко второму порту подключается локальная сеть организации, и этот порт становится внутренним LAN-портом. К третьему, DMZ-порту, подсоединяются общедоступные серверы. Схема такой сети изображена на рисунке 1.1.

К основным функциям аппаратных МЗЭ относятся следующие:

1) фильтрация входящих или исходящих пакетов на основе правил, определяемых политикой безопасности сети;

2) поддержка службы аутентификации, авторизации и учета **AAA** (*Authentication Authorization and Accounting*);

3) поддержка маршрутизации (статической маршрутизации, маршрутизации по умолчанию, а также протоколов динамической маршрутизации);

4) реализация технологии виртуальных частных сетей **VPN** (*Virtual Private Network*)**,** позволяющей обеспечить одно или несколько защищенных (шифруемых) сетевых соединений поверх другой сети;

5) реализация некоторых других функций (обеспечение отказоустойчивости, балансировка нагрузки, расширенная защита от вредоносных программ и проч.).

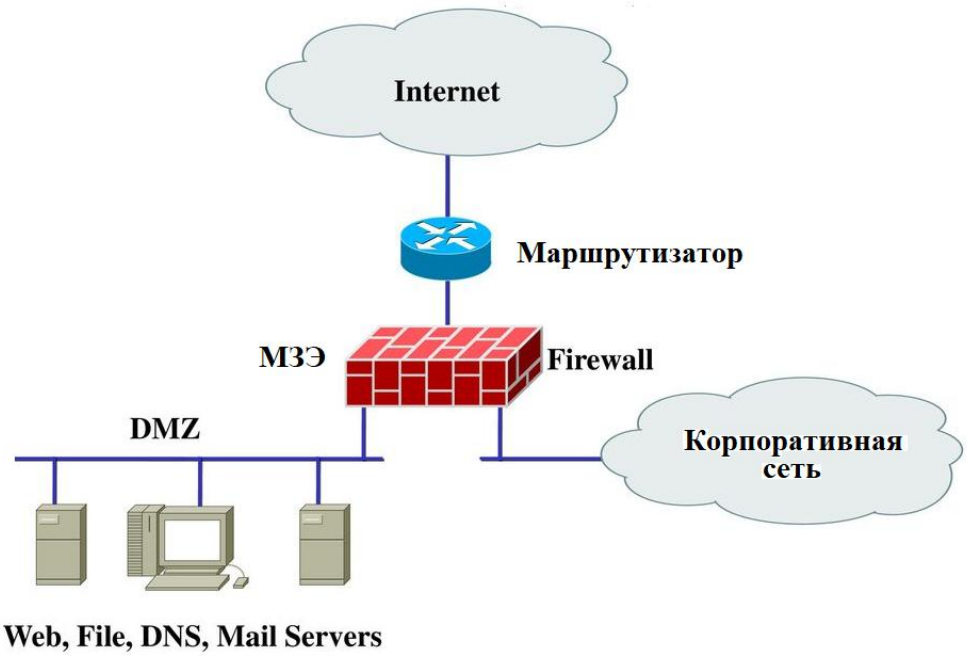

Рисунок 1.1 – Схема корпоративной сети с DMZ и подключением к Интернет

Фильтрация пакетов в ASA может выполняться в упрощенном виде, при котором процесс фильтрации входящего или исходящего пакета осуществляется на основе правил, определенных в списке доступа ACL, который был применен к устройству.

В более сложном варианте осуществляется ф**ильтрация с учетом состояния.** В этом случае ASA, по умолчанию, выполняет отслеживание состояния пакета, проверяя подлежит ли передача пакета с более высокого уровня безопасности на более низкий уровень или наоборот. Если трафик инициируется устройствами с более высокими уровнями безопасности для устройств с более низкими уровнями безопасности (в качестве получателя), а трафик ответа TCP и UDP будет разрешен, то возможна передача по протоколу telnet с устройства с низким уровнем безопасности на устройство более высокого уровня безопасности. Это связано с тем, что поддерживается база данных с отслеживанием состояния (в которой сохраняются записи об источнике и устройстве назначения, такие как IP-адрес, номера портов), поскольку проверка с отслеживанием состояния включена по умолчанию.

1.2. Краткая характеристика аппаратных защитных экранов

К одним из самых популярных межсетевых защитных экранов относятся устройства адаптивной безопасности Cisco ASA серии 5500. Это устройства безо-

пасности, сочетающие в себе классические функции файрволла с возможностями VPN, функции предотвращения вторжений и антивирусов. Они способны обеспечивать защиту от угроз до того, как атаки распространятся на сети. Серия ASA 5500 состоит из ряда устройств: ASA 5505, 5506, 5510 … 5585, ASA 5500-X различающихся набором защитных функций, быстродействием, объемом памяти, возможностью масштабирования.

Несмотря на то, что эти устройства не рекомендуется в настоящее время использовать в Российской Федерации, изучение их возможностей и особенностей конфигурации продолжает осуществляться в учебном процессе. Это связано с тем, что модели устройств ASA 5505 и 5506 представлены в системе симуляции компьютерных Cisco Packet Tracer, а система команд и способы конфигурации совместимы с отечественными моделями защитных экранов, в частности с устройствами ESR-20 … 200, выпускаемой компанией Eltex, а также с другими типами отечественных программно-аппаратных файрволлов.

1.3. Основные технические характеристики МЭ ASA 5505 и 5506

Межсетевой экран Cisco ASA5505 представляет собой программно управляемое аппаратное устройство настольного типа и является полнофункциональным устройством безопасности для небольших предприятий и их филиалов. В устройстве реализованы высокопроизводительные сервисы межсетевого экрана, функциональность SSL и IPsec VPN, шифрование Data Encryption Standard (DES), а также различные сетевые сервисы. Интегрированный графический менеджер Cisco Adaptive Security Device Manager (ASDM) позволяет быстро развернуть и легко управлять устройством Cisco ASA 5505, что сокращает эксплуатационные затраты компаний. В Cisco ASA 5505 встроен 8-портовый коммутатор 10/100 Fast Ethernet с динамической группировкой портов для создания до трех отдельных сетей VLAN, передающих трафик домашних, рабочих сетей, а также Интернет-трафик. В этом случае повышается эффективность сегментации сети и ее безопасность. Пропускная способность межсетевого экрана до 150 Мбит/с.

В Cisco ASA 5505 имеется два порта Power over Ethernet (PoE), что упрощает подключение IP-телефонов с возможностями VoIP (без участия оператора), а также развертывание внешних точек беспроводного доступа для расширения мобильных возможностей сети.

Cisco ASA 5505 входит в состав оборудования студенческой версии симулятора Packet Tracer Student.

Межсетевой экран Cisco ASA 5506 является дальнейшим развитием линейки аппаратных устройств семейства ASA 5500. Устройство обеспечивает высокую степень защиты от сетевых угроз в крупных центрах обработки данных благодаря следующим возможностям: глубокой проверке сети, анализу отдельных потоков, безопасности подключений за счет оценки защищенности оконечных устройств, а также поддержке передачи голосовых и видеоданных через VPN. Устройство обеспечивает расширенную поддержку интеллектуальных информационных сетей

благодаря улучшенной сетевой интеграции, отказоустойчивости и масштабируемости.

ASA 5506 оснащен восьмью сетевыми интерфейсами Gigabit Ethernet RJ-45 (8P8C). Пропускная способность файрволла составляет 250 Мбит/с, а пропускная способность IPSec VPN равна 100 Mbps

Cisco ASA 5506 входит в состав оборудования симулятора Packet Tracer версии 8.1 и старше.

1.4. Основные технические характеристики отечественных МЭ

Отечественной промышленностью разработан и выпускается целый ряд межсетевых защитных экранов [https://habr.com/ru/articles/726662/]. Межсетевые защитные экраны **Diamond** от российского производителя ООО «ТСС». Компания разрабатывает МЭ семейства Diamond с целью комплексного обеспечения информационной безопасности. Данные МЭ позволяют решать задачи шифрования высокоскоростных каналов связи, межсетевого экранирования, а также обнаружения и предотвращения вторжений.

МЭ Diamond имеют аппаратное исполнение, могут быть интегрированы в любую сетевую инфраструктуру предприятия. Аппаратные межсетевые экраны «Diamond VPN/FW» разбиты на серии с похожими техническими характеристиками в зависимости от архитектуры процессора и скорости выполнения функций средств защиты.

К основным функциям многофункционального комплекса сетевой защиты Diamond VPN/FW относятся:

- криптографическая защита каналов передачи данных (L2overVPN/L3overVPN) с применением отечественных криптографических алгоритмов;
- межсетевое экранирование в режиме коммутатора (прозрачный режим) и в режиме маршрутизатора;
- система обнаружения и предотвращения вторжений (СОВ/СПВ).

Скорость передачи данных зависит от модели МЭ и занимает диапазон от 1,8 Гбит/с (Diamond VPN/FW-4101) до 35 Гбит/с (Diamond VPN/FW-7151).

Следующим вариантом межсетевого экрана является программно-аппаратный комплекс защиты компьютерных сетей компании «Код безопасности». Аппаратные межсетевые экраны этой компании представлены двумя линейками — «**Континент 3**» и «**Континент 4**». В каждой линейке идет подразделение на МЭ базовой производительности, средней производительности, высокой производительности. В линейке «Континент 3» реализован МЭ для крупных центров обработки данных, а в «Континент 4» используются модели с виртуальным исполнением. В устройствах «Континент-3» реализованы следующие функции:

- криптографическая защита трафика на канальном уровне (L2 VPN-сеть);
- защита трафика на сетевом уровне (L3 VPN-сеть);
- маршрутизация трафика;

- режим работы МЗЭ;
- высокая отказоустойчивость серверов управления;
- анализ сетевого трафика, обнаружение и предотвращение атак;
- мониторинг всех компонентов устройства;
- защита удаленного подключения.

МЗЭ Континент 3 рекомендуются для защиты государственных информационных систем, финансовых систем, критической информационной инфраструктуры, защиты информации в здравоохранении, обеспечения безопасности персональных данных.

«Континент 4» представляет собой целый комплекс защитных средств в одном устройстве: межсетевой экран, криптошлюз, криптокоммутатор, детектор атак, центр управления сетью, причем всеми этими компонентами можно управлять из консоли.

Скорость передачи данных зависит от модели МЗЭ и занимает диапазон от 1,2 Гбит/с до 40 Гбит/с.

Одной из распространенных отечественных файрволлов является линейка межсетевых защитных экранов предприятия Eltex, в состав которой входят устройства **ESR-100/200/1000 FSTEC A4.** Типовые функции, выполняемые с помощью межсетевых экранов этого типа, следующие:

- построение защищенного периметра сети (NAT, Firewall);
- разграничение доступа пользователей;
- организация защищенных сетевых туннелей между филиалами компаний (IP over GRE, Ethernet over GRE, IPIP);
- построение распределенных частных сетей VLAN, объединение удаленных офисов компаний в единую сеть;
- фильтрация сетевых данных по различным критериям (включая фильтрацию по приложениям);
- взаимодействие с существующей сетевой инфраструктурой заказчика, использование для этого определяемых отраслевыми стандартами типов каналов связи: выделенные и коммутируемые линии, потоки E1;
- маршрутизация данных (RIP2, OSPF, BGP);
- балансировка нагрузки;
- резервирование WAN-соединений.

Скорость передачи данных в ESR-100 10/100/1000 МГбит/с, а в ESR-1000 – 1/10 Гбит/с.

2. Настройка межсетевого защитного экрана Cisco ASA 5505

2.1. Интерфейсы и уровни безопасности ASA-5505

В настоящей работе предстоит исследовать сеть с межсетевым защитным экраном типа Cisco ASA 5505, который является аппаратным межсетевым экраном с инспектированием сессий с сохранением состояния (stateful inspection). От-

личие ASA 5505 от большинства старших моделей ряда ASA 5500 является то, что устройство имеет 8-портовый коммутатор второго уровня 10/100 номерами Et0/0-Et0/7. В связи с этим требуется создание нескольких виртуальных сетей с логическими интерфейсами сетевого уровня (L3). Чтобы получить интерфейсы L3 уровня, необходимо создать виртуальные интерфейсы VLAN, задать им IP-адреса и привязать их к физическим интерфейсам.

В ASA 5505 уже при его изготовлении создано три интерфейса безопасности: внешний (**outside**), внутренний (**inside**) и DMZ (**dmz**). По умолчанию, интерфейс Ethernet0/0 приписан к VLAN 2. Это внешний (outside) интерфейс, тот, который подключается к Интернету. Другие 7 интерфейсов (Ethernet0/1… 0/7) принадлежат по умолчанию VLAN 1 и предназначены для подключения устройств внутренней сети inside. ASA5505 предоставляет внешним пользователям ограниченный доступ к DMZ и блокирует им доступ к внутренним ресурсам. В то же время внутренние пользователи имеют доступ к DMZ и внешним ресурсам.

В ASA 5505 также установлен DHCP сервер, задан статический адрес внутренней сети 192.168.1.0/24. Внешний интерфейс с названием outside обычно уже включен и сам получает адрес по DHCP. В МЗЭ 5505 уже настроена трансляция адресов из устройств сети, подключенной к интерфейсу inside, в адрес интерфейса outside.

ASA может работать в двух режимах: **routed** (режим маршрутизатора, по умолчанию) и **transparent** (прозрачный межсетевой экран, когда ASA функционирует как мост с фильтрацией).

В режиме routed на каждом интерфейсе должны быть заданы ip адрес, маска, уровень безопасности (security-level) и имя интерфейса. В процессе настройки интерфейс надо принудительно включить (поднять), так как по умолчанию все интерфейсы находятся в состоянии «выключено администратором». А внутренний интерфейс с названием inside уже настроен на самый безопасный уровень и включен.

Процесс отнесения физических портов к определенной VLAN, присвоения им имени, задания IP адреса и уровня безопасности, реализуется следующей группой команд, записываемых в ASA5505 с интерфейса командной строки CLI.

```
ciscoasa(config)#interface Ethernet0/2
ciscoasa(config)#switchport access vlan 3
ciscoasa(config)#interface vlan 3
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#ip address 192.168.2.1 255.255.255.0
ciscoasa(config-if)#security-level 80
ciscoasa(config-if)#no shutdown
```

Параметр «уровень безопасности» (security level) – это число от 0 до 100, которое позволяет сравнить 2 интерфейса и определить, кто из них более «безопасен». Параметр используется качественно, а не количественно, т.е. важно только

отношение «больше-меньше». По умолчанию трафик, идущий «наружу», т.е. с интерфейса с большим уровнем безопасности на интерфейс с меньшим уровнем безопасности, пропускается, сессия запоминается и обратно пропускаются только ответы по этим сессиям. Трафик же, идущий «внутрь», по умолчанию запрещен.

Межсетевое экранирование создается между логическими interface vlan. Поэтому, как правило, уровень безопасности интерфейсов подбирается таким образом, чтобы максимально соответствовать логической топологии сети. Сама топология представляет из себя зоны безопасности и правила взаимодействия между ними. Классической схемой считается присвоение разным интерфейсам разных уровней безопасности. Никто не запрещает сделать уровень безопасности на разных интерфейсах одинаковым, однако по умолчанию обмен трафиком между такими интерфейсами запрещен. Такой трафик можно сознательно разрешить, дав команду

same-security-traffic permit inter-interface

В этом случае следует иметь в виду, что между интерфейсами с одинаковым уровнем безопасности не возникает межсетевого экранирования, а только маршрутизация. Поэтому такой подход применяется для интерфейсов, относящихся к одной и той же логической зоне безопасности. (например, 2 локальные сети пользователей, объединяемые при помощи ASA).

При настройках сети целесообразно использовать параметр «имя интерфейса» (**nameif**) вместо его номера. Это позволяет в дальнейшем использовать в настройках не физическое наименование интерфейса, а его имя, которое является более информативным (**inside, outside, dmz, partner** и т.д.). При конфигурации интерфейса можно набрать начало его названия и табулятором (нажатием кнопки TAB) продолжить его до конца, если набранное начало однозначно идентифицирует интерфейс.

2.2. Маршрутизация в межсетевом защитном экране

Как у любого маршрутизатора сети (ASA тоже им является, т.к. использует таблицу маршрутизации для передачи пакетов), пакеты с интерфейсов автоматически отмечаются в таблице маршрутизации с пометкой «Присоединенные» (connected) при условии, что сам интерфейс находится во включенном состоянии «up». Те сети, которые ASA сама не знает, нужно описать. Это можно сделать вручную, используя команду

ciscoasa(config#route {interface} {network} {mask} {next-hop} [{administrative distance}] [track {#}]

Указывается тот интерфейс, за которым надо искать next-hop, т.к. ASA сама не делает такого поиска (в отличие от обычного маршрутизатора cisco). Следует иметь в виду, что в таблицу маршрутизации попадает только один маршрут в сеть назначения, в отличие от классическим маршрутизаторов, где может использо-

ваться до 16 параллельных путей. Маршрут по умолчанию задается таким же образом.

ciscoasa(config)# route {interface} 0.0.0.0 0.0.0.0 {next-hop}

Например,

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 200.150.100.1

Если ASA не имеет в таблице маршрутизации записи о сети назначения пакета, то пакет отбрасывается.

Динамическая маршрутизация на ASA возможна по протоколам RIPv1,2, OSPF, EIGRP. Настройка этих протоколов на ASA очень похожа на настройку маршрутизаторов cisco.

2.3. Удаленное управление межсетевым защитным экраном

ASA, как и большинство устройств cisco, предоставляет несколько способов удаленного управления. Самое простое и небезопасное – по протоколу telnet. Чтобы предоставить доступ на ASA по telnet необходимо явно указать, с каких хостов и сетей и на каком интерфейсе разрешен доступ, а также необходимо задать пароль на telnet. командой passwd:

ciscoasa(config)#telnet 192.168.1.128 255.255.255.128 inside

ciscoasa(config)#telnet 192.168.1.254 255.255.255.255 inside passwd {пароль}

В дальнейших примерах конфигурации, с целью сокращения записи, имя межсетевого экрана с режимом конфигурации (**ciscoasa(config)#)** не указывается.

В целях безопасности работа по удаленной конфигурации следует использовать протокол **SSH**. Однако, для обеспечения доступа по ssh кроме явного указания того, с каких хостов можно заходить для управления устройством, необходимо также задать RSA ключи, необходимые для шифрования данных о пользователе. По умолчанию в ASA 5505 для подключения по ssh используется пользователь с именем **pix** и пароль, задаваемый командой passwd (пароль).

```
! Задаем имя домена
domain name {имя}
!
! имя хоста
hostname {имя}
!
! После этого можно сгенерировать ключи
crypto key generate rsa
!
```

```
! Разрешаем ssh
ssh 192.168.1.128 255.255.255.128 inside
ssh 1.2.3.4 255.255.255.255 outside
passwd {пароль}
```

Как правило, на ASA начиная с версии 7.2 имя домена уже задано (domain.invalid) и ключи по умолчанию (дефолтные) сгенерированы, однако как минимум это надо проверить командой

show crypto key mypubkey rsa

Наличие хотя бы каких-то ключей RSA уже позволяет работать по ssh. Но можно дополнительно создать и ключевые пары, не заданные по умолчанию. Для этого надо указать явно имя ключевой пары

crypto key generate rsa label {имя пары}

Чтобы удалить ключевую пару (или все пары) используется команда

crypto key zeroize rsa [label {имя пары}]

ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5

После любых действий с ключевыми парами (создание, удаление) следует обязательно сохранить изменения. Для этого можно использовать стандартные команды cisco

ciscoasa(config)#copy running-config startup-config

ciscoasa(config)#write memory

или короткий вариант последней команды **wr**

2.4. Настройка трансляции адресов в ASA

Для доступа из локальной сети в Интернет необходимо, чтобы частные адреса локальной корпоративной сети были транслированы в публичный адрес. При настройке ASA возможно установить статическую или динамическую трансляцию адресов (**NAT).** Статическая трансляция обычно осуществляется один к одному, т.е. внутренний IP-адрес локальной сети транслируется в IP-адрес публичной сети. Причем, трансляция может осуществляться в обе стороны.

В современных версиях Cisco ASA есть 2 способа реализации статической адресации сетевых адресов (**Static NAT**):

1) через объекты (**object NAT**);
2) ручная настройка NAT (**manual NAT**).

Эти способы отличаются по логике настройки и синтаксису команд, но оба приводят к одному и тому же результату. В первом способе (object NAT) строки, описывающие правило трансляции адресов, привязываются к конкретному объекту (**имя + ip адрес**). Во втором способе (**manual NAT**) в отдельной строке с помощью все тех же объектов указываются адреса оригинального пакета и преобразованного (source и destination).

Настройка трансляции адресов различается для разных версий прошивки устройств. Версию прошивки можно узнать при вводе команды **show ver** или **sh running-config.**

Для модели ASA 5505, используемом в студенческой версии Packet Tracer 6.2, а также в системах симуляции старших версий

ciscoasa#sh ver
Cisco Adaptive Security Appliance Software Version 8.4(2).

Для версии 8.3.X и выше применяется настройка маршрутизации Cisco ASA через объекты (**object NAT**). При этом требуется с**оздать object network и разрешить трансляцию адресов.** Это реализуется следующим образом.

```
ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
```

Наиболее часто Static NAT используется для трансляции частного адреса внутреннего сервера в публичный адрес. Фрагмент сценария статической трансляции внутреннего адреса сервера в публичный имеет вид:

```
object network inside_server_real host 192.168.253.10
nat (inside,outside) static 62.105.149.237
```

Или, то же самое через object network:

```
object network inside_server_global
host 62.105.149.237
object network inside_server_real
host 192.168.253.10
nat (inside,outside) static inside_server_global
```

Динамическая NAT работает только наружу, т.е. трафик может быть инициирован только изнутри локальной сети наружу в публичную сеть, при этом множество внутренних адресов транслируются только на один внешний.

В следующем примере трансляция будет вестись на адрес, который установлен (висит) на интерфейсе outside

object network inside_lan_1
subnet 192.168.2.0 255.255.255.0
nat (inside,outside) dynamic interface

Вместо слова **interface** можно указывать конкретный адрес, отличный от адреса самого интерфейса **outside**,

В этом варианте трансляция будет вестись на определённый адрес.

object network inside_lan_1
subnet 192.168.2.0 255.255.255.0
nat (inside,outside) dynamic 62.105.149.238

Как видно из этих примеров, NAT привязывается к объектам сети, или внутреннему хосту.

В ASA может быть реализован широко используемый метод настройки с использованием веб-браузера. Этот метод называется ASDM (Adaptive Security Device Manager). Для доступа используется безопасный протокол https. Обеспечение доступа настраивается очень похоже на настройку ssh: необходимо выработать или убедиться в наличии установленных по умолчанию RSA ключей и указать, откуда можно подключаться.

domain name {имя}
hostname {имя}
crypto key generate rsa

! Включаем сам https сервер, по умолчанию он зачастую уже включен. При включении

! генерирует самоподписанный сертификат.
http server enable
! Разрешаем https
http 192.168.1.128 255.255.255.128 inside
http 1.2.3.4 255.255.255.255 outside

Если больше ничего не настраивать, то доступ будет обеспечен без указания пользователя. Если же был указан пароль на привилегированный режим командой

enable password {пароль} ,

то при подключении надо в качестве пароля указывать именно его, не указывая пользователя.

При работе с конкретным сетевым экраном надо проверить, что во флеш-памяти ASA находится файл ASDM, соответствующий используемой ОС.

dir flash:

show flash

Доступ по ASDM возможен только от имени пользователя с уровнем привилегий 15 (максимальный, означает, что пользователю можно все настраивать).

Следует иметь в виду, что правила трансляции адресов не открывают доступ к тем или иным ресурсам сами собой. Для этой цели необходимо также создать списки доступа (**access lists**) и привязать их к соответствующим интерфейсам.

3. Лабораторная работа 1

ИССЛЕДОВАНИЕ НАЧАЛЬНОЙ КОНФИГУРАЦИИ ЗАЩИТНОГО ЭКРАНА ASA 5505 И ВОЗМОЖНОЙ ЕЕ ИЗМЕНЕНИЯ

3.1. Цель работы

Углубление и закрепление теоретических знаний в области безопасности локальных компьютерных сетей и исследование механизмов защиты периметра локальных компьютерных сетях (ЛКС) на основе аппаратного межсетевого защитного экрана. Формирование навыков моделирования компьютерных сетей и конфигурирования аппаратного сетевого защитного экрана для обеспечения защиты локальных сетей.

3.2. Описание лабораторной установки

В качестве лабораторной установки используется персональный компьютер с инсталлированной система моделирования компьютерных сетей Packet Tracer v.6.2, студенческая версия или старше. Исследованию подлежит корпоративная фрагмент компьютерной сети, топология которой изображена на рисунке 3.1. Локальная сеть филиала компании представлена рабочими станциями PC-0 и PC-1 и коммутатором Switch0, который подключен к сетевому экрану ASA0. В сети также может организована выделенная демилитаризованная зона DMZ, в которой расположен DMZ Server, подключенный к файрволлу ASA0 через коммутатор Switch1. Выход локальной сети соединен с публичной сетью путем подключения межсетевого экрана к маршрутизатору провайдера Router0. Необходимо так сконфигурировать сеть, чтобы обеспечить взаимодействие по протоколу TCP с удаленным WWW-сервером. ASA должен быть настроен для управления администратором сети филиала с PC-B1 так и удаленным администратором с компьютера Admin.

В ASA 5505 уже при его изготовлении создано **три интерфейса безопасности**: внешний (**outside**), внутренний (**inside**) и DMZ (**dmz**) с предустановленными уровнями безопасности внутренней и внешней сетей. По умолчанию, интерфейс Ethernet0/0 приписан к VLAN 2. Это внешний (outside) интерфейс, тот, который подключается к Интернету. Другие 7 интерфейсов (Ethernet0/1… 0/7) принадлежат по умолчанию VLAN 1 и предназначены для подключения устройств внутренней сети inside. ASA5505 предоставляет внешним пользователям ограниченный доступ к DMZ и блокирует им доступ к внутренним ресурсам. В то же время внутренние пользователи имеют доступ к DMZ и внешним ресурсам.

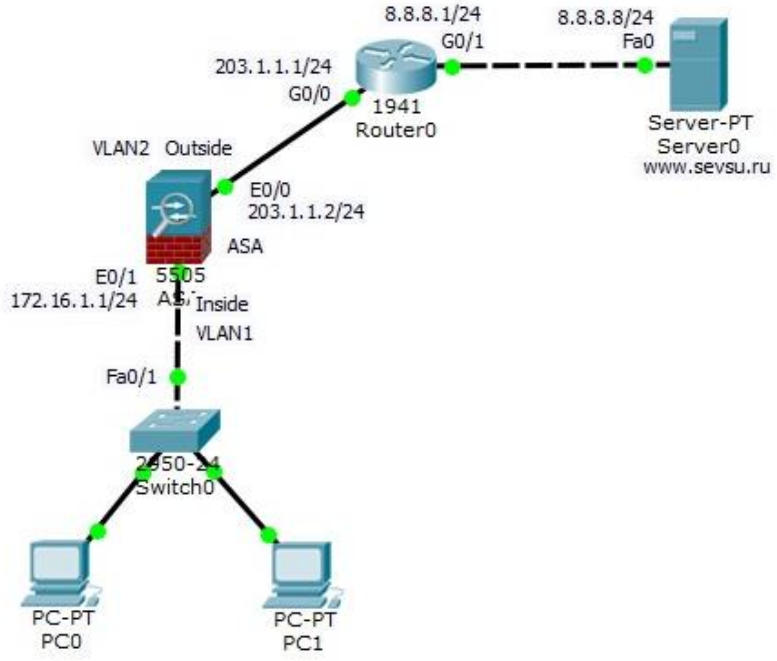

Рисунок 3.1 – Топология исследуемой локальной компьютерной сети

В ASA 5505 также установлен DHCP сервер, задан статический адрес внутренней сети 192.168.1.0/24. Внешний интерфейс с названием outside обычно уже включен и сам получает адрес по DHCP. В МЭЭ 5505 уже настроена трансляция адресов из устройств сети, подключенной к интерфейсу inside, в адрес интерфейса outside. Схема интерфейсов межсетевого экрана изображена на рисунке 3.2.

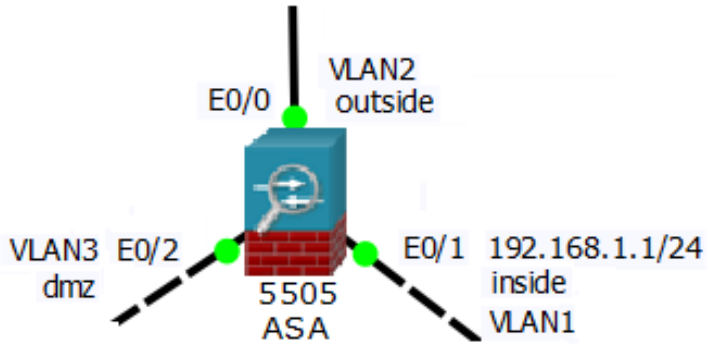

Рисунок 3.2 – Схема начальной настройки интерфейсов ASA 5505
в симуляторе Cisco Packet Tracer

3.3. Методические рекомендации по выполнению исследований

Команды настройки защитного экрана ASA 5505 и их последовательность зависят от версии операционной системы IOS. Поэтому перед конфигурацией сетевого экрана следует определить версию операционной системы и параметры конфигурации, установленные по умолчанию. Сделать это можно путем задания команды **show running-config** или **show ver**.

Для просмотра всех параметров начальной конфигурации ASA 5505 следует воспользоваться командой ciscoasa#sh running-config. Пароль для перехода в режим глобальной конфигурации пока пустой. Вид сообщения, выводимого при выполнении команды sh running-config приведено в Приложении А.

При анализе сообщения можно убедиться, что не зависимо от версии симулятора, начиная с версии Cisco Packet Tracer Student и выше, в симуляторе используется ASA **Version 8.4(2).**

Убрать конфигурацию, созданную по умолчанию, можно Clear all configuration. Восстановить конфигурацию по умолчанию можно командой

ciscoasa#write erase
Erase configuration in flash memory? [confirm]

Нажать Enter

Убрать конфигурацию, созданную по умолчанию, также можно следующим образом:

ciscoasa(config)#int VLAN 1
ciscoasa(config-if)#no IP address

При этом выдается предупреждение, что привязки, создаваемые программой DHCP daemon, на интерфейсе «inside» очищены, пул адресов удален.
WARNING: DHCPD bindings cleared on interface 'inside', address pool removed.

Установить новый адрес VLAN 1, указанный на схеме (рисунок 3.1), инициировать DHCP-сервер защитного экрана и задать новый пул адресов, соответствующий адресу VLAN 1 возможно следующим образом.

ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#dhcp address 172.16.1.5-172.16.1.35 inside
ciscoasa(config)#

Для проверки осуществления смены адресов достаточно установить курсор над защитным экраном и компьютерами (рисунок 3.3).

Обратите внимание, что DHCP сервер защитного экрана 5505 выдал компьютеру также и адрес шлюза по умолчанию (Gateway).

Для установки IP-адресов VLAN 1 и VLAN 2, согласно указанным на схеме исследуемой сети, можно воспользоваться следующим сценарием:

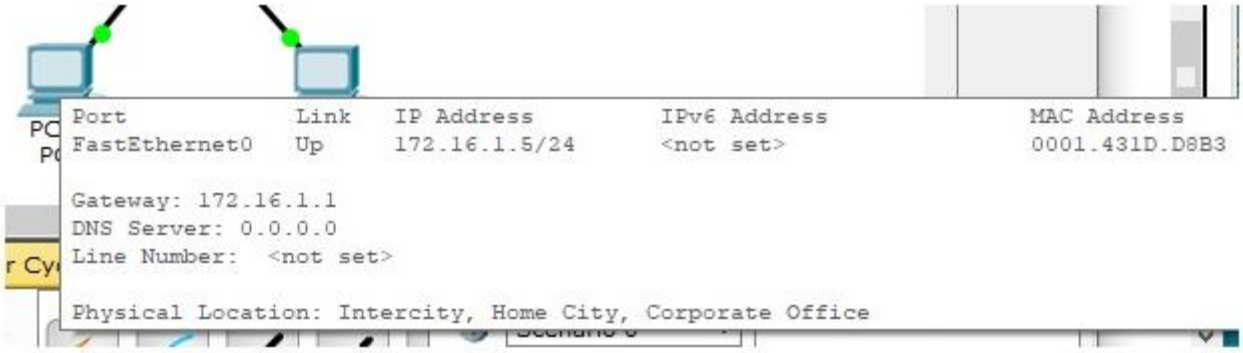

Рисунок 3.3 – Проверка IP-адреса на компьютере PC0

ciscoasa(config)#int vlan 1
ciscoasa(config-if)#ip address 172.16.1.1 255.255.255.0
ciscoasa(config-if)#no shutdown
ciscoasa(config-if)#

ciscoasa(config-if)#exit
ciscoasa(config)#int vlan 2
ciscoasa(config-if)#ip address 203.1.1.2 255.255.255.0
ciscoasa(config-if)#no sh

ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#

Чтобы связать интерфейсы Ethernet 0/0 и Ethernet 0/1 с VLAN 2 и VLAN 1 соответственно нужно выполнить следующие команды.

ciscoasa(config-if)#exit
ciscoasa(config)#int eth 0/0
ciscoasa(config-if)#switchport access vlan 2
ciscoasa(config-if)#exit
ciscoasa(config)#int eth 0/1
ciscoasa(config-if)#switchport access vlan 1
ciscoasa(config-if)#exit
ciscoasa(config)#

Маршрутизатор по умолчанию на Cisco ASA устанавливается следующим образом:

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 203.1.1.1

При конфигурации маршрутизатора провайдера задаются IP-адреса на всех его интерфейсах. Для исследуемой сети сценарий настройки имеет вид:

Router0 (config)#interface gigabitEthernet 0/0
Router0 (config-if)#ip address 203.1.1.1 255.255.255.0
Router0 (config-if)#no shutdown

Router0 (config)#interface gigabitEthernet 0/1
Router0 (config-if)#ip address 8.8.8.1 255.255.255.0
Router0 (config-if)#no shutdown

Для установки динамической маршрутизации на Router0 по протоколу OSPF используется следующая последовательность команд:

Router0(config)#router ospf 1
Router0(config-router)#network 203.1.1.0 0.0.0.255 area 0
Router0(config-router)#network 8.8.8.0 0.0.0.255 area 0

Создание объекта Network и разрешение трансляции адресов NAT

ciscoasa(config)#object network LAN
ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

Пингование предполагает поступление на пакет запроса пакета ответа. Но ASA пропускает трафик только с интерфейса более высокого уровня безопасности на более низкий, а в обратном направлении не пропускает. Разрешить пропуск пакетов с более низкого уровня безопасности на более высокий, т.е. с внешней сети во внутреннюю (outside > inside) можно путем настройки отдельного списка доступа.

Создать такой список можно следующим образом.

ciscoasa(config)#access-list inside_to_internet extended permit tcp any any
ciscoasa(config)#access-list inside_to_internet extended permit icmp any any
ciscoasa(config)#access-group inside_to_internet in interface outside

Выполнить проверку наличия списка доступа.

ciscoasa(config)#sh running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2

```
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 172.16.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address 203.1.1.2 255.255.255.0
!
object network LAN
subnet 172.16.1.0 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 203.1.1.1 1
!
access-list inside_to_internet extended permit tcp any any
access-list inside_to_internet extended permit icmp any any
!
access-group inside_to_internet in interface outside
```

Проверка пингованием прохождения тестовых пакетов с компьютера PC0 с адресом 172.16.1.6 на удаленный Server0 с адресом 8.8.8.8.

Можно заметить, теперь пакеты пигования успешно проходят в обе стороны

```
PC>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=1ms TTL=126
Reply from 8.8.8.8: bytes=32 time=13ms TTL=126
Reply from 8.8.8.8: bytes=32 time=12ms TTL=126
Reply from 8.8.8.8: bytes=32 time=15ms TTL=126

Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Minimum = 1ms, Maximum = 15ms, Average = 10ms

Переключиться в режим симуляции и пошагово проследить путь распространения кадров и пакетов. Анализ заголовков пакетов показывает (рисунок 3.4), что произошла замена частного IP-адреса 172.16.1.6 на публичный 203.1.1.2

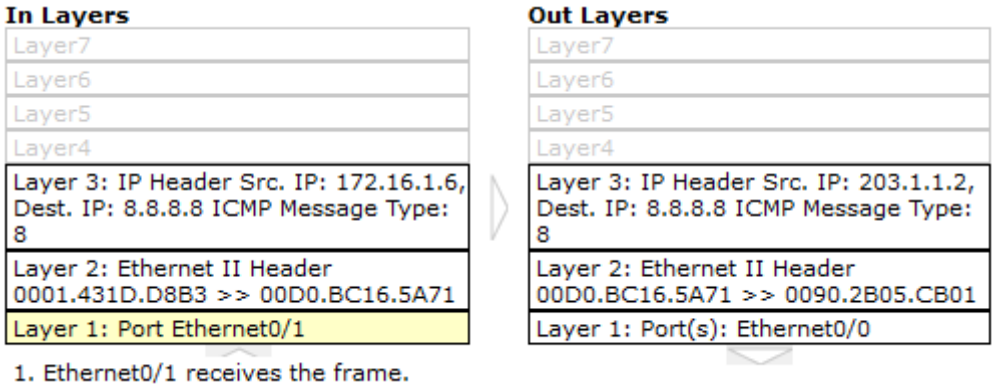

Рисунок 3.4 – Иллюстрация процедуры трансляции адресов

3.4. Программа работы

1. Повторить по рекомендуемой литературе методы адресации и управление доступом (списки доступа) в компьютерных сетях, а также устройство и особенности конфигурирования межсетевого защитного экрана типа Cisco ASA 5055.

2. Создать в окне Packet Tracer схему исследуемой сети, изображенной на рисунке 3.1 без установки адресов, указанных на этой схеме.

3. Проанализировать параметры начальной конфигурации защитного экрана и выяснить версию сетевой операционной системы, а также сохранить для отчета начальные настройки ASA 5505.

4. Убрать конфигурацию ASA 5505, созданную по умолчанию и проверить еще раз получившуюся конфигурацию:

5. Установить новый адрес VLAN 1, указанный в таблице вариантов (Приложение Б), инициировать DHCP-сервер защитного экрана и задать новый пул адресов, соответствующий адресу VLAN 1 и убедиться, смена адресов выполнена.

6. Установить IP-адреса VLAN 1 и VLAN 2 согласно заданному варианту (Приложение Б) и сконфигурировать на Cisco ASA маршрутизатор по умолчанию.

7. Исследовать созданную настройку параметров ASA 5505 путем исполнения команды **show running-config** и убедиться, что все параметры сконфигурированы верно.

8. Выполнить конфигурацию интерфейсов маршрутизатора интернет провайдера и установить динамическую маршрутизацию по протоколу OSPF. Используя инструмент **Inspect** (иконка «Лупа»), убедиться, что настройка прошла успешно.

9. Выполнить конфигурацию устройства ASA 5505, обеспечивающую динамическую трансляцию частных адресов подсети 172.16.1.0 в публичный адрес, выделенный для внешнего интерфейса. При этом использовать процедуру создание object network.

10. Создать списки доступа, обеспечивающие передачу пакетов ответа по протоколам ICMP (для процедуры ping) и TCP для обращения к WEBсерверу и выполнить проверку списка доступа.

11. Выполнить проверку доступа к удаленному серверу.

12. Переключиться в режим симуляции и пошагово проследить путь распространения кадров и пакетов и трансляции адресов в заголовках пакетов.

13. Составить отчет по результатам исследований.

3.5. Содержание отчета

1. Титульный лист.
2. Цель и программа лабораторной работы.
3. Исходные данные в соответствии с индивидуальным вариантом.
4. Скриншот с топологией локальной сети.
5. Команды и скриншоты этапов настройки локальной сети.
6. Скриншоты результатов тестирования сети.
7. Выводы.

3.6. Контрольные вопросы

1. Что называется периметром защищаемой компьютерной сети и каковы функции защиты периметра?
2. Какие устройства и системы реализуют функции защиты периметра сети?
3. Что представляет собой межсетевой защитный экран и каковы его функции??
4. На какой платформе реализуются межсетевые защитные экраны?
5. Каковы преимущества программно-аппаратного защитного экрана от чисто программного?
6. Что представляет собой демилитаризованная зона корпоративной компьютерной сети?
7. Каково минимальное количество портов создается в файрволлах и каково их назначение?
8. Дайте краткую характеристику программно-аппаратных МЗЭ моделей Cisco ASA.
9. Какие типы отечественных аппаратных межсетевых защитных экранов применяются в корпоративных компьютерных сетях и какие типовые функции реализуются в этих устройствах?

10. Каким образом на ASA 5505 можно создать интерфейсы третьего уровня (L3)?
11. В каких режимах может функционировать МЭ ASDA 5505?
12. Что представляет собой уровень безопасности и каковы правила присвоения этих уровней интерфейсам защитного экрана?
13. Каким образом реализуется удаленное управление межсетевым защитным экраном?
14. Какие виды трансляции адресов реализуются в ASA 5505?
15. Какой командой можно версию операционной системы и параметры конфигурации ASA 5505?
16. Как на ASA 5505 указывается маршрутизатор по умолчанию?
17. Как на ASA 5505 устанавливается динамическая маршрутизация по протоколу OSPF?

4. Лабораторная работа 2

ИССЛЕДОВАНИЕ КОНФИГУРАЦИИ ЗАЩИТНОГО ЭКРАНА ASA 5505 ФИЛИАЛА КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

4.1. Цель работы

Углубление и закрепление теоретических знаний в области безопасности локальных компьютерных сетей и исследование механизмов защиты в локальных компьютерных сетях (ЛКС) на основе программно-аппаратных межсетевых защитных экранов с возможностью удаленного администрирования сетью филиала с компьютера центрального офиса. Закрепление навыков моделирования компьютерных сетей и конфигурирования аппаратного сетевого защитного экрана для обеспечения защиты локальных сетей.

4.2. Описание лабораторной установки

В качестве лабораторной установки используется персональный компьютер с инсталлированной система моделирования компьютерных сетей Packet Tracer v.6.2, студенческая версия или старше. Исследованию подлежит корпоративная компьютерная сеть некоторой компании, состоящая из сети филиала и топология которой изображена на рисунке 4.1.

Локальная сеть филиала компании представлена рабочей станцией PC-B и коммутатором Switch2, подключенного к сетевому экрану ASA0. В сети также имеется выделенная демилитаризованная зона DMZ, в которой расположен DMZ Server, соединенный с файрволлом ASA0 через коммутатор Switch1. Выход локальной сети соединен с публичной сетью путем подключения межсетевого экрана к маршрутизатору провайдера Router1.

Должно быть обеспечено удаленное управление корпоративной сетью филиала с рабочей станции администратора Admin центрального офиса компании. Рабочая станции Admin подключена к глобальной сети через коммутатор switch3 и маршрутизатор Router3. Маршрутизатор Router2 является маршрутизатором провайдера.

ASA должен быть настроен для управления администратором сети филиала с PC-B так и удаленным администратором с компьютера Admin. Интерфейсы VLAN уровня 3 обеспечивают доступ к трем областям, созданным в процессе создания сети: *inside, outside* и *dmz*. Предполагается, что Интернет-провайдером выделен сети филиала публичный IP-адрес 209.165.200.226/29, который будет использоваться для преобразования адресов на ASA.

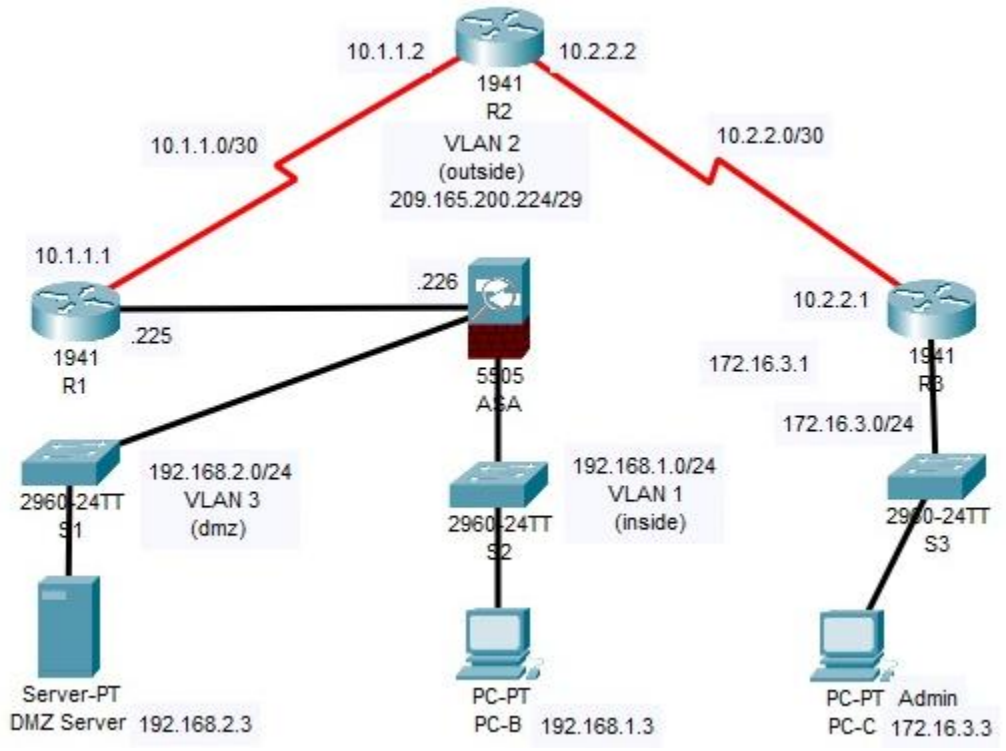

Рисунок 4.1 – Схема исследуемой сети филиала

4.3. Программа работы

1. Изучить по рекомендованной литературе теоретический материал, относящийся к построению защищенных компьютерных сетей.

2. Запустить систему моделирования сетей Packet Tracer и составить в рабочем окне схему сети, изображенную на рисунке 4.1.

3. С помощью команды ciscoasa#show running-config исследовать параметры начальной конфигурации ASA5505 и скопировать их для отчета по лабораторной работе.

4. Проверить получение IP-адресов компьютерами, подключенными к коммутатору Switch2, от DHCP-сервера, предустановленного на ASA5505.

Примечание: не забывайте активировать DHCP-сервер для получения IP адресов компьютерами, подключаемыми к коммутатору.

5. Подключая дополнительные PC к коммутатору Switch2 проследить за автоматической установкой IP-адресов на этих компьютерах.

6. Сконфигурировать недостающие параметры телекоммуникационного оборудования сети в соответствии с таблицей 4.1. Задать также параметры статической маршрутизации для Router1-Router3.

Примечание: Конфигурацию оборудования можно осуществлять с командной строки либо частично используя графический интерфейс.

7. Задать параметры статической маршрутизации для Router1-Router3.

8. Настроить процедуру трансляции адресов.

9. Создать списки доступа, обеспечивающие передачу пакетов ответа по протоколам ICMP (для процедуры ping) и TCP для обращения к WEBсерверу и выполнить проверку списка доступа.

10. Выполнить проверку доступа компьютера Admin к локальной сети предариятия.

11. Переключиться в режим симуляции и пошагово проследить путь распространения кадров и пакетов и трансляции адресов в заголовках пакетов.

12. Составить отчет по результатам исследований.

Таблица 4.1 – Параметры конфигурации телекоммуникационного оборудования

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	209.165.200.225	255.255.255.248	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.16.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	NA
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	NA
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	NA
DMZ Server	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

4.4. Методика выполнения исследований

4.4.1. Исследование параметров начальной конфигурации

Для исследования параметров начальной конфигурации ASA 5505 следует воспользоваться командой show running-config

4.4.2. Конфигурацию недостающих параметров сети

Конфигурация интерфейсов маршрутизаторов и рабочих станций может быть выполнена с помощью графического интерфейса Packet Tracer или с помощью интерфейса командной строки соответствующих устройств.

Настройка внутренних и внешних интерфейсов межсетевого экрана выполняется за четыре шага:

а) установить адрес логического интерфейса VLAN 1 для внутренней (*inside*) сети 192.168.1.0/24 и задать наивысший уровень безопасности 100.

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

б) установить адрес логического интерфейса VLAN 2 для внешней (*outside*) сети 209.165.200.224/29, задать минимальный уровень безопасности 0 и включить интерфейса VLAN 2.

```
ciscoasa(config-if)# ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)# security-level 0 (config-if)# interface vlan 2
ciscoasa(config-if)# ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)# security-level 0 (config-if)# nameif outside
ciscoasa(config-if)# ip address 209.165.200.226 255.255.255.248
ciscoasa(config-if)# security-level 0
```

в) выполнить проверку созданной конфигурации с помощью команды **show interface ip brief.** Если какие-либо ранее настроенные физические или логические интерфейсы не находятся в состоянии включено (up/up), то следует устранить неполадки.

г) проверить наличие связи компьютера PC-B с ASA путем посылки эхо-запроса по адресу внутреннего интерфейса ASA (192.168.1.1); убедиться путем пингования, что связь PC-B с VLAN 2 (внешним интерфейсом) отсутствует.

4.2.3. Настройка на внешнем интерфейсе ASA статического маршрута по умолчанию.

Настройка выполняется для того, чтобы устройство ASA могло получать доступ к внешним сетям. Для этого нужно создать с помощью команды **route** маршрут по умолчанию «из четырех нулей», связать его с внешним интерфейсом ASA и установить IP-адрес (209.165.200.225) на интерфейсе G0/0 маршрутизатора R1, который будет использоваться в качестве шлюза по умолчанию.

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

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

Проверить, что ASA может успешно отправлять эхо-запрос по IP-адресу (10.1.1.1) интерфейса. При отсутствии связи следует выявить и исправить ошибки в конфигурации.

Убедиться пингованием, что связь компьютера PC-B с внешний интерфейсом VLAN 2 (outside) по IP-адресу 209.165.200.226 отсутствует.

4.2.4. Настрока процедуры преобразования адресов с помощью протокола трансляции адресов и использованием сетевых объектов.

Для реализации этой настройки нужно **с**оздать сетевой объект с именем **inside-net** и назначить ему атрибуты с помощью команд **subnet** и **nat**.

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

Проверить конфигурацию объектов NAT с помощью команды **show run**. Затем отправить эхо-запрос с компьютера PC-B на интерфейс G0/0 маршрутизатора R1 по IP-адресу 209.165.200.225. Эхо-запросы должны завершиться ошибкой.

Выполнить команду **show nat** на ASA для просмотра преобразованных и непреобразованных элементов.

Обратите внимание, что среди эхо-запросов с компьютера PC-B четыре были преобразованы, а четыре – нет. Исходящие эхо-запросы были преобразованы и отправлены по назначению. Эхо-ответы были заблокированы политикой безопасности межсетевого защитного экрана.

4.2.5. Установка DHCP-сервера на защитном экране ASA 5505

Эта процедура выполняется за несколько шагов:
а) настроить пул адресов DHCP и включить его на внутреннем интерфейсе ASA.

```
ciscoasa(config)# dhcpd address 192.168.1.5-192.168.1.36 inside
```

б) указать IP-адрес DNS-сервера, который нужно сообщить клиентам.

```
ciscoasa(config)# dhcpd dns 209.165.201.2 interface inside
```

в) запустить демон DHCP в ASA для прослушивания запросов DHCP-клиентов на включенном внутреннем (inside) интерфейсе

```
ciscoasa(config)# dhcpd enable inside
```

г) заменить на компьютере PC-B статический IP-адрес на адрес DHCP-клиента и убедиться, что он получил IP-адрес от сервера DHCP.

4.2.6. Настройка AAA на использование локальной базы данных для аутентификации пользователей

Выполняется следующими двумя действиями:

а) определить локального пользователя с именем **admin** с помощью команды **username**. Задать пароль **adminpa55**.

ciscoasa(config)# username admin password adminpa55

б) настроить функцию AAA на использование локальной базы данных ASA для аутентификации пользователей по протоколу SSH.

ciscoasa(config)#aaa authentication ssh console LOCAL

4.2.7. Настройка удаленного доступа к ASA.

Устройство ASA можно настроить так, чтобы оно принимало подключения с одного или нескольких хостов во внутренней или внешней сети. На этом этапе хосты из внешней сети могут использовать для связи с ASA только протокол SSH.

Устройства внутренней сети могут получать доступ к ASA с помощью SSH-сеансов. Для реализации этой процедуры необходимо выполнить два действия:

а) создать пару ключей RSA, которая требуется для поддержки подключений SSH. Поскольку на устройстве ASA по умолчанию уже имеются ключи RSA, в качестве ответа нужно ввести **no**, когда будет предложено их заменить.

ciscoasa (config)# crypto key generate rsa modulus 1024

При этом будет выдано предупреждение WARNING: You have a RSA keypair already defined named <Default-RSA-Key>.
Do you really want to replace them? [yes/no]: **no**
ERROR: Failed to create new RSA keys named <Default-RSA-Key>

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

ciscoasa(config)# ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)# ssh 172.16.3.3 255.255.255.255 outside
ciscoasa(config)# ssh timeout 10

в) установить SSH-сеанс связи компьютера PC-C с интерфейсом ASA с адресом 209.165.200.226. Устранить неполадки, если они возникнут.

PC> ssh -l admin 209.165.200.226

г) установить SSH-сеанс связи компьютера PC-B с интерфейсом ASA с адресом 192.168.1.1. При отсутствии ответа устранить неполадки.

PC> **ssh -l admin 192.168.1.1**

4.2.8. Настройка DMZ, статического преобразования сетевых адресов (NAT) и списков контроля доступа (ACL)

Интерфейс G0/0 маршрутизатора R1 и внешний интерфейс ASA уже используют адреса 209.165.200.225 и .226 соответственно. В данной работе нужно

использовать глобальный адрес 209.165.200.227 и статическую трансляцию адресов NAT для предоставления доступа к серверу DMZ. Эта процедура выполняется за два этапа.

1 этап: настройка интерфейса DMZ VLAN 3 на ASA.

а) настроить DMZ VLAN 3, где будет располагаться веб-сервер с открытым доступом и назначить этой сети IP-адрес **192.168.2.1/24**. Затем присвоить ей имя **dmz** и уровень безопасности **70**. Поскольку сервер DMZ не нуждается в связи с внутренними пользователями, следует отключить отправку сообщений на интерфейс VLAN 1. По умолчанию уровень безопасности DMZ имеет нулевое значение.

```
ciscoasa (config)# interface vlan 3
ciscoasa (config-if)# ip address 192.168.2.1 255.255.255.0
ciscoasa (config-if)# no forward interface vlan 1
ciscoasa (config-if)# nameif dmz
ciscoasa (config-if)# security-level 70
```

б) назначить физический интерфейс E0/2 в ASA для DMZ VLAN 3 и включить интерфейс.

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

в) проверить правильность настроек можно с помощью следующих команд:

- **show interface ip brief** для отображения состояния всех интерфейсов ASA;
- **show ip address** для отображения информации по интерфейсам VLAN 3-го уровня;
- **show switch vlan** - отображение внутренних и внешних сетей VLAN, настроенных на ASA, и назначенных портов.

2 этап: настройка статического преобразования NAT на сервере DMZ с помощью сетевого объекта.

Создать сетевой объект с именем **dmz-server** и назначить ему статический IP-адрес сервера DMZ (192.168.2.3).

В режиме определения объекта ввести команду **nat**, указывающую, что данный объект используется для преобразования адреса DMZ во внешний адрес с помощью статического протокола NAT, и ввести общедоступный преобразованный адрес 209.165.200.227.

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

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

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

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

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

4 этап: проверка доступа к серверу DMZ.

4.4. Содержание отчета

1. Титульный лист.
2. Цель и программа лабораторной работы.
3. Исходные данные в соответствии с индивидуальным вариантом.
4. Скриншот с топологией локальной сети.
5. Команды и скриншоты этапов настройки локальной сети.
6. Скриншоты результатов тестирования сети.
7. Выводы.

4.5. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие действия следует выполнить при настройке интерфейсов межсетевого защитного экрана?
2. Какие уровни безопасности присваиваются устройству ASA 5505?
3. Как на ASA задается статический маршрут по умолчанию?
4. В чем состоит настройка DHCP-сервера на ASA 5505?
5. Что называется периметром защищаемой компьютерной сети и каковы функции защиты периметра?
6. Какие устройства и системы реализуют функции защиты периметра сети?
7. Что представляет собой межсетевой защитный экран и каковы его функции??
8. На какой платформе реализуются межсетевые защитные экраны?
9. Каковы преимущества программно-аппаратного защитного экрана от чисто программного?

10. Что представляет собой демилитаризованная зона корпоративной компьютерной сети?
11. Каково минимальное количество портов создается в файрволлах и каково их назначение?
12. Дайте краткую характеристику программно-аппаратных МЗЭ моделей Cisco ASA.
13. Какие типы отечественных аппаратных межсетевых защитных экранов применяются в корпоративных компьютерных сетях и какие типовые функции реализуются в этих устройствах?
14. Каким образом на ASA 5505 можно создать интерфейсы третьего уровня (L3)?
15. В каких режимах может функционировать МЗЭ ASDA 5505?
16. Что представляет собой уровень безопасности и каковы правила присвоения этих уровней интерфейсам защитного экрана?
17. Каким образом реализуется удаленное управление межсетевым защитным экраном?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Юрайт, 2023. — 161 с. — URL: https://urait.ru/bcode/512268 (дата обращения: 08.04.2024). — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный.
2. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Юрайт, 2023. — 309 с. — URL: https://urait.ru/bcode/511998 (дата обращения: 08.04.2024). — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный.
3. Аппаратные и программные средства защиты информации : учебное пособие / Душкин А. В., Кольцов А., Кравченко А. – Воронеж : Научная книга, 2016. - 232 с. - URL: https://znanium.com/catalog/product/923168 (дата обращения: 08.04.2024).– Режим доступа: по подписке. — ISBN 978-5-4446-0746-6. - Текст : электронный.
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Юрайт, 2023. — 473 с. — URL: https://urait.ru/bcode/511138 (дата обращения: 08.04.2024). — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный.
5. Чернега, В. С. Компьютерные сети : учебное пособие для студентов направления "Компьютерные науки" вузов / В. С. Чернега, Б. Платтнер. - Севастополь : СевНТУ, 2006. - 499 с. : ил ; 21 см. - Библиография: с. 489-491. — Текст : непосредственный.
6. Обзор и сравнение межсетевых экранов отечественных производителей https://habr.com/ru/articles/726662/
7. Обзор межсетевых экранов и систем обнаружения вторжений, сертифицированных ФСТЭК России. https://www.anti-malware.ru/analytics/Market_Analysis/firewalls-and-intrusion-detection-systems-certified-by-FSTEC#part4111
8. Маршрутизаторы серии ESR: ESR-100, ESR-200, ESR-1000. Версии ПО esr-100-1.0.7-ST, esr-200-1.0.7-ST esr-1000-1.0.7-ST. Руководство по эксплуатации. https://zscom.ru/image/data/2017_new_data/eltex/esr_series_user_manual_1.2.0.pdf https://eltexalatau.kz/upload/iblock/ac4/rukovodstvo_po_ekspluatatsii_esr_fstec.pdf?ysclid=lumfe3iez8637008561

ПРИЛОЖЕНИЕ А
Данные по конфигурации оборудования исследуемой сети (рисунок 3.1)

Вариант	Публичный адрес сети	Адрес VLAN1	Адрес сервера
1	115.10.95.2/24	192.168.1.0/24	11.11.11.12
2	210.87.31.5/24	172.18.0.0/16	22.22.22.22
3	180.24.65.7/24	192.168.3.0/24	33.33.33.32
4	160.12.33.2/24	172.20.10.0/24	44.44.44.42
5	27.145.31.3/24	172.30.20.0/24	55.55.55.56
6	75.167.22.5/24	192.168.5.0/24	66.66.66.64
7	220.46.28.2/24	172.10.12.0/24	77.77.77.76
8	49.212.73.4/24	10.20.2.0/24	88.88.88.88
9	13.17.126.8/24	10.1.12.0/24	99.99.99.92
10	103.51.12.2/24	172.31.9.0/24	15.15.15.14

ПРИЛОЖЕНИЕ Б

Сообщение, выводимое при просмотре начальной конфигурации межсетевого защитного экрана ASA 5505

```
ciscoasa>
ciscoasa>en
Password:
ciscoasa#sh running-config
: Saved
:
ASA Version 8.4(2)
!
hostname ciscoasa
names
!
interface Ethernet0/0
switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
nameif outside
security-level 0
ip address dhcp
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
```

```
!
telnet timeout 5
ssh timeout 5
!
dhcpd address 192.168.1.5-192.168.1.35 inside
dhcpd enable inside
!
dhcpd auto_config outside
```

У ч е б н о е и з д а н и е

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ПЕРИМЕТРА ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Учебно-методическое пособие

Составитель: **Чернега** Виктор. Степанович

В авторской редакции

Изд. № 84/2024. Объем 2,5 п.л. Усл. печ. л. 2,32. Уч.-изд. л. 2,45.
Издательский центр ФГАОУ ВО «Севастопольский государственный университет»