

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**ОТЧЕТ ПО ПРАКТИКЕ**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Автор |  | | |  | Ковалев Д. П. | | | |
|  | (подпись, дата) | | |  |  | | | |
| Обозначение | ИиВТ.10.05.01 | | Группа | | | | ВКБ32 |
| Направление подготовки | | 10.05.01 Компьютерная безопасность | | | | | |
| Профиль | Математические методы защиты информации | | | | | | |
| Проверил |  | | |  | |  | |
|  | (подпись, дата) | | |  | |  | |

Ростов-на-Дону

2025

**Содержание**

[**Практическая работа №1** 3](#_Toc191680973)

[**1. Разбор конфигурации: основные компоненты** 4](#_Toc191680974)

[**1.1. ISAKMP (Phase 1) — Установление защищенного канала** 4](#_Toc191680975)

[**1.2. IPSec (Phase 2) — Настройки шифрования трафика** 6](#_Toc191680976)

[**1.3. Применение политики IPSec (Crypto Map)** 6](#_Toc191680977)

[**2. Настройки интерфейсов и NAT** 7](#_Toc191680978)

[**3. Маршрутизация (IP Routing)** 8](#_Toc191680979)

[**4. Контроль трафика (Access Control Lists)** 9](#_Toc191680980)

[**4.1. ACL 110 (для VPN)** 9](#_Toc191680981)

[**4.2. ACL 150 (для NAT)** 9](#_Toc191680982)

[**5. Описание работы схемы** 9](#_Toc191680983)

[**6. Итог** 10](#_Toc191680984)

**Практическая работа №1**

**Условие:** сделать 3 офиса по 5 компьютеров в каждом, соединить их через маршрутизаторы с VPN и в каждом офисе сделать выход в интернет через NAT для всех 15 компьютеров.

**Цель**: научиться строить корпоративные сети в Cisco Packet Tracer.

Эта конфигурация представляет собой настройку трех маршрутизаторов, соединенных между собой с использованием **IPSec VPN**. Они обеспечивают защищенное соединение между сетями **192.168.1.0/24**, **192.168.2.0/24** и **192.168.3.0/24**, каждая из которых подключена к отдельному маршрутизатору.

Изображение выглядит как диаграмма, линия, текст, карта

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 1 – строение сети

**1. Разбор конфигурации: основные компоненты**

**1.1. ISAKMP (Phase 1) — Установление защищенного канала**

В каждой конфигурации роутера задается политика **ISAKMP** (Internet Security Association and Key Management Protocol — это протокол, используемый для установления **Security Associations (SA)** — безопасных соединений между двумя устройствами. Он является частью процесса настройки **IPSec VPN**), которая определяет параметры аутентификации и шифрования для установления туннеля:

crypto isakmp policy 10

encr aes

authentication pre-share

group 2

* **encr aes** – используется **AES** (Advanced Encryption Standard) для шифрования трафика.
* **authentication pre-share** – применяется **предварительно разделенный ключ (PSK)** для аутентификации.
* **group 2** – применяется **группа 2** (1024-битные ключи Diffie-Hellman) для генерации общего ключа.

Проверим, что политика применилась, результат представлен на рисунке 2.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 2 – проверка применения политики

Теперь настроим обмен ключами **ISAKMP**. На каждом маршрутизаторе указываются адреса удаленных маршрутизаторов, с которыми должен устанавливаться VPN-туннель, используя команды ниже:

crypto isakmp key cisco address 100.0.2.2

crypto isakmp key cisco address 100.0.3.2

В каждой конфигурации **PSK** ("cisco") настроен для определенных peer (соседних маршрутизаторов).

Как мы можем проверить, что все применялось? Для этого можем использовать команду “show crypto ipsec sa”. Результат представлен на рисунке 3.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 3 – проверка применения настроек

**SA (Security Association)** — это соглашение между двумя устройствами (например, роутерами) о параметрах безопасности, которые будут использоваться для защиты данных. SA определяет. **SA (Security Association)** — это соглашение между двумя устройствами (например, роутерами) о параметрах безопасности, которые будут использоваться для защиты данных. SA определяет.

**1.2. IPSec (Phase 2) — Настройки шифрования трафика**

Определяется **IPSec Transform-set**, который указывает, какие алгоритмы шифрования и аутентификации используются:

crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

* **esp-3des** – используется **3DES** для шифрования пакетов.
* **esp-sha-hmac** – аутентификация трафика выполняется с использованием **HMAC-SHA**.

Эта команда создает **IPSec Transform-set** — набор параметров, которые определяют, как будет защищен трафик в **фазе 2 IPSec (IKE Phase 2)**.

Для просмотра “transform-set” можно использовать команду, которая представлена ниже:

show crypto ipsec transform-set

У меня был такой результат, который представлен ниже на рисунке 4.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 4 – результат команды “show crypto ipsec transform-set“

**1.3. Применение политики IPSec (Crypto Map)**

**“Crypto map”** — это ключевой элемент настройки IPSec VPN на роутерах Cisco. Он связывает все компоненты IPSec (такие как transform-set, ACL, peer-адреса) и применяет их к интерфейсу роутера.

Каждый маршрутизатор связывает **IPSec-туннели** с определенным **peer** (соседом):

crypto map VPN-MAP 10 ipsec-isakmp

set peer 100.0.2.2

set transform-set VPN-SET

match address 110

* **crypto map VPN-MAP 10 ipsec-isakmp** – создается **карта криптографии (crypto map)**, которая указывает, что это IPSec-конфигурация.
* **set peer 100.0.2.2** – указывается **IP-адрес удаленного маршрутизатора** (партнера по VPN).
* **set transform-set VPN-SET** – используется **определенный transform-set** (набор шифрования и аутентификации).
* **match address 110** – используется **ACL 110** для выбора трафика, который должен проходить через VPN.

Аналогичные настройки присутствуют для второго удаленного узла.

**2. Настройки интерфейсов и NAT**

**NAT (Network Address Translation) —** это технология, которая позволяет устройствам в локальной сети (**LAN**) с частными **IP**-адресами взаимодействовать с устройствами в глобальной сети (например, Интернет) с использованием публичных IP-адресов.

Каждый маршрутизатор имеет два активных интерфейса:

* **GigabitEthernet0/0** – подключен к внешней сети (**интернету**), используется для VPN и NAT.
* **GigabitEthernet0/1** – локальная сеть (**LAN**).

Пример настройки для маршрутизатора 1:

interface GigabitEthernet0/0

ip address 100.0.1.2 255.255.255.0

ip nat outside

duplex auto

speed auto

crypto map VPN-MAP

* **ip nat outside** – указывает, что этот интерфейс используется для NAT.
* **crypto map VPN-MAP** – применяет конфигурацию **IPSec VPN** к интерфейсу.

Локальный интерфейс:

interface GigabitEthernet0/1

ip address 192.168.1.1 255.255.255.0

ip nat inside

duplex auto

speed auto

* **ip nat inside** – трафик с этого интерфейса может подвергаться NAT.

**NAT (Перевод сетевых адресов):**

ip nat inside source list 150 interface GigabitEthernet0/0 overload

Этот параметр включает **динамический NAT с перегрузкой (PAT)** для локальных адресов. **PAT (Port Address Translation)**, также известный как **NAT Overload**, — это расширение NAT, которое позволяет множеству устройств в локальной сети использовать **один публичный IP-адрес** для выхода в Интернет. Это достигается за счет использования уникальных **портов** для каждого соединения.

Для проверки, что NAT работает используем команду: “show running-config | include nat”.

**3. Маршрутизация (IP Routing)**

Для того чтобы маршрутизаторы могли отправлять трафик в интернет или в другие сети, настроены **маршруты по умолчанию**:

ip route 0.0.0.0 0.0.0.0 100.0.1.1

Этот маршрут указывает, что **весь неизвестный трафик** должен отправляться на **шлюз 100.0.1.1**.

**4. Контроль трафика (Access Control Lists)**

Два **ACL** управляют, какой трафик идет через **IPSec VPN** и какой через **NAT**:

**4.1. ACL 110 (для VPN)**

Этот список разрешает передавать трафик между локальными сетями:

access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

* **Разрешается передача данных между 192.168.1.0 и 192.168.2.0**.
* **Разрешается передача данных между 192.168.1.0 и 192.168.3.0**.

**4.2. ACL 150 (для NAT)**

Этот список запрещает перевод в NAT трафика, предназначенного для **VPN**, но разрешает доступ в интернет:

access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 150 permit ip 192.168.1.0 0.0.0.255 any

* **Запрещается NAT между 192.168.1.0 и 192.168.2.0**.
* **Запрещается NAT между 192.168.1.0 и 192.168.3.0**.
* **Остальной трафик (например, в интернет) разрешен**.

Для проверки того какие у нас access-list применились для роутера используем команду: “show access-lists”. Результат представлен на рисунке 5.

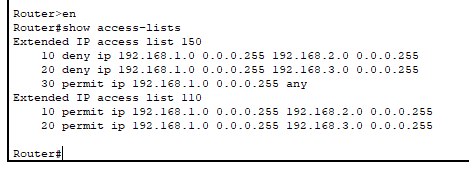


Рисунок 5 – access-list для Router0

**5. Описание работы схемы**

1. Когда устройство в **192.168.1.0/24** (например, 192.168.1.10) отправляет данные в **192.168.2.0/24**, трафик попадает под ACL 110.
2. Пакеты **не подвергаются NAT**, так как ACL 150 запрещает NAT для внутреннего трафика.
3. Пакеты **зашифровываются** с помощью **IPSec VPN** (используется crypto map VPN-MAP).
4. **Шифрованные пакеты** передаются по сети **100.0.1.0/24** на **100.0.2.2**.
5. Удаленный маршрутизатор **расшифровывает пакеты** и передает их в **192.168.2.0/24**.
6. Обратный процесс происходит при ответе от **192.168.2.0/24** в **192.168.1.0/24**.

**Если же трафик идет в интернет, он проходит NAT и выходит через интерфейс GigabitEthernet0/0.**

**6. Итог**

* **VPN на основе IPSec** между **тремя маршрутизаторами**.
* **NAT** настроен для выхода в интернет.
* **Контроль трафика** с помощью **ACL**.
* **Маршруты по умолчанию** для связи с интернетом.

Эта конфигурация позволяет **безопасно соединять три локальные сети через VPN**.