**Практическое занятие № 1**

**«Построение VPN туннеля между двумя подсетями, защищаемыми шлюзами безопасности «С-Терра Шлюз». Аутентификация на определенных ключах»**

## Введение

Данный сценарий описывает настройку безопасного взаимодействия между защищаемыми подсетями центрального офиса и филиала. Обеспечение безопасного взаимодействия достигается путем шифрования и туннелирования трафика с применением отечественных отраслевых стандартов ГОСТ и протокола IPsec.

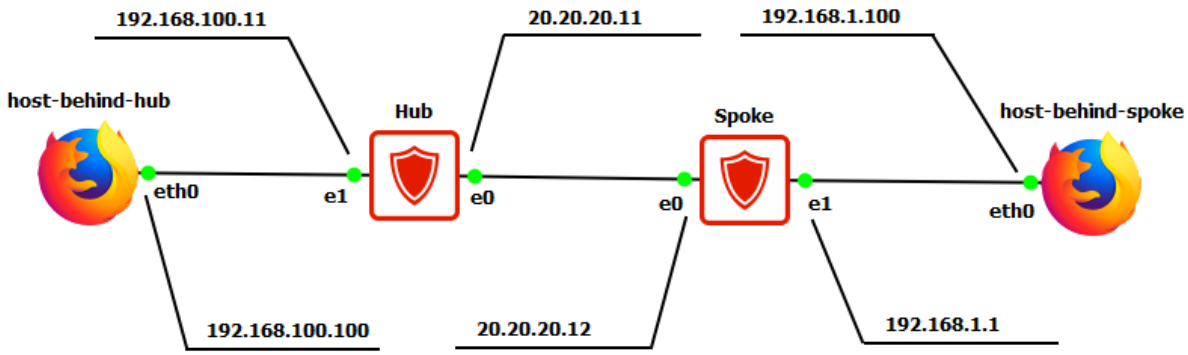
Все остальные соединения разрешены, но защищаться при помощи IPsec не будут.

В рамках данного сценария для аутентификации используются предопределенные ключи.

## Требования к инфраструктуре

1. Требования к устройствам.
   1.1. В качестве host-behind-… может использоваться любое устройство, аналогичное функционалу персонального компьютера (webterm-new, Kali Linux CLI, Linux CLI и т.д.)
2. Требования к сетевому взаимодействию.
   2.1. Между устройствами стенда должна быть обеспечена IP связность.

## Схема взаимодействия




## Общая логика работы

1. Размещение устройств

1.1. В центральном офисе размещаются: криптошлюз С-Терра Шлюз (Hub) и персональный компьютер (host_behind_hub).

1.2. В филиале размещаются: криптошлюз С-Терра Шлюз (Spoke) и персональный компьютер (host_behind_spoke).

## Настройка устройства Hub

Перед вводом шлюза безопасности в эксплуатацию, администратор должен провести начальную инициализацию шлюза – ввести лицензию на VPN-продукт и провести инициализацию с помощью биологического датчика случайных чисел (био ДСЧ). Все эти действия выполняются администратором с помощью консоли шлюза.

1. Откройте консоль виртуальной машины Hub.

В окне виртуальной машины шлюза безопасности Hub войдите под пользователем `administrator` с паролем по умолчанию – `s-terra`. При входе появится сообщение:

```
System is no initialized. Please run “initialize” command to start initialization procedure
```

Запустите процедуру инициализации, введя команду `initialize` и нажмите `enter`.

2. В появившемся окне запускается генератор случайных чисел. Необходимо нажимать на клавиши, указанные на окне генератора, до окончания инициализации.

```
Progress: [            ]
Press key: G
```

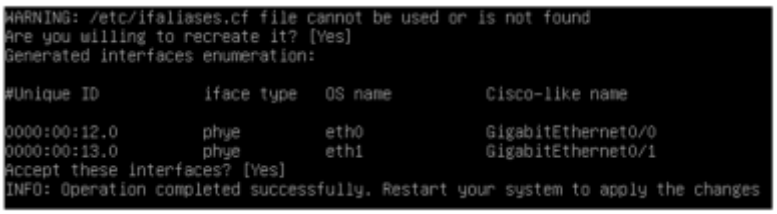
3. Далее необходимо ввести лицензию на шлюз безопасности. Введите `product code, customer code, license number, license code` для С-Терра Шлюз (лицензия хранится в файле «Лицензии С-Терра»). Данные для ввода чувствительны к регистру:

```
Enter product code: _
Enter customer code:
Enter license number:
Enter license code:
```

Если все данные введены правильно, подтвердите их корректность:

```
Is the above data correct? Y
```

Если потребуется, согласитесь пересоздать файл соответствия имен сетевых интерфейсов:




После ввода лицензии и подтверждения корректности введённых данных, должен запуститься IPsec драйвер:

```
Initialization completed.
Some settings will take effect after OS reboot only.

Network traffic is blocked.
To unblock network traffic, please setup network security policy
or use “run csconf_mgr activate” command to activate the predefined
permissive network security policy now.
```

Изначально шлюз настроен на блокирование сетевого трафика, кроме DHCP. Измените эту политику, применяя пустую политику безопасности:

```
run csconf_mgr activate
```

На этом инициализация шлюза закончена. Перейдите к настройке политик безопасности шлюза Hub. Отправьте устройство на перезагрузку командой `reboot`.

## Начальные настройки

В С-Терра Шлюз версии 4.3 реализовано 2 консоли, имеющие следующие названия:

- **CLI разграничения доступа (или Initial CLI);**
- **Crypto Gateway CLI (CGW CLI).**

CLI разграничения доступа служит для локальной аутентификации, а также для:

- инициализации;
- формирования запросов на сертификат устройства;
- импортирования сертификатов в базу продукта «С-Терра СиЭсПи»;

- обновления ключевой информации в базе продукта «С-Терра СиЭсПи»;
- применение настроек от С-Терра КП;
- переход в CGW CLI

CGW CLI используется для настройки функций СКЗИ и МЭ. CGW CLI имеет схожий синтаксис с Cisco IOS (Cisco Like Console). В консолях работает автозаполнение клавишей TAB.

1. Перейдите в консоль Initial CLI.

> Данные по умолчанию для **Initial CLI**:
>
> **Пользователь:** `administrator`
>
> **Пароль:** `s-terra`
>
> Пример успешного доступа к консоли:
>
> `administrator@sterragate]_`

2. Смените пароль по умолчанию для консоли **Initial CLI** на учебный пароль **MIET123** (в процессе эксплуатации шлюза для пользователя **Initial CLI** пароль может быть любой), введя команду:

```
administrator@sterragate] change user password

Old user password:<старый пароль>
New user password:<новый пароль>
Re-type new password: <повтор нового пароля>
```

3. Перейдите в Linux консоль (пользователь root) устройства, введя команду `system`. Смените пароль по умолчанию пользователя **root** на учебный пароль **miettcs**, введя команду:

```
administrator@sterragate] system
root@sterragate:# passwd
Enter new UNIX password:
Re-type new UNIX password:

passwd: password updated successfully
```

4. Для выхода из пользователя root наберите команду `logout`.

## Создание политики безопасности

Настройка шлюза осуществляется с помощью **Crypto Gateway CLI** (CGW CLI).

1. Перейдите в консоль управления CGW CLI, введя команду:

```
administrator@sterragate] configure
```

Данные по умолчанию для **CGW CLI**:

**Пользователь:** `cscons`

**Пароль:** `csp`

Пример успешного доступа к консоли: `sterragate#`

2. Смените пароль по умолчанию для консоли **CGW CLI** на учебный пароль **miet** (в процессе эксплуатации шлюза для пользователя CGW CLI пароль может быть любой), введя команду:

```
sterragate#configure terminal
sterragate(config)#username cscons password <пароль>
```

3. Задайте имя шлюза командой:

```
sterragate(config)#hostname Hub
```

4. Перейдите в консоль Crypto Gateway CLI с изменёнными параметрами для входа и из конфигурационного режима смените пароль на учебный пароль (russia) на вход в привилегированный режим. Для этого введите команду:

```
Hub(config)#enable secret 0
```

`0` – ввод ключа в незашифрованном виде.

Пароль по умолчанию для привилегированного режима: `csp`.

5. В настройках интерфейсов задайте ip-адреса и приведите их в режим «no shutdown» (по умолчанию сетевые интерфейсы выключены).

```
Hub(config)#interface GigabitEthernet0/0
Hub(config-if)#ip address 20.20.20.11 255.255.255.0
Hub(config-if)#no shutdown
Hub(config-if)#exit
Hub(config)#interface GigabitEthernet0/1
Hub(config-if)#ip address 192.168.100.11 255.255.255.0
Hub(config-if)#no shutdown
Hub(config-if)#exit
```

6. Задайте статический маршрут до подсети 192.168.1.0/24 через шлюз Spoke:

```
Hub(config)#ip route 192.168.1.0 255.255.255.0 20.20.20.12
```

7. Задайте тип идентификации:

```
Hub(config)#crypto isakmp identity address
```

8. Настройте параметры DPD (dead peer detection) для отслеживания состояния IPsec соединений, где в первой команде 1 – это период времени отсутствия входящего трафика, 3 – количество секунд, которое нужно подождать, чтобы отправлять пакеты процесса keepalived (DPD-запрос). Во второй команде параметр 3 – это время ожидания ответа от партнёра на DPD-запрос:

```
Hub(config)# crypto isakmp keepalive 1 3
Hub(config)# crypto isakmp keepalive retry-count 3
```

Механизм DPD используется для детектирования отказа партнёра в рамках IKE соединения. DPD отсылает периодические keepalive сообщения и при отсутствии ответа от IKE партнёра за заданный интервал времени удаляет текущий туннель и пытается заново построить соединение.

9. Задайте параметры для IKE:

```
Hub(config)# crypto isakmp policy 1
Hub(config-isakmp)# hash gost341112-256-tc26
Hub(config-isakmp)# authentication pre-share
Hub(config-isakmp)# group vko2
Hub(config-isakmp)# exit
```

10. Задайте предопределённый ключ (в данном случае ключ - KEY):

```
Hub(config)#crypto isakmp key KEY address 20.20.20.12
```

Важно! Согласно правилам пользования, использование предопределённых ключей разрешается только в тестовых целях. В рабочей сети необходимо использовать аутентификацию на цифровых сертификатах. Переход на сертификаты описан в практической работе №2.

```
Hub(config)# crypto ipsec transform-set GOST esp-gost28147-4m-imit
Hub(cfg-crypto-trans)#mode tunnel
Hub(cfg-crypto-trans)#exit
```

11. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа из сети 192.168.100.0/24 в сеть 192.168.1.0/24:

```
Hub(config)#ip access-list extended LIST
Hub(config-ext-nacl)#permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
Hub(config-ext-nacl)#exit
```

12. Создайте статическую крипто-карту (имя CMAP, раздел 1):

```
Hub(config)# crypto map CMAP 1 ipsec-isakmp
```

13. Укажите трафик, который необходимо защищать:

```
Hub(config-crypto-map)# match address LIST
```

14. Укажите алгоритмы защиты трафика:

```
Hub(config-crypto-map)# set transform-set GOST
```

15. Укажите IP-адрес партнера в рамках IPsec соединения. В данной лабораторной работе — это внешний IP-адрес устройства С-Терра Шлюз (20.20.20.12):

```
Hub(config-crypto-map)# set peer 20.20.20.12
Hub(config-crypto-map)# exit
Hub(config)#
```

16. Привяжите крипто-карту к интерфейсу, на котором будет терминироваться туннель:

```
Hub(config)#interface GigabitEthernet0/0
Hub(config-if)#crypto map CMAP
Hub(config-if)#exit
```

17. Для дальнейшего возможного просмотра логов на компьютере примените команду logging trap в режиме `debugging`:

```
Hub(config)#logging trap debugging
Hub(config)#exit
Hub#
```

По умолчанию все логи устройства сохраняются локально. При необходимости можно указать ip адрес syslog-сервера.

Настройка устройства Hub в cisco-like консоли завершена. При выходе из конфигурационного режима происходит конвертация, сохранение и загрузка конфигурации в «startup config».

Текст cisco-like конфигурации представлен в Приложении к практическому занятию.

## Настройка шлюза Spoke

Инициализация шлюза безопасности, начальные настройки и смена паролей происходят аналогично настройке Hub, за исключением используемой лицензии. Конфигурирование шлюза производится так же из

initial CLI и из CGW CLI. Перейдите к настройке политики безопасности из CGW CLI:

1. Задайте имя шлюза Spoke;
2. В настройках интерфейсов задайте ip-адреса;
3. Задайте статический маршрут до подсети 192.168.100.0/24 через шлюз Spoke;
4. Задайте тип идентификации;
5. Настройте параметры DPD (dead peer detection) для отслеживания состояния IPsec соединений;
6. Задайте параметры для IKE;
7. Задайте предопределенный ключ (в данном случае ключ - KEY);
8. Создайте набор преобразований для IPsec;
9. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа из сети 192.168.1.0/24 в сеть 192.168.100.0/24;
10. Создайте статическую крипто-карту (имя CMAP, раздел 1);
11. Привяжите крипто-карту к интерфейсу, на котором будет терминироваться туннель;

Для дальнейшего возможного просмотра логов на компьютере примените команду logging trap в режиме debugging:

```
Spoke(config)#logging trap debugging
Spoke(config)#exit
```

Настройка устройства Spoke в cisco-like консоли завершена. При выходе из конфигурационного режима происходит конвертация и загрузка конфигурации.

## Настройка устройств host_behind_hub и host_behind_spoke

Настройте IP-адрес и шлюз по умолчанию для каждого устройства, согласно схеме.

## Проверка работоспособности стенда

1. В консолях обоих шлюзов (Hub и Spoke) выполните команду show run из **CGW CLI**:

```
Hub#sh run
```

Убедитесь, что конфигурации соответствуют друг другу (в конфигурациях обоих шлюзов есть списки доступа, разделы криптокарты, политики и т.д.). Проверка конфигураций – первое, с чего начинается troubleshooting.

2. На устройстве host_behind_spoke из командной строки выполните команду ping (проверка доступности сетевого устройства) 192.168.100.100:

```
C:\Users\User01>ping 192.168.100.100

Обмен пакетами с 192.168.100.100 по 32 байт:

Ответ от 192.168.100.100: число байт=32 время=596мс TTL=125
Ответ от 192.168.100.100: число байт=32 время=8мс TTL=125
Ответ от 192.168.100.100: число байт=32 время=9мс TTL=125
Ответ от 192.168.100.100: число байт=32 время=8мс TTL=125

Статистика Ping для 192.168.100.100:
 Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
 Минимальное = 8мсек, Максимальное = 596 мсек, Среднее = 155 мсек
```

3. Убедитесь в наличии защищенных IKE и IPsec соединений на Hub:

```
GW1#show crypto isakmp sa

ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (20.20.20.12,500)-(20.20.20.11,500) active 1968 1836

GW1#show crypto ipsec sa

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent
Rcvd
1 1 (192.168.1.0-192.168.1.255,*)-(192.168.100.0-192.168.100.255,*) * ESP
tunn
448 384
```

## Приложение

## Конфигурация Hub

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
crypto isakmp keepalive 1 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 russia
aaa new-model
!
!
hostname GW1
enable password russia
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication pre-share
 group vko2
!
crypto isakmp key KEY address 20.20.20.12
!
crypto ipsec transform-set GOST esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set GOST
 set peer 20.20.20.12
!
interface GigabitEthernet0/0
 ip address 20.20.20.11 255.255.255.0
 crypto map CMAP
!
interface GigabitEthernet0/1
 ip address 192.168.100.11 255.255.255.0
!
!
ip route 192.168.1.0 255.255.255.0 20.20.20.12
!
end
```

## Конфигурация Spoke

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity address
crypto isakmp keepalive 1 3
crypto isakmp keepalive retry-count 3
username cscons privilege 15 password 0 russia
aaa new-model
!
!
hostname GW2
enable password russia
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr gost
 hash gost341112-256-tc26
 authentication pre-share
 group vko2
!
crypto isakmp key KEY address 20.20.20.11
!
crypto ipsec transform-set GOST esp-gost28147-4m-imit
!
ip access-list extended LIST
 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set GOST
 set peer 20.20.20.11
!
interface GigabitEthernet0/0
 ip address 20.20.20.12 255.255.255.0
 crypto map CMAP
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
!
!
ip route 192.168.100.0 255.255.255.0 20.20.20.11
!
end
```