Закрытое акционерное общество «НТЦ КОНТАКТ»

УТВЕРЖДАЮ

Директор

ЗАО «НТЦ КОНТАКТ»

_____А.А.Тепляков

1 декабря 2021 г.

КОМПЛЕКС ПРОГРАММНО-АППАРАТНЫЙ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «БАС»

Инструкция по настройке отказоустойчивого защищенного соединения при помощи протокола VRRP между двумя подсетями

СЮИК.465634.001 ИС45

Содержание

Настоящая инструкция распространяется на «Комплекс программно-аппаратный криптографической защиты информации «БАС» СЮИК.465634.001 (далее – ПАК «БАС»), предназначенный для защиты информации, циркулирующей в каналах передачи данных.

Настоящая инструкция является расширением Руководства по эксплуатации ПАК «БАС» СЮИК.465634.001 РЭ и предназначена для облегчения работы администратора при создании типовой схемы включения ПАК «БАС» для построения защищенного соединения.

Настоящая инструкция предназначена для администратора, имеющего навыки работы с ОС Linux и сетевым администрированием. Для понимания принципов работы ПАК «БАС» администратор должен ознакомиться с документом «Комплекс программно-аппаратный криптографической защиты информации «БАС». Руководство по эксплуатации» СЮИК.465634.001 РЭ прежде, чем преступить к настройкам согласно данной инструкции.

Инструкция описывает порядок настройки ПАК «БАС» для построения отказоустойчивого защищенного соединения при помощи протокола VRRP между двумя подсетями.

1 Описание соединения (стенда)

Схема включения ПАК «БАС» для построения защищенного соединения между двумя подсетями приведена на рисунке 1.

Данная схема может быть применена при объединении сети двух удаленных офисов или для подключения филиала к центральному офису.

Данный сценарий описывает подключение к защищаемой при помощи ПАК «БАС» 1 – ПАК «БАС» 2 подсети (ПК 1) другой защищаемой при помощи ПАК «БАС» 3 подсети (ПК 2). ПАК «БАС» 1 – ПАК «БАС» 2 объединены в кластер для создания отказоустойчивого решения при помощи протокола VRRP.

VRRP (от англ. **Virtual Router Redundancy Protocol**) – сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путём объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети.

Отказоустойчивость соединения достигается объединением нескольких ПАК «БАС» в кластер. Кластеру присваиваются виртуальные IP-адреса. Один из ПАК «БАС» становится главным (MASTER), а второй – второстепенным (BACKUP). Главному (MASTER) ПАК «БАС» присваивается виртуальный IP-адрес. Трафик, идущий на виртуальный адрес, обрабатывает главным (MASTER) ПАК «БАС». Если главный ПАК «БАС» становится недоступным, второстепенный ПАК «БАС» принимает состояние MASTER, и начинает обрабатывать трафик, заменяя собой отказавший. В зависимости от выполненных настроек, при восстановлении работоспособности первого ПАК «БАС», он может возвращать себе статус MASTER и начать заниматься обработкой трафика, либо принять статус BACKUP и ждать выхода из строя, который выполняет роль MASTER, и только после этого заменить его (второй вариант снижает количество переподключений).

После того как виртуальный IP-адрес перешел к другому владельцу (ПАК «БАС»), подключаемый ПАК «БАС» 3 должен выполнить повторную инициализацию соединения. Это реализуется при помощи протокола DPD.

DPD (от англ. **Dead Peer Detection**) – метод обнаружения неработающих одноранговых узлов обмена ключами (IKE). Метод использует шаблоны трафика IPsec, чтобы свести к минимуму количество сообщений, необходимых для подтверждения доступности однорангового узла. DPD используется для восстановления потерянных ресурсов в случае обнаружения мертвого однорангового узла, а также для выполнения аварийного переключения однорангового узла IKE.

Сообщения DPD отправляются только в том случае, если входящий трафик ESP не был замечен в течение времени dpddelay, указанного в настройках. Если входящий ESP трафик существует, то предполагает, что другой одноранговый узел все еще жив. Если другой одноранговый узел не отвечает на сообщения DPD, выполняется действие, настроенное в dpdaction.

Безопасное соединение обеспечивается путем шифрования передаваемых данных с использованием белорусских криптографических алгоритмов, определенных в СТБ 34.101.31-2020.

В данном сценарии для создания защищенного соединения будут использованы протоколы IKE (Internet Key Exchange) версии 2 с использованием расширенного протокола аутентификации EAP (Extensible Authentication Protocol), схема которого определена в СТБ 34.101.66-2014 п. 7.5 (EAP-BSTS).

Подключение ПАК «БАС» к сети передачи данных, а также к сети электропитания проводится в соответствии с Руководством по эксплуатации СЮИК.465634.001 РЭ.

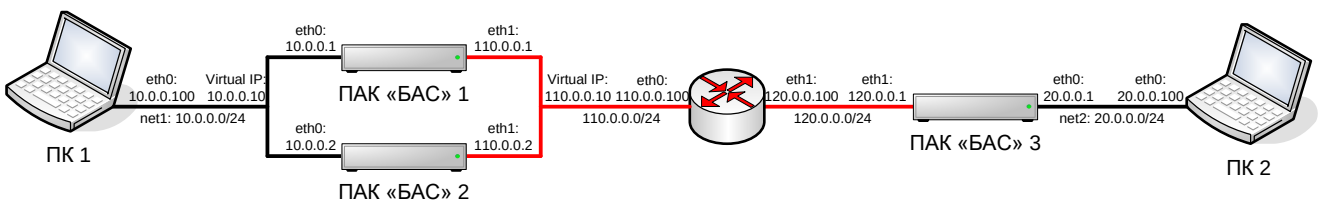

Рисунок 1 – Схема стенда

2 Настройка соединения (стенда)

Для настройки соединения (стенда) необходимо выполнить настройку всех его составляющих: настроить оба ПАК «БАС» и оба ПК из защищаемых подсетей.

Для настройки ПАК «БАС» необходимо выполнить следующие операции:

– смена пароля администратора;

– настройка сетевых интерфейсов;

– настройка даты и времени;

– управление ключевой информацией (генерация ключевой пары, экспорт открытого ключа из устройства в виде запроса на получение СОК и импорт открытого ключа в устройство в виде СОК);

– настройка программного обеспечения.

Для настройки ПК из защищаемых подсетей необходимо выполнить настройку сетевых интерфейсов.

2.1 Настройка ПАК «БАС» 1

Для настройки ПАК «БАС» 1 необходимо войти в его консоль, используя транспортный логин **server** и пароль **11111111**.

```
server login: server
Password:
server@server:~$
```

2.1.1 Смена пароля администратора

ВНИМАНИЕ: СМЕНА ТРАНСПОРТНОГО ПАРОЛЯ ЯВЛЯЕТСЯ ОБЯЗАТЕЛЬНОЙ

Для смены пароля необходимо воспользоваться командой **passwd**, после чего ввести транспортный пароль **11111111**, а затем задать и подтвердить новый. Пароль должен быть не менее 8 символов.

```
server@server:~$ passwd
Смена пароля для server.
current password:
Новый пароль :
Повторите ввод нового пароля :
passwd: пароль успешно обновлен
```

2.1.2 Настройка сетевых интерфейсов

Для настройки сетевых интерфейсов необходимо отредактировать файл **/etc/network/interfaces** при помощи текстового редактора **nano**, задав IP-адреса и маски интерфейсов.

```
server@server:~$ sudo nano /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

auto lo
iface lo inet loopback

iface eth0 inet static
address 10.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 110.0.0.1
netmask 255.255.255.0
gateway 110.0.0.100
auto eth1
```

Сохраните изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдите из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

2.1.3 Настройка VRRP

Поддержка ПАК «БАС» протокола VRRP осуществляется при помощи пакета **keepalived**.

Для настройки VRRP необходимо заполнить файл **/etc/keepalived/keepalived.conf** при помощи текстового редактора **nano**.

```
server@server:~$ sudo nano /etc/keepalived/keepalived.conf

# Configuration File for keepalived

# Группа интерфейсов.
# Если хотя бы один из этих интерфейсов перейдет в состояние FAULT,
# то будет считаться, что все перешли в состояние FAULT,
# и все ip перейдут на резервный сервер
vrrp_sync_group BAS {
        group {
               BAS_eth0
               BAS_eth1
        }
}

# Настройка VRRP
vrrp_instance BAS_eth0 {
# Интерфейс к которому будет привязан виртуальный IP
        interface eth0
# Номер группы (число от 1 до 255) одинаковый для всех серверов из кластера;
        virtual_router_id 10
# Приоритет хоста.
# Тот хост, который имеет больший приоритет, будет являться MASTER.
# По-умолчанию значение равно 100.
        priority 110
# Время в секундах между VRRP запросами между хостами в instance.
# По-умолчанию 1 секунда
        advert_int 1
# Действие при появлении сервера с более высоким приоритетом
# добавление параметра nopreempt вызовет переход IP-адреса,
# только после выхода из строя текущего устройства.
# Исключение параметра nopreempt из конфигурационного файла вызовет переход IP-адреса,
# после появлении сервера с более высоким приоритетома.
        nopreempt
# Метод аутентификации между хостами в кластере
        authentication {
               auth_type PASS
               auth_pass 12345678
        }
```

```
# Виртуальный отказоустойчивый IP-адрес
        virtual_ipaddress {
               10.0.0.10 dev eth0 label eth0:vip
        }
}

vrrp_instance BAS_eth1 {
        interface eth1
        virtual_router_id 20
        priority 110
        advert_int 1
        nopreempt
        authentication {
               auth_type PASS
               auth_pass 12345678
        }
        virtual_ipaddress {
               110.0.0.10 dev eth1 label eth1:vip
        }
}
```

2.1.4 Настройка даты и времени

Для установки даты и времени необходимо воспользоваться командой **date MMDDHHmmYYYY**

где:

MM – месяц;

DD – день;

HH – часы;

mm – минуты;

YYYY – год.

```
server@server:~$ sudo date 010112002022
[sudo] пароль для server:
Сб янв 1 12:00:00 +03 2022
```

Для вступления всех настроек в силу перезагрузите ПАК «БАС» 1.

```
server@server:~$ sudo reboot
```

2.1.5 Управление ключевой информацией

Для надежной аутентификации участники IPsec-соединения должны обладать неизвлекаемым личным ключом, а также парным ему открытым ключом в составе сертификата. В связи с этим необходимо выполнить:

– генерацию личного ключа;

– формирование запроса на выпуск сертификата открытого ключа;

– экспорт запроса на получение сертификата открытого ключа;

– импорт сертификата открытого ключа в ПАК «БАС».

Последовательность действия по управлению ключевой информацией описана в документе «Комплекс программно-аппаратный криптографической защиты информации «БАС». Инструкция по управлению ключевой информацией. СЮИК.465634.001 ИС21».

2.1.6 Настройка программного обеспечения

Настройка программного обеспечения ПАК «БАС» 1 заключается в редактировании файла **/usr/local/etc/ipsec.conf** при помощи текстового редактора **nano**.

```
server@server:~$ sudo nano /usr/local/etc/ipsec.conf

config setup
        charondebug = "ike 1, lib 1, cfg 1, cnt 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 1h
        rekeymargin = 5m
        mobike = no

        ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
        esp = belt_cfb-belt_mac
```

```
        left = 100.0.0.10
        leftsubnet = 10.0.0.0/24
        leftid = %any
        leftcert = cert00001.cer
        leftauth = eap-bsts
        auto = route

        dpdaction = clear
        closeaction = clear

conn Claster-BAS3
        right = 120.0.0.1
        rightsubnet = 20.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightsendcert = never
```

Сохраните изменения в файле, нажав сочетание клавиш **Ctrl+O**, и выйдите из текстового редактора **nano**, нажав сочетание клавиш **Ctrl+X**.

Запустите (перезапустите) IPsec соединение

```
server@server:~$ sudo ipsec restart
Stopping strongSwanCont IPsec...
Starting strongSwanCont 5.8.4 IPsec [starter]...
```

Убедиться в том, что программное обеспечение ПАК «БАС» 1 подгрузило сертификат открытого ключа и сопоставило его с личным ключом, можно при помощи команды **ipsec listcerts**.

```
server@server:~$ sudo ipsec listcerts
List of X.509 End Entity Certificates:
  subject:     "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-
аппаратный криптографической защиты информации "БАС". Сервер защиты"
  issuer:      "CN=УЦ для тестирования, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
  validity:    not before   Jan 1 00:00:00 2021, ok
               not after    Jan 1 00:00:00 2023, ok (expired in 365 days)
  serial:      01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  certificatePolicies:
               1.2.112.0.2.0.34.101.78.2.70
  authkeyId:   01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  sudjkeyId:   01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  pubkey:      BIGN 512 bits, has private key
  keyid:       01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  subjkey:     01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
```

О том, что программное обеспечение ПАК «БАС» 1 верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key**.

2.2 Настройка ПАК «БАС» 2

Настройка ПАК «БАС» 2 проводится аналогично ПАК «БАС» 1, при этом:

– файл **/etc/network/interfaces** будет иметь вид:

```
server@server:~$ sudo nano /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

auto lo
iface lo inet loopback

iface eth0 inet static
address 10.0.0.2
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 110.0.0.2
netmask 255.255.255.0
gateway 110.0.0.100
auto eth1
```

– файл **/etc/keepalived/keepalived.conf** будет иметь вид:

```
server@server:~$ sudo nano /etc/keepalived/keepalived.conf

# Configuration File for keepalived

# Группа интерфейсов.
# Если хотя бы один из этих интерфейсов перейдет в состояние FAULT,
# то будет считаться, что все перешли в состояние FAULT,
# и все ip перейдут на резервный сервер
vrrp_sync_group BAS {
        group {
               BAS_eth0
               BAS_eth1
        }
}

# Настройка VRRP
vrrp_instance BAS_eth0 {
# Интерфейс к которому будет привязан виртуальный IP
        interface eth0
# Номер группы (число от 1 до 255) одинаковый для всех серверов из кластера;
        virtual_router_id 10
```

```
# Приоритет хоста.
# Тот хост, который имеет больший приоритет, будет являться MASTER.
# По-умолчанию значение равно 100.
        priority 100
# Время в секундах между VRRP запросами между хостами в instance.
# По-умолчанию 1 секунда
        advert_int 1
# Действие при появлении сервера с более высоким приоритетом
# добавление параметра nopreempt вызовет переход IP-адреса,
# только после выхода из строя текущего устройства.
# Исключение параметра nopreempt из конфигурационного файла вызовет переход IP-адреса,
# после появлении сервера с более высоким приоритетома.
        nopreempt
# Метод аутентификации между хостами в кластере
        authentication {
                auth_type PASS
                auth_pass 12345678
        }
# Виртуальный отказоустойчивый IP-адрес
        virtual_ipaddress {
                10.0.0.10 dev eth0 label eth0:vip
        }
}

vrrp_instance BAS_eth1 {
        interface eth1
        virtual_router_id 20
        priority 100
        advert_int 1
        nopreempt
        authentication {
                auth_type PASS
                auth_pass 12345678
        }
        virtual_ipaddress {
                110.0.0.10 dev eth1 label eth1:vip
        }
}
```

– файл **/usr/local/etc/ipsec.conf** будет иметь вид:

```
server@server:~$ sudo nano /usr/local/etc/ipsec.conf

config setup
        charondebug = "ike 1, lib 1, cfg 1, cnt 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 1h
```

```
        rekeymargin = 5m
        mobike = no

        ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
        esp = belt_cfb-belt_mac

        left = 100.0.0.10
        leftsubnet = 10.0.0.0/24
        leftid = %any
        leftcert = cert00002.cer
        leftauth = eap-bsts
        auto = route

        dpdaction = clear
        closeaction = clear

conn Claster-BAS3
        right = 120.0.0.1
        rightsubnet = 20.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightsendcert = never
```

2.3 Настройка ПАК «БАС» 3

Настройка ПАК «БАС» 3 проводится аналогично ПАК «БАС» 1, с расширенными настройками протокола DPD,при этом:

– файл **/etc/network/interfaces** будет иметь вид:

```
server@server:~$ sudo nano /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

auto lo
iface lo inet loopback

iface eth0 inet static
address 20.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 120.0.0.1
netmask 255.255.255.0
gateway 120.0.0.100
auto eth1
```

– файл **/usr/local/etc/ipsec.conf** будет иметь вид:

```
server@server:~$ sudo nano /usr/local/etc/ipsec.conf

config setup
        charondebug = "ike 1, lib 1, cfg 1, cnt 1"

# Add connections here.
conn %default
        keyexchange = ikev2
        ikelifetime = 24h
        lifetime = 1h
        rekeymargin = 5m
        mobike = no

        ike = belt_cfb-belt_hmac-prfbrng_hmac-ecp256bign-keyrep
        esp = belt_cfb-belt_mac

        left = 120.0.0.1
        leftsubnet = 20.0.0.0/24
        leftid = %any
        leftcert = cert00003.cer
        leftauth = eap-bsts
        auto = route

        dpdaction = clear
        closeaction = clear
        dpddelay = 10s

conn BAS3-Claster
        right = 110.0.0.10
        rightsubnet = 10.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightsendcert = never
```

2.3.1 Настройка DPD

Время начала работы протокола DPD, а также действия, выполняемые по результатам работы, были определен в файле **/usr/local/etc/ipsec.conf**. Протокол DPD начнет работу через 10 секунд (dpddelay = 10s) после того, как входящий ESP трафик будет отсутствовать. Если за время работы протокола DPD удаленный узел не начнет отвечать на DPD запросы, будет считаться, что он неработоспособен, и

туннель будет удален (dpdaction = clear). После чего будут установлены ловушки ожидания трафика, подпадающие под политику IPsec (auto = route). При появлении такого трафика будет предпринята попытка установить новое IPsec соединение.

ПАК «БАС» позволяет выполнить дополнительные настройки времени работы DPD. Уменьшение времени работы протокола DPD повышает доступность информационной системы, так как уменьшается время отсутствия IPsec туннеля (в случае реального сбоя), но при этом увеличивается количество необязательных служебных обменов при нормальной работе. Увеличение времени работы протокола DPD, наоборот, приведет к уменьшению количество необязательных служебных обменов при нормальной работе, но увеличивается время отсутствия IPsec туннеля (в случае реального сбоя).

Время работы протокола DPD должно выбираться Администратором безопасности информационной системы с учетом параметров описанных выше.

Относительное время ожидания повторной передачи (ΔT_{dpd}) (время между n и n-1 DPD запросом) рассчитывается по формуле:

$$\Delta T_{dpd} = t \cdot b^{(n-1)}$$

Абсолютное время работы протокола DPD является суммой времени между каждой из n попыток повторной передачи.

Время ожидания повторной передачи в демоне IKE можно настроить глобально с помощью параметров в файле **/usr/local/etc/strongswan.conf**.

Следующие ключи используются для настройки поведения повторной передачи:

Параметр	Значение по умолчанию	Описание
charon.retransmit_tries	5	Количество повторных передач до принятия решения об отказе (n)
charon.retransmit_timeout	4.0	Время ожидания ответа в секундах (t)
charon.retransmit_base	1.8	База экспоненциального отката (b)

Таким образом:

Количество повторных передач	Формула	Относительное время ожидания	Абсолютное время ожидания
1	$4 \cdot 1{,}8^0$	4 с	4 с
2	$4 \cdot 1{,}8^1$	7 с	11 с
3	$4 \cdot 1{,}8^2$	13 с	24 с
4	$4 \cdot 1{,}8^3$	23 с	47 с
5	$4 \cdot 1{,}8^4$	42 с	89 с
и т. д.	$4 \cdot 1{,}8^5$	76 с	165 с

Следовательно, при использовании настроек по умолчанию абсолютное время работы протокола DPD составит 165 секунд. А время до повторной попытки установить новое IPsec соединение еще больше на значение параметра dpddelay.

Сделаем расчет необходимых настроек из предположения, что максимально допустимое время отсутствия IPsec в информационной системе составляет 30 секунд.

Выберем количество повторных передач до принятия решения об отказе (n) равное 3, а база экспоненциального отката (b) равную 1.

Таким образом:

Количество повторных передач	Формула	Относительное время ожидания	Абсолютное время ожидания
1	$4 \cdot 1^0$	4 с	4 с
2	$4 \cdot 1^1$	4 с	8 с
3	$4 \cdot 1^2$	4 с	12 с
и т. д.	$4 \cdot 1^3$	4 с	16 с

Следовательно, при использовании выбранных настроек время до повторной попытки установить новое IPsec соединение составит 16 + 10 = 26 секунд.

Таким образов, файл **/usr/local/etc/strongswan.conf** будет иметь вид:

```
server@server:~$ sudo nano /usr/local/etc/strongswan.conf
charon {
        load_modular = yes
        send_vendor_id = yes
        retransmit_tries = 3
        retransmit_base = 1
        plugins {
               include strongswan.d/charon/*.conf
        }
}
```

2.4 Настройка ПК 1

Настройка ПК 1 заключается в настройке сетевого интерфейса. В ПК 1 необходимо установить IP-адрес, входящий в защищаемую подсеть **10.0.0.0/24**, а в качестве основного шлюза указать IP-адрес ПАК «БАС» 1:

IP-адрес: 10.0.0.100

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.0.10

2.5 Настройка ПК 2

Настройка ПК 2 аналогична ПК 1:

IP-адрес: 20.0.0.10

Маска подсети: 255.255.255.0

Основной шлюз: 20.0.0.1

3 Проверка работоспособности

Для проверки работоспособности соединения (стенда) необходимо с ПК 2 выполнить **ping** ПК 1.

```
C:\Documents and Settings\Администратор>ping 10.0.0.100

Обмен пакетами с 10.0.0.100 по 32 байт:

Превышен интервал ожидания для запроса.
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64

Статистика Ping для 10.0.0.100:
    Пакетов: отправлено = 4, получено = 3, потеряно = 1 (25% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

При этом первый пакет инициализирует IPsec соединение, а последующие передаются по защищенному туннелю.

Убедиться в том, что передача данных идет по защищенному туннелю, можно, подав команду **ipsec statusall** в командную строку ПАК «БАС» 3.

```
server@server:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.4, Linux 4.19.194-ckt-bas, x86_64):
uptime: 60 seconds, since Jan 1 13:00:00 2022
malloc: sbrk 2297856, mmap 0, used 260720, free 2037136
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
loaded plugins: charon random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 dnskey pem fips-prf gmp xcbc cmac hmac contactcrypto usbbar bpki attr kernel-netlink resolve socket-default stroke vici updown xauth-generic dhcp counters eap-bsts eap-bpace
Listening IP addresses:
  20.0.0.1
  120.0.0.1
Connections:
BAS3-Claster:  120.0.0.1...110.0.0.10 IKEv2, dpddelay=10s
BAS3-Claster:  local: [CN=BAS00003, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты] uses EAP_BSTS authentication
BAS3-Claster:  cert: "CN=BAS00003, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS3-Claster:  remote: uses EAP_BSTS authentication
BAS3-Claster:  child: 20.0.0.0/24 === 10.0.0.0/24 TUNNEL, dpdaction = clear
```

```
Routed Connections:
BAS3-Claster {1}:     ROUTED, TUNNEL, requid 1
BAS3-Claster {1}:     20.0.0.0/24 === 10.0.0.0/24
Security Associations (1 up, 0 connecting):
BAS3-Claster[1]:      ESTABLISHED 15 seconds ago, 120.0.0.1[CN=BAS00003, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]...110.0.0.10[CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]
BAS3-Claster[1]:      IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP reauthentication in 23 hours
BAS3-Claster[1]:      IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECP_256_BIGN
BAS3-Claster{1}:      INSTALLED, TUNNEL, requid, ESP SPIs: cbe8a626_i c9e7890e_o
BAS3-Claster{1}:      BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o (3 pkts, 13s ago), rekeying in 55 minutes
BAS3-Claster{1}:      20.0.0.0/24 === 10.0.0.0/24
server@server:~$
```

Как видно из последних двух строк, установлен туннель между подсетями **20.0.0.0/24 === 10.0.0.0/24**, по туннелю было передано по 3 пакета в каждую сторону (**ping**), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**. Туннель установлен между ПАК «БАС» 3 и ПАК «БАС» 1, это видно по информации из сертификатов.

Выполним с ПК 2 бесконечный **ping** ПК 1. сымитирует сбой электропитания, отключив ПАК «БАС» 1 от сети.

```
C:\Documents and Settings\Администратор>ping 10.0.0.100 -t

Обмен пакетами с 10.0.0.100 по 32 байт:

Превышен интервал ожидания для запроса.
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Превышен интервал ожидания для запроса.
...
Превышен интервал ожидания для запроса.
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.100: число байт=32 время<1мс TTL=64
...
```

Ответ на ping отсутствовал 26 секунд, после чего возобновился.

Узнать о состоянии IPsec соединения можно, подав команду **ipsec statusall** в командную строку ПАК «БАС» 3.

```
server@server:~$ sudo ipsec statusall
Status of IKE charon daemon (strongSwan 5.8.4, Linux 4.19.194-ckt-bas, x86_64):
uptime: 60 seconds, since Jan 1 13:00:00 2022
malloc: sbrk 2297856, mmap 0, used 260720, free 2037136
worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 3
loaded plugins: charon random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8
pkcs12 dnskey pem fips-prf gmp xcbc cmac hmac contactcrypto usbbar bpki attr kernel-netlink
resolve socket-default stroke vici updown xauth-generic dhcp counters eap-bsts eap-bpace
Listening IP addresses:
  20.0.0.1
  120.0.0.1
Connections:
BAS3-Claster:  120.0.0.1...110.0.0.10 IKEv2, dpddelay=10s
BAS3-Claster:  local:  [CN=BAS00003, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты] uses EAP_BSTS
authentication
BAS3-Claster:  cert:  "CN=BAS00003, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS3-Claster:  remote: uses EAP_BSTS authentication
BAS3-Claster:  child: 20.0.0.0/24 === 10.0.0.0/24 TUNNEL, dpdaction = clear
Routed Connections:
BAS3-Claster {1}:     ROUTED, TUNNEL, reqid 1
BAS3-Claster {1}:     20.0.0.0/24 === 10.0.0.0/24
Security Associations (1 up, 0 connecting):
BAS3-Claster[1]:      ESTABLISHED 15 seconds ago, 120.0.0.1[CN=BAS00003, C=BY, L=г.Минск,
O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации
"БАС". Сервер защиты]...110.0.0.10[CN=BAS00002, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт",
D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]
BAS3-Claster[1]:      IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP
reauthentication in 23 hours
BAS3-Claster[1]:      IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECP_256_BIGN
BAS3-Claster{1}:      INSTALLED, TUNNEL, reqid, ESP SPIs: cbe8a626_i c9e7890e_o
BAS3-Claster{1}:      BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o
(3 pkts, 13s ago), rekeying in 55 minutes
BAS3-Claster{1}:      20.0.0.0/24 === 10.0.0.0/24
server@server:~$
```

Как видно из последних двух строчек, установлен туннель между подсетями **20.0.0.0/24 === 10.0.0.0/24**, по туннелю было передано по 3 пакета в каждую сторону (**ping**), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**. При этом туннель установлен между ПАК «БАС» 3 и ПАК «БАС» 2, это видно по информации из сертификатов.

ПАК «БАС» 2 при помощи протокола VRRP установил сбой на ПАК «БАС» 1 и заменил его, приняв на себя роль MASTER. ПАК «БАС» 3, инициировал DPD обмен, по окончание которого удалил туннель и установил новый, с ПАК «БАС» 2.