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 защищенного соединения между двумя подсетями с использованием встроенного межсетевого экрана

СЮИК.465634.001 ИС37

Подп. и дата | Инв. № дубл. | Взам. Инв. № | Подп. и дата | Инв. № подл.

Содержание

1 Описание соединения (стенда) 4

2 Настройка стенда для определения необходимости межсетевого экрана 6

2.1 Смена пароля администратора 6

2.2 Настройка сетевых интерфейсов ПАК «БАС» 1 7

2.3 Настройка ПК 1 7

2.4 Настройка сетевых интерфейсов ПАК «БАС» 2 8

2.5 Настройка ПК 2 8

3 Проверка работоспособности стенда 9

4 Настройка межсетевого экрана 10

4.1 Настройка межсетевого экрана ПАК «БАС» 1 11

4.2 Настройка межсетевого экрана ПАК «БАС» 2 12

5 Управление ключевой информацией 13

6 Настройка программного обеспечения ПАК «БАС» 14

6.1 Настройка ПАК «БАС» 1 14

6.2 Настройка ПАК «БАС» 2 16

7 Проверка работоспособности 17

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 защищенного соединения между двумя подсетями.

1 Описание соединения (стенда)

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

Данный сценарий описывает применение встроенного в ПАК «БАС» межсетевого экрана на примере построения защищенного соединения между двумя подсетями. Встроенный межсетевой экран может быть применен к любой схеме подключения ПАК «БАС», при использовании принципов, описанных в данном сценарии.

Межсетевой экран ПАК «БАС» предназначен для осуществления контроля и фильтрации проходящего через него сетевого трафика в соответствии с заданными правилами.

ПАК «БАС» обеспечивает межсетевую защиту данных при помощи встроенного в ядро ОС Linux компонента Netfilter.

Netfilter – межсетевой экран (брандмауэр), компонент ядра ОС Linux, обеспечивающий фильтрацию и модификацию трафика.

Управление межсетевым экраном Netfilter производится из пространства пользователя с помощью команд iptables.

Iptables – название пользовательской утилиты (запускаемой из командной строки), предназначенной для управления системой Netfilter. С её помощью администраторы создают и изменяют правила, управляющие фильтрацией и перенаправлением пакетов.

Описание работы и настроек встроенного межсетевого экрана представлено в документе «Комплекс программно-аппаратный криптографической защиты информации «БАС». Встроенное программное обеспечение. Межсетевой экран. Руководство оператора» BY.СЮИК.00368-02 34 01 или в документации на iptables в сети Internet.

ПАК «БАС» поставляется с ненастроенным межсетевым экраном. Его настройка должна выполняться Администратором исходя из потребностей.

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.

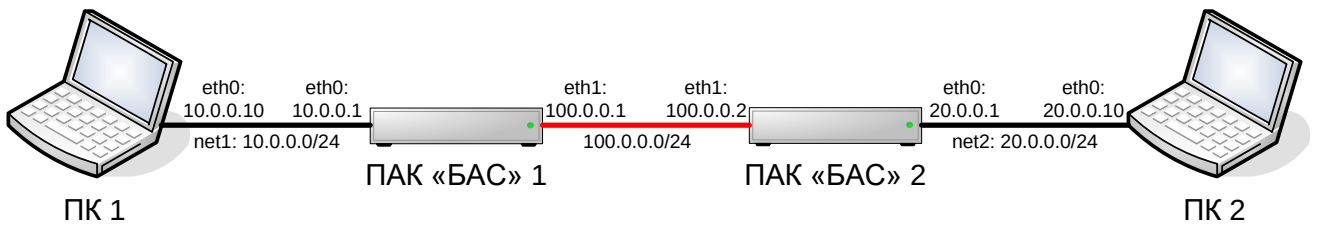

Рисунок 1 – Схема стенда

2 Настройка стенда для определения необходимости межсетевого экрана

Перед настройкой межсетевого экрана необходимо собрать и выполнить настройку всех его составляющих стенда: настроить оба ПАК «БАС» и оба ПК из защищаемых подсетей.

Для предварительной настройки ПАК «БАС» необходимо выполнить следующие операции:

– смена пароля администратора;

– настройка сетевых интерфейсов.

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

2.1 Смена пароля администратора

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

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

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
```

2.2 Настройка сетевых интерфейсов ПАК «БАС» 1

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 100.0.0.1
netmask 255.255.255.0
gateway 100.0.0.2
auto eth1
```

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

2.3 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: 10.0.0.10

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.0.1

2.4 Настройка сетевых интерфейсов ПАК «БАС» 2

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 20.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 100.0.0.2
netmask 255.255.255.0
gateway 100.0.0.1
auto eth1
```

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

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 стенда

ПАК «БАС» является VPN-сервером, в связи с этим он обеспечивает маршрутизацию транзитных IP-пакетов, т.е. пакетов не предназначенных для него, или IP-форвардинг. Пакет, пришедший на один порт ПАК «БАС» и не предназначенный ему, пройдет через ПАК «БАС» и выйдет через другой порт.

Для проверки IP-форвардинга в ПАК «БАС» необходимо с ПК 1 выполнить **ping** ПАК «БАС» 2.

```
C:\Documents and Settings\Администратор>ping 100.0.0.2

Обмен пакетами с 100.0.0.2 по 32 байт:
Ответ от 100.0.0.2: число байт=32 время<1мс TTL=64
Ответ от 100.0.0.2: число байт=32 время<1мс TTL=64
Статистика Ping для 100.0.0.2:
    Пакетов: отправлено = 2, получено = 2, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
```

Или с ПАК «БАС» 1 выполнить **ping** ПК 2.

```
server@server:~$ ping 20.0.0.10
PING 20.0.0.10 (20.0.0.10) 56(84) bytes of data
64 bytes from 20.0.0.10: icmp_seq=1 ttl=63 times=1.00 ms
64 bytes from 20.0.0.10: icmp_seq=1 ttl=63 times=1.00 ms
^C
--- 20.0.0.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss. Time 4 ms
rtt min/avg/max/mdev = 1.00/1.00/1.00/0 ms
```

Таким образом ПАК «БАС» 1 пропускает через себя пакеты (не предназначенные для него) от ПК 1 к ПАК «БАС» 2 и в обратном направлении, а ПАК «БАС» 2 пропускает через себя пакеты (не предназначенные для него) от ПК 2 к ПАК «БАС» 1 и в обратном направлении.

После установки IPsec соединения будет установлена политики шифрования трафика, и все пакеты от ПК 1 к ПК 2 и в обратном направлении будут подпадать под эту политику и будут зашифрованы.

Пакеты, не подпадающие под политику шифрования, будут подпадать под правила IP-форвардинга.

4 Настройка межсетевого экрана

Из описанного выше примера очевидно, что могут существовать две угрозы:

– несанкционированная передача данных через ПАК «БАС» (как во внутреннею, так и во внешнюю сеть);

– несанкционированное подключение к самому ПАК «БАС».

Угроза несанкционированной передачи данных через ПАК «БАС» может быть снята путем блокировки возможности передачи данных между портами. Для этого необходимо передать межсетевому экрану следующие команды:

```
server@server:~$ sudo iptables -A FORWARD -i eth0 -o eth1 -j DROP
server@server:~$ sudo iptables -A FORWARD -i eth1 -o eth0 -j DROP
```

Данные команды заблокируют передачу данных как от порта eth0 к eth1, так и от eth1 к eth0. Если ПАК «БАС» имеет более 2 портов, то данные команды необходимо применить ко всем используемым портам.

Однако, данные настройки межсетевого экрана приведут к тому, что после установки IPsec-соединения ПАК «БАС» не будет пропускать даже трафик, подпадающий под политику шифрования. Данная проблема решается специальными настройками программного обеспечения.

Угроза несанкционированное подключение к самому ПАК «БАС» может быть снята путем блокировки порта, выходящего во внешнюю сеть. Для этого необходимо передать межсетевому экрану следующую команду:

```
server@server:~$ sudo iptables -A INPUT -i eth1 -j DROP
```

Однако данные настройки межсетевого экрана приведут к тому, что ПАК «БАС» будет отбрасывать все пакеты, в том числе и IPsec. Для работы IPsec необходимо предварительно разрешить работу протокола UDP на 500 и 4500 портах, а также 50 протокол (протокол ESP). Для этого необходимо передать межсетевому экрану следующие команды:

```
server@server:~$ sudo iptables -A INPUT -p udp --dport 500 -j ACCEPT
server@server:~$ sudo iptables -A INPUT -p udp --dport 4500 -j ACCEPT
server@server:~$ sudo iptables -A INPUT -p 50 -j ACCEPT
```

4.1 Настройка межсетевого экрана ПАК «БАС» 1

Настройка межсетевого экрана может быть выполнена путем редактирования файл **/etc/network/interfaces** при помощи текстового редактора **nano**. В этом случае настройки межсетевого экрана установятся сразу после конфигурирования сетевых 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 100.0.0.1
netmask 255.255.255.0
gateway 100.0.0.2
up iptables -A INPUT -p udp --dport 500 -j ACCEPT
up iptables -A INPUT -p udp --dport 4500 -j ACCEPT
up iptables -A INPUT -p 50 -j ACCEPT
up iptables -A INPUT -i eth1 -j DROP
up iptables -A FORWARD -i eth0 -o eth1 -j DROP
up iptables -A FORWARD -i eth1 -o eth0 -j DROP
auto eth1
```

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

4.2 Настройка межсетевого экрана ПАК «БАС» 2

Настройка межсетевого экрана может быть выполнена путем редактирования файл **/etc/network/interfaces** при помощи текстового редактора **nano**. В этом случае настройки межсетевого экрана установятся сразу после конфигурирования сетевых 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 20.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 100.0.0.2
netmask 255.255.255.0
gateway 100.0.0.1
up iptables -A INPUT -p udp --dport 500 -j ACCEPT
up iptables -A INPUT -p udp --dport 4500 -j ACCEPT
up iptables -A INPUT -p 50 -j ACCEPT
up iptables -A INPUT -i eth1 -j DROP
up iptables -A FORWARD -i eth0 -o eth1 -j DROP
up iptables -A FORWARD -i eth1 -o eth0 -j DROP
auto eth1
```

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

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:

– настройку даты и времени;

– генерацию личного ключа;

– формирование запроса на выпуск сертификата открытого ключа;

– экспорт запроса на получение сертификата открытого ключа;

– импорт сертификата открытого ключа в ПАК «БАС».

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
```

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».

6 Настройка программного обеспечения ПАК «БАС»

Настройка программного обеспечения ПАК «БАС» при использовании межсетевого экрана практически не отличается от настройки без него. При настройках необходимо сообщить IPsec-демону, что на ПАК «БАС» настроен межсетевой экран. В этом случае, после установки IPsec-соединения программное обеспечение автоматически выполнит настройки межсетевому экрану, разрешающие прохождение трафика, подпадающего под политику шифрования. Данные настройки также автоматически будут отменены, после того как IPsec-туннель перестанет существовать. Сообщения IPsec-демону об настроенном межсетевом экране передается в параметрах **leftfirewall** и **rightfirewall**.

6.1 Настройка ПАК «БАС» 1

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 = 100.0.0.1
        leftsubnet = 10.0.0.0/24
        leftid = %any
        leftcert = cert00001.cer
```

```
        leftauth = eap-bsts
        leftfirewall = yes
        auto = route

        dpdaction = clear
        closeaction = clear

conn BAS1-BAS2
        right = 100.0.0.2
        rightsubnet = 20.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightfirewall = yes
        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**.

6.2 Настройка ПАК «БАС» 2

Настройка ПАК «БАС» 2 проводится аналогично ПАК «БАС» 1, при этом 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 = 100.0.0.2
        leftsubnet = 20.0.0.0/24
        leftid = %any
        leftcert = cert00002.cer
        leftauth = eap-bsts
        leftfirewall = yes
        auto = route

        dpdaction = clear
        closeaction = clear

conn BAS2-BAS1
        right = 100.0.0.1
        rightsubnet = 10.0.0.0/24
        rightid = %any
        rightauth = eap-bsts
        rightfirewall = yes
        rightsendcert = never
```

7 Проверка работоспособности

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

```
C:\Documents and Settings\Администратор>ping 10.0.0.10

Обмен пакетами с 10.0.0.10 по 32 байт:

Превышен интервал ожидания для запроса.
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64
Ответ от 10.0.0.10: число байт=32 время<1мс TTL=64

Статистика Ping для 10.0.0.10:
    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» 1 или ПАК «БАС» 2.

```
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:
  10.0.0.1
  100.0.0.1
Connections:
BAS1-BAS2:     100.0.0.1...100.0.0.2 IKEv2, dpddelay=30s
BAS1-BAS2:     local: [CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты] uses EAP_BSTS authentication
BAS1-BAS2:     cert: "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS1-BAS2:     remote: uses EAP_BSTS authentication
BAS1-BAS2:     child: 10.0.0.0/24 === 20.0.0.0/24 TUNNEL, dpdaction = clear
```

```
Routed Connections:
BAS1-BAS2{1}:  ROUTED, TUNNEL, requid 1
BAS1-BAS2{1}:  10.0.0.0/24 === 20.0.0.0/24
Security Associations (1 up, 0 connecting):
BAS1-BAS2[1]:  ESTABLISHED 15 seconds ago, 100.0.0.1[CN=BAS00001, C=BY, L=г.Минск, O=ЗАО
"НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС".
Сервер защиты]...100.0.0.2[CN=BAS00002, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]
BAS1-BAS2[1]:  IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP reauthentication
in 23 hours
BAS1-BAS2[1]:  IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECP_256_BIGN
BAS1-BAS2{1}:  INSTALLED, TUNNEL, requid, ESP SPIs: cbe8a626_i c9e7890e_o
BAS1-BAS2{1}:  BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o (3 pkts,
13s ago), rekeying in 55 minutes
BAS1-BAS2{1}:  10.0.0.0/24 === 20.0.0.0/24
server@server:~$
```

Как видно из последних двух строк, установлен туннель между подсетями **10.0.0.0/24 === 20.0.0.0/24**, по туннелю было передано по 3 пакета в каждую сторону (**ping**), защищенных при помощи алгоритмов **BELT_CFB_256/BELT_MAC**.

При этом, если выполнить запрос **ping**, не подпадающий под политику шифрования, например, с ПК 1 выполнить **ping** ПАК «БАС» 2 или с ПАК «БАС» 1 выполнить **ping** ПК 2, то ответы получены не будут. Данные запросы **ping** не будут переданы через ПАК «БАС».