

**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 фильтрацией по полям сертификатов  
СЮИК.465634.001 ИС34**

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

## Содержание

1	Описание соединения (стенда) .....	4
2	Настройка соединения (стенда) .....	6
2.1	Настройка ПАК «БАС» 1 .....	6
2.1.1	Смена пароля администратора .....	7
2.1.2	Настройка сетевых интерфейсов .....	7
2.1.3	Настройка даты и времени .....	8
2.1.4	Управление ключевой информацией .....	8
2.1.5	Настройка программного обеспечения .....	9
2.2	Настройка ПАК «БАС» 2 .....	11
2.3	Настройка ПАК «БАС» 3 .....	13
2.4	Настройка ПК 1 .....	15
2.5	Настройка ПК 2 .....	15
2.6	Настройка ПК 3 .....	15
2.7	Настройка ПК 4 .....	15
3	Проверка работоспособности .....	16

Подп. и дата		Инв. № дубл.		Взам. Инв. №		Подп. и дата		
Инв. № подл.	Разраб.	Воронцова	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>		
Пров.	Фёдоров					Лит.	Лист	Листов
Н. контр.	Васильев					0 0 <sub>1</sub>	2	18
Утв.	Тепляков					<b>ЗАО «НТЦ КОНТАКТ»</b>		
						Комплекс программно-аппаратный криптографической защиты информации «БАС» Инструкция по настройке защищенного соединения между двумя подсетями с фильтрацией по полям сертификатов		

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 приступить к настройкам согласно данной инструкции.

Инструкция описывает порядок настройки ПАК «БАС» для построения защищенного соединения между двумя подсетями.

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

Изм	Лист	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>	Лист
						3

## 1 Описание соединения (стенда)

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

Данный сценарий может являться продолжением сценария динамически расширяемой сети или сети с использованием динамического NAN. Т.е. сети в которой заранее неизвестен IP-адрес с которого будет осуществляться подключение. При этом известен, например, серийный номер ПАК «БАС», который осуществляет защиту, или город, в котором располагается филиал.

Рассмотрим ситуация, когда имеется центральный офис в Минске, с ресурсами, размещенными на ПК1 и ПК4, защита выполняется при помощи ПАК «БАС» 1, а также два филиала: в Гомеле и Витебске, находящиеся за динамическими NAT, защита выполняется при помощи ПАК «БАС» 2 и ПАК «БАС» 3 соответственно. Причем пользователям из Гомеля ПК2 необходимо обеспечить доступ к ресурсам, находящимся на ПК1, но не давать доступ к ресурсам на ПК4, а пользователям из Витебска ПК3 необходимо обеспечить доступ к ресурсам, находящимся на ПК4, но не давать доступ к ресурсам на ПК1.

Проблема данного сценария в том, что заранее не известно с какого адреса будет выполняться IPsec подключение. Поэтому сложно настроить IPsec политики. Однако известны некоторые данные устройств: их серийный номер и место дислокации.

При установке IPsec соединения ПАК «БАС» высылает партнеру запрос на установку, в котором содержится идентификатор устройства (соединения) – указывается в параметре **leftid**. При использовании для аутентификации сертификатов открытого ключа в качестве идентификатора используется поле **subjectAltName** из сертификата, при его отсутствии поле **subject**.

Выполним настройку IPsec соединения с использованием фильтрации значений полей сертификата для маршрутизации трафика.

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм	Лист	№ докум.	Подп.	Дата

**СЮИК.465634.001 ИС34**

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

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.

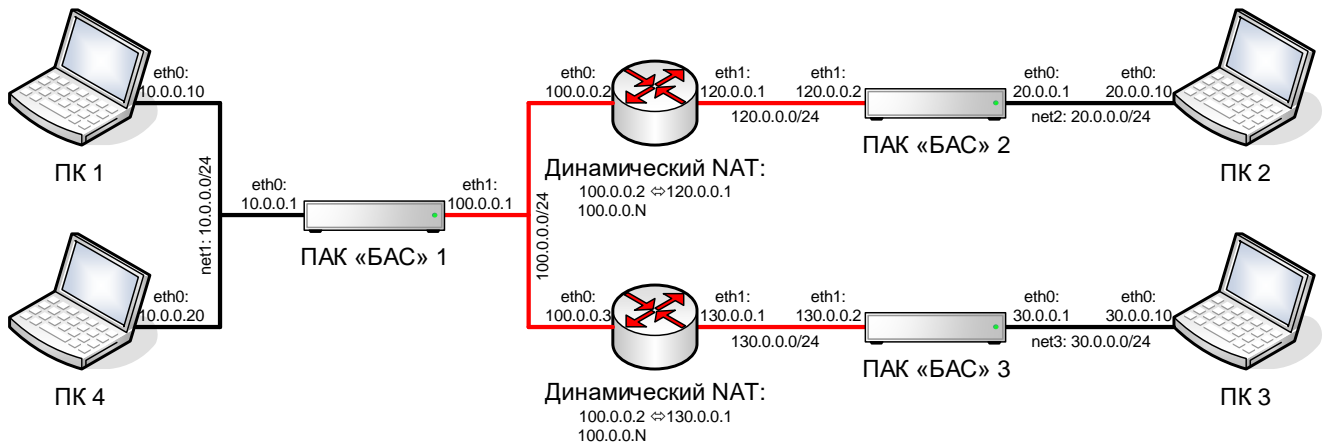


Рисунок 1 – Схема стенда

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

Изм.	Лист	№ докум.	Подп.	Дата

СЮИК.465634.001 ИС34

## 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 **1111111**.

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

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС34	Лист
						6
Изм	Лист	№ докум.	Подп.	Дата		

## 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 100.0.0.1
netmask 255.255.255.0
auto eth1
```

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

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

Изм.	Лист	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>	Лист
						7

### 2.1.3 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
```

### 2.1.4 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».

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

Изм.	Лист	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>	Лист
						8



## 2.1.5 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 = 100.0.0.1
    leftid = %any
    leftcert = cert00001.cer
    leftauth = eap-bsts
    auto = route
    dpdaction = clear
    closeaction = clear

conn BAS1-BAS2
    leftsubnet = 10.0.0.10/32
    right = %any
    rightsubnet = 20.0.0.0/24
    rightid = "CN=BAS00002, C=BY, L=г.Гомель, O=*, D=*"
    rightauth = eap-bsts
    rightsendcert = never

conn BAS1-BAS3
    leftsubnet = 10.0.0.20/32
    right = %any
    rightsubnet = 30.0.0.0/24
    rightid = "CN=BAS00003, C=BY, L=г.Витебск, O=*, D=*"
    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**.

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм	Лист	№ докум.	Подп.	Дата

**СЮИК.465634.001 ИС34**

## 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**.

Значения поля **subject** сертификата устанавливаются при формировании запроса на выпуск сертификата. Для данного сертификата поле **subject** имеет значение "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты". Данное значение и будет использоваться в качестве идентификатора устройства при IPsec соединении.

Ожидаемые значения полей **subject** ПАК «БАС» 2 и ПАК «БАС» 3 указаны в параметрах **rightid**. При этом значения значимых полей указаны полностью, а поля, значение которых может принимать любое значение заменено на символ \*.

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата
Изм.	Лист	№ докум.	Подп.	Дата

**СЮИК.465634.001 ИС34**

Лист

10

## 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 20.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 120.0.0.2
netmask 255.255.255.0
gateway 120.0.0.1
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 = 120.0.0.2
    leftsubnet = 20.0.2.0/24
    leftid = %any
    leftcert = cert00002.cer
    leftauth = eap-bsts
    auto = route
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС34	Лист
						11
Изм.	Лист	№ докум.	Подп.	Дата		

```
dpdaction = clear
closeaction = clear
```

```
conn BAS2-BAS1
right = 100.0.0.1
rightsubnet = 10.0.0.10/32
rightid = %any
rightauth = eap-bsts
rightsendcert = never
```

### 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» 2 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=BAS00002, C=BY, L=г.Гомель, 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» 2 верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key**.

Для данного сертификата поле subject имеет значение "CN=BAS00002, C=BY, L=г.Гомель, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты". Это значение и будет использоваться в качестве идентификатора устройства при IPsec соединении.

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

## 2.3 Настройка ПАК «БАС» 3

Настройка ПАК «БАС» 3 проводится аналогично ПАК «БАС» 2, 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 30.0.0.1
netmask 255.255.255.0
auto eth0

iface eth1 inet static
address 130.0.0.2
netmask 255.255.255.0
gateway 130.0.0.1
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-prfbnrg_hmac-ecp256bign-keyrep
    esp = belt_cfb-belt_mac

    left = 130.0.0.2
    leftsubnet = 30.0.2.0/24
    leftid = %any
    leftcert = cert00003.cer
    leftauth = eap-bsts
    auto = route
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	СЮИК.465634.001 ИС34	Лист
						13
Изм.	Лист	№ докум.	Подп.	Дата		

```
dpdaction = clear
closeaction = clear
```

```
conn BAS2-BAS1
right = 100.0.0.1
rightsubnet = 10.0.0.20/32
rightid = %any
rightauth = eap-bsts
rightsendcert = never
```

### 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» 3 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=BAS00003, C=BY, L=г.Витебск, 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» 3 верно подгрузило сертификат открытого ключа и сопоставило его с личным ключом, свидетельствует запись **pubkey: BIGN 512 bits, has private key**.

Для данного сертификата поле subject имеет значение "CN=BAS00003, C=BY, L=г.Витебск, O=ЗАО "НТЦ Контакт", D=Комплекс программно-аппаратный криптографической защиты информации "БАС". Сервер защиты". Это значение и будет использоваться в качестве идентификатора устройства при IPsec соединении.

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

## 2.4 Настройка ПК 1

Настройка ПК 1 заключается в настройке сетевого интерфейса.

IP-адрес: 10.0.0.10

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.0.1

## 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

## 2.6 Настройка ПК 3

Настройка ПК 3 аналогична ПК 1:

IP-адрес: 30.0.0.10

Маска подсети: 255.255.255.0

Основной шлюз: 30.0.0.1

## 2.7 Настройка ПК 4

Настройка ПК 4 аналогична ПК 1:

IP-адрес: 10.0.0.20

Маска подсети: 255.255.255.0

Основной шлюз: 10.0.0.1

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

Изм	Лист	№ докум.	Подп.	Дата

**СЮИК.465634.001 ИС34**

### 3 Проверка работоспособности

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

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

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.

Затем с ПК 3 выполнить **ping** ПК 4.

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

Обмен пакетами с 10.0.0.20 по 32 байт:

```
Превышен интервал ожидания для запроса.  
Ответ от 10.0.0.20: число байт=32 время<1мс TTL=64  
Ответ от 10.0.0.20: число байт=32 время<1мс TTL=64  
Ответ от 10.0.0.20: число байт=32 время<1мс TTL=64
```

Статистика Ping для 10.0.0.20:

```
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.

```
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
```

Инв. № подл.	Подп. и дата	Взам. Инв. №	Инв. № дубл.	Подп. и дата	Инв. № подл.	Лист
						16
<b>СЮИК.465634.001 ИС34</b>						Лист



```

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 ushbar bpkc attr kernel-netlink
resolve socket-default stroke vici updown xauth-generic dhcp counters eap-bsts eap-bpacc
Listening IP addresses:
  10.0.0.1
  100.0.0.1
Connections:
BAS1-BAS2: 100.0.0.1...%any 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: [CN=BAS00002, C=BY, L=г.Гомель, O=*, D=*] uses EAP_BSTS
authentication
BAS1-BAS2: child: 10.0.0.10/32 === 20.0.0.0/24 TUNNEL, dpdaction = clear
BAS1-BAS3: 100.0.0.1...%any IKEv2, dpddelay=30s
BAS1-BAS3: 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-BAS3: cert: "CN=BAS00001, C=BY, L=г.Минск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты"
BAS1-BAS3: remote: [CN=BAS00003, C=BY, L=г.Витебск, O=*, D=*] uses EAP_BSTS
authentication
BAS1-BAS3: child: 10.0.0.20/32 === 20.0.0.0/24 TUNNEL, dpdaction = clear
Security Associations (2 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.Гомель, 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, rekey, 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}: 10.0.0.10/32 === 20.0.0.0/24
BAS1-BAS3[2]: 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]...100.0.0.3[CN=BAS00003, C=BY, L=г.Витебск, O=ЗАО "НТЦ Контакт", D=Комплекс
программно-аппаратный криптографической защиты информации "БАС". Сервер защиты]
BAS1-BAS3[2]: IKEv2 SPIs: 0974252c95682c2f_i 400423a99128d35d_r*, EAP reauthentication
in 23 hours
BAS1-BAS3[2]: IKE proposal: BELT_CFB/BELT_HMAC/PRF_BRNG_HMAC_HBELT/ECP_256_BIGN
BAS1-BAS3{2}: INSTALLED, TUNNEL, rekey, ESP SPIs: cbe8a626_i c9e7890e_o
BAS1-BAS3{2}: BELT_CFB_256/BELT_MAC, 252 bytes_i (3 pkts, 13s ago), 252 bytes_o (3 pkts,
13s ago), rekeying in 55 minutes
BAS1-BAS3{2}: 10.0.0.20/24 === 30.0.0.0/24

```

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

Изм	Лист	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>	Лист
						17

Как видно из вывода команды, установлено 2 туннеля между подсетями **10.0.0.10/32 === 20.0.0.0/24** и **10.0.0.20/32 === 30.0.0.0/24**, по туннелям было передано по 3 пакета в каждую сторону (**ping**), защищенных при помощи алгоритмов **BELT\_CFB\_256/BELT\_MAC**.

При этом необходимо если с ПК 2 выполнить **ping** ПК 4, то ответ получен не будет. Аналогично, если с ПК 3 выполнить **ping** ПК 1, то ответ получен не будет. Данные запросы **ping** не попадут в существующие политики установленных IPSec соединений и не установят новые соединения.

Таким образом ПАК «БАС» 1 выполнил маршрутизацию трафика с разделением по ресурсам, используя фильтрацию полей сертификата при установке IPsec соединения.

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

Изм	Лист	№ докум.	Подп.	Дата	<b>СЮИК.465634.001 ИС34</b>	Лист
						18