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 сертификатов, выпущенных разными удостоверяющими центрами

СЮИК.465634.001 ИС30

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

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 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 подключение к защищаемой при помощи ПАК «БАС» 1 подсети (ПК 1) другой защищаемой при помощи ПАК «БАС» 2 подсети (ПК 2), при этом ПАК «БАС» 1 и ПАК «БАС» 2 используют сертификаты, выпущенные разными удостоверяющими центрами.

Реализация данного сценария практически не отличается от сценария построения защищенного соединения между двумя подсетями. Единственным отличием является то, что оба ПАК «БАС» до начала работы должны знать о двух точках доверия, т.е. иметь оба корневых сертификата.

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.

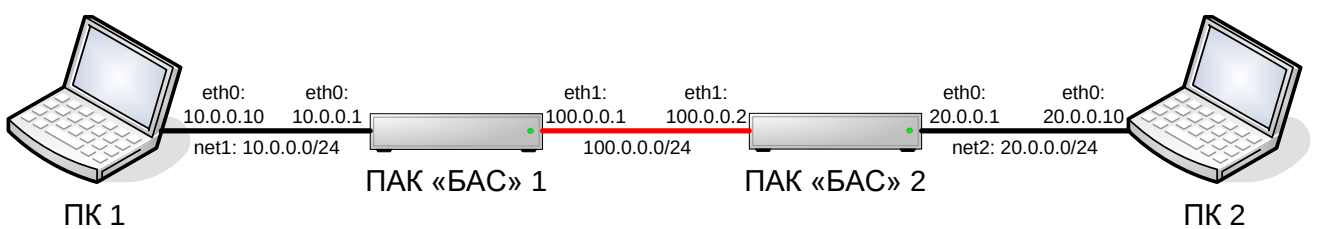

Рисунок 1 – Схема стенда

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 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**.

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», при этом в папку **/usr/local/etc/ipsec.d/cacerts/** необходимо поместить корневые сертификаты всех Удостоверяющих центров.

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
        leftsubnet = 10.0.0.0/24
        leftid = %any
        leftcert = cert00001.cer
        leftauth = eap-bsts
        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
        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**.

Убедиться в том, что программное обеспечение ПАК «БАС» 1 подгрузило оба корневых сертификата, можно при помощи команды **ipsec listcacerts**.

```
server@server:~$ sudo ipsec listcacerts

List of X.509 End Entity Certificates:
  subject:     "CN=УЦ для тестирования, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
  issuer:      "CN=УЦ для тестирования, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
  validity:    not before    Jan 1 00:00:00 2020, ok
               not after     Jan 1 00:00:00 2030, ok (expired in 3285 days)
  serial:      01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
  flags:       CA   CRLSign   oscpSigning   self-signed
  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


  subject:     "CN=УЦ для тестирования 2, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
  issuer:      "CN=УЦ для тестирования 2, C=BY, L=г.Минск, O=ЗАО 'НТЦ КОНТАКТ'"
```

```
validity:     not before    Jan 1 00:00:00 2020, ok
              not after     Jan 1 00:00:00 2030, ok (expired in 3285 days)
serial:       01:23:45:67:89:ab:cd:ef:00:01:23:45:67:89:ab:cd:ef:00
flags:        CA   CRLSign   oscpSigning   self-signed
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
```

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 100.0.0.2
netmask 255.255.255.0
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 = 100.0.0.2
        leftsubnet = 20.0.0.0/24
        leftid = %any
        leftcert = cert00002.cer
        leftauth = eap-bsts
        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
        rightsendcert = never
```

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 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 10.0.0.10

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**.