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 аутентификацией по протоколу BPACE

СЮИК.465634.001 ИС23

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

Содержание

1 Описание соединения (стенда) 4

2 Настройка соединения (стенда) 5

2.1 Настройка ПАК «БАС» 1 5

2.1.1 Смена пароля администратора 6

2.1.2 Настройка сетевых интерфейсов 6

2.1.3 Настройка даты и времени 7

2.1.4 Управление ключевой информацией 7

2.1.5 Настройка программного обеспечения 8

2.2 Настройка ПАК «БАС» 2 9

2.3 Настройка ПК 1 10

2.4 Настройка ПК 2 10

3 Проверка работоспособности 11

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.

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

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. 7.6 (EAP-BPACE).

Данный способ создания защищенного соединения позволяет выполнить аутентификацию с использованием известного обеим сторонам пароля.

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

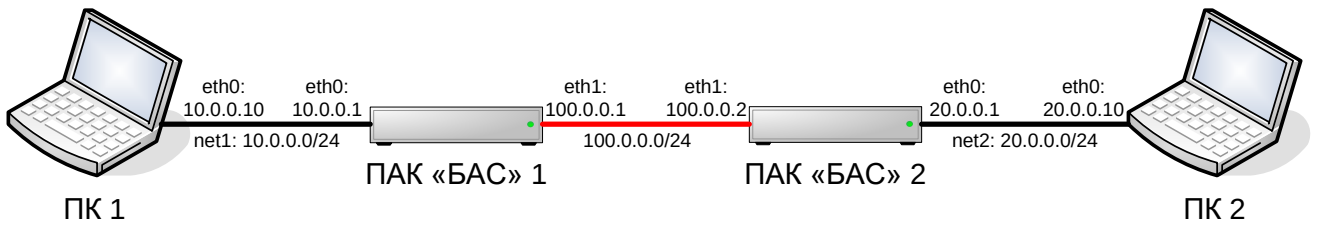

Рисунок 1 – Схема стенда

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;

– 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 аутентификации при помощи протокола BPACE оба участника IPsec-соединения должны владеть секретным паролем.

Пароль задается в файле **/usr/local/etc/ipsec.secrets** в следующем формате.

```
Идентификатор : Тип_аутентификации «Пароль»
```

В качестве идентификатора указывается значение, которое присылает удаленная сторона при запросе IPsec-соединения (устанавливается в параметре leftid на удаленной стороне).

В качестве типа аутентификации необходимо использовать значение EAP.

В качестве пароля необходимо использовать длинные случайные последовательности.

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

BAS2 : EAP “12345678”
```

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 = BAS1
        leftauth = eap-bpace
        auto = route

        dpdaction = clear
        closeaction = clear

conn BAS1-BAS2
        right = 100.0.0.2
        rightsubnet = 20.0.0.0/24
        rightid = BAS2
        rightauth = eap-bpace
        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]...
```

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.secrets** будет иметь вид:

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

BAS1 : EAP “12345678”
```

– 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 = BAS2
        leftauth = eap-bpace
        auto = route

        dpdaction = clear
        closeaction = clear

conn BAS2-BAS1
        right = 100.0.0.1
        rightsubnet = 10.0.0.0/24
        rightid = BAS1
        rightauth = eap-bpace
        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:  [BAS1] uses EAP_BPACE authentication
BAS1-BAS2:     remote: [BAS2] uses EAP_BPACE authentication
BAS1-BAS2:     child: 10.0.0.0/24 === 20.0.0.0/24 TUNNEL, dpdaction = clear
Routed Connections:
BAS1-BAS2{1}:  ROUTED, TUNNEL, reqid 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[BAS1]...100.0.0.2[BAS2]
     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**.