УТВЕРЖДЕНО

РТНК.450003.001РЭ-ЛУ

Устройство программно-аппаратное

«Клиент ДСП 4.5»

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Настройка

РТНК.450003.001РЭ

Листов 54

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

Copyright © S-Terra Bel 2008 - 2021

Содержание

Copyright © S-Terra Bel 2008 - 2021

Лицензионное Соглашение

о праве использования программного продукта «Клиент ДСП 4.5» производства ООО «С-Терра Бел»

© 2008 – 2021 ООО «С-Терра Бел». Все права защищены.

Для целей настоящего Лицензионного Соглашения используются следующие основные термины и их определения:

«Продукт» - компьютерная программа «Клиент ДСП 4.5», включающая в себя программный код и сопроводительную документацию в бумажной (печатной) и электронной форме.

«ПАК» – изготовленное и введенное Производителем в гражданский оборот на территории Республики Беларусь программно-аппаратное устройство «Клиент ДСП 4.5», включающее установленный в него экземпляр Продукта.

«Конечный Пользователь» - физическое или юридическое лицо, которое законно приобрело у Производителя экземпляр Продукта в составе ПАК.

«Производитель» – Общество с ограниченной ответственностью «С-Терра Бел», являющееся производителем ПАК и обладателем исключительных прав на Продукт.

«Сторонние компоненты» – объекты интеллектуальной собственности, принадлежащие третьим лицам и включенные Производителем в состав Продукта или использованные Производителем при создании Продукта на основании открытых лицензий в соответствии с публичными лицензионными договорами, которые являются неотъемлемой частью настоящего Лицензионного Соглашения.

Настоящее Лицензионное Соглашение определяет условия использования Конечным Пользователем Продукта, экземпляр которого законно приобретен Конечным пользователем у Производителя в составе ПАК. Вознаграждение Производителю за предоставление Конечному Пользователю прав на использование Продукта включено в цену ПАК, если иное не определено в договоре, на основании которого Конечный Пользователь приобрел ПАК.

Начиная использовать Продукт, Конечный Пользователь в соответствии с пунктом 7 статьи 44 Закона Республики Беларусь от 17.05.2011 г. № 262-З «Об авторском праве и смежных правах» заключает с Производителем настоящее Лицензионное Соглашение, в том числе выражает свое согласие со всеми условиями настоящего Лицензионного Соглашения и принимает на себя обязательства, предусмотренные настоящим Лицензионным Соглашением.

Исключительные права на Продукт принадлежат Производителю и защищаются законодательством Республики Беларусь и международными договорами.

В соответствии с настоящим Лицензионным Соглашением Конечному Пользователю как лицу, правомерно владеющему экземпляром Продукта, предоставляется неисключительное право использовать только один экземпляр Продукт на территории Республики Беларусь путем запуска Продукта и работы с ним (использования заложенных в Продукт функциональных возможностей) только в составе ПАК, принадлежащего Конечному Пользователю, и только в качестве персонального средства защиты информации, хранящейся и обрабатываемой в электронных устройствах (ПЭВМ, смартфон, планшет), принадлежащих Конечному пользователю.

Конечный пользователь не вправе:

- использовать Продукт для целей, не предусмотренных настоящим Лицензионным Соглашением;

- распространять экземпляр или копии Продукта, а равно любую часть Продукта, включая Сторонние компоненты, в том числе путем предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Продукта путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения;
- дизассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и компоненты Продукта, вносить какие-либо изменения в бинарный код программ
- совершать в отношении Продукта иные действия, прямо не разрешенные настоящим Лицензионным Соглашением, либо нарушающие законодательство Республики Беларусь и применимые международные договоры.

В состав Продукта могут входить Сторонние компоненты, использование которых Конечным Пользователем регулируется настоящим Лицензионным Соглашением и открытыми лицензиями (публичными лицензионными договорами) соответствующих правообладателей.

Фирменные наименования, названия произведений и продуктов, упомянутые в настоящем Лицензионном Соглашении или в Продукте, могут являться зарегистрированными торговыми марками (товарными знаками), права на которые принадлежат их владельцам. Упоминание указанных обозначений не направлено на индивидуализацию Продукта, способствующую его отличию от однородных товаров других лиц. В частности,
«Debian» является зарегистрированной в США торговой маркой Software in the Public Interest, Inc. (Программное обеспечение в интересах общества) и управляется проектом Debian,
Торговая марка «Linux» принадлежит создателю и основному разработчику ядра Линусу Торвальдсу.

Конечный Пользователь осведомлен о том, что нарушение условий настоящего Лицензионного Соглашения влечет предусмотренную законом ответственность, включая обязанность Конечного Пользователя выплатить Производителю компенсацию за каждое нарушение в размере до пятидесяти тысяч базовых величин.

Настоящее Лицензионное Соглашение вступает в силу с момента начала использования Продукта Конечным Пользователем и действует на протяжении всего срока использования Продукта, если иной срок действия прав на использование Продукта не определен в договоре, на основании которого Конечный Пользователь приобрел ПАК. Действие настоящего Лицензионного Соглашения прекращается с момента прекращения права собственности (права хозяйственного ведения, права оперативного управления) Конечного Пользователя на ПАК, а также в случае одностороннего отказа Конечного Пользователя от Лицензионного Соглашения.

Досрочное прекращение (расторжение) настоящего Лицензионного Соглашения не влечет обязанность Производителя по возврату или компенсации Конечному Пользователю какой-либо части цены, уплаченной Конечным Пользователем за ПАК и Продукт, или возмещению Конечному Пользователю убытков, вызванных прекращением (расторжением) Лицензионного Соглашения.

В случае прекращения настоящего Лицензионного Соглашения Конечный Пользователь должен незамедлительно уничтожить все информационные носители, содержащие программный код и прочие компоненты Продукта.

Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Настоящее Лицензионное Соглашение не содержит каких-либо гарантий в отношении функциональности и соответствия Продукта любым техническим требованиям, стандартам и условиям. Требования к качеству Продукта могут регулироваться применимым законодательством, обязательными требованиями технических нормативных правовых актов и условиями договора, на основании которого Конечным Пользователем приобретен ПАК.

Производитель не дает каких-либо гарантий в отношении работоспособности и пригодности Сторонних компонентов.

Производитель не несет ответственность за любые убытки, которые могут быть причинены Конечному пользователю в результате использования Продукта.

В случае выявления и демонстрации Конечным Пользователем Производителю воспроизводимой (повторяющейся) критической ошибки Продукта, при которой Продукт не

выполняет основные функции безопасности (шифрование трафика, контроль доступа), что приводит к нарушению безопасности сети Конечного Пользователя, Производитель обязуется по письменному запросу Конечного Пользователя разработать и безвозмездно представить Конечному Пользователю обновление Продукта, в котором указанная критическая ошибка будет устранена.

Напечатано в Республике Беларусь

ООО «С-Терра Бел»

220012, г. Минск ул. Чернышевского, д. 10А, пом. 611

Телефон: (+375 17) 280 6000

Эл.почта: info@s-terra.by

https://s-terra.by

Комплект поставки

В комплект поставки Программно-аппаратного устройства «Клиент ДСП 4.5» (далее – ПАУ «Клиент ДСП») входит:

№ пп	Элемент комплекта	Пояснения
1	Файл «belvpngate_4.5.200414av+c3_arm64.deb»	файл установки комплекса для ОС Linux/Debian
2	Файлы «ПАУ Клиент ДСП 4.5-XX.pdf»	документ в электронном виде «Программно-аппаратное устройство «Клиент ДСП 4.5». Руководство по эксплуатации»
3	Сертификат соответствия техническому регламенту Республики Беларусь	заверенная копия документа на бумажном носителе
4	Лицензия на использование экземпляра «Клиент ДСП»	набор данных пользователя комплекса, передаваемый на любом носителе или в электронном виде

Другая документация по особенностям использования программно-аппаратного устройства «Клиент ДСП 4.5» доступна для загрузки на сайте компании: https://www.s-terra.by

Copyright © S-Terra Bel 2008 - 2021

Назначение и функции ПАУ «Клиент ДСП»

ПАУ «Клиент ДСП» является средством шифрования/расшифрования сетевого трафика с контролем целостности по СТБ 34.101.31.

Количество туннелей шифрования – определяется лицензией (от 3 до без ограничений).

ПАУ «Клиент ДСП» обеспечивает:

1. создание виртуальных частных сетей (VPN) по технологии IPsec VPN;

2. защиту трафика между ПЭВМ и различными узлами сети и защиту трафика самого устройства безопасности на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP в рамках международных стандартов:

a. Security Architecture for the Internet Protocol – RFC2401
b. IP Authentication Header (AH) – RFC2402
c. IP Encapsulating Security Payload (ESP) – RFC2406
d. Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
e. The Internet Key Exchange (IKE) – RFC2409
f. The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407;

3. пакетную stateless фильтрацию трафика;

4. контекстную (stateful) фильтрацию для протоколов TCP и FTP;

5. работу по расписанию для правил пакетной фильтрации;

6. классификацию и маркирование трафика;

7. возможность применения различных наборов правил обработки трафика на различных виртуальных сетевых интерфейсах;

8. возможность получения сертификатов открытых ключей по протоколу LDAP;

9. поддержку сертификатов открытых ключей ГосСУОК;

10. событийное протоколирование (по протоколу syslog), с возможностью объединять события в группы и задавать для каждой группы свой независимый уровень протоколирования;

11. сбор статистики для мониторинга (по протоколу SNMP v1 и v2c);

12. маскировку топологии защищаемого сегмента сети (туннелирование трафика);

13. возможность задания дополнительной аутентификации партнера на основе запросов на RADIUS сервер;

14. возможность загрузки локальной политики безопасности из внешнего файла;

15. защиту сети, подсети и самого шлюза от несанкционированного доступа;

16. контроль целостности программной и информационной части программного обеспечения ПАУ;

17. построение отказоустойчивых схем, в том числе кластерных решений, горячее резервирование и балансировку.

Управление ПАУ «Клиент ДСП» осуществляется:

1. централизованно-удаленно, посредством программного продукта «Bel VPN KP»;

2. локально и удаленно по протоколу SSH с помощью интерфейса командной строки;

3. локально, при помощи конфигурационного текстового файла, описывающего политику безопасности.

ПАУ «Клиент ДСП» использует криптографическую библиотеку программного средства электронной цифровой подписи и шифрования «AvC ver.1.0» (РБ.ЮСКИ.13000-01).

ПАУ «Клиент ДСП» работает под управлением операционной системы GNU/Linux Debian 11,

ПАУ «Клиент ДСП» реализует требования Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» – ТР 2013/027/BY (взаимосвязанные ТНПА):

Copyright © S-Terra Bel 2008 - 2021

СТБ 34.101.31-2020 (пп. 7.3, 7.5)	Шифрование в режиме гаммирования с обратной связью и выработка имитовставки
СТБ 34.101.66-2014 (приложение А)	Формирование общего ключа по протоколу Диффи — Хеллмана
СТБ 34.101.47-2017 (п. 6.2)	Генерация псевдослучайных чисел в режиме счетчика
СТБ 34.101.17-2012	Синтаксис запроса на получение сертификата
СТБ 34.101.19-2012 (разделы 6-8)	Форматы сертификата открытого ключа и списка отозванных сертификатов, а также их расширений
	Верификация маршрута сертификации
СТБ 34.101.78-2019 (пп. 8.2, 8.3, 8.5)	Структура и атрибуты запроса на получение сертификата; форматы сертификата открытого ключа и списка отозванных сертификатов
СТБ 34.101.45-2013 (п. 6.2)	Генерация личного и открытого ключей и проверка ключей (алгоритмы управления параметрами и ключами)
СТБ 34.101.27-2011 (класс 1)	Требования безопасности
СТБ 34.101.73-2017 (пп. 7.3, 7.4)	Межсетевой экран сетевого и транспортного уровней

Также реализованы функции, определенные в ТНПА Республики Беларусь, обеспечивающие функционирование ПК Bel VPN Gate (подтверждение соответствия не требуется):

СТБ 34.101.45-2013 (п. 7.1)	Электронная цифровая подпись на основе эллиптических кривых
СТБ 34.101.45-2013 (приложение Е)	Парольная защита личного ключа
СТБ 34.101.31-2020 (п. 7.8)	Функция хеширования
«Программные продукты Bel VPN. Методика создания и распределения ключевых данных» BY.PTHK.45000 91 01	Управление криптографическими ключами, рекомендованное ОАЦ

Copyright © S-Terra Bel 2008 - 2021

Инициализация ПАУ «Клиент ДСП» при первом старте

При первом запуске ПАУ «Клиент ДСП» после загрузки ОС появляется предупреждение "`System is not initialized. Please run /opt/VPNagent/bin/init.sh to start initialization procedure`" и приглашение для входа в ОС.

Ниже пошагово описаны действия, которые необходимо выполнить для инициализации ПАУ «Клиент ДСП».

Шаг 1: Запустить скрипт `/opt/VPNagent/bin/init.sh` для старта процедуры начальной инициализации ПАУ «Клиент ДСП».

Во время выполнения, инициализационный скрипт может быть прерван нажатием комбинации клавиш `Ctrl+C`.

При возникновении ошибки процесс инициализации прерывается и на экран выдается сообщение об ошибке.

Шаг 2: Далее проводится инициализация начального значения ДСЧ.

Шаг 3: Далее запрашивается лицензионная информация на ПАУ «Клиент ДСП» (сведения, необходимые для ввода находятся на бланке «Лицензии на использование ПК Клиент ДСП», входящем в комплект поставки):

```
You have to enter license for Bel VPN
```

Предлагаются следующие пункты для ввода:

```
Available product codes:
 VPN1
 VPN2
 VPN3
 GATE100
 GATE100B
 GATE100V
 GATE1000
 GATE1000V
 GATE3000
 GATE7000
 GATE10000
 RVPN
 RVPNV
 BELVPN
 BELVPNV
 UVPN
 UVPNV
 KZVPN
```

Copyright © S-Terra Bel 2008 - 2021

KZVPNV

`Enter product code:` – ввести код продукта

`Enter customer code:` – ввести код конечного пользователя

`Enter license number:` – ввести номер лицензии

`Enter license code:` – ввести код лицензии

Шаг 4: Следует вопрос о корректности введенных данных:"`Is the above data correct?`". После получения подтверждения инициализация продолжается без дополнительных вопросов. Если получен отрицательный ответ – предлагается ввести лицензионную информацию повторно.

Шаг 5: Далее запускается vpn-демон, создается пользователь "`cscons`" с назначенным ему начальным паролем "`csp`".

Если инициализация завершилась успешно, то выдается сообщение: "Initialization complete". При последующих стартах системы предупреждение о необходимости инициализации системы не выдается.

Если инициализация завершилась неуспешно, то об этом выдаётся соответствующее сообщение. При следующем старте комплекса администратору снова будет выдаваться предупреждение об инициализации.

При инициализации ПАУ «Клиент ДСП» устанавливается политика безопасности, при которой интерфейсы устройства пропускают все пакеты – Default Driver Policy = Passall.

Для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "cscons" (начальный пароль "csp"),

Для входа в ОС предназначено имя "root".

Сразу после инициализации программного комплекса автоматически запускается утилита cspvpn_verify для проверки целостности установленного комплекса ПАУ «Клиент ДСП», которая описана в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.РТНК.45000 34 01-3).

Утилита управления ключевыми контейнерами cryptocont размещается в каталоге /opt/Avest/bin. Подробное описание данной утилиты приведено в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды» (BY.РТНК.45000 34 01-3).

Copyright © S-Terra Bel 2008 - 2021

Регистрация Лицензии на ПАУ «Клиент ДСП»

Регистрация Лицензии на ПАУ выполняется во время инициализации ПАУ «Клиент ДСП», но если появится необходимость перерегистрировать Лицензию после инициализации, то используется утилита `lic_mgr`.

Утилита `lic_mgr`, описанная в документе «Программные продукты Bel VPN. Руководство пользователя. Специализированные команды», запускается из интерфейса командной строки:

```
lic_mgr set -p PRODUCT_CODE -c CUSTOMER_CODE -n LICENSE_NUMBER
-l LICENSE_CODE
```

Copyright © S-Terra Bel 2008 - 2021

Изменение паролей

При первом подключении пользователь **"root"** с правами системного администратора ОС имеет пароль **“cisc0123”**, который ПАУ предложит изменить сразу после успешной аутентификации пользователя. При этом необходимо соблюдать требования безопасности к новому паролю:

- пароль должен состоять не менее чем из 8 символов;

- пароль должен содержать хотя бы один символ верхнего регистра;

- пароль должен содержать хотя бы один символ нижнего регистра;

- пароль должен содержать хотя бы одну цифру;

- пароль должен содержать хотя бы один специальный символ (“@”, “#”, “$” и т.д.).

Специальный пользователь, созданный в процессе инсталляции с именем "cscons", имеет пароль "csp" и уровень привилегий 15. Ему предоставляется возможность управлять настройками ПАУ «Клиент ДСП» и создавать политику безопасности. Рекомендуется после инсталляции изменить пароль этого пользователя. Изменение пароля пользователя, создание новых пользователей с разными уровнями привилегий осуществляется в специализированной консоли – в интерфейсе командной строки либо локально, либо удаленно с использованием команды username password или username secret.

Задание пароля для доступа к привилегированному (а также к конфигурационному) режиму для пользователей с уровнями привилегий от 0 до 14 осуществляется командами enable password или enable secret.

Copyright © S-Terra Bel 2008 - 2021

Настройка интерфейсов

Настройка интерфейсов выполняется:

- если политика безопасности создается с использованием cisco-like консоли, то и настройка интерфейсов должна выполняться там же (при помощи команд cisco-like консоли);
- если политика безопасности создается путем написания конфигурационного текстового файла, то настройку интерфейсов рекомендуется выполнять при помощи средств ОС (команда `ifconfig`).

Cisco-like консоль автоматически запускается при входе в систему пользователем “cscons”. Пользователи, обладающие административными привилегиями, могут запустить консоль командой `cs_console` из каталога `/opt/VPNagent/bin/`.

Посмотреть IP-адреса интерфейсов можно с использованием команды cisco-like консоли `show running-config`. Для настройки адресов требуется сначала войти в глобальный конфигурационный режим консоли, используя команду `configure terminal`, а затем – в режим `interface configuration`, задав команду `interface type port/number`. Данная команда позволяет управлять настройками только зарегистрированных сетевых интерфейсов. Изменения, сделанные в этом режиме, вступают в действие немедленно и сохраняются в загрузочных скриптах ОС. Команды консоли описаны в документе «Программные продукты Bel VPN. Руководство пользователя. Cisco-like команды».

Для просмотра IP-адресов интерфейсов в ОС используется команда `ifconfig –a`.

Назначение IP-адресов интерфейсам

Изменить IP-адреса и маски подсети сетевых интерфейсов можно:

- при помощи команд cisco-like консоли;
- при помощи команды `ifconfig`.

Назначение IP-адресов в cisco-like консоли

1. Войдите в режим interface configuration:

```
interface fastethernetport/number
```

1. Назначьте интерфейсу IP-адрес и маску:

```
ip address IP-адрес маска
```

Повторное задание IP-адреса замещает предыдущее значение.

Для того, чтобы увидеть сделанные изменения в конфигурации, используйте команду `show running-config`.

Назначение IP-адресов командой ifconfig

1. При помощи команды `ifconfig` назначьте адрес и маску интерфейсу, например:

```
ifconfig имя интерфейса IP-адрес netmask маска up
```

2. Вызовите скрипт, сохраняющий данные об интерфейсе в конфигурационных файлах:

```
/bin/ni_saveif.sh имя интерфейса
```

Назначение нескольких IP-адресов одному интерфейсу

Copyright © S-Terra Bel 2008 - 2021

Назначение IP-адресов в cisco-like консоли

Различаются primary и secondary IP-адреса. В качестве primary адреса выбирается первый по списку адрес, остальные – в качестве secondary. Primary адрес может быть только один. Адресов secondary может быть несколько.

В режиме interface configuration введите команду:

```
ip address IP-адрес маска secondary
```

Назначение IP-адресов командой ifconfig

Назначить несколько IP-адресов одному интерфейсу, т.е. создать несколько виртуальных (логических) интерфейсов, можно при помощи команды `ifconfig`.

1. Создайте сначала виртуальный интерфейс:

```
ifconfig имя_интерфейса:1 IP-адрес netmask маска up
```

3. Вызовите скрипт, сохраняющий данные об интерфейсе в конфигурационных файлах:

```
/bin/ni_saveif.sh имя_интерфейса
```

Добавление сетевых интерфейсов

1. В зависимости от типа интерфейса добавьте в файл `/etc/ifaliases.cf` строку:

для Ethernet 1000 Mbit

```
interface (name="GigabitEthernet0/X" pattern="Y")
```

для Ethernet 100Mbit и др.:

```
interface (name="FastEthernet0/X" pattern="Y")
```

X – номер физического порта ethernet

Y – имя интерфейса в операционной системе.

4. Необходимо пересчитать хэш-сумму измененного файла. Запустите утилиту `integr_mgr calc`:

```
integr_mgr calc –f ifaliases.cf
```

5. Перезапустите vpn-демона, выполнив команду:

```
/etc/init.d/vpngate restart
```

Настройка сетевых интерфейсов, поддерживающих 802.1Q

Интерфейс 802.1Q является расширением обычного Ethernet интерфейса (см. Стандарт IEEE 802.1Q). Для примера настроим VLAN-интерфейс 10 на интерфейсе `eth0 двумя способами`.

Настройка в cisco-like консоли:

В файле /etc/ifaliases.cf должна присутствовать строка:

```
interface (name="GigabitEthernet0/0" pattern="eth0")
```

Команды для настройки:

```
(config)#interface GigabitEthernet0/0.10
(config-subif)#encapsulation dot1Q 10
```

Copyright © S-Terra Bel 2008 - 2021

```
(config-subif)#ip address 192.168.0.2 255.255.255.0
```

Настройка без использования cisco-like консоли:

1. В файл `/etc/network/interfaces`, в раздел ###netifcfg-begin###, добавьте строки:

```
auto eth0.10
iface eth0.10 inet static
address 192.168.0.2
netmask 255.255.255.0
vlan_raw_device eth0
```

6. Добавьте в файл `/etc/ifaliaces.cf` следующую строку:

```
interface (name="FastEthernet0/0.10" pattern="eth0.10")
```

7. Пересчитайте хэш-сумму измененного файла `ifaliaces.cf`, запустив утилиту `integr_mgr calc`:

```
integr_mgr calc –f ifaliases.cf
```

8. Поднимите интерфейс:

```
ifup eth0.10
```

9. Перезапустите vpn-демона, выполнив команду:

```
/etc/init.d/vpngate restart
```

Настройка MTU интерфейса

Настроить значение MTU сетевого интерфейса, которое задает максимальный размер пакета, передаваемого без фрагментации через данный интерфейс, можно, используя либо средства ОС, либо команду mtu интерфейса командной строки консоли.

Настройка MTU сетевого интерфейса в ОС Debian осуществляется следующим образом:

1. в файл `/etc/network/interfaces`, в раздел ###netifcfg-begin###, в описание выбранного сетевого интерфейса добавьте строчку:

```
MTU YYYY
```

`YYYY` – размер MTU сетевого интерфейса.

10. Перезапустите сетевого демона, выполнив команду:

```
/etc/init.d/networking restart
```

Таким образом устанавливается постоянное значение MTU.

Установка значения MTU интерфейса на время одной сессии (до перезагрузки ОС) осуществляется командой:

```
ifconfig eth0 mtu YYYY (для интерфейса fa 0/0)
ifconfig eth1 mtu YYYY (для интерфейса fa 0/1)
```

`YYYY` – размер MTU сетевого интерфейса.

Перезагрузка LSP при изменении состояния интерфейсов

Периодически VPN демон (vpnsvc) устройства опрашивает операционную систему об изменениях в состоянии интерфейсов. Если в последний опрос произошли какие-либо изменения по сравнению с предыдущим, то автоматически происходит перезагрузка политики безопасности (LSP), загруженной в базе комплекса.

Изменения в состоянии интерфейсов могут быть следующими:

Copyright © S-Terra Bel 2008 - 2021

- состав интерфейсов;
- IP-адрес интерфейса;
- маска IP-адреса интерфейса;
- индекс интерфейса;
- Broadcast адрес.

Copyright © S-Terra Bel 2008 - 2021

Настройка переменных окружения

Имеется возможность настроить некоторые переменные окружения, которые могут повлиять на работу ПАУ «Клиент ДСП» или дать возможность получить дополнительную информацию в лог-файле.

Можно изменить значения следующих переменных окружения:

CSP_SYS_RESPONSE_TIMEOUT

CSP_LOG_TASK_TIME

CSP_LOG_TASK_QUEUE_PERIOD

VPNGATE_CONFIGURED

Начальные значения, установленные инсталлятором, для всех переменных окружения равны 0 и совпадают со значениями, установленными по умолчанию.

Изменить значение переменных окружения можно следующим образом:

1. отредактировать файл `/etc/default/vpngate`

11. перезапустить vpn-демона, выполнив команду

```
/etc/default/vpngate restart
```

Описание переменных окружения

CSP_SYS_RESPONSE_TIMEOUT задает максимальное время (в секундах), на которое vpn-демон может "подвиснуть" перед тем как аварийно закончить свою работу. "Подвисание" – состояние, когда ни одна из рабочих нитей не может взяться за выполнение задания. По достижении указанного времени vpn-демон сам аварийно завершает свою работу и создает core-файл.

Механизм слежения за зависанием vpn-демона позволяет завершить работу неработоспособного демона и запустить новую сессию, тем самым повысив отказоустойчивость системы.

Если CSP_SYS_RESPONSE_TIMEOUT = 0, то механизм слежения за зависанием vpn-демона не включается.

Переменные окружения CSP_LOG_TASK_TIME и CSP_LOG_TASK_QUEUE_PERIOD используются службой поддержки для диагностики различных ситуаций. Обе переменные задают время, по истечении которого в файл лога выдаются сообщения. CSP_LOG_TASK_QUEUE_PERIOD выдает сообщения уровня `info`, CSP_LOG_TASK_TIME выдает сообщения уровня `warning`.

CSP_LOG_TASK_TIME задает время (в секундах), которое должно быть затрачено на выполнение одной задачи. При превышении заданного времени в файл лога будет выдаваться сообщение о большем затраченном времени на выполнение одной задачи:

```
Event Manager profiler: task time is <n> sec (src=<hex> dst=<hex> idx=<n> proc=<hex>)
```

Если CSP_LOG_TASK_TIME = 0, то сообщение в файл лога не выводится.

CSP_LOG_TASK_QUEUE_PERIOD задает период (в секундах), с которым в файл лога будут выдаваться сообщения о времени ожидания задачи в очереди и длине очереди задач. Сообщения выводятся следующего вида:

Copyright © S-Terra Bel 2008 - 2021

Event Manager profiler: waiting time of task queue is <n> sec, queue length is <n> tasks

Если CSP_LOG_TASK_QUEUE_PERIOD = 0, то сообщения в файл лога не выводятся.

VPNGATE_CONFIGURED показывает выполнил ли пользователь процесс инициализации ПАУ «Клиент ДСП». Может принимать значения: yes или no.

Copyright © S-Terra Bel 2008 - 2021

Настройка NTP (Network Time Protocol)

Для синхронизации часов с NTP-сервером точного времени в ОС используется демон `chronyd`, который может выступать как в роли сервера, так и клиента, в зависимости от настроек, заданных в конфигурационном файле `/etc/chrony/chrony.conf`. По умолчанию демон настроен как NTP-клиент, и в качестве NTP сервера задан belgim.by.

ВАЖНО: из-за особенностей ПАУ «Клиент ДСП» при каждом отключении устройства от питания время сбрасывается на время сборки эталонного образца. После подключения питания и наличии подключения к сети Интернет, время синхронизируется с временем NTP сервера ориентировочно в течение 5 минут.

Настройка NTP-клиента

Для настройки Linux NTP-клиента, в файле `/etc/chrony/chrony.conf` должны присутствовать строки, задающие следующие параметры:

Параметр `server` задает NTP-сервер, который будет использоваться для синхронизации времени NTP-клиентом:

```
server <server_addr>
```

`<server_addr>` – IP-адрес или доменное имя NTP-сервера.

Параметр `driftfile` указывает файл, в котором хранится погрешность системных часов:

```
driftfile /var/lib/chrony/chrony.drift
```

Параметр `logdir` задает директорию для лог-файла:

```
logdir /var/log/chrony
```

Управление демоном

Для управления демоном `chronyd` используется утилита chronyc.

Возможные параметры и команды запуска утилиты chronyc можно узнать, выполнив команду:

```
man chronyc
```

Проверка работы NTP-сервера

Команда `chronyc tracking` выводит список источников точного времени и их характеристики.

Время при работе с сертификатами

В сертификате время указано относительно Гринвича.

ПАУ «Клиент ДСП» работает с сертификатами в локальном времени.

Время жизни сертификата не зависит от временного пояса.

Copyright © S-Terra Bel 2008 - 2021

Время жизни сертификата будет зависеть от сезонного перевода часов, т. к. время корректируется в фиксированный момент по локальному времени, поэтому может возникнуть сбой именно в момент перевода часов в разных поясах. Как только перевод будет окончен во всех поясах, время жизни сертификата в них будет одинаковым.

Copyright © S-Terra Bel 2008 - 2021

Настройка NAT на ПАУ «Клиент ДСП»

Обработка трафика ПАУ «Клиент ДСП» осуществляется в той же последовательности, что и в Cisco IOS – исходящие пакеты проходят через NAT (Network Address Translation), потом происходит их шифрование (если необходимо), а входящие пакеты – сначала расшифровываются (если необходимо), а затем над ними осуществляется трансляция адресов.

Управление настройками NAT на ПАУ «Клиент ДСП» осуществляется средствами ОС.

В ОС Linux NAT настраивается при помощи утилиты iptables. Описание `iptables` можно посмотреть командой `man iptables`.

Использование NAT позволяет производить трансляцию следующих видов:

- Статический NAT – выполняется взаимно-однозначное отображение внутренних IP-адресов во внешние. Этот вид трансляции может использоваться при настройке IPsec-туннеля между подсетями с одинаковым адресным пространством.
- Динамический NAT – в этом случае происходит динамическая трансляция внутренних локальных IP-адресов в пул глобальных IP-адресов или в адрес внешнего интерфейса устройства. Этот вид трансляции также может использоваться для IPsec-трафика между подсетями, а также для открытого доступа к интернет-серверам.
- Port Address Translation (PAT) или Network Address Port Translation (NAPT) – адреса назначения в пакетах, приходящих на адрес внешнего интерфейса устройства, подменяются на локальные в зависимости от порта TCP, что позволяет организовать доступ к нескольким серверам в локальной сети. Этот сценарий можно использовать как совместно с IPsec, так и для открытого трафика.

Во всех приведенных трансляциях поддерживается работа по протоколу FTP.

Copyright © S-Terra Bel 2008 - 2021

Создание политики безопасности ПАУ «Клиент ДСП»

В данном разделе рассмотрены основные принципы создания политики безопасности программно-аппаратного устройства «Клиент ДСП» и даны лишь общие понятия. Более подробное описание дано в соответствующих документах, в зависимости от выбранного способа настройки ПАУ.

Способы создания политики безопасности

Настроить ПАУ «Клиент ДСП» или создать политику безопасности возможно:

- Локально или удаленно по протоколу SSH с использованием команд интерфейса командной строки, описанных в документе «Программные продукты Bel VPN. Cisco-like команды» (такую конфигурацию будем называть «cisco-like конфигурацией»). Написанные команды являются родственными Cisco IOS 12.4 (13a).
- Создав текстовый конфигурационный файл и загрузив его на ПАУ с помощью специализированных команд. Создание такого файла описано в документе «Программные продукты Bel VPN. Создание конфигурационного файла» (такую конфигурацию будем называть «native-конфигурацией» или «LSP-конфигурацией»). Команды, при помощи которых можно загрузить конфигурационный файл, описаны в документе .
- Централизованно–удаленно с использованием программного продукта Bel VPN KP, предназначенного для управления всей линией продуктов, производимых компанией «С-Терра Бел», и описанного в документе «Программный продукт Bel VPN KP. Руководство пользователя».

Copyright © S-Terra Bel 2008 - 2021

Сценарии создания политики безопасности ПАУ «Клиент ДСП»

Рассмотрим некоторые **возможные сценарии настройки ПАУ «Клиент ДСП»** в зависимости от операционной системы устройства, защиту трафика которого необходимо обеспечить с помощью ПАУ «Клиент ДСП».

Построение VPN туннеля между ПАК «Шлюз безопасности Bel VPN Gate 4.5» и ПАУ «Клиент ДСП 4.5» подключенного к АРМ под управлением ОС Windows (аутентификация на ТСОК)

Описание стенда

Сценарий иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и автоматизированным рабочим местом (АРМ) пользователя, защищенного ПАУ «Клиент ДСП 4.5» (устройство Client1). Для защиты будет построен VPN туннель между устройствами GW1 и Client1. АРМ сможет общаться по защищенному каналу (VPN) с устройствами из подсети SN1 (в частности с IPHost1). Адрес АРМ неизвестен заранее. В ходе построения защищенного соединения АРМ получает адрес от Client1 по DHCP.

В рамках данного сценария для аутентификации партнеры будут использовать сертификаты.

Параметры защищенного соединения:

IKE параметры:

Аутентификация – на сертификатах открытого ключа ЭЦП по СТБ 34.101.45-2013;

Алгоритм шифрования – СТБ 34.101.31-2020 (раздел 7.3);

Алгоритм вычисления хеш-функции – СТБ 34.101.31-2020 (раздел 7.8);

Протокол согласования ключей – протокол Диффи-Хеллмана на эллиптических кривых (СТБ 34.101.66-2014).

IPsec параметры:

Туннельный режим, протокол ESP:

Алгоритм шифрования – СТБ 34.101.31-2020 (раздел 7.3);

Алгоритм контроля целостности – СТБ 34.101.31-2020 (раздел 7.5).

Схема стенда (Рисунок 1):

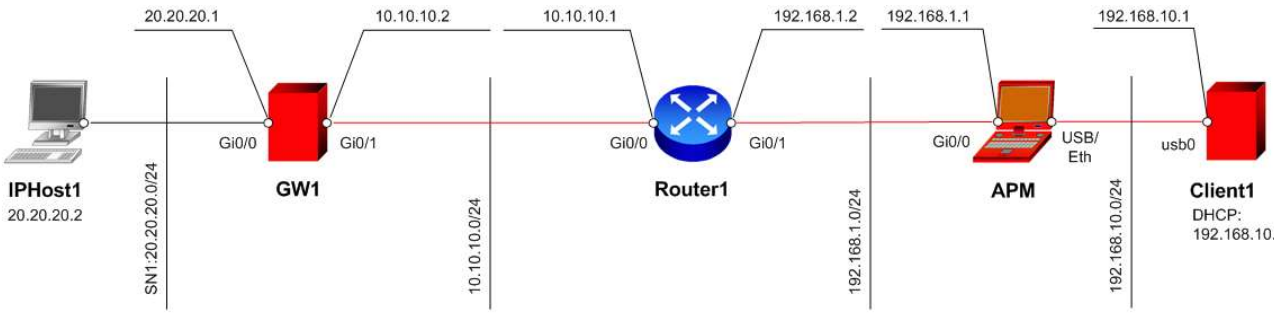

Рисунок 1

Настройка стенда

Настройка шлюза безопасности GW1

Настройку начните со шлюза безопасности GW1. Все настройки производятся через локальную консоль или удаленно (SSH с правами суперпользователя) по доверенному каналу связи.

Инициализация шлюза описывается в документации на ПАК «Bel VPN Gate 4.5» – pak_bel_vpn_gate_45_manual (раздел «Инициализация ПАК Bel VPN Gate 4.5 при первом старте»).

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на ПАК «Bel VPN Gate 4.1» – bel_vpn_gate_45_userguides-1 («Руководство пользователя», раздел «Работа с сертификатами»).

Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

1. Для входа в консоль запустите cs_console:

```
root@belvpngate:~# cs_console
belvpngate>en
Password:
```

Пароль по умолчанию: csp.

2. Перейдите в режим настройки:

```
belvpngate#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

3. В настройках интерфейсов задайте IP-адреса:

```
belvpngate(config)#interface GigabitEthernet 0/0
belvpngate(config-if)#ip address 20.20.20.1 255.255.255.0
belvpngate(config-if)#no shutdown
belvpngate(config-if)#exit
belvpngate(config)#interface GigabitEthernet 0/1
belvpngate(config-if)#ip address 10.10.10.2 255.255.255.0
belvpngate(config-if)#no shutdown
belvpngate(config-if)#exit
```

4. Задайте адрес шлюза по умолчанию:

```
belvpngate(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

5. Выйдите из cisco-like интерфейса:

Copyright © S-Terra Bel 2008 - 2021

```
belvpngate(config)#end
belvpngate#exit
```

Формирование запроса и регистрация сертификата

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

6. При необходимости установите правильное системное время.

```
root@belvpngate:~# date MMDDHHmmYYYY
```

MM – месяц;
DD – день;
HH – часы;
mm – минуты;
YYYY – год

Пример установки даты:

```
root@belvpngate:~# date 042013152021
Wed Apr 20 13:15:00 UTC 2021
```

Данная запись соответствует 20 апреля 2021 года 13:15.

7. Создайте папку /opt/certs:

```
root@belvpngate:~# mkdir /opt/certs
```

8. Создайте контейнер на ключевом носителе:

```
root@belvpngate:~#/opt/Avset/bin/cryptocont n -n=контейнер -p=пароль
```

контейнер – название создаваемого контейнера, для создания на НКИ (носителе ключевой информации) ДОЛЖНО содержать в начале названия префикс ***"av:"***;
пароль – пароль (PIN) для доступа к носителю ключевой информации AvPass/AvBign.

Пример создания криптоконтейнера на НКИ:

```
root@belvpngate:~#/opt/Avest/bin/cryptocont n -n=av:container -p=12345678
```

9. Сформируйте запрос на сертификат.

```
root@belvpngate:~#/opt/Avset/bin/cryptcont r -n=контейнер -p=пароль -cn=CommonName
-c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

контейнер – название контейнера, созданного на предыдущем шаге;
пароль – пароль (PIN) для доступа к носителю ключевой информации;
CommonName – идентификатор устройства;
OrgName – наименование организации;
OrgUnitName – наименование подразделения;
путь_к_файлу – путь к файлу с создаваемым запросом, рекомендуется указывать расширение ***".req"***.
Пример создания запроса:

```
root@belvpngate:~#/opt/Avest/bin/cryptocont r -n=av:container -p=12345678 -cn=GW1
-c=BY -o=S-TerraBel -t=Research -f=/opt/certs/GW1.req
```

10. Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением ***p7b*** или ***cer***).
Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные cer файлы.
11. Доставьте файлы сертификатов на Шлюз безопасности в предварительно созданный на нем каталог /opt/certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp исходный_файл root@адрес_шлюза:/путь_к_файлу
```

исходный файл – путь к файлу сертификата;
адрес_шлюза – сетевой адрес Шлюза;

Copyright © S-Terra Bel 2008 - 2021

путь_к_файлу – полный путь для сохранения файла на Шлюзе.

Пример передачи файла на Шлюз безопасности:

```
pscp D:\ca.cer root@10.10.10.2:/opt/certs
…
Store key in cache? (y/n)
root@10.10.10.2's password:
```

Важно: Среда передачи в этом случае должна быть доверенной

12. Выполните импорт сертификата УЦ в базу Шлюза используя утилиту cert_mgr:

```
root@belvpngate:~# cert_mgr import –f путь_к_файлу –t
```

путь_к_файлу – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@belvpngate:~# cert_mgr import –f /opt/cert/UC.cer –t
1 OK C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
```

13. Выполните импорт локального (личного) сертификата в базу Шлюза:

```
root@belvpngate:~# cert_mgr import –f путь_к_файлу –kc контейнер –kcp пароль
```

путь_к_файлу – полный путь к файлу сертификата УЦ;
контейнер – название контейнера, созданного ранее. Если контейнер храниться на ключе, введите серийный номер ключа в формате av:**серийный номер**:**название контейнера**;
пароль – пароль для доступа к ключевому носителю информации.
Пример импорта:

```
root@belvpngate:~#cert_mgr import -f /opt/cert/GW1.cer -kc av:
AVP012345678910:container -kcp 12345678
1 OK CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

14. Выведите список сертификатов, находящихся в базе Шлюза, командой **cert_mgr show** и проверьте наличие записей **trusted** и **local**:

```
root@belvpngate:~# cert_mgr show
```

Пример вывода:

```
root@belvpngate:~# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted     C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 Status: local CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите cs_console:

```
root@belvpngate:~# cs_console
belvpngate>en
Password:
```

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

15. Перейдите в режим настройки:

```
belvpngate#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

16. Смените пароль по умолчанию:

```
belvpngate(config)#username cscons password <пароль>
```

17. Смените название шлюза:

```
belvpngate(config)#hostname GW1
```

18. Задайте тип идентификации:

```
GW1(config)#crypto isakmp identity dn
```

19. Задайте параметры для IKE:

```
GW1(config)#crypto isakmp policy 1
GW1(config-isakmp)#hash belt
GW1(config-isakmp)#encryption belt
GW1(config-isakmp)#authentication belt-sig
GW1(config-isakmp)#group beltdh
GW1(config-isakmp)#exit
```

20. Создайте набор преобразований для IPsec:

```
GW1(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

21. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit ip 20.20.20.0 0.0.0.255 192.168.10.0 0.0.0.255
GW1(config-ext-nacl)#exit
```

22. Создайте динамическую крипто-карту:

```
GW1(config)#crypto dynamic-map DMAP 1
GW1(config-crypto-map)#match address LIST
GW1(config-crypto-map)#set transform-set TSET
GW1(config-crypto-map)#set pfs beltdh
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

23. Привяжите динамическую карту к статической:

```
GW1(config)#crypto map CMAP 1 ipsec-isakmp dynamic DMAP
```

24. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
GW1(config)#interface GigabitEthernet 0/1
GW1(config-if)#crypto map CMAP
GW1(config-if)#exit
```

25. Отключите обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)#revocation-check none
GW1(ca-trustpoint)#exit
```

26. Настройка устройства GW1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
GW1(config)#end
GW1#exit
```

27. Убедитесь что все сертификаты активны – статус сертификата должен быть **active**:

```
root@belvpngate:~# cert_mgr check
```

Пример:

```
root@belvpngate:~# cert_mgr check
1 State: Active C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 State: Active CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

В **Приложении** представлен текст cisco-like конфигурации для шлюза GW1.

Настройка клиента ПАУ «Клиент ДСП 4.5» (Client1)

Все настройки производятся на АРМ администратора, к которому подключен ПАУ «Клиент ДСП 4.5», через Serial-порт или удаленно (SSH с правами суперпользователя) по доверенному каналу связи. Для примера на АРМ администратора установлена ОС Windows 10 Домашняя, тип системы 64-разрядная, версия 20H2, сборка 19042.1023.

28. Подключите ПАУ «Клиент ДСП 4.5» к АРМ администратора через свободный USB-порт.
29. Для подключения и дальнейшей настройки Client 1 по Serial-порт необходимо зайти в «Диспетчер устройств», открыть вкладку «Порты (COM и LTP)» и посмотреть порядковый номер COM-порта (Рисунок 2).

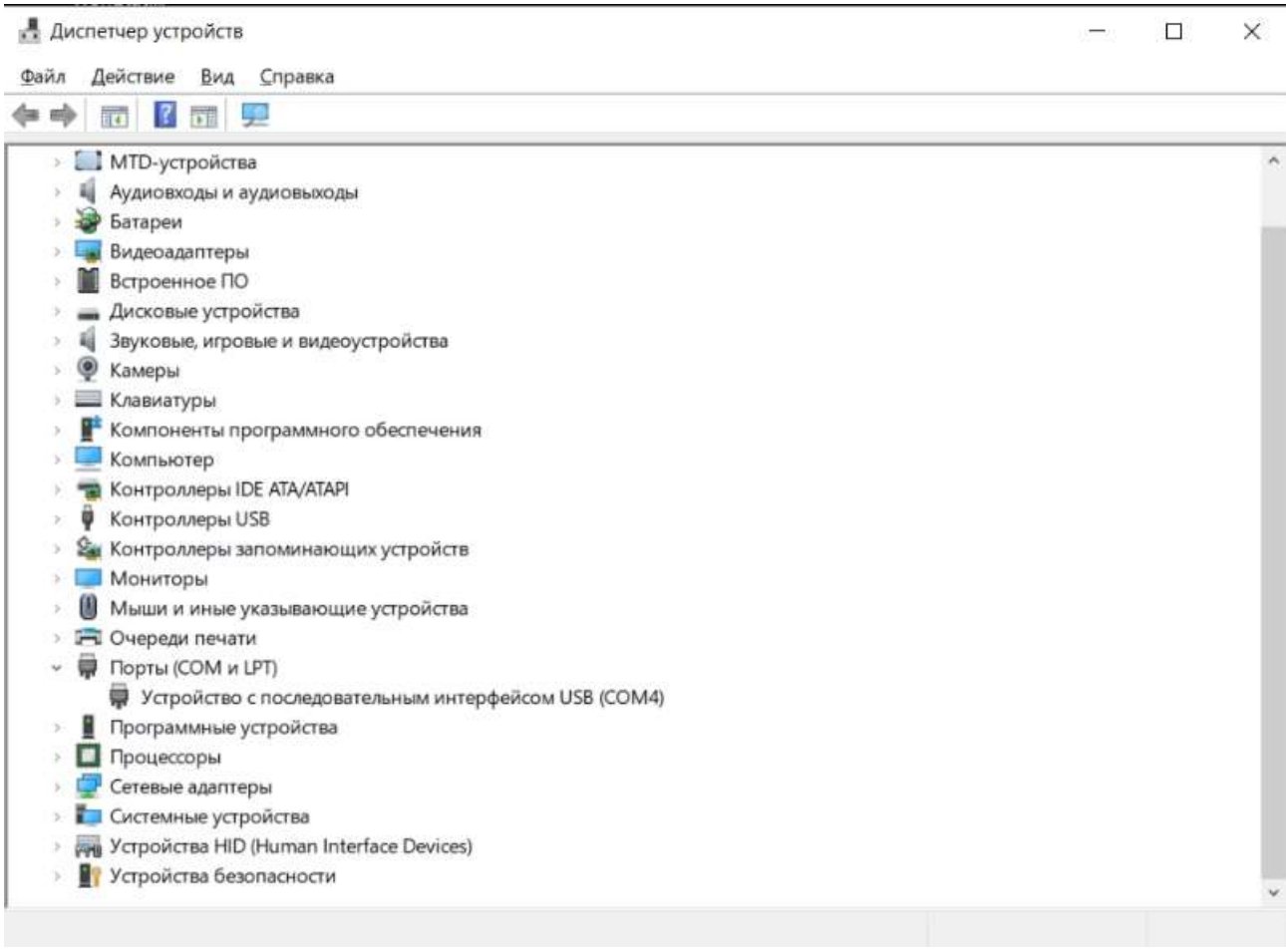

Рисунок 2.

30. Для подключения и дальнейшей настройки Client1 по SSH необходимо узнать IP-адрес для подключения. Для этого запустите командную строку и выполните команду:

```
C:\Users\Пользователь>ipconfig
```

Из списка Адаптеров найдите тот, который появился при подключении Client1 (Рисунок 3).

Copyright © S-Terra Bel 2008 - 2021

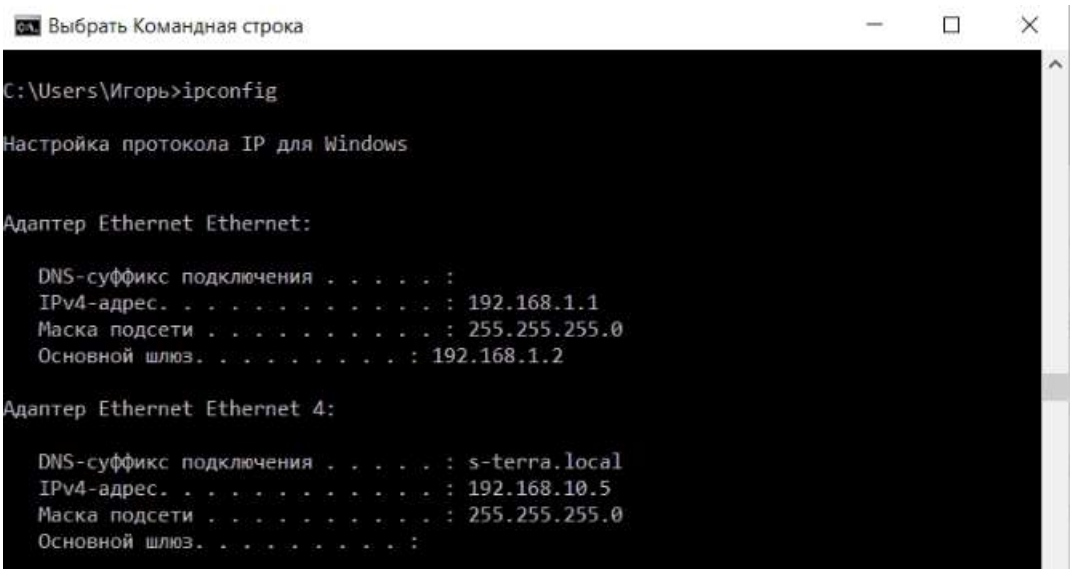

Рисунок 3.

IP-адрес Client1 будет первый адрес подсети из которой получен адрес для Адаптера (Адаптер Ethernet Ethernet 4) - **192.168.10.1**

31.С помощью программы для удаленного управления (PuTTY, WinSCP или др.) выберите способ подключения по Serial-порту (скорость укажите 115200) или SSH (Рисунок 4).

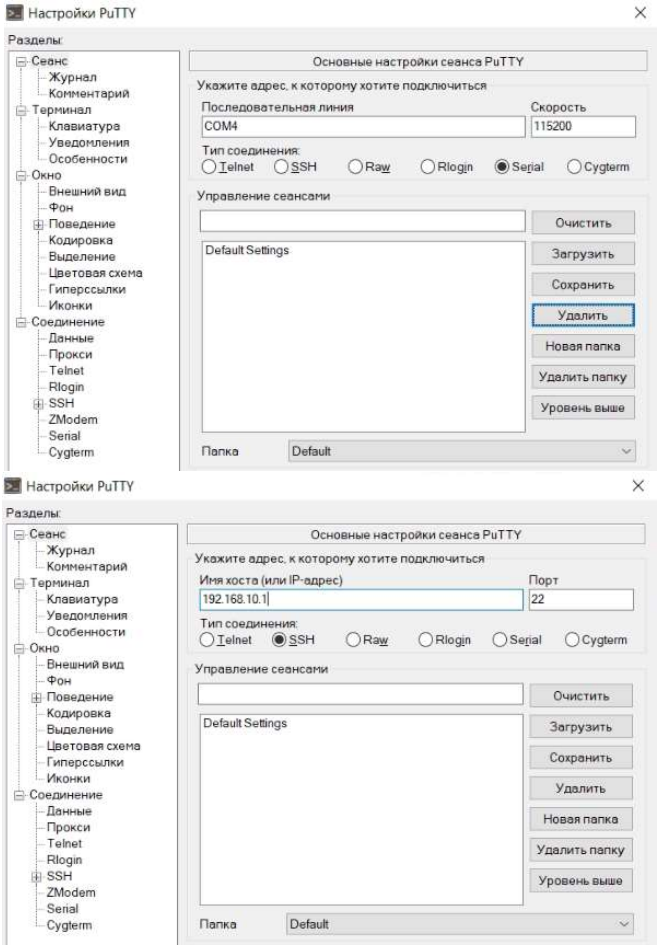

Рисунок 4.

Инициализация клиента Client1 описывается в документации на ПАУ «Клиент ДСП 4.5» – («Руководство по эксплуатации», раздел «Инициализация ПАУ «Клиент ДСП 4.5» при первом старте»).

Copyright © S-Terra Bel 2008 - 2021

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на Программные продукты Bel VPN – («Руководство пользователя. Специализированные команды», раздел «Работа с сертификатами»).

Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

32. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpn-dsp>en
Password:
```

Пароль по умолчанию: csp.
33. Перейдите в режим настройки:

```
belvpn-dsp#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

34. В настройках интерфейсов задайте IP-адреса:

```
belvpn-dsp(config)#interface FastEthernet 0/1
belvpn-dsp(config-if)#ip address 192.168.10.1 255.255.255.0
belvpn-dsp(config-if)#no shutdown
belvpn-dsp(config-if)#exit
```

35. Задайте адрес Client4 по умолчанию:

```
belvpn-dsp(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.5
```

36. Выйдите из cisco-like интерфейса:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

Формирование запроса и регистрация сертификата

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

37. При необходимости установите правильное системное время.

```
root@belvpn-dsp:~# date MMDDHHmmYYYY
```

MM – месяц;
DD – день;
HH – часы;
mm – минуты;
YYYY – год

Пример установки даты:

```
root@belvpn-dsp:~# date 042013152021
Wed Apr 20 13:15:00 UTC 2021
```

Данная запись соответствует 20 апреля 2021 года 13:15.
38. Создайте папку /opt/certs:

```
root@belvpn-dsp:~# mkdir /opt/certs
```

39. Создайте контейнер на ключевом носителе:

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptocont n –n=контейнер –p=пароль
```

контейнер – название создаваемого контейнера;
пароль – пароль (PIN) для доступа к контейнеру

Пример создания криптоконтейнера:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont n -n=container -p=12345678
```

40. Сформируйте запрос на сертификат.

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptcont r -n=контейнер -p=пароль -cn=CommonName
-c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

контейнер – название контейнера, созданного на предыдущем шаге;
пароль – пароль (PIN) для доступа к контейнеру;
CommonName – идентификатор устройства;
OrgName – наименование организации;
OrgUnitName – наименование подразделения;
путь_к_файлу – путь к файлу с создаваемым запросом, рекомендуется указывать расширение ***“.req”***.
Пример создания запроса:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont r -n=container -p=12345678 -cn=GW1
-c=BY -o=S-TerraBel -t=Research -f=/opt/certs/Client1.req
```

41. Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением ***p7b*** или ***cer***).
Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные cer файлы.
42. Доставьте файлы сертификатов на Client1 безопасности в предварительно созданный на нем каталог /opt/certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp исходный_файл root@адрес_клиента:/путь_к_файлу
```

исходный файл – путь к файлу сертификата;
адрес_шлюза – сетевой адрес Client1;
путь_к_файлу – полный путь для сохранения файла на Client1.

Пример передачи файла на Client1:

```
pscp D:\ca.cer root@192.168.10.1:/opt/certs
…
Store key in cache? (y/n)
root@192.168.10.1's password:
```

Важно: Среда передачи в этом случае должна быть доверенной

43. Выполните импорт сертификата УЦ в базу Client1 используя утилиту cert_mgr:

```
root@belvpn-dsp:~# cert_mgr import -f путь_к_файлу -t
```

путь_к_файлу – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@belvpn-dsp:~# cert_mgr import -f /opt/cert/UC.cer -t
1 OK C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
```

44. Выполните импорт локального (личного) сертификата в базу Client1:

```
root@belvpn-dsp:~# cert_mgr import -f путь_к_файлу -kc контейнер -kcp пароль
```

путь_к_файлу – полный путь к файлу сертификата УЦ;
контейнер – название контейнера, созданного ранее;
пароль – пароль для доступа к контейнеру.
Пример импорта:

```
root@belvpn-dsp:~#cert_mgr import -f /opt/cert/GW1.cer -kc container -kcp 12345678
1 OK CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

45. Выведите список сертификатов, находящихся в базе Client1, командой **cert_mgr show** и проверьте наличие записей **trusted** и **local**:

```
root@belvpn-dsp:~# cert_mgr show
```

Пример вывода:

```
root@belvpn-dsp:~# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted     C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 Status: local CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для Client1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpn-dsp>en
Password:
```

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

46. Перейдите в режим настройки:

```
belvpn-dsp#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

47. Смените пароль по умолчанию:

```
belvpn-dsp(config)#username cscons password <пароль>
```

48. Смените название шлюза:

```
belvpn-dsp(config)#hostname belvpn-dsp
```

49. Задайте тип идентификации:

```
belvpn-dsp(config)#crypto isakmp identity dn
```

50. Задайте параметры для IKE:

```
belvpn-dsp(config)#crypto isakmp policy 1
belvpn-dsp(config-isakmp)#hash belt
belvpn-dsp(config-isakmp)#encryption belt
belvpn-dsp(config-isakmp)#authentication belt-sig
belvpn-dsp(config-isakmp)#group beltdh
belvpn-dsp(config-isakmp)#exit
```

51. Создайте набор преобразований для IPsec:

```
belvpn-dsp(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
belvpn-dsp(cfg-crypto-trans)#mode tunnel
belvpn-dsp(cfg-crypto-trans)#exit
```

52. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
belvpn-dsp(config)#ip access-list extended LIST
belvpn-dsp(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 20.20.20.0 0.0.0.255
belvpn-dsp(config-ext-nacl)#exit
```

53. Создайте динамическую крипто-карту:

```
belvpn-dsp(config)#crypto map CMAP 1 ipsec-isakmp
belvpn-dsp(config-crypto-map)#match address LIST
belvpn-dsp(config-crypto-map)#set transform-set TSET
belvpn-dsp(config-crypto-map)#set pfs beltdh
belvpn-dsp(config-crypto-map)#set peer 10.10.10.2
```

Copyright © S-Terra Bel 2008 - 2021

```
belvpn-dsp(config-crypto-map)#exit
```

54. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
belvpn-dsp(config)#interface FastEthernet0/1
belvpn-dsp(config-if)#crypto map CMAP
belvpn-dsp(config-if)#exit
```

55. Отключите обработку списка отозванных сертификатов (CRL):

```
belvpn-dsp(config)#crypto pki trustpoint s-terra_technological_trustpoint
belvpn-dsp(ca-trustpoint)#revocation-check none
belvpn-dsp(ca-trustpoint)#exit
```

56. Настройка устройства Client1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

57. Убедитесь, что все сертификаты активны – статус сертификата должен быть **active**:

```
root@belvpn-dsp:~# cert_mgr check
```

Пример:

```
root@belvpn-dsp:~# cert_mgr check
1 State: Active C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 State: Active CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

В **Приложении** представлен текст cisco-like конфигурации для клиента Client1.

58. Зайдите в настройки DHCP-сервера и пропишите маршруты для шифрованного трафика. Данные маршруты автоматически будут добавлены на АРМ пользователя при подключении Client1:

```
root@belvpn-dsp:~# sudo nano /etc/dhcp/dhcpd.conf
```

В блоке описания подсети 192.168.10.0 пропишите маршрут(ы):

```
subnet 192.168.10.0 netmask 255.255.255.0 {
   range 192.168.10.5 192.168.10.254;
   option subnet-mask 255.255.255.0;
   option rfc3442-classless-static-routes 24, 20, 20, 20, 192, 168, 10,
1;
   option ms-classless-static-routes 24, 20, 20, 20, 192, 168, 10, 1;
}
```

для примера прописан маршрут 20.20.20.0/24 192.168.10.1, где

option rfc3442-classless-static-routes - настройка передачи маршрута в ОС Linux;
option ms-classless-static-routes - настройка передачи маршрута в ОС Windows;
24 – маска подсети;
20, 20, 20 – подсеть шифрованного трафика (20.20.20.0);
192, 168, 10, 1 – хост за которым будет доступна данная подсеть.

Сохраните внесенные изменения в файле dhcpd.conf.

Настройка автоматизированного рабочего места (АРМ) пользователя

Настройка АРМ состоит из нескольких этапов:

- подключение ПАУ «Клиент ДСП 4.5» (Client1);
- настройка политики обработки трафика на АРМ;
- проверка работоспособности.

Все настройки производятся на АРМ пользователя, к которому подключен ПАУ «Клиент ДСП 4.5».

Для примера:

на АРМ пользователя установлена ОС Windows 10 Домашняя, тип системы 64-разрядная, версия 20H2, сборка 19042.1023.

Подключение ПАУ «Клиент ДСП 4.5» (Client1)

59. Подключите ПАУ «Клиент ДСП 4.5» к АРМ пользователя через свободный USB-порт.
60. Убедитесь, что ПАУ «Клиент ДСП 4.5» подключен к АРМ пользователя, выполнив команду:

```
C:\Users\Пользователь>ipconfig
```

В списке должен появиться новый адаптер, в нашем примере **Адаптер Ethernet Ethernet 4** (Рисунок 5).

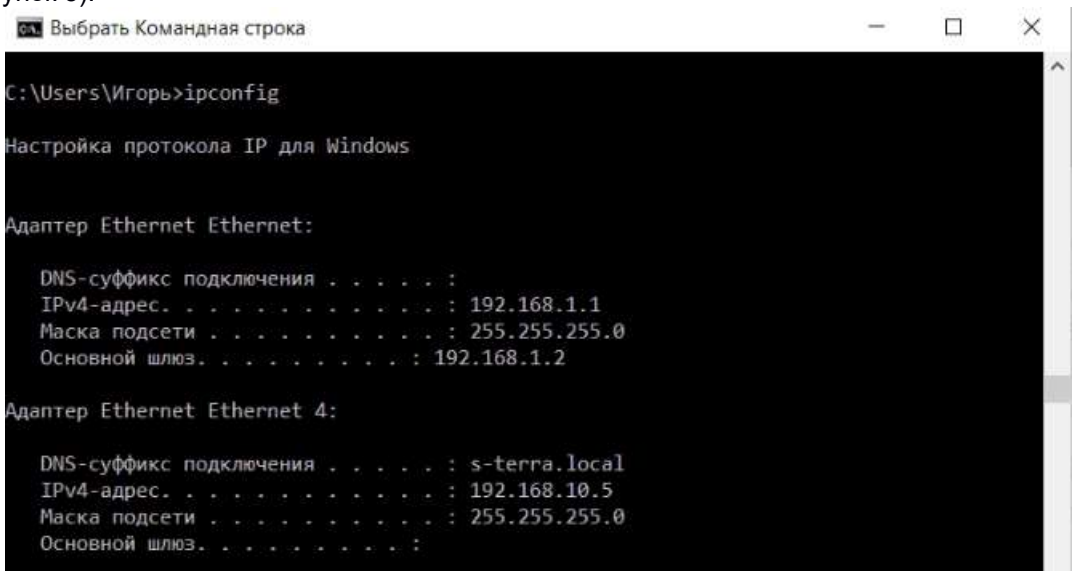

Рисунок 5.

IP-адрес ПАУ «Клиент ДСП 4.5» будет первый адрес подсети из которой получен адрес для адаптера (Адаптер Ethernet Ethernet 4) - **192.168.10.1**

61. Выполните команду, чтобы проверить доступность ПАУ «Клиент ДСП 4.5»:

```
C:\Users\Пользователь>ping 192.168.10.1
Обмен пакетами с 192.168.10.1 по с 32 байтами данных:
Ответ от 192.168.10.1: число байт=32 время=1мс TTL=62
Ответ от 192.168.10.1: число байт=32 время=1мс TTL=62
Ответ от 192.168.10.1: число байт=32 время=1мс TTL=62
Ответ от 192.168.10.1: число байт=32 время=1мс TTL=62

Статистика Ping для 192.168.10.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 1 мсек, Среднее = 1 мсек
```

Настройка политики обработки трафика на АРМ

62. Откройте «Настройку параметров адаптера» (Рисунок 6).

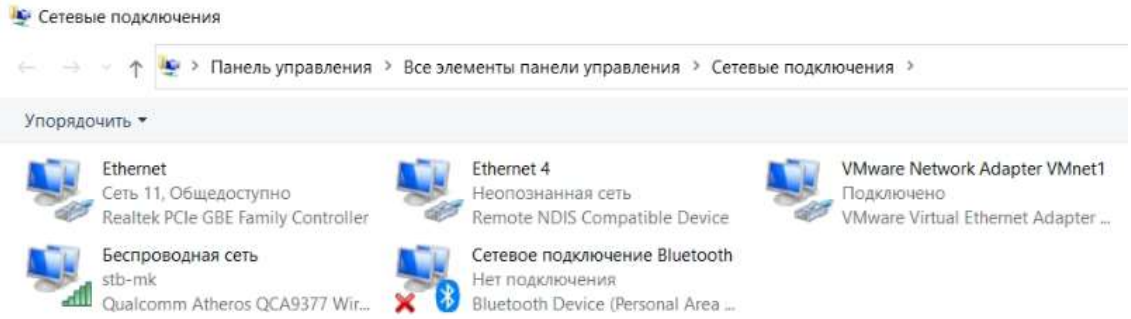

Рисунок 6.

Зайдите в свойства адаптера, который подключен к модему, или внешнему сетевому оборудованию (по умолчанию - Ethernet). В свойствах перейдите на вкладку «Доступ», выберите параметр «Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера» и в выпадающем списке пункта «Подключение домашней сети» укажите адаптер, к которому подключен ПАУ «Клиент ДСП 4.5» (Рисунок 7) – **Ethernet 4**.

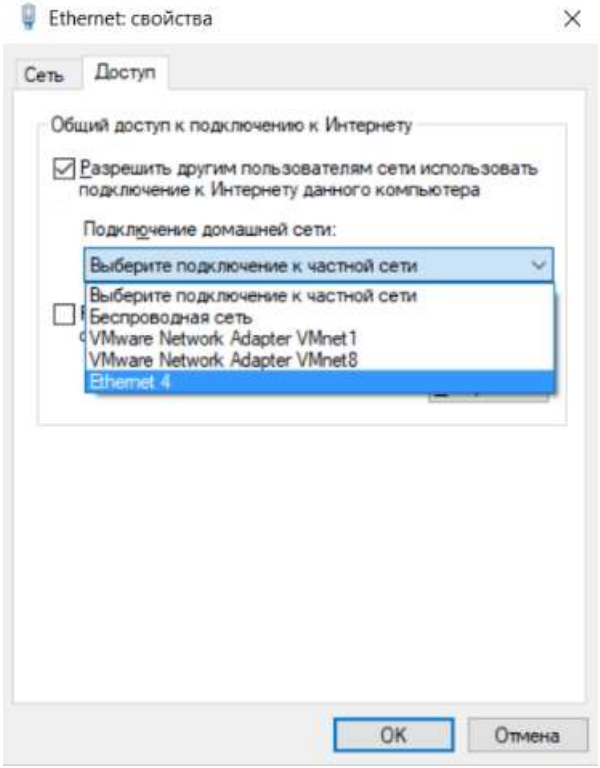

Рисунок 7.

Сохраните изменение настроек.

63. Зайдите в свойства адаптера, к которому подключен ПАУ «Клиент ДСП 4.5» – **Ethernet 4**. В окне компонент выберите параметр «IP версии 4 (TCP/IPv4)» и нажмите на кнопку «Свойства» под окном (Рисунок 8).

Copyright © S-Terra Bel 2008 - 2021

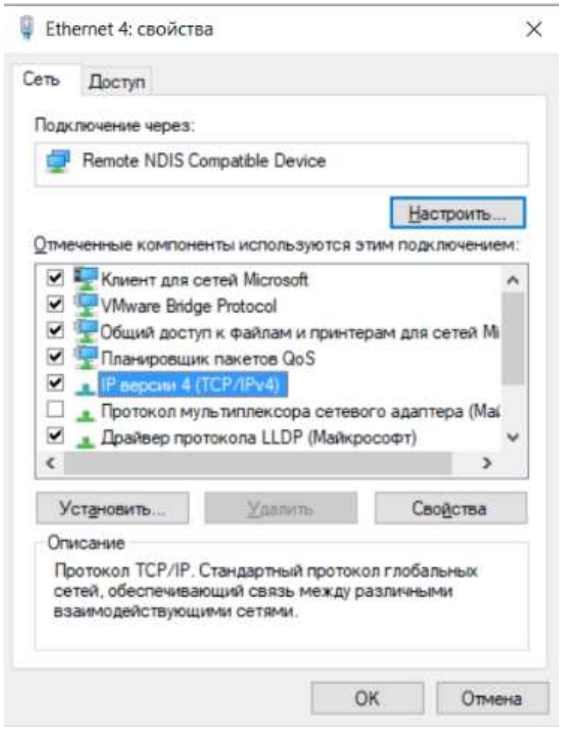

Рисунок 8.

В открывшемся окне выберите пункты «Получить IP-адрес автоматически» и «Получить адрес DNS-сервера автоматически» (Рисунок 9).

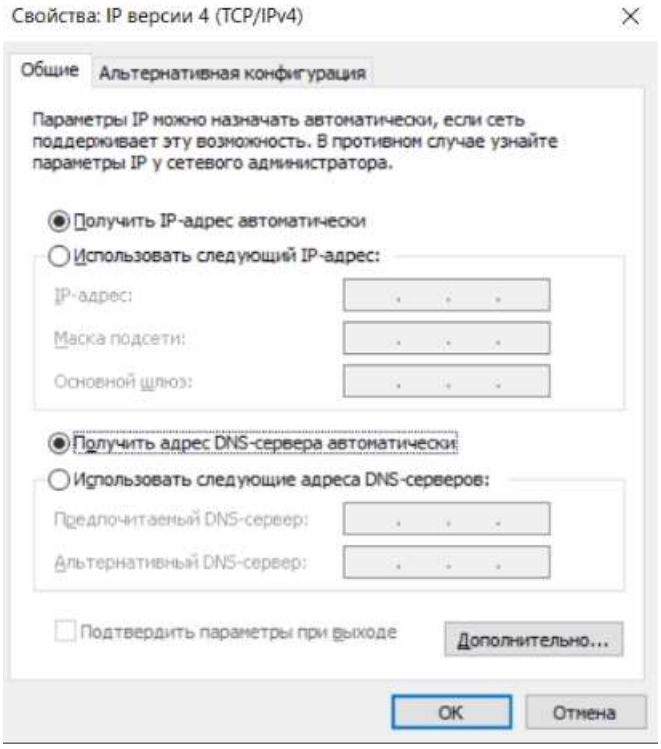

Рисунок 9.

Сохраните внесенные изменения адаптера.

Указанную выше настройку политики обработки трафика на АРМ необходимо производить каждый раз после перезагрузки АРМ. При использовании режима «гибернация» данные настройки сохраняются.

Copyright © S-Terra Bel 2008 - 2021

Проверка работоспособности

После того, как настройка всех устройств завершена, инициируйте создание защищенного соединения.

На устройстве АРМ пользователя выполните команду ping:

```
C:\Users\Пользователь>ping 20.20.20.2
Обмен пакетами с 20.20.20.2 по с 32 байтами данных:
Ответ от 20.20.20.2: число байт=32 время=166мс TTL=62
Ответ от 20.20.20.2: число байт=32 время=2мс TTL=62
Ответ от 20.20.20.2: число байт=32 время=3мс TTL=62
Ответ от 20.20.20.2: число байт=32 время=8мс TTL=62

Статистика Ping для 20.20.20.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 2мсек, Максимальное = 166 мсек, Среднее = 44 мсек
```

В результате выполнения этой команды между устройствами АРМ пользователя и GW1 будет установлен VPN туннель.

Так же в этом можно убедиться на устройстве GW1, выполнив команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (10.10.10.2,4500)-(192.168.1.1,62402) active 1968 3484

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (20.20.20.2,*)-(192.168.10.5,*) * ESP nat-t-tunn 192 192
```

Copyright © S-Terra Bel 2008 - 2021

Текст cisco-like конфигурации для шлюза GW1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr belt
 hash belt
 authentication belt-sig
 group beltdh
!
!
crypto ipsec transform-set TSET esp-belt esp-belt-mac
!
ip access-list extended LIST
 permit ip 20.20.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
!
crypto dynamic-map DMAP 1
 match address LIST
 set transform-set TSET
 set pfs beltdh
 reverse-route
!
crypto map CMAP 1 ipsec-isakmp dynamic DMAP
!
interface GigabitEthernet0/0
 ip address 20.20.20.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 10.10.10.2 255.255.255.0
 crypto map CMAP
!
!
ip route 0.0.0.0 0.0.0.0 10.10.10.1
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
…
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F
quit
!
```

```
end
```

Текст cisco-like конфигурации для клиента Client1

```
!
version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 password 0 csp
aaa new-model
!
!
hostname GW1
enable password csp
!
!
!
logging trap debugging
!
!
crypto isakmp policy 1
 encr belt
 hash belt
 authentication belt-sig
 group beltdh
!
crypto ipsec transform-set TSET esp-belt esp-belt-mac
!
ip access-list extended LIST
 permit ip 192.168.10.0 0.0.0.255 20.20.20.0 0.0.0.255
!
!
crypto map DMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set pfs beltdh
 set peer 10.10.10.2
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 crypto map CMAP
!
ip route 0.0.0.0 0.0.0.0 192.168.10.5
!
crypto pki trustpoint s-terra_technological_trustpoint
 revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 4E4B0B11EFDB389E4E86244CDAA1B275
30820216308201C5A00302010202104E4B0B11EFDB389E4E86244CDAA1B27530
…
009B097DD81A81CFC792664AAC9E6908587195AE17A5D526DE196CB0D5B7E713
E9D07F4DC61F04CDBC87579FC44CE66D524CF742F2784805733F
quit
!
end
```

Построение VPN туннеля между ПАК «Шлюз безопасности Bel VPN Gate 4.5» и ПАУ «Клиент ДСП 4.5» подключенного к АРМ под управлением ОС Linux (аутентификация на ТСОК)

Описание стенда

Сценарий аналогичен предыдущему рассмотренному (см. Рис.1) и иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и автоматизированным рабочим местом (АРМ) пользователя, защищенного клиентом «Bel VPN Client-DSP 4.5» (устройство Client1). Для защиты будет построен VPN туннель между устройствами GW1 и Client1. АРМ сможет общаться по защищенному каналу (VPN) с устройствами из подсети SN1 (в частности с IPHost1). Адрес АРМ неизвестен заранее. В ходе построения защищенного соединения АРМ получает адрес от Client1 по DHCP.

В рамках данного сценария для аутентификации партнеры также будут использовать сертификаты

Настройка стенда

Настройка шлюза безопасности GW1

Аналогично, как и в предыдущем сценарии.

Настройка клиента ПАУ «Клиент ДСП 4.5» (Client1)

Все настройки производятся на АРМ администратора, к которому подключен ПАУ «Клиент ДСП 4.5», через SSH по доверенному каналу связи. Для примера на АРМ администратора установлена ОС 20.04.1-Ubuntu, тип системы x86_64 GNU/Linux.

1. Подключите ПАУ «Клиент ДСП 4.5» к АРМ администратора через свободный USB-порт.
2. Для подключения и дальнейшей настройки Client1 по SSH необходимо узнать IP-адрес для подключения. Для этого запустите командную строку и выполните команду:

```
s-terra@s-terra-Default-string:~$ip a
```

Из списка Адаптеров найдите тот, который появился при подключении Client1 (Рисунок 2).

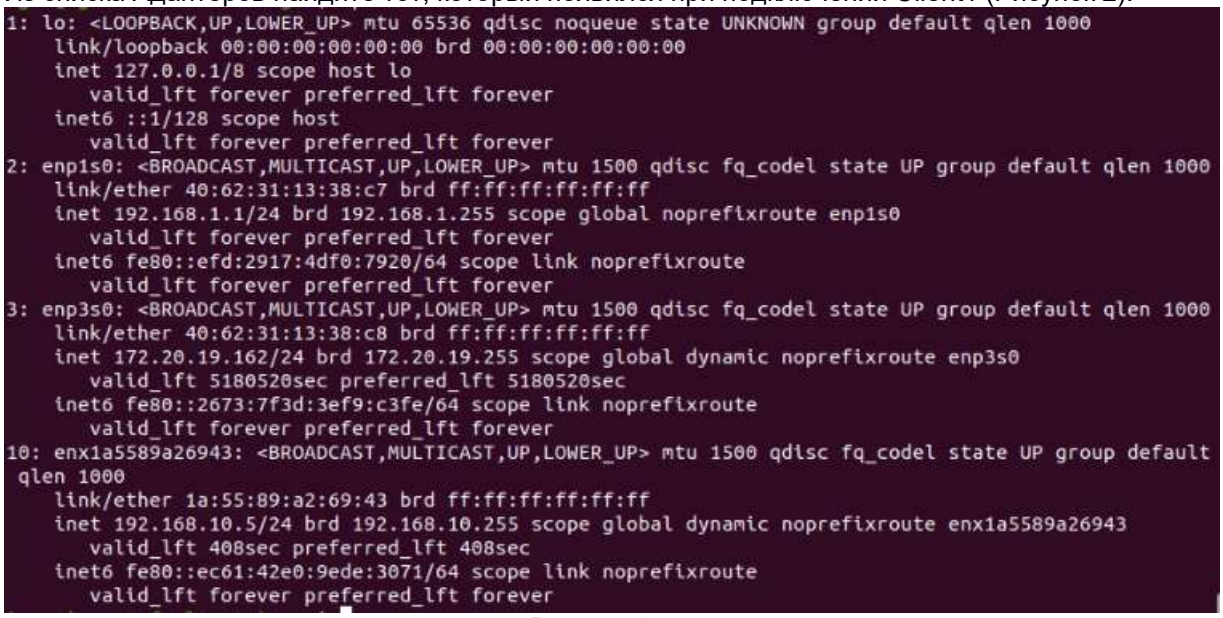

Рисунок 2.

IP-адрес Client1 будет первый адрес подсети из которой получен адрес для адаптера (enx1a5589a26943) - **192.168.10.1**
3. Подключитесь по SSH используя командную строку.

```
s-terra@s-terra-Default-string:~$ssh root@192.168.10.1
```

Инициализация клиента Client1 описывается в документации на ПАУ «Клиент ДСП 4.5» – («Руководство по эксплуатации», раздел «Инициализация ПАУ Клиент ДСП 4.5 при первом старте»).

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на Программные продукты Bel VPN – («Руководство пользователя. Специализированные команды», раздел «Работа с сертификатами»).

Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

4. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpn-dsp>en
Password:
```

Пароль по умолчанию: csp.
5. Перейдите в режим настройки:

```
belvpn-dsp#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

6. В настройках интерфейсов задайте IP-адреса:

```
belvpn-dsp(config)#interface FastEthernet 0/1
belvpn-dsp(config-if)#ip address 192.168.10.1 255.255.255.0
belvpn-dsp(config-if)#no shutdown
belvpn-dsp(config-if)#exit
```

7. Задайте адрес Client4 по умолчанию:

```
belvpn-dsp(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.5
```

8. Выйдите из cisco-like интерфейса:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

Формирование запроса и регистрация сертификата

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

9. При необходимости установите правильное системное время.

```
root@belvpn-dsp:~# date MMDDHHmmYYYY
```

MM – месяц;
DD – день;
HH – часы;
mm – минуты;
YYYY – год

Пример установки даты:

```
root@belvpn-dsp:~# date 042013152021
Wed Apr 20 13:15:00 UTC 2021
```

Данная запись соответствует 20 апреля 2021 года 13:15.

10. Создайте папку /opt/certs:

```
root@belvpn-dsp:~# mkdir /opt/certs
```

11. Создайте контейнер:

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptocont n -n=контейнер -p=пароль
```

контейнер – название создаваемого контейнера;
пароль – пароль (PIN) для доступа к контейнеру

Пример создания криптоконтейнера:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont n -n=container -p=12345678
```

12. Сформируйте запрос на сертификат.

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptcont r -n=контейнер -p=пароль -cn=CommonName
-c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

контейнер – название контейнера, созданного на предыдущем шаге;
пароль – пароль (PIN) для доступа к контейнеру;
CommonName – идентификатор устройства;
OrgName – наименование организации;
OrgUnitName – наименование подразделения;
путь_к_файлу – путь к файлу с создаваемым запросом, рекомендуется указывать расширение ***".req"***.
Пример создания запроса:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont r -n=container -p=12345678 -cn=GW1
-c=BY -o=S-TerraBel -t=Research -f=/opt/certs/Client1.req
```

13. Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением ***p7b*** или ***cer***).
Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные cer файлы.
14. Доставьте файлы сертификатов на Client1 безопасности в предварительно созданный на нем каталог /opt/certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, применив команду:

```
pscp исходный_файл root@адрес_клиента:/путь_к_файлу
```

исходный файл – путь к файлу сертификата;
адрес_шлюза – сетевой адрес Client1;
путь_к_файлу – полный путь для сохранения файла на Client1.

Пример передачи файла на Client1:

```
pscp D:\ca.cer root@192.168.10.1:/opt/certs
…
Store key in cache? (y/n)
root@192.168.10.1's password:
```

Важно: Среда передачи в этом случае должна быть доверенной

15. Выполните импорт сертификата УЦ в базу Client1 используя утилиту cert_mgr:

```
root@belvpn-dsp:~# cert_mgr import -f путь_к_файлу -t
```

путь_к_файлу – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@belvpn-dsp:~# cert_mgr import -f /opt/cert/UC.cer -t
1 OK C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
```

16. Выполните импорт локального (личного) сертификата в базу Client1:

```
root@belvpn-dsp:~# cert_mgr import -f путь_к_файлу -kc контейнер -kcp пароль
```

Copyright © S-Terra Bel 2008 - 2021

путь_к_файлу – полный путь к файлу сертификата УЦ;
контейнер – название контейнера, созданного ранее;
пароль – пароль для доступа к контейнеру.
Пример импорта:

```
root@belvpn-dsp:~#cert_mgr import -f /opt/cert/GW1.cer -kc container -kcp 12345678
1 OK CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

17. Выведите список сертификатов, находящихся в базе Client1, командой **cert_mgr show** и проверьте наличие записей **trusted** и **local**:

```
root@belvpn-dsp:~# cert_mgr show
```

Пример вывода:

```
root@belvpn-dsp:~# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted     C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 Status: local CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для Client1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpngate>en
Password:
```

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

18. Перейдите в режим настройки:

```
belvpn-dsp#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

19. Смените пароль по умолчанию:

```
belvpn-dsp(config)#username cscons password <пароль>
```

20. Смените название шлюза:

```
belvpn-dsp(config)#hostname belvpn-dsp
```

21. Задайте тип идентификации:

```
belvpn-dsp(config)#crypto isakmp identity dn
```

22. Задайте параметры для IKE:

```
belvpn-dsp(config)#crypto isakmp policy 1
belvpn-dsp(config-isakmp)#hash belt
belvpn-dsp(config-isakmp)#encryption belt
belvpn-dsp(config-isakmp)#authentication belt-sig
belvpn-dsp(config-isakmp)#group beltdh
belvpn-dsp(config-isakmp)#exit
```

23. Создайте набор преобразований для IPsec:

```
belvpn-dsp(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
belvpn-dsp(cfg-crypto-trans)#mode tunnel
belvpn-dsp(cfg-crypto-trans)#exit
```

24. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

Copyright © S-Terra Bel 2008 - 2021

```
belvpn-dsp(config)#ip access-list extended LIST
belvpn-dsp(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 20.20.20.0 0.0.0.255
belvpn-dsp(config-ext-nacl)#exit
```

25. Создайте динамическую крипто-карту:

```
belvpn-dsp(config)#crypto map CMAP 1 ipsec-isakmp
belvpn-dsp(config-crypto-map)#match address LIST
belvpn-dsp(config-crypto-map)#set transform-set TSET
belvpn-dsp(config-crypto-map)#set pfs beltdh
belvpn-dsp(config-crypto-map)#set peer 10.10.10.2
belvpn-dsp(config-crypto-map)#exit
```

26. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
belvpn-dsp(config)#interface FastEthernet0/1
belvpn-dsp(config-if)#crypto map CMAP
belvpn-dsp(config-if)#exit
```

27. Отключите обработку списка отозванных сертификатов (CRL):

```
belvpn-dsp(config)#crypto pki trustpoint s-terra_technological_trustpoint
belvpn-dsp(ca-trustpoint)#revocation-check none
belvpn-dsp(ca-trustpoint)#exit
```

28. Настройка устройства Client1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

29. Убедитесь, что все сертификаты активны – статус сертификата должен быть **active**:

```
root@belvpn-dsp:~# cert_mgr check
```

Пример:

```
root@belvpn-dsp:~# cert_mgr check
1 State: Active C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 State: Active CN=GW1,C=BY,O=S-TerraBel,OU=Research
```

В **Приложении** представлен текст cisco-like конфигурации для клиента Client1.

Настройка автоматизированного рабочего места (АРМ) пользователя

Настройка АРМ состоит из нескольких этапов:

подключение ПАУ Bel VPN Client-DSP 4.5 (Client1);
настройка политики обработки трафика на АРМ;
проверка работоспособности.

Все настройки производятся на АРМ пользователя, к которому подключен ПАУ «Клиент безопасности Bel VPN Client-DSP 4.5».

Для примера:

Для примера на АРМ пользователя установлена ОС 20.04.1-Ubuntu, тип системы x86_64 GNU/Linux.

Подключение ПАУ Bel VPN Client-DSP 4.5 (Client1)

30. Подключите ПАУ «Клиент безопасности Bel VPN Client-DSP 4.5» к АРМ пользователя через свободный USB-порт.
31. Убедитесь, что ПАУ «Клиент безопасности Bel VPN Client-DSP 4.5» подключен к АРМ пользователя, выполнив команду в терминале:

```
s-terra@s-terra-Default-string:~$ip a
```

В списке должен появиться новый адаптер, в нашем примере **адаптер enx1a5589a26943** (Рисунок 3).

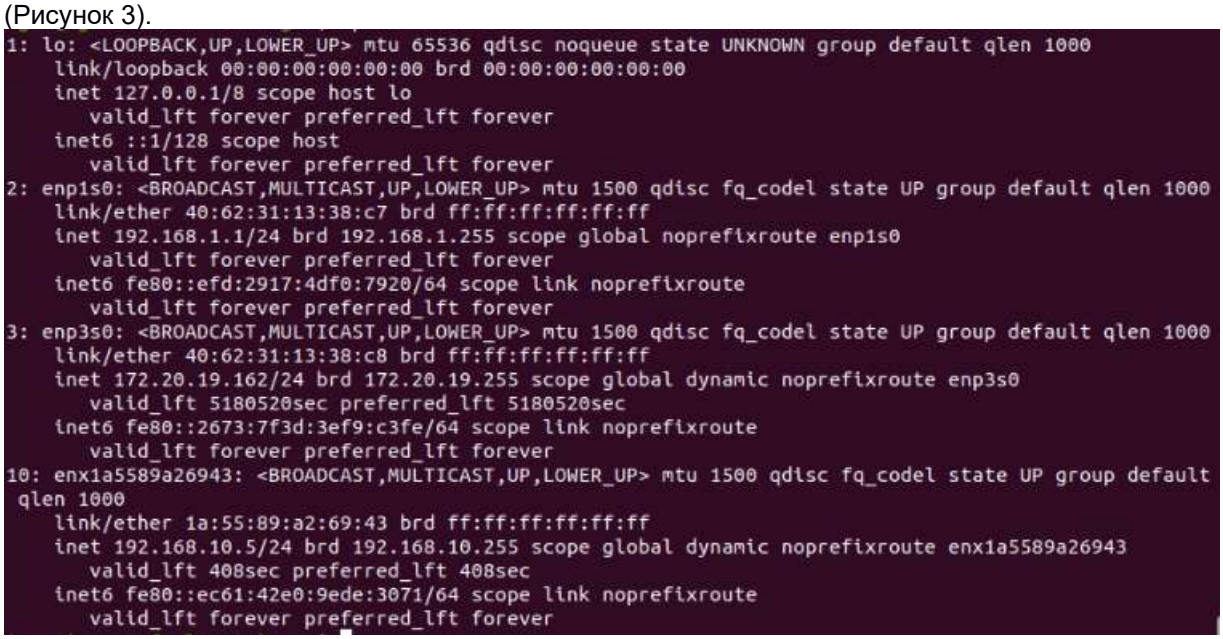

Рисунок 3.

IP-адрес ПАУ «Клиент ДСП 4.5» будет первый адрес подсети из которой получен адрес для адаптера (enx1a5589a26943) - **192.168.10.1**

32. Выполните команду, чтобы проверить доступность ПАУ «Клиент ДСП» (Рисунок 4):

```
s-terra@s-terra-Default-string:~$ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.751 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.863 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.707 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.721 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=0.779 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=0.916 ms
64 bytes from 192.168.10.1: icmp_seq=7 ttl=64 time=0.783 ms
64 bytes from 192.168.10.1: icmp_seq=8 ttl=64 time=1.04 ms
64 bytes from 192.168.10.1: icmp_seq=9 ttl=64 time=0.610 ms
64 bytes from 192.168.10.1: icmp_seq=10 ttl=64 time=0.760 ms
64 bytes from 192.168.10.1: icmp_seq=11 ttl=64 time=0.851 ms
^C
--- 192.168.10.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10145ms
rtt min/avg/max/mdev = 0.610/0.798/1.041/0.110 ms
```

Рисунок 4.

Проверка работоспособности

После того, как настройка всех устройств завершена, инициируйте создание защищенного соединения.

На устройстве АРМ пользователя выполните команду ping:

```
ping 20.20.20.2
```

В результате выполнения этой команды между устройствами АРМ пользователя и GW1 будет установлен VPN туннель.

Так же в этом можно убедиться на устройстве GW1, выполнив команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
```

```
1 1 (10.10.10.2,4500)-(192.168.1.1,62402) active 1968 3484

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (20.20.20.2,*)-(192.168.10.5,*) * ESP nat-t-tunn 192 192
```

Построение VPN туннеля между ПАК «Шлюз безопасности Bel VPN Gate 4.5» и ПАУ «Клиент ДСП 4.5» подключенного к АРМ под управлением ОС macOS Big Sur (аутентификация на ТСОК)

Описание стенда

Сценарий аналогичен предыдущему рассмотренному (см. Рис.1) и иллюстрирует построение защищенного соединения между подсетью SN1, защищаемой шлюзом безопасности «Bel VPN Gate», и автоматизированным рабочим местом (АРМ) пользователя, защищенного клиентом «Bel VPN Client-DSP 4.5» (устройство Client1). Для защиты будет построен VPN туннель между устройствами GW1 и Client1. АРМ сможет общаться по защищенному каналу (VPN) с устройствами из подсети SN1 (в частности с IPHost1). Адрес АРМ неизвестен заранее. В ходе построения защищенного соединения АРМ получает адрес от Client1 по DHCP.

В рамках данного сценария для аутентификации партнеры также будут использовать сертификаты

Настройка стенда

Настройка шлюза безопасности GW1

Аналогично, как и в предыдущем сценарии.

Настройка клиента ПАУ «Клиент ДСП 4.5» (Client1)

Все настройки производятся на АРМ администратора, к которому подключен ПАУ «Клиент ДСП 4.5», через Serial-порт (Вариант 1) или удаленно (по SSH (Вариант 2) с правами суперпользователя) по доверенному каналу связи.

Для примера на АРМ администратора установлена ОС macOS Big Sur.

Подключите ПАУ «Клиент ДСП 4.5» к АРМ администратора через свободный USB-порт.

1. Вариант 1:

Для подключения и дальнейшей настройки Client1 через последовательный порт необходимо в терминале набрать команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % ls /dev/tty.usbmodem*
```

результатом вывода команды будет путь к устройству (Рисунок 5), к которому необходимо подключиться с помощью команды:

```
s-terrabel@MacBook-Air-S-Terra ~ % screen /dev/tty.usbmodem000013
```

Copyright © S-Terra Bel 2008 - 2021

Рисунок 5.

2. Вариант 2:

Для подключения и дальнейшей настройки Client1 по SSH необходимо узнать IP-адрес для подключения. Для этого запустите командную строку и выполните команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % ifconfig
```

Из списка Адаптеров найдите тот, который появился при подключении Client1 (Рисунок 6).

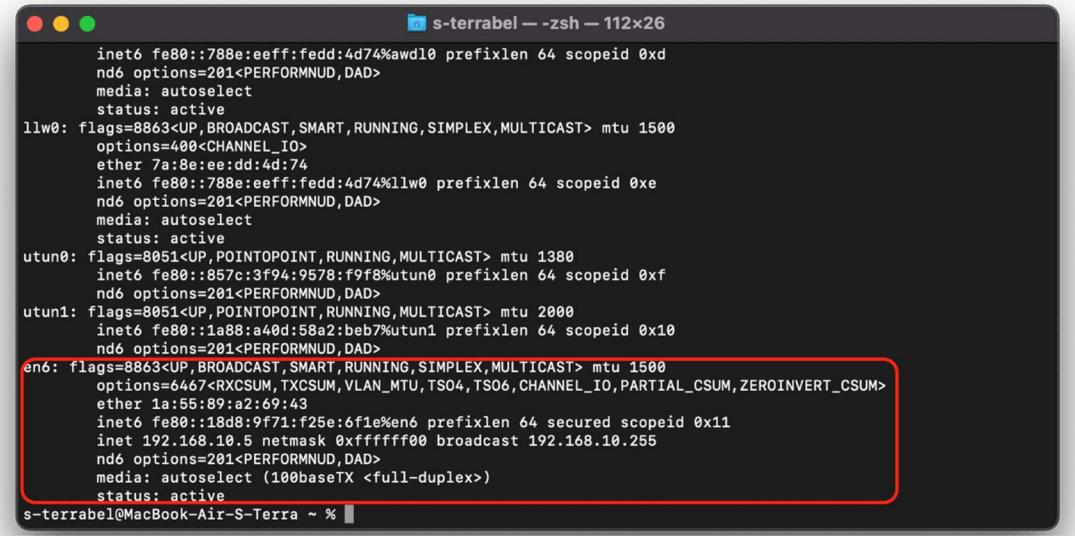

Рисунок 6.

IP-адрес Client1 будет первый адрес подсети из которой получен адрес сетевого интерфейса (en6) - **192.168.10.1**

3. Для подключения по SSH введите команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % ssh root@192.168.10.1
```

Инициализация клиента Client1 описывается в документации на ПАУ «Клиент ДСП 4.5» – («Руководство пользователя», раздел «Инициализация ПАУ Клиент ДСП 4.5 при первом старте»).

В данном сценарии для аутентификации используются сертификаты. Для корректной работы необходимо зарегистрировать сертификат CA (УЦ) и локальный сертификат.

В данном сценарии список отозванных сертификатов (CRL) не используется и будет отключен. Информацию об использовании CRL можно найти в документации на Программные продукты Bel VPN – («Руководство пользователя. Специализированные команды», раздел «Работа с сертификатами»).

Настройка интерфейсов

IP-адреса для интерфейсов рекомендуется настроить через cisco-like консоль.

4. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpn-dsp>en
Password:
```

Copyright © S-Terra Bel 2008 - 2021

Пароль по умолчанию: csp.

5. Перейдите в режим настройки:

```
belvpn-dsp#conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

6. В настройках интерфейсов задайте IP-адреса:

```
belvpn-dsp(config)#interface FastEthernet 0/1
belvpn-dsp(config-if)#ip address 192.168.10.1 255.255.255.0
belvpn-dsp(config-if)#no shutdown
belvpn-dsp(config-if)#exit
```

7. Задайте адрес Client4 по умолчанию:

```
belvpn-dsp(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.5
```

8. Выйдите из cisco-like интерфейса:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

Формирование запроса и регистрация сертификата

Для регистрации CA сертификата (сертификата УЦ) необходимо выполнить следующие действия:

9. При необходимости установите правильное системное время.

```
root@belvpn-dsp:~# date MMDDHHmmYYYY
```

MM – месяц;
DD – день;
HH – часы;
mm – минуты;
YYYY – год

Пример установки даты:

```
root@belvpn-dsp:~# date 042013152021
Wed Apr 20 13:15:00 UTC 2021
```

Данная запись соответствует 20 апреля 2021 года 13:15.

10. Создайте папку /opt/certs:

```
root@belvpn-dsp:~# mkdir /opt/certs
```

11. Создайте контейнер:

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptocont n -n=контейнер -p=пароль
```

контейнер – название создаваемого контейнера;
пароль – пароль (PIN) для доступа к контейнеру

Пример создания криптоконтейнера:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont n -n=container -p=12345678
```

12. Сформируйте запрос на сертификат.

```
root@belvpn-dsp:~#/opt/Avset/bin/cryptcont r -n=контейнер -p=пароль -cn=CommonName
-c=BY -o=OrgName -t=OrgUnitName -f=путь_к_файлу
```

контейнер – название контейнера, созданного на предыдущем шаге;
пароль – пароль (PIN) для доступа к контейнеру;
CommonName – идентификатор устройства;
OrgName – наименование организации;
OrgUnitName – наименование подразделения;
путь_к_файлу – путь к файлу с создаваемым запросом, рекомендуется указывать расширение ***“.req”***.

Copyright © S-Terra Bel 2008 - 2021

Пример создания запроса:

```
root@belvpn-dsp:~#/opt/Avest/bin/cryptocont r -n=container -p=12345678 -cn=GW1
-c=BY -o=S-TerraBel -t=Research -f=/opt/certs/Client1.req
```

13.Передайте полученный запрос сертификата в УЦ и получите файл сертификата (с расширением ***p7b*** или ***cer***).
Если вы получили файл сертификата в формате p7b, выполните экспорт в отдельные cer файлы.

14.Доставьте файлы сертификатов на Client1 безопасности в предварительно созданный на нем каталог /opt/certs. Для доставки можно воспользоваться утилитой pscp, применив команду:

```
scp исходный_файл root@адрес_клиента:/путь_к_файлу
```

исходный файл – путь к файлу сертификата;
адрес_шлюза – сетевой адрес Client1;
путь_к_файлу – полный путь для сохранения файла на Client1.

Пример передачи файла на Client1:

```
s-terrabel@MacBook-Air-S-Terra ~ % pscp ca.cer  root@192.168.10.1:/opt/certs
```

Важно: Среда передачи в этом случае должна быть доверенной

15.Выполните импорт сертификата УЦ в базу Client1 используя утилиту cert_mgr:

```
root@belvpn-dsp:~# cert_mgr import –f путь_к_файлу –t
```

путь_к_файлу – полный путь к файлу сертификата УЦ

Пример импорта:

```
root@belvpn-dsp:~# cert_mgr import –f /opt/cert/UC.cer –t
1 OK C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
```

Важно: Обратите внимание на применение обязательного параметра «-t» (trusted) при импорте сертификата УЦ.

16.Выполните импорт локального (личного) сертификата в базу Client1:

```
root@belvpn-dsp:~# cert_mgr import –f путь_к_файлу –kc контейнер –kcp пароль
```

путь_к_файлу – полный путь к файлу сертификата УЦ;
контейнер – название контейнера, созданного ранее;
пароль – пароль для доступа к контейнеру.
Пример импорта:

```
root@belvpn-dsp:~#cert_mgr import -f /opt/cert/GW1.cer -kc container -kcp 12345678
1 OK CN=Client1,C=BY,O=S-TerraBel,OU=Research
```

17.Выведите список сертификатов, находящихся в базе Client1, командой **cert_mgr show** и проверьте наличие записей **trusted** и **local**:

```
root@belvpn-dsp:~# cert_mgr show
```

Пример вывода:

```
root@belvpn-dsp:~# cert_mgr show
Found 2 certificates. No CRLs found.
1 Status: trusted     C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 Status: local CN=Client1,C=BY,O=S-TerraBel,OU=Research
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для Client1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль запустите cs_console:

```
root@belvpn-dsp:~# cs_console
belvpn-dsp>en
Password:
```

Пароль по умолчанию: csp.

Важно: пароль по умолчанию необходимо сменить.

18. Перейдите в режим настройки:

```
belvpn-dsp#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

19. Смените пароль по умолчанию:

```
belvpn-dsp(config)#username cscons password <пароль>
```

20. Смените название шлюза:

```
belvpn-dsp(config)#hostname belvpn-dsp
```

21. Задайте тип идентификации:

```
belvpn-dsp(config)#crypto isakmp identity dn
```

22. Задайте параметры для IKE:

```
belvpn-dsp(config)#crypto isakmp policy 1
belvpn-dsp(config-isakmp)#hash belt
belvpn-dsp(config-isakmp)#encryption belt
belvpn-dsp(config-isakmp)#authentication belt-sig
belvpn-dsp(config-isakmp)#group beltdh
belvpn-dsp(config-isakmp)#exit
```

23. Создайте набор преобразований для IPsec:

```
belvpn-dsp(config)#crypto ipsec transform-set TSET esp-belt esp-belt-mac
belvpn-dsp(cfg-crypto-trans)#mode tunnel
belvpn-dsp(cfg-crypto-trans)#exit
```

24. Опишите трафик, который планируется защищать. Для этого создайте расширенный список доступа:

```
belvpn-dsp(config)#ip access-list extended LIST
belvpn-dsp(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 20.20.20.0 0.0.0.255
belvpn-dsp(config-ext-nacl)#exit
```

25. Создайте динамическую крипто-карту:

```
belvpn-dsp(config)#crypto map CMAP 1 ipsec-isakmp
belvpn-dsp(config-crypto-map)#match address LIST
belvpn-dsp(config-crypto-map)#set transform-set TSET
belvpn-dsp(config-crypto-map)#set pfs beltdh
belvpn-dsp(config-crypto-map)#set peer 10.10.10.2
belvpn-dsp(config-crypto-map)#exit
```

26. Привяжите крипто-карту к интерфейсу, на котором будет туннель:

```
belvpn-dsp(config)#interface FastEthernet0/1
belvpn-dsp(config-if)#crypto map CMAP
belvpn-dsp(config-if)#exit
```

27. Отключите обработку списка отозванных сертификатов (CRL):

```
belvpn-dsp(config)#crypto pki trustpoint s-terra_technological_trustpoint
belvpn-dsp(ca-trustpoint)#revocation-check none
belvpn-dsp(ca-trustpoint)#exit
```

Copyright © S-Terra Bel 2008 - 2021

28.Настройка устройства Client1 в cisco-like консоли завершена. При выходе из конфигурационного режима происходит загрузка конфигурации:

```
belvpn-dsp(config)#end
belvpn-dsp#exit
```

29.Убедитесь, что все сертификаты активны – статус сертификата должен быть **active**:

```
root@belvpn-dsp:~# cert_mgr check
```

Пример:

```
root@belvpn-dsp:~# cert_mgr check
1 State: Active C=BY,L=Minsk,O=S-TerraBel,OU=Research,CN=UC
2 State: Active CN=Client1,C=BY,O=S-TerraBel,OU=Research
```

В **Приложении** представлен текст cisco-like конфигурации для клиента Client1.

30.Зайдите в настройки DHCP-сервера и пропишите маршруты для шифрованного трафика. Данные маршруты автоматически будут добавлены на АРМ пользователя при подключении Client1:

```
root@belvpn-dsp:~# sudo nano /etc/dhcp/dhcpd.conf
```

В блоке описания подсети 192.168.10.0 пропишите маршрут(ы):

```
subnet 192.168.10.0 netmask 255.255.255.0 {
   range 192.168.10.5 192.168.10.254;
   option subnet-mask 255.255.255.0;
   option rfc3442-classless-static-routes 24, 20, 20, 20, 192, 168, 10,
1;
   option ms-classless-static-routes 24, 20, 20, 20, 192, 168, 10, 1;
}
```

для примера прописан маршрут 20.20.20.0/24 192.168.10.1, где

option rfc3442-classless-static-routes - настройка передачи маршрута в ОС Linux;
option ms-classless-static-routes - настройка передачи маршрута в ОС Windows;
24 – маска подсети;
20, 20, 20 – подсеть шифрованного трафика (20.20.20.0);
192, 168, 10, 1 – хост за которым будет доступна данная подсеть.

Сохраните внесенные изменения в файле dhcpd.conf.

Настройка автоматизированного рабочего места (АРМ) пользователя

Настройка АРМ состоит из нескольких этапов:

- подключение ПАУ «Клиент ДСП 4.5» (Client1);
- настройка политики обработки трафика на АРМ;
- проверка работоспособности.

Все настройки производятся на АРМ пользователя, к которому подключен ПАУ «Клиент ДСП 4.5».

Для примера:

на АРМ пользователя установлена ОС macOS Bir Sur.

Подключение ПАУ «Клиент ДСП 4.5» (Client1)

31.Подключите ПАУ «Клиент ДСП 4.5» к АРМ пользователя через свободный USB-порт.

32.Убедитесь, что ПАУ «Клиент ДСП 4.5» подключен к АРМ пользователя, выполнив команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % ifconfig
```

В списке должен появиться новый адаптер, в нашем примере **en6** (Рисунок 7).

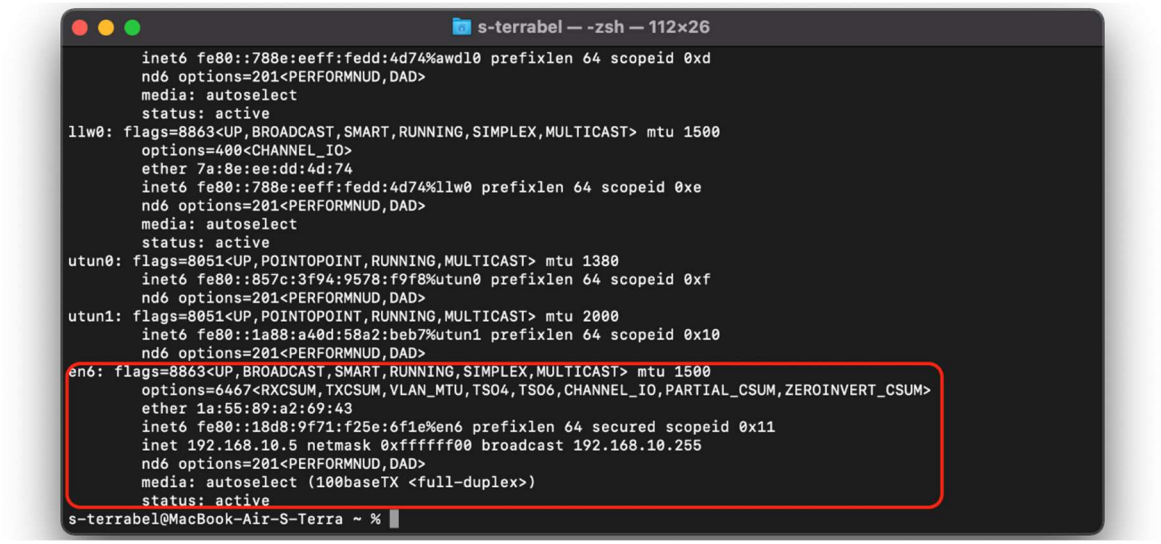

Рисунок 7.

IP-адрес ПАУ «Клиент ДСП 4.5» будет первый адрес подсети из которой получен адрес сетевого интерфейса (en6) - **192.168.10.1**

33. Выполните команду (Рисунок 8), чтобы проверить доступность ПАУ «Клиент ДСП 4.5»:

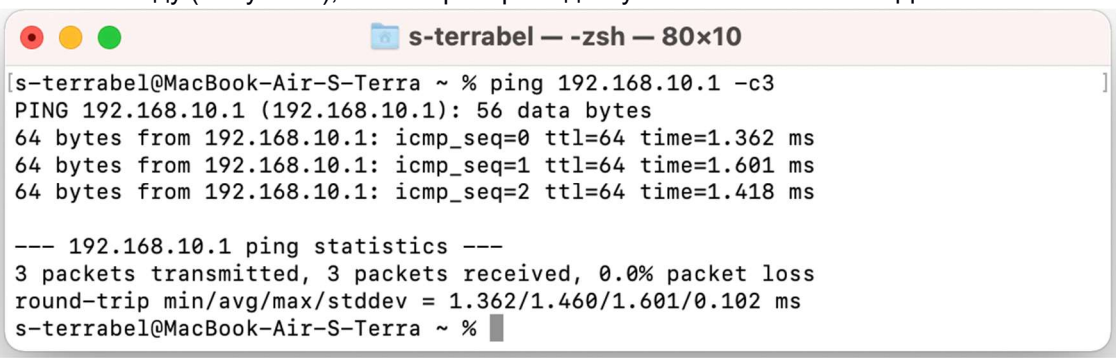

Рисунок 8.

Настройка политики обработки трафика на АРМ

34. Для настройки преобразования адресов (NAT) на сетевом интерфейсе подключенном к внешней сети (en0) создайте файл с именем /opt/nat.sh, используя команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % sudo nano /opt/nat.sh
```

со следующим содержимым:

```
#!/bin/bash
pfctl -d
sysctl -w net.inet.ip.forwarding=1
echo "nat on en0 from 192.168.10.1 to any -> (en0)" | pfctl -f -
pfctl -e
```

35. Дайте права на выполнение созданного файла используя команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % sudo chmod +x /opt/nat.sh
```

и выполните файл использую команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % /opt/nat.sh
```

36. Для применения настроек NAT при перезагрузке ОС, создайте файл /Library/LaunchDaemon/by.s-terra.vpnclient.plist, использую команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % sudo nano /Library/LaunchDaemon/by.s-
terra.vpnclient.plist
```

Copyright © S-Terra Bel 2008 - 2021

со следующим содержимым:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-
1.0.dtd">
<plist version="1.0">
   <dict>
            <key>Label</key>
            <string>by.s-terra.vpnclient</string>
            <key>ProgramArguments</key>
                    <array>
                            <string>/opt/nat.sh</string>
                    </array>
            <key>RunAtLoad</key>
            <true/>
   </dict>
</plist>
```

и загрузите этот файл в ОС используя команду:

```
s-terrabel@MacBook-Air-S-Terra ~ % launchctl load -w /Library/LaunchDaemon/by.s-
terra.vpnclient.plist
```

Проверка работоспособности

После того, как настройка всех устройств завершена, инициируйте создание защищенного соединения.

На устройстве АРМ пользователя выполните команду ping (Рисунок 9):

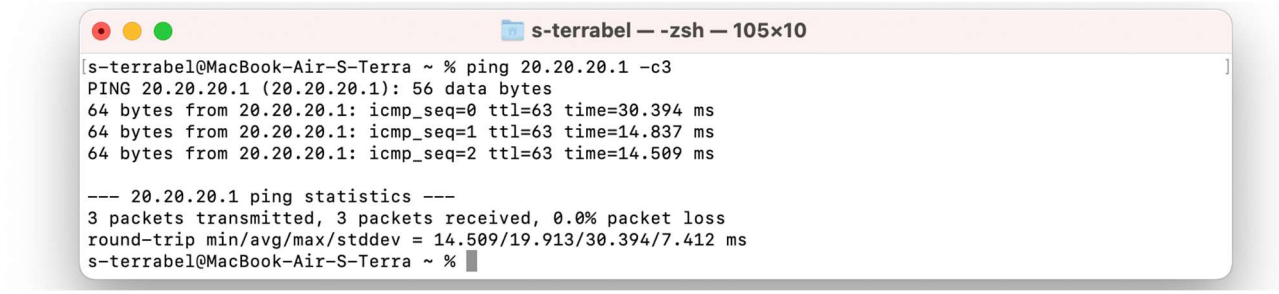

Рисунок 9

В результате выполнения этой команды между устройствами АРМ пользователя и GW1 будет установлен VPN туннель.

Так же в этом можно убедиться на устройстве GW1, выполнив команду:

```
root@GW1:~# sa_mgr show
```

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) State Sent Rcvd
1 1 (10.10.10.2,4500)-(192.168.1.1,62402) active 1968 3484

IPsec connections:
Num Conn-id (Local Addr,Port)-(Remote Addr,Port) Protocol Action Type Sent Rcvd
1 1 (20.20.20.2,*)-(192.168.10.5,*) * ESP nat-t-tunn 192 192
```

Copyright © S-Terra Bel 2008 - 2021