УТВЕРЖДЕНО

BY.РТНК.00001-03 34 01-5-ЛУ

Программно-аппаратный комплекс

«Шлюз безопасности Bel VPN Gate 3.0.1»

РУКОВОДСТВО ОПЕРАТОРА

Руководство администратора

Общие настройки

BY.РТНК.00001-03.01 34 01-5

Листов 18

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

2012

Общие настройки

После инсталляции Продукта Bel VPN Gate проводятся следующие настройки программно-аппаратного комплекса:

- Если планируется проводить настройки и управлять локальной политикой безопасности шлюза при помощи консоли удаленно по протоколу SSH1, то после инсталляции Bel VPN Gate рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать защищенный канал для настройки и конфигурирования политики безопасности. Создание начальной конфигурации описано в разделе «Начальная конфигурация для удаленного управления шлюзом» документа «Bel VPN Gate 3.0.1 Приложение». При использовании протокола SSH2 загрузка начальной конфигурации не нужна.
- Регистрация Лицензий на Продукт Bel VPN Gate, если они не были зарегистрированы в процессе инсталляции
- Назначение IP-адресов интерфейсам модуля или аппаратной платформы, если необходимо изменить IP-адреса и маски сетевых интерфейсов
- Назначение нескольких IP-адресов одному интерфейсу шлюза безопасности, если необходимо
- Установка или снятие драйвера Продукта на интерфейс аппаратной платформы в ОС Solaris, если необходимо
- Установка или снятие драйвера Продукта на интерфейс аппаратной платформы в ОС Linux, если необходимо
- Добавление сетевых интерфейсов, если изменился состав интерфейсов
- Добавление сетевых интерфейсов, поддерживающих 802.1Q, в ОС Red Hat Linux 9, если необходимо расширить Ethernet интерфейс
- Настройка многопроцессорности - производится настройка параметров продукта для достижения наилучшей производительности многопроцессорной аппаратной платформы.
- Изменение паролей рекомендуется выполнить.
- Создание и регистрация предопределенных ключей (Preshared keys), если аутентификация осуществляется на предопределенных ключах.
- Регистрация сертификатов, если аутентификация осуществляется на сертификатах.
- Настройка переменных окружения используется, чтобы сбалансировать нагрузку на шлюз - ограничить количество одновременно строящихся SAs, избежать пиковых нагрузок, получить дополнительную информацию для диагностики в файле лога.

После выполнения всех настроек перейдите к созданию политики безопасности шлюза, предварительно ознакомившись со «Сценариями конфигурирования».

Регистрация Лицензий после инсталляции

Регистрация Лицензии на Bel VPN Gate

Если в процессе инсталляции не была зарегистрирована Лицензия на Продукт Bel VPN Gate, то в ОС Linux регистрация Лицензии на Bel VPN Gate после инсталляции производится утилитой `lic_mgr`.

Утилита **`lic_mgr`**, описанная в документе «Специализированные команды», запускается из интерфейса командной строки из каталога Продукта `/opt/VPNagent/bin`:

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

Назначение IP-адресов интерфейсам

Прежде чем настраивать VPN соединения, необходимо назначить IP-адреса интерфейсам модуля или аппаратной платформы, если они не были назначены в процессе инсталляции Bel VPN Gate.

Чтобы просмотреть IP-адреса интерфейсов шлюза безопасности, можно воспользоваться системной командой `ifconfig –a`.

Изменение IP-адресов и маски сетевых интерфейсов можно осуществить одним из двух способов:

- запустить скрипт `ipsetup`
- редактированием “вручную” соответствующих конфигурационных файлов.

Скрипт ipsetup

Для изменения IP-адресов запустите в ОС Solaris скрипт `/usr/sbin/ipsetup (в ОС Linux – /bin/ipsetup)` без опций, который будет запрашивать последовательно IP-адрес и маску подсети для всех интерфейсов:

```
"Please, enter IP address/mask for eth0 or word "none" to
disable the interface [10.10.10.1/24]:"
```

Предлагается ввести IP-адрес и маску подсети для указанного сетевого интерфейса или слово `"none"` для отключения интерфейса. В квадратных скобках указано текущее значение IP-адреса/маски и формат, в котором они должны быть введены. При вводе пустой строки сохраняется текущее значение.

Может возникнуть ошибка в следующих случаях:

- при вводе в другом формате IP-адреса и маски подсети
- при дополнении IP-адреса слева нулями.

При обнаружении ошибки восстанавливается предыдущее значение адреса и маски, и предлагается ввести данные еще раз.

Изменение конфигурационных файлов происходит только после ввода всех параметров и их проверки.

Скрипт `ipsetup` можно прервать нажатием комбинации `Ctrl-C`.

Текущее имя хоста в скрипте не выводится и не запрашивается, так как изменить имя хоста нужно в cisco-like консоли `(cs_console)`.

Редактирование конфигурационных файлов

ОС Red Hat Linux 9

В ОС Red Hat Linux 9 изменить IP-адрес интерфейса можно, отредактировав файлы `/etc/hosts` и

`/etc/sysconfig/network-scripts/ifcfg-`**`имя_интерфейса`**`.`

Для обновления конфигурации сетевого интерфейса необходимо перезагрузить шлюз или выполнить команды:

```
ifdown имя_интерфейса

ifup имя_интерфейса
```


Если изменить параметры интерфейса нужно только на одну сессию, можно воспользоваться командой `ifconfig` или командами `ip link и ip address`. Например:

```
ifconfig eth0 192.168.15.2 netmask 255.255.255.0 up
```

или

```
ip link set dev eth0 up
ip address add 192.168.15.2/24 dev eth0
```

После перезагрузки шлюза безопасности эти изменения исчезнут.

Назначение нескольких IP-адресов одному интерфейсу

ОС Red Hat Linux 9

Вариант 1

Перед тем как назначить несколько IP-адресов одному интерфейсу необходимо создать в каталоге `/etc/sysconfig/network-scripts/` соответствующее количество файлов `ifcfg-имя_интерфейса:alias`.

Например, можно скопировать файл `ifcfg-eth0`, присвоив ему разные имена-псевдонимы:

```
cp ifcfg-eth0 ifcfg-eth0:0
cp ifcfg-eth0 ifcfg-eth0:1
cp ifcfg-eth0 ifcfg-eth0:2
```

Затем отредактировать эти файлы, указав имя виртуального интерфейса и IP-адрес.

Перезагрузить сетевой сервис:

```
service network restart
```

Вариант 2

При этом варианте назначения адресов, введенные изменения будут действовать только до перезагрузки шлюза безопасности.

Назначить дополнительный IP-адрес сетевому интерфейсу можно командой `ifconfig`. Например:

```
ifconfig eth0:1 192.168.15.2 netmask 255.255.255.0
```

или

```
ip addr add IP-адрес1/маска dev имя_интерфейса label
имя_интерфейса:1
ip addr add IP-адрес2/маска dev имя_интерфейса label
имя_интерфейса:2
```

Затем задать имя виртуального интерфейса в файле `/etc/hosts`.

Установка/снятие драйвера Продукта на интерфейс в ОС Linux

Проходящие через интерфейс пакеты обрабатываются драйвером Продукта, если драйвер установлен на интерфейсе.

Если нужно снять драйвер Продукта с какого-либо интерфейса, то отключите обработку трафика встроенными средствами Bel VPN Gate:

- с помощью утилиты **`if_mgr remove`** удалите из базы данных запись о том, что данный интерфейс является защищаемым. Это сведет затраты ресурсов компьютера на обработку пакетов в драйвере на данном интерфейсе к минимуму.

Для установки (восстановления) драйвера Продукта на сетевом интерфейсе выполните обратную опрацию:

- с помощью утилиты **`if_mgr add`** зарегистрируйте в базе данных Продукта запись о том, что данный интерфейс является защищаемым.

Перезагрузка LSP при изменении состояния интерфейсов

Периодически демон (vpnsvc) продукта 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 Продукта.

Изменения в состоянии интерфейсов могут быть следующими:

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

Добавление сетевых интерфейсов

ОС Red Hat Linux 9

Если необходимо добавить сразу несколько интерфейсов, каждый шаг можно выполнять для всех добавляемых интерфейсов сразу.

1. В файл `/etc/hosts` добавить соответствие IP-адреса нового интерфейса и имени. Ниже это имя обозначено как `имя_интерфейса`. Имя интерфейса не должно совпадать с другими именами, перечисленными в файлах `/etc/hosts`.
2. В файл `/etc/sysconfig/network-scripts/ifcfg- имя_интерфейса` внести адрес и маску подсети.

   Перезагрузить шлюз или поднять интерфейс вручную командой:

   ```
   ifup имя_интерфейса
   ```

3. Зарегистрировать интерфейс в базе продукта командой:

   ```
   /opt/VPNagent/bin/if_mgr add -n имя_интерфейса
   -l имя_интерфейса
   ```


Добавление сетевых интерфейсов, поддерживающих 802.1Q, в ОС Red Hat Linux 9

Интерфейс 802.1Q является расширением обычного Ethernet интерфейса (см. Стандарт IEEE 802.1Q).

В Продукте, работающем под управлением ОС Red Hat Linux 9, можно добавить несколько интерфейсов 802.1Q.

Если необходимо добавить сразу несколько интерфейсов 802.1Q, то каждый шаг нужно выполнять для каждого добавляемого интерфейса.

1. Создать файл `/etc/sysconfig/network-scripts/ifcfg-`**`имя_интерфейса.vid_интерфейса`** (например, `ifcfg-eth1.100`) следующего содержания:

   ```
   DEVICE=имя_интерфейса.vid_интерфейса
   ONBOOT=yes
   IPADDR=адрес_интерфейса
   NETMASK=сетевая_маска_интерфейса
   BROADCAST=широковещательный_адрес
   VLAN=yes
   VID=vid_интерфейса
   ```

2. Перезагрузить ОС или активизировать интерфейс командой

   ```
   ifup имя_интерфейса.vid_интерфейса
   ```

3. Зарегистрировать интерфейс в Продукте командой

   ```
   /opt/VPNagent/bin/if_mgr add -n имя_интерфейса.vid_интерфейса -l логическое_имя_интерфейса.
   ```

Интерфейсы 802.1Q конфигурируются и работают в Продукте также, как и другие интерфейсы.

Настройка параметров многопроцессорной обработки трафика в ОС Linux

Если программно-аппаратная платформа имеет более одного процессора, то для достижения наилучшей производительности шлюза безопасности Bel VPN Gate в ОС Red Hat Linux 9 выполните следующие действия:

- установите количество криптоконтекстов на один SA равным NNN, где NNN лежит в диапазоне между 2 и половиной количества процессорных ядер:
  - в файле `/opt/VPNagent/etc/agent.ini` измените значение параметра

    ```
    DefaultCryptoContextsPerIPSecSA=NNN
    ```

  - или в загружаемой LSP в структуре `IPsecAction` присвойте значение NNN атрибуту

    ```
    CryptoContextsPerIPSecSA=NNN
    ```

- установите количество нитей в драйвере равным количеству процессорных ядер:

- в файле /`etc/modules.conf` в конец строки, начинающейся с `options vpndrvr`, допишите `pcap_thr_num=NNN` (или измените существующее значение, если есть).
  Если нужно установить количество нитей, превышающее количество процессорных ядер, то в конец той же строки дополнительно добавьте `pcap_thr_bound=0` (не рекомендуется).

Количество криптоконтекстов на один SA не рекомендуется устанавливать больше количества нитей.

Изменение паролей

После инсталляции Продукта пользователь "root" с правами системного администратора имеет пустой пароль, который изменяется системными средствами:

- зайдите в систему пользователем "root"
- выполните команду "passwd"
- введите новый пароль.

Специальный пользователь, созданный в процессе инсталляции с именем "cscons", имеет пароль "csp" и уровень привилегий 15. Ему предоставляется возможность управлять настройками Bel VPN Gate 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.

В интерфейсе командной строки изменение пароля и создание новых пользователей осуществляется командами **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**.

Создание и регистрация предопределенных ключей (Preshared keys)

Перед загрузкой LSP, созданной в виде конфигурационного файла, следует создать и зарегистрировать предопределенный ключ для создания соединения с каждым из партнеров. Предопределенный ключ создается и записывается в файл, а его регистрация в базе Продукта осуществляется специализированной командой **`key_mgr import`**.

При создании политики безопасности посредством команд интерфейса командной строки существует возможность здесь же создать и зарегистрировать предопределенные ключи в базе Продукта.

После регистрации предопределенных ключей перейдите к созданию политики безопасности шлюза, предварительно ознакомившись со «Сценариями конфигурирования».

Регистрация сертификатов

Регистрация локальных сертификатов

Перед созданием политики безопасности любым способом следует зарегистрировать локальные сертификаты в базе Продукта. Для регистрации используется специализированная команда **cert_mgr import**. В параметрах команды указывается путь к файлу (контейнеру) с локальным сертификатом и контейнеру с секретным ключом.

Регистрация CA сертификатов

Зарегистрировать CA сертификат в базе Продукта можно двумя способами:

- с помощью специализированной команды **cert_mgr import**
- в консоли командами **crypto ca trustpoint** и **crypto ca certificate chain.** Используя последнюю команду можно зарегистрировать цепочку CA сертификатов.

Подробно работа с сертификатами – отсылка локального сертификата партнеру, получение сертификата партнера по IKE, LDAP, получение CRL и др. описана в документе «Сценарии конфигурирования».

После того, как сертификаты зарегистрированы, перейдите к созданию политики безопасности шлюза, предварительно ознакомившись со «Сценариями конфигурирования».

Настройка переменных окружения

Имеется возможность настроить некоторые переменные окружения, которые могут повлиять на работу Bel VPN Gate или дать возможность получить дополнительную информацию в лог-файле.

Можно изменить значения следующих переменных окружения в файле `/etc/init.d/vpngate`:

- CSP_IKE_RESP_MAX
- CSP_IKE_PH1_LIFETIME_DELTA
- CSP_SYS_RESPONSE_TIMEOUT
- CSP_LOG_TASK_TIME
- CSP_LOG_TASK_QUEUE_PERIOD.

Начальные установленные значения всех переменных окружения равны 0.

Начальные установленные значения переменных совпадают со значениями, установленными по умолчанию (когда переменные отсутствуют в файле `/etc/init.d/vpngate` либо заданы некорректные значения).

CSP_IKE_RESP_MAX	данный параметр задает максимальное количество одновременно проводимых сессий со всеми партнерами в качестве ответчика. Это позволяет ограничить нагрузку на шлюз при лавинных запросах на создание соединений со стороны клиентов. Оптимальное значение порога имеет смысл подбирать в зависимости от производительности шлюза, количества клиентов и их активности. Изменять параметр необходимо перед (ре)стартом сервиса.

Необходимость данной настройки возникает при интенсивной загрузке шлюза Bel VPN Gate в качестве ответчика. Например, после перезагрузки конфигурации при интенсивном входящем трафике со стороны большого количества партнеров, которые одновременно начинают создавать SA со шлюзом, который также начинает создание SA сразу со многими партнерами. При этом у шлюза ресурсов (процессор, память) не хватает, чтобы успеть построить SA за заданное время. Решить такую проблему можно - ограничить количество одновременно строящихся SAs.

Переменная CSP_IKE_RESP_MAX позволяет сбалансировать нагрузку на шлюз и тем самым уменьшить время создания SA.

Определить оптимальное значение этой переменной можно по следующему алгоритму:

- эмпирически установить ограничение в `X` соединений и при этом с помощью утилиты `prstat` посмотреть уровень загрузки шлюза в процентах, пусть это будет y%;
- оптимальное значение переменной можно вычислить следующим образом:

  90% * (x соединений - 20 соединений)/(y% - 20%).

Если значение переменной CSP_IKE_RESP_MAX = 0, то это означает, что используется значение по умолчанию, которое для данной версии Bel VPN Gate равно 50.

CSP_IKE_PH1_LIFETIME_DELTA	задает процент от времени жизни (LifetimeSeconds в IKETransform) установленного ISAKMP SA. В пределах заданного значения выбирается случайная величина, на которую будет уменьшено первоначально установленное время жизни ISAKMP SA для данной сессии. И при каждом установлении ISAKMP SA будет выполняться такая процедура уменьшения времени жизни. Переменной CSP_IKE_PH1_LIFETIME_DELTA можно задавать значения от 1 до 50 процентов.

Необходимость в задании переменной CSP_IKE_PH1_LIFETIME_DELTA появилась при интенсивной загрузке шлюза Bel VPN Gate, чтобы рассредоточить моменты пересоздания ISAKMP SA с одинаковыми временами жизни. Например, после перезагрузки конфигурации при интенсивном входящем трафике со стороны большого количества партнеров, происходит одновременное создание ISAKMP SA и наступает момент пиковой нагрузки. После того, как с партнерами созданы SA, которые живут определенное время, и если оно одинаковое, то опять наступает момент пиковой нагрузки.

Переменная CSP_IKE_PH1_LIFETIME_DELTA позволяет случайным образом уменьшить время жизни SA, что приводит к рассредоточению по времени момента пересоздания SA для всех партнеров, снижению нагрузки на шлюз и тем самым уменьшить время пересоздания ISAKMP SA.

Если значение CSP_IKE_PH1_LIFETIME_DELTA = 0, то процедура уменьшения времени жизни SA не применяется.

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 уровня `info`.

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:

	`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: `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.