

ЗАО «С-Терра СиЭсПи»
124460, г. Москва, Зеленоград, проезд 4806, д.6, этаж 4-й
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: <http://www.s-terra.com>



Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.1”

Руководство администратора

Настройка шлюза

РЛКЕ.00005-01 90 03

03.04.2012

Содержание

Настройка шлюза	3
Этапы настройки шлюза безопасности	3
Общие настройки шлюза.....	3
Регистрация Лицензий после инициализации	4
Изменение паролей	5
Настройка интерфейсов	6
Настройка переменных окружения	12
Настройка параметров многопроцессорной обработки трафика для Gate3000 и Gate7000	15
Настройка NTP (Network Time Protocol)	17
Настройка NAT на шлюзе безопасности	19
Построение VPN туннеля между шлюзом безопасности CSP VPN Gate 3.1 и рабочим местом администратора для удаленной настройки шлюза	20
Способы создания политики безопасности	29
Загрузка политики безопасности	29
Конвертирование	30
Приложение.....	31
Управление службой vpngate	31
Текст cisco-like конфигурации для устройства GW1	32
Текст LSP для устройства GW1	33
Текст LSP для устройства AdminHost	35

Настройка шлюза

Перед настройкой шлюза безопасности, использующего СКЗИ «КриптоПро CSP 3.6» в режиме КС1/КС2, рекомендуется ознакомиться с правилами пользования, изложенными в документе [«Программный комплекс CSP VPN Gate. Версия 3.1. Правила пользования»](#) (Rules.pdf).

Перед настройкой шлюза и созданием политики безопасности выполните инициализацию программного комплекса CSP VPN Gate 3.1, которая описана в документах [«Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6»](#)», [«Инициализация CSP VPN Gate при использовании СКЗИ «Крипто-КОМ 3.2»](#) или [«Руководство по установке и настройке NME-RVPN модуля \(MCM\)»](#).

Этапы настройки шлюза безопасности

Настройка программно-аппаратного комплекса (ПАК) и модуля NME-RVPN в исполнении MCM осуществляется в два этапа:

- [общая настройка шлюза](#)
- [создание политики безопасности шлюза](#).

Общие настройки шлюза

Перечислим общие настройки шлюза, описанные подробно далее:

- [Регистрация Лицензий](#) на продукт CSP VPN Gate и КриптоПро CSP 3.6, если их необходимо перерегистрировать
- [Изменение паролей](#) рекомендуется выполнить
- [Настройка интерфейсов](#):
 - [Назначение IP-адресов](#) интерфейсам
 - [Назначение нескольких IP-адресов](#) одному интерфейсу
 - [Добавление](#) сетевых интерфейсов
 - [Установка или снятие](#) драйвера Продукта на интерфейс аппаратной платформы, если необходимо
 - [Настройка MTU](#) интерфейса
 - [Перезагрузка LSP](#) при изменении состояния интерфейсов
- [Настройка переменных окружения](#) для балансировки нагрузки на шлюз
- [Настройка многопроцессорности](#) для ПАК Gate3000 и Gate7000 для достижения наилучшей производительности ПАК
- [Синхронизация часов](#) на шлюзе безопасности с NTP-сервером точного времени
- [Настройка NAT](#)
- Если планируется настраивать шлюза удаленно по протоколу SSH1 или SSH2 при помощи интерфейса командной строки, рекомендуется [загрузить начальную конфигурацию](#) для создания [защищенного канала](#) конфигурационных сессий.

Регистрация Лицензий после инициализации

Регистрация Лицензии на CSP VPN Gate

Если возникнет необходимость перерегистрировать Лицензию на продукт CSP VPN Gate, то регистрация Лицензии после инициализации 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
```

Регистрация Лицензии на КристоПро CSP 3.6

В случае необходимости перерегистрировать лицензию на СКЗИ "КристоПро CSP 3.6" следует запустить утилиту:

```
/opt/cprocsp/sbin/ia32/cpconfig -license -set xxxxxxxx,
```

где

xxxxxxx – серийный номер продукта "КристоПро CSP 3.6".

Для регистрации драйверной части лицензии выполните команду:

```
/opt/cprocsp/sbin/ia32/set_driver_license.sh
```

После регистрации перезапустите `vpn`-демона, выполнив команду:

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

В ОС Solaris 10 перезапустить `vpn`-демона можно также командой (см. раздел «Управление службой `vpngate`»):

```
svcadm restart vpngate
```

Изменение паролей

После инициализации 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 CSP 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`.

Настройка интерфейсов

Перед назначением IP-адресов интерфейсам модуля или аппаратной платформы просмотрите IP-адреса интерфейсов при помощи системной команды `ifconfig -a` или командой cisco-like консоли `show running-config`.

Необходимо отметить, что настройку интерфейсов следует производить по-разному, в зависимости от того, каким образом выполняется настройка шлюза безопасности. Если политика безопасности создается с использованием cisco-like консоли, то настройка интерфейсов должна выполняться при помощи команд консоли, если политика безопасности создается путем написания конфигурационного файла, то настройку рекомендуется выполнять при помощи команды `ifconfig` и специальных утилит, входящих в CSP VPN Gate.

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/`.

Для входа в глобальный конфигурационный режим системы используйте команду `configure terminal`. Затем, чтобы настроить сетевые интерфейсы, необходимо войти в режим `interface configuration`, задав команду `interface type port/number` (имя сетевого интерфейса в консоли формируется по шаблону "fastethernet0/x", где x – неотрицательное число, независимо от реального типа интерфейса). 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 «Cisco-like команды» (`Console_command_reference.pdf`).

Назначение IP-адресов интерфейсам

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

- при помощи команд cisco-like консоли
- при помощи команды `ifconfig` и специальных утилит.

Назначение IP-адресов в cisco-like консоли

1. Войдите в режим `interface configuration`:

```
interface fastethernetport/number
```

2. 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`

в ОС Solaris 10

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:

```
/usr/sbin/ni_saveif.sh имя_интерфейса
```

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

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

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`.

В ОС Solaris 10

1. Создайте сначала виртуальный интерфейс:

```
ifconfig имя_интерфейса:1 plumb
```

```
ifconfig имя_интерфейса:2 plumb
```

```
ifconfig имя_интерфейса:1 IP-адрес1 netmask маска up
```

```
ifconfig имя_интерфейса:2 IP-адрес2 netmask маска up
```

(Замечание: имя_интерфейса:0 указывает на интерфейс, на котором назначаются виртуальные интерфейсы).

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

```
/usr/sbin/ni_saveif.sh имя_интерфейса
```

3. Зарегистрируйте интерфейс в CSP VPN Gate с помощью специальной команды `if_mgr add`, которая описана в документе «[Специализированные команды](#)» (Util_reference.pdf).

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

1. Создайте сначала виртуальный интерфейс:

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

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

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

3. Зарегистрируйте интерфейс в CSP VPN Gate с помощью специальной команды `if_mgr add`, которая описана в документе «[Специализированные команды](#)» (Util_reference.pdf).

Добавление сетевых интерфейсов

в ОС Solaris 10

1. Поднимите новый сетевой интерфейс командой:

```
ifconfig имя_интерфейса plumb IP-адрес netmask маска up
```

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

```
/usr/sbin/ni_saveif.sh имя_интерфейса
```

3. Зарегистрируйте интерфейс в CSP VPN Gate с помощью утилиты `if_mgr add`:

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

ОС Red Hat Enterprise Linux 5 (CentOS 5)

1. Поднимите новый сетевой интерфейс командой:

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

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

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

3. Зарегистрируйте интерфейс в CSP VPN Gate с помощью утилиты `if_mgr add`:

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

Добавление сетевых интерфейсов, поддерживающих 802.1Q

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

ОС Red Hat Enterprise Linux 5 (CentOS 5)

Чтобы добавить интерфейс 802.1Q в Продукт, выполните следующие действия:

1. Создайте файл

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

следующего содержания:

```
DEVICE=имя_интерфейса.vlan_id
```

```
VLAN=yes
```

```
ONBOOT=no
```

```
IPADDR=адрес интерфейса
```

```
NETMASK=сетевая_маска
```

2. Для каждого из созданных 802.1Q интерфейсов необходимо в конец файла

```
/etc/rc.d/rc.local
```

добавить строчку:

```
ifup имя_интерфейса.vlan_id
```

3. Выполните команду

```
ifup имя_интерфейса.vlan_id
```

или перезапустите vpn-демона, выполнив команду

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

При необходимости зарегистрируйте интерфейс в CSP VPN Gate с помощью утилиты `if_mgr add`.

в ОС Solaris 10

1. Поднимите интерфейс командой:


```
ifconfig имя_интерфейса plumb
```

где имя_интерфейса представлено в виде

<имя ethernet-интерфейса без_цифр><id_vlan X 1000+номер интерфейса>

Например, чтобы создать vlan интерфейс с id 4 на интерфейсе nge1, задайте команду
ifconfig nge4001 plumb

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

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

3. Перезагрузите шлюз или поднимите интерфейс вручную командой ifconfig.

При необходимости зарегистрируйте интерфейс в CSP VPN Gate с помощью утилиты if_mgr add.

Установка/снятие драйвера Продукта на интерфейс

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

в ОС Solaris

Снять или установить драйвер Продукта на какой-либо интерфейс можно по одному из следующих сценариев:

отключение обработки трафика встроенными средствами CSP VPN Gate:

1. с помощью утилиты if_mgr remove удалите из базы Продукта запись о том, что данный интерфейс является защищаемым.

снятие драйвера Продукта с сетевого интерфейса (вариант 1):

1. выполните команду:

```
ifconfig <имя_интерфейса> modlist
```

2. найдите слово "vpndrvr" в выводе утилиты. Перед этим словом будет указано число – позиция драйвера в стеке (<pos>)

3. далее выполните команду:

```
ifconfig <имя_интерфейса> modremove vpndrvr@<pos>
```

Драйвер будет удален с сетевого интерфейса до пересоздания этого интерфейса (при помощи команды ifconfig unplumb/ifconfig plumb или перезагрузки компьютера).

снятие драйвера Продукта с сетевого интерфейса (вариант 2):

1. найдите номер устройства драйвера сетевого интерфейса (major). Для этого выполните команду

```
grep <имя_драйвера> /etc/name_to_major",
```

где

<имя_драйвера> – имя сетевого интерфейса без числа на конце.

2. выполните команды:

```
autopush -r -M <major> -m 0
```

```
ifconfig <имя_интерфейса> unplumb plumb <конфигурационные  
парамеры...>,
```

где

<конфигурационные парамеры...> – стандартные параметры сетевого интерфейса (IP-адрес, маска подсети и т.д.).

После выполнения команды "`autopush ...`" и до перезагрузки, драйвер Продукта не будет установлен на вновь созданные сетевые интерфейсы того же типа.

снятие драйвера Продукта с сетевых интерфейсов одного типа:

3. закомментируйте соответствующую строчку в файле "`/etc/iu.ap`".
4. перезагрузите компьютер или воспользуйтесь предыдущим способом для немедленного снятия драйвера.

установка (восстановление) драйвера Продукта на сетевом интерфейсе (после снятия драйвера вышеописанными методами):

1. верните измененные строки в файле `/etc/iu.ap`.
2. перезагрузите компьютер или выполните команду

```
autopush -f /etc/iu.ap
```
3. пересоздайте сетевые интерфейсы (`ifconfig unplumb plumb ...`).

установка драйвера Продукта на сетевом интерфейсе нового типа:

1. добавьте строчку в файл `/etc/iu.ap` с именем драйвера нового интерфейса (по аналогии с уже существующими)
2. выполните команду

```
autopush -f /etc/iu.ap
```
3. перезагрузите или создайте (пересоздайте) новый сетевой интерфейс.
4. зарегистрируйте интерфейс в CSP VPN Gate с помощью утилиты `if_mgr add`.

в ОС Linux

Снятие драйвера Продукта с какого-либо интерфейса осуществляется отключением обработки трафика встроенными средствами CSP VPN Gate:

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

Установка (восстановление) драйвера Продукта на сетевом интерфейсе выполняется обратной операцией:

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

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.

в ОС Solaris 10

Настройка MTU сетевого интерфейса осуществляется следующим образом:

1. в файле `/etc/hostname.e1000gX` добавьте строчку

```
mtu YYYY
```

где

X – номер интерфейса

YYYY – размер MTU сетевого интерфейса.

2. перезагрузите ОС.

Таким образом устанавливается постоянное значение MTU.

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

```
ifconfig e1000g0 mtu YYYY (для интерфейса fa 0/0)
```

```
ifconfig e1000g1 mtu YYYY (для интерфейса fa 0/1)
```

где

YYYY – размер MTU сетевого интерфейса.

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

Настройка MTU сетевого интерфейса осуществляется следующим образом:

1. в файле /etc/sysconfig/network-scripts/ifcfg-ethX добавьте строку

```
MTU=YYYY
```

где

X – номер интерфейса, а YYYY - размер MTU сетевого интерфейса.

2. перезагрузите ОС

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)
```

где

YYYY - размер MTU сетевого интерфейса.

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.

Настройка переменных окружения

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

Можно изменить значения следующих переменных окружения:

- CSP_IKE_RESP_MAX
- CSP_IKE_PH1_LIFETIME_DELTA
- CSP_SYS_RESPONSE_TIMEOUT
- CSP_LOG_TASK_TIME
- CSP_LOG_TASK_QUEUE_PERIOD
- CSP_IKE_ASYNC_DH.

Начальные значения, установленные инсталлятором, для всех переменных окружения равны 0 и совпадают со значениями, установленными по умолчанию. Исключение составляет переменная окружения CSP_IKE_ASYNC_DH, у которой начальное значение зависит от операционной системы: в ОС Solaris оно равно 1, а в ОС Linux – 0.

в ОС Solaris 10

Выполните команды для изменения значений переменных окружения:

1. `svccfg -s vpngate setenv <envvar name> <value>`
2. `svcadm refresh vpngate`
3. `svcadm restart vpngate`

где

`<envvar name>` – имя переменной окружения

`<value>` – значение переменной.

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

Изменить значение переменных окружения можно следующим образом:

1. отредактировать файл `/etc/init.d/vpngate`
2. перезапустить vpn-демона, выполнив команду
`/etc/init.d/vpngate restart.`

Описание переменных окружения

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 CSP 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.

Если значение переменной `CSP_IKE_RESP_MAX = 0`, то это означает, что используется значение по умолчанию, которое для данной версии CSP 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 CSP 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: <pre>Task time is <n> sec (src=<hex> dst=<hex> idx=<n> proc=<hex>)</pre> 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: <pre>Waiting time of task queue is <n> sec, queue length is <n> tasks.</pre> Если CSP_LOG_TASK_QUEUE_PERIOD = 0, то сообщения в файл лога не выводятся.
Переменная окружения CSP_IKE_ASYNC_DH задает синхронный или асинхронный режим генерации ключевой пары и вычисления общего секретного ключа (разделяемого секрета) по алгоритму Диффи-Хеллмана (или его реализации – VKO).	
CSP_IKE_ASYNC_DH	задает режим генерации ключевых пар. При включении асинхронного режима повышается производительность по созданию ISAKMP SA и IPsec SA на многопроцессорных платформах. Асинхронный режим включается установкой переменной окружения CSP_IKE_ASYNC_DH в единицу.

Настройка параметров многопроцессорной обработки трафика для Gate3000 и Gate7000

Если программно-аппаратная платформа имеет более одного процессора, то производительность шлюза безопасности CSP VPN Gate зависит от многих факторов – используемого криптопровайдера, количества криптоконтекстов, приходящихся на один SA, и других факторов. А количество криптоконтекстов на один SA, в свою очередь, зависит от количества процессорных ядер, количества SA, однонаправленности или двунаправленности трафика, количества используемых криптоалгоритмов. И определение оптимального количества криптоконтекстов производится экспериментально. Для начала вычислите диапазон значений, которые может принимать количество криптоконтекстов на один SA (N_c), следуя выражению:

$$NNN / (N_{alg} * N_{dir} * N_{sa}) - 1 \leq N_c \leq NNN,$$

где

N_c – количество криптоконтекстов на один SA

NNN – количество процессорных ядер

N_{alg} – количество используемых алгоритмов

N_{dir} – количество направлений трафика

N_{sa} – количество IPsec SA

Например,

количество процессорных ядер $NNN=8$

количество используемых алгоритмов $N_{alg}=2$ (в режиме ESP алгоритм шифрования и проверки целостности (CipherAlg и IntegrityAlg))

количество направлений трафика $N_{dir}=2$ (двунаправленный)

количество соединений $N_{sa}=1$

Тогда в этом случае количество криптоконтекстов на один SA лежит в диапазоне

$$1 \leq N_c \leq 8.$$

в ОС Solaris 10

Далее выполните следующие действия:

- установите количество криптоконтекстов на один SA из вычисленного диапазона значений:
 - в файле `/opt/VPNagent/etc/agent.ini` измените значение параметра `DefaultCryptoContextsPerIPSecSA=Nc`
 - или в загружаемой LSP в структуре `IPsecAction` присвойте значение N_c атрибуту `CryptoContextsPerIPSecSA=Nc`
- установите количество нитей в драйвере, равным количеству процессорных ядер (NNN):
 - в файле `/etc/system` добавьте строку `set vpdnrvr:pcap_nthreads = NNN`
- установите размер внутренней очереди пакетов, равным YYY , где YYY лежит в диапазоне от $NNN+1$ до $2*NNN$ (включительно):
 - в файле `/etc/system` добавьте строку

```
set vpndrvr:pcap_pkt_q_size = YYY
```

4. перезагрузите ОС.

Меняя количество криптоконтекстов в пределах вычисленного диапазона значений, экспериментально определите его оптимальное значение, при котором шлюз безопасности показывает более высокую производительность.

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

Далее выполните следующие действия:

1. установите количество криптоконтекстов на один SA, равным Nc:
 - в файле `/opt/VPNagent/etc/agent.ini` измените значение параметра `DefaultCryptoContextsPerIPSecSA=Nc`
 - или в загружаемой LSP в структуре `IPsecAction` присвойте значение Nc атрибуту `CryptoContextsPerIPSecSA=Nc`
2. установите количество нитей в драйвере, равным количеству процессорных ядер (NNN):
 - в файле `/etc/modprobe.d/vpndrvr.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)

3. перезагрузите ОС.



Рекомендация

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

Меняя количество криптоконтекстов в пределах вычисленного диапазона значений, экспериментально определите его оптимальное значение, при котором шлюз безопасности показывает наилучшую производительность.



Замечание

Для однопроцессорных платформ **Gate100/Gate100B** и для модуля **NME-RVPN (в исполнении MCM)** по умолчанию установлены оптимальные значения, которые не требуют вмешательства пользователя, а именно:

количество криптоконтекстов на один SA равно 1

количество нитей в драйвере равно 1.

Настройка NTP (Network Time Protocol)

в OS Solaris 10

На шлюзе безопасности CSP VPN Gate для синхронизации часов с NTP-сервером точного времени необходимо создать файл `/etc/inet/ntp.conf`, содержащий строку

```
server <server_addr>
```

где

`<server_addr>` адрес NTP-сервера, который можно использовать для синхронизации.

Запустите ntp-сервис:

```
svcadm enable ntp
```

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

На шлюзе безопасности для синхронизации часов с NTP-сервером точного времени необходимо выполнить следующие действия:

1. создайте файл `/etc/ntp.conf`, содержащий строки

```
server <server_addr>
restrict default ignore
```

где

`<server_addr>` адрес NTP-сервера, который следует использовать для синхронизации.

Добавьте этот же адрес в файл `/etc/ntp/step-tickers`.

2. внешний NTP-сервер не должен изменять текущую конфигурацию или запрашивать ваш Linux NTP-сервер, поэтому введите следующую строку:

```
restrict <server_addr> mask 255.255.255.255 nomodify notrap noquery
```

3. если к вашему Linux NTP-серверу будут поступать запросы на NTP синхронизацию от других компьютеров вашей сети, то добавьте в файл строку:

```
restrict <addr_local_network> mask <addr_local_mask> nomodify notrap
```

где

`<addr_local_network>` адрес локальной подсети которую должен обслуживать Linux NTP-сервер

`<addr_local_mask>` маска подсети.

4. чтобы Linux NTP-сервер имел полный доступ к самому себе без любых ограничений, впишите строку:

```
restrict 127.0.0.1
```

5. сохраните полученный файл и для автоматического запуска NTP сервиса при каждом рестарте системы выполните:

```
chkconfig ntpd on
```

Для первого запуска NTP сервиса без перезагрузки системы выполните:

```
service ntpd start
```

Время при работе с сертификатами:

1. В сертификате время указано относительно Гринвича
2. Шлюз работает с сертификатами в локальном времени
3. Время жизни сертификата не зависит от временного пояса
4. 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.

Настройка NAT на шлюзе безопасности

Обработка трафика шлюзом безопасности 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 шлюзе безопасности осуществляется средствами ОС.

в OS Solaris 10

Настройка NAT в ОС Solaris 10 осуществляется с использованием пакета IP Filter, описанного в документации по ОС Solaris, например, на сайте <http://docs.sun.com>.

в ОС Red Hat Enterprise Linux 5 (CentOS 5)

В ОС Red Hat Enterprise Linux 5 (CentOS 5) NAT настраивается при помощи утилиты iptables. Описание iptables можно посмотреть на сайте [проекта Netfilter](#).

Использование NAT на шлюзе безопасности 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 шлюза. 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 шлюза, 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.

Построение VPN туннеля между шлюзом безопасности CSP VPN Gate 3.1 и рабочим местом администратора для удаленной настройки шлюза

Сценарий иллюстрирует построение защищенного соединения между шлюзом безопасности GW1 и компьютером AdminHost. Пользователь компьютера AdminHost сможет построить доверенный сеанс со шлюзом безопасности GW1, используя для взаимной аутентификации локальные сертификаты открытых ключей, и управлять им через доверенный сеанс по протоколу SSH. Адрес компьютера администратора считается заранее неизвестным и может находиться за динамическим NAT-ом. В качестве криптопровайдера будет использован «КриптоПро CSP» версии 3.6. Схема стенда показана на рисунке 1, IP-адреса показаны для примера.

Параметры защищенного соединения:

- Аутентификация на сертификатах
- IKE parameters:
 - Encryption algorithm – GOST 28147-89
 - Hash algorithm – GOST R 34.11-94
 - DH-group – VKO GOST R 34.10-2001
- IPsec parameters:
 - ESP encryption algorithm – GOST 28147-89
 - ESP authentication – GOST R 34.11-94 HMAC

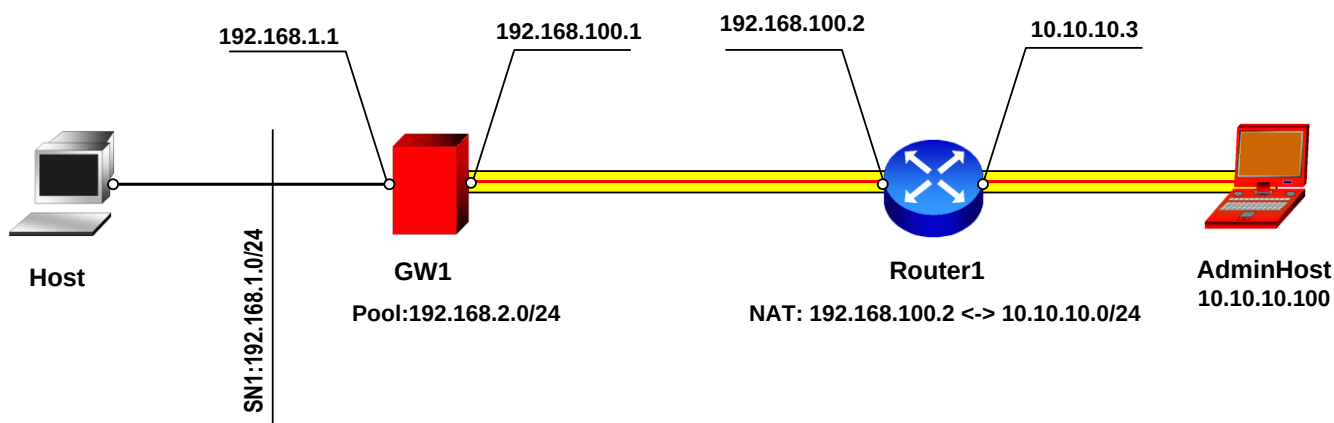


Рисунок 1

Настройка шлюза безопасности GW1

СКЗИ CSP VPN Gate на шлюзе безопасности GW1 должен быть предварительно инициализирован в соответствии с документом «Руководство администратора». Инициализация S-Terra Gate при использовании СКЗИ «КриптоПро CSP 3.6». Все настройки производятся через локальную консоль.

Для начала требуется зарегистрировать сертификаты: сертификат УЦ, локальный сертификат, а также, при необходимости, CRL(список отозванных сертификатов).

Регистрация СА сертификата (сертификата УЦ)

Для регистрации СА сертификата необходимо выполнить следующие действия:

1. Доставьте файл СА сертификата на шлюз безопасности в предварительно созданный каталог, например, /certs. Для доставки можно воспользоваться утилитой pscp.exe из пакета Putty, например, для файла ca.cer:

```
pscp ca.cer root@192.168.1.1:/certs
```



Предупреждение

Среда передачи в этом случае должна быть доверенной

2. С помощью утилиты cert_mgr, входящей в состав продукта, зарегистрируйте сертификат в базе продукта:

```
[root@GW1 /]#cd /opt/VPNagent/bin
[root@GW1 bin]#cert_mgr import -f /certs/ca.cer -t
```

Параметр -t в данной команде указывает на то, что импортируемый сертификат – доверенный (сертификат УЦ).

Регистрация локального сертификата

Перед регистрацией локального сертификата в базе продукта выполните следующие действия:

1. Сформируйте запрос на сертификат, например, с именем субъекта сертификата "C=RU,OU=Sales,CN=GW1", на шлюзе безопасности с использованием утилиты cert_mgr:

```
[root@GW1 /]#cd /opt/VPNagent/bin
[root@GW1 bin]# cert_mgr create -subj "C=RU,OU=Sales,CN=GW1" -
GOST_R3410EL -f local_GW1.req
```

Далее следует просьба нажимать клавиши:

```
Press keys...
```

```
[.....]
```

2. Полученный бинарный файл с запросом сохраните в кодировке Base64, выполнив команду:

```
cat local_GW1.req | base64 > local_GW64.req
```

3. Зайдите на шлюз безопасности по протоколу SSH, например, запустив с отдельно стоящего компьютера Putty Configuration, и для вывода запроса на экран выполните команду:

```
cat local_GW64.req
```

В результате будет выдано на экран примерно следующее:

```
MIH5MIGpAgEAMB8xCzAJBgNVBAYTAlJVMRAwDgYDVQQDEwdTLVRlcnJhMGMwHAYGKoUDAgITMBIG
ByqFAwIClWEGByqFAwICHgEDQwAEQI7+0gl5euynz0x/ZybvVPwqtRlSVT7DyvB/HQSEPT8K7Uuj
IeV+Cw1YOMiNz+jBeE4tqFWw10MvC5dZMOwFAQuqHjAcBgkqhkiG9w0BCQ4xDzANMAsgA1UdDwQE
AwIHgDAIBgYqhQMCAgMDQDDuei+qY0yXOxeCRlnnwZZI0B9baMXSmzebqiPsoXiu7vzpeU5xNzQ2
Q/I514rEcZfhYdkfivQQfJT/Gldlwmk
```

4. Выделите мышкой полученный запрос и скопируйте его в файл или буфер, а затем отошлите в Центр Сертификации для создания локального сертификата. Отсылка запроса на сертификат описана в документе «Приложение».
5. Вы получили локальный сертификат для шлюза безопасности из Центра Сертификации. Далее его следует доставить на шлюз, опять воспользовавшись утилитой `pscp.exe` из пакета Putty, например, для файла `gw1.cer`:

```
pscp gw1.cer root@192.168.1.1:/certs
```

6. Зарегистрируйте локальный сертификат в базе продукта, используя утилиту `cert_mgr`. Импорт производится следующей командой:

```
[root@GW1 bin]# cert_mgr import -f /certs/gw1.cer
```

```
1 OK C=RU,OU=Sales,CN=GW1
```

7. Убедитесь, что сертификаты импортированы успешно:

```
[root@GW1 bin]# cert_mgr show
```

```
Found 2 certificates. No CRLs found.
```

```
1 Status: trusted 1.2.840.113549.1.9.1=presale@s-  
terra.com,C=RU,L=Moscow,O=S-Terra CSP,OU=Presale,CN=PresaleCA
```

```
2 Status: local C=RU,OU=Sales,CN=GW1
```

Создание политики безопасности

После регистрации сертификатов необходимо создать политику безопасности для GW1. Создавать политику рекомендуется в интерфейсе командной строки. Для входа в консоль перейдите в директорию `/opt/VPNagent/bin/` и запустите `cs_console`.

```
[root@GW1 /]# cs_console  
GW1>en  
Password:
```

Пароль по умолчанию: `csp`.

Перейдите в режим настройки:

```
GW1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
GW1(config)#
```

Задайте адрес шлюза по умолчанию:

```
GW1 (config)# ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

Задайте пул адресов:

```
GW1 (config)# ip local pool POOL 192.168.2.1 192.168.2.254
```

Задайте тип идентификации:

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

Задайте параметры для IKE (здесь и далее в сценарии названия алгоритмов `md5`, `des`, `rsa-sig` указываются для соблюдения формата команд Cisco, но транслируются в названия российских алгоритмов, указанных выше в описании стенда):

```
GW1 (config)#crypto isakmp policy 1  
GW1 (config-isakmp)# hash md5  
GW1 (config-isakmp)# encryption des  
GW1 (config-isakmp)# authentication rsa-sig  
GW1 (config-isakmp)# group vko  
GW1 (config-isakmp)#exit
```

Создайте набор преобразований для IPsec (здесь и далее в сценарии названия алгоритмов `esp-3des`, `esp-md5-hmac` указываются для соблюдения формата команд Cisco, но транслируются в названия российских алгоритмов, указанных выше в описании стенда):

```
GW1(config)#crypto ipsec transform-set TSET esp-des esp-md5-hmac
GW1(cfg-crypto-trans)#mode tunnel
GW1(cfg-crypto-trans)#exit
```

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

```
GW1(config)#ip access-list extended LIST
GW1(config-ext-nacl)#permit tcp host 192.168.100.1 eq 22 any
GW1(config-ext-nacl)#exit
```

Опишите требования, которым должен удовлетворять сертификат партнера (администратора):

```
GW1(config)#crypto identity my_Admin
GW1(config-crypto-identity)#dn C=RU,L=Moscow,O=S-Terra
CSP,OU=Presale,CN=Admin_host
GW1(config-crypto-identity)#exit
```

Создайте динамическую криптокарту:

```
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 pool POOL
GW1(config-crypto-map)#set identity my_Admin
GW1(config-crypto-map)#reverse-route
GW1(config-crypto-map)#exit
```

Привяжите динамическую карту к статической:

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

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

```
GW1 (config)#interface FastEthernet0/0
GW1 (config-if)#crypto map CMAP
GW1 (config-if)#exit
```

В настройках интерфейсов вы также можете задать IP-адреса, если это не было сделано раньше

Отключим обработку списка отозванных сертификатов (CRL):

```
GW1(config)#crypto pki trustpoint s-terra_technological_trustpoint
GW1(ca-trustpoint)#crl optional
GW1(ca-trustpoint)#exit
```

Настройка устройства GW1 завершена. При выходе из конфигурационного режима происходит загрузка конфигурации.

Команда `crypto identity my_Admin` в данном случае описывает сертификат электронной подписи пользователя, только с которым будет возможно установление соединения для обработки трафика, описанного в листе доступа LIST командой `ip access-list extended LIST`.

В Приложении представлен текст [cisco-like конфигурации](#) и [текст LSP](#).

Настройка рабочего места администратора AdminHost

Настройка рабочего места администратора состоит из нескольких этапов: получение сертификата и секретных ключей, формирование установочного пакета для целевого компьютера AdminHost и установка этого пакета. В случае если ключи были сгенерированы вне целевого компьютера, их требуется туда доставить защищенным образом (например, на токене).

Создадим установочный пакет для AdminHost. Создавать установочный пакет можно как на AdminHost так и на компьютере администратора. Во вкладке Auth укажите путь к СА и пользовательскому сертификату, а также контейнер с секретными ключами (Рисунок 2).

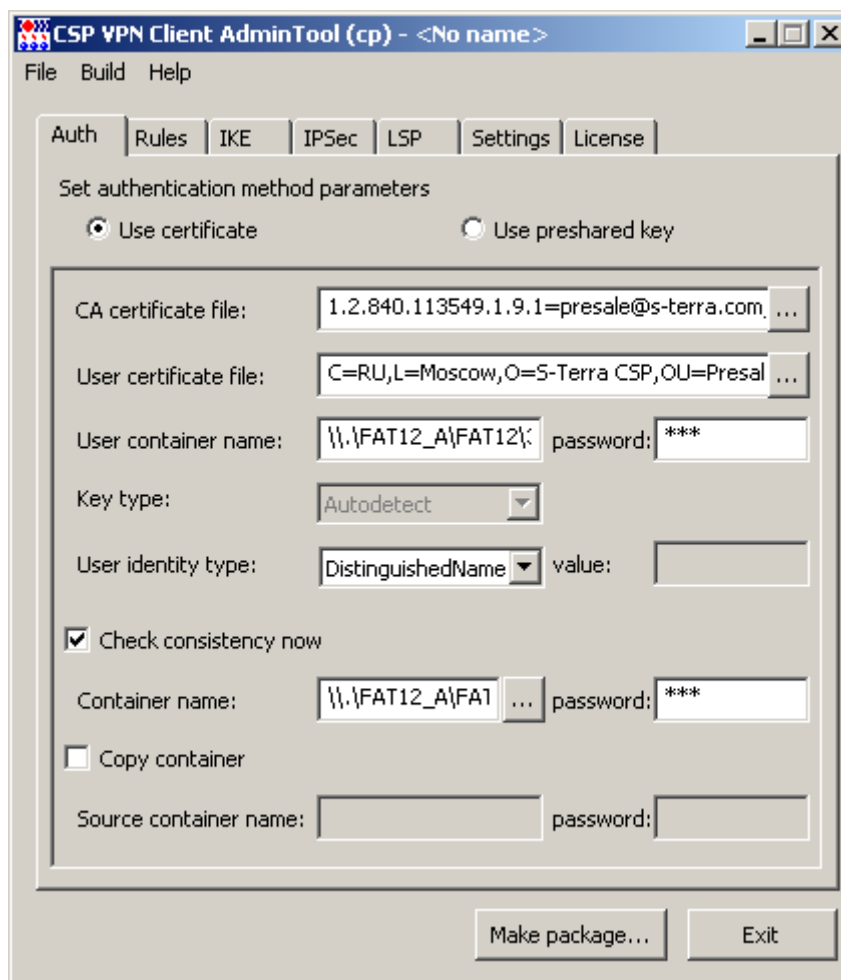


Рисунок 2

На вкладке “Rules”(Рисунок 3) настройте правило фильтрации и защиты трафика. Второе правило разрешает весь трафик.

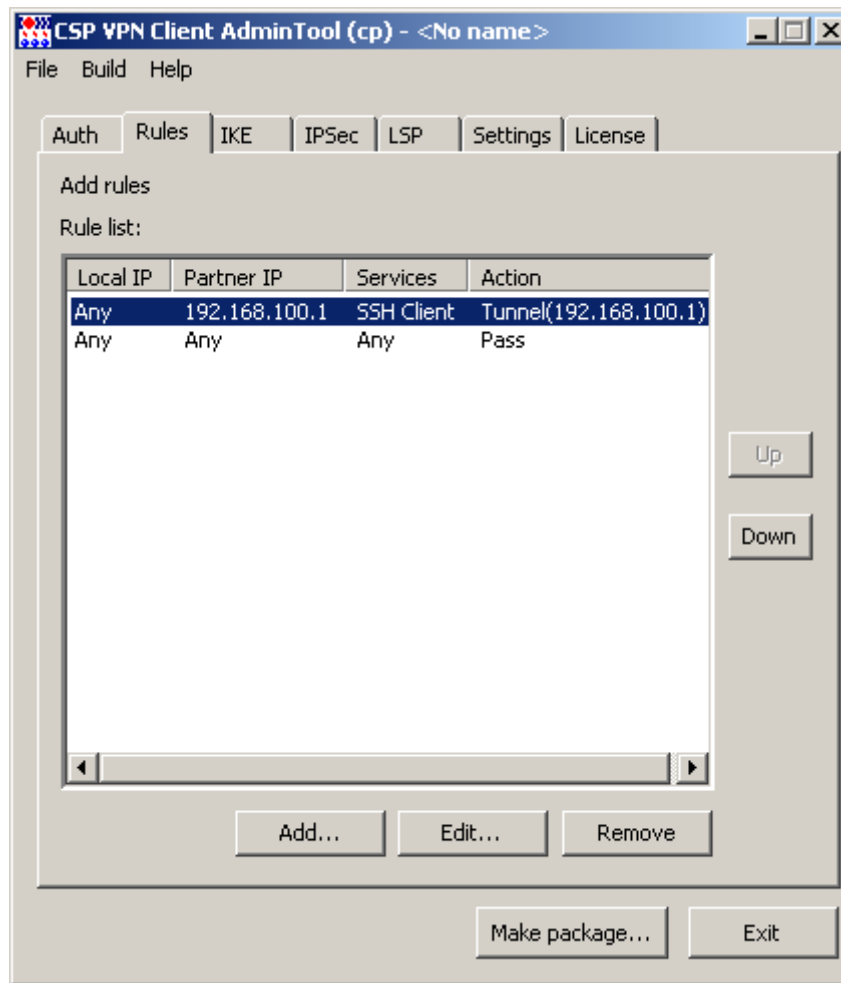


Рисунок 3

Для этого в окне "Add Rule" укажите IP-адрес партнера (шлюза) и IP-адрес шлюза, с которым будет построено защищенное соединение (Рисунок 4). Установите переключатель в положение "Protect using IPsec". Разрешите только SSH-трафик.

Add Rule

Set rule parameters

Local IP Addresses

☒ Any
☐ Custom

IP Address	Subnet Mask

Add... Edit... Remove

Partner IP Addresses

☐ Any
☒ Custom

IP Address	Subnet Mask
192.168.100.1	255.255.255.255

Add... Edit... Remove

Services and Protocols

☐ Any
☒ Custom

Name	Ports
SSH Client	-

Add... Edit... Remove

Action

☐ Pass
☐ Drop
☒ Protect using IPSec

Tunnel IP Addresses of IPSec partner:

☐ Use random IP Address order

192.168.100.1	Up
	Down

Add... Edit... Remove

OK Cancel

Рисунок 4

Закройте окно “Add Rule”.

На вкладке “Rules” поднимите вверх созданное правило.

На вкладке “IPSec” поднимите вверх правило, соответствующее настроенному на шлюзе IPSec Transform Set (Рисунок 5)

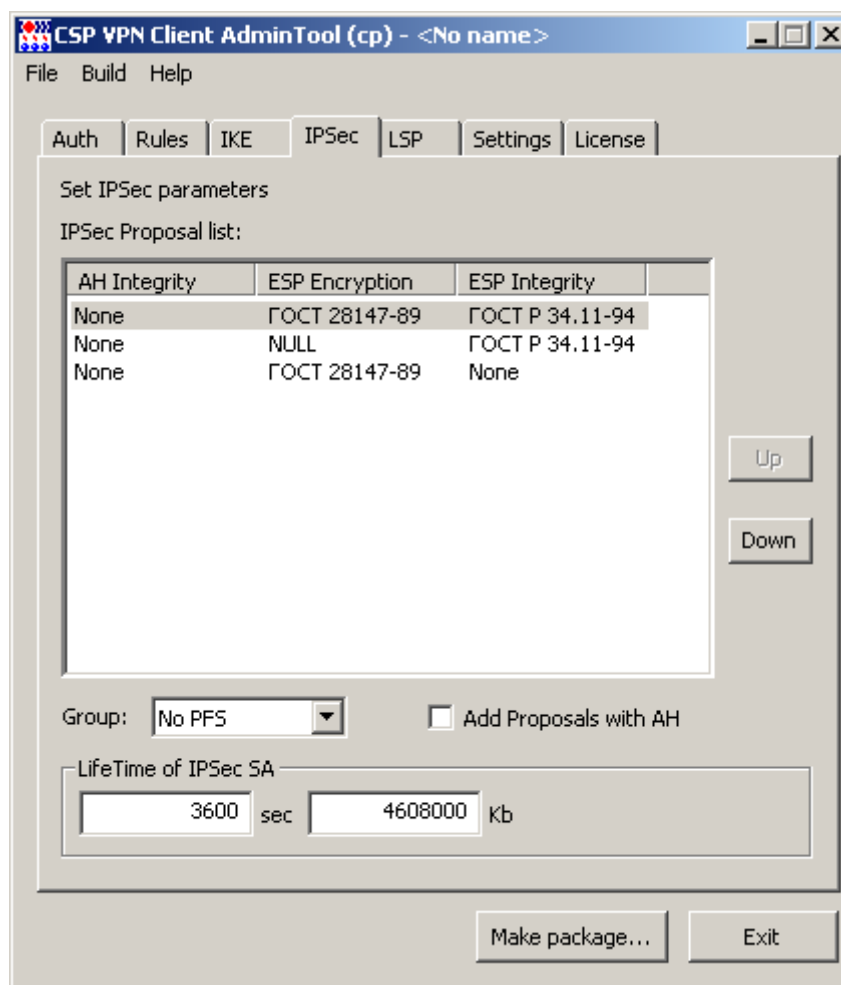


Рисунок 5

На вкладке License введите лицензию на продукт CSP VPN Client.

Сохраните файл созданного проекта, на тот случай, если захотите в будущем сделать похожий инсталляционный пакет. Для этого нажмите File->Save Project

Далее сгенерируйте инсталляционный exe-файл с помощью кнопки “Make package...”

Вставьте в целевой компьютер AdminHost носитель с секретными ключами и установите на нем полученный инсталляционный exe-файл и перезагрузите компьютер.

Кроме того, настройте на нем IP-адрес и шлюз по умолчанию.

В Приложении представлен [текст LSP](#).

Настройка устройства Router1

На устройстве нужно настроить соответствующие IP-адреса и динамический NAT.

Проверка работоспособности стенда

После того, как настройка GW1 и AdminHost завершена, инициируем создание защищенного соединения.

На рабочем компьютере администратора зайдите на шлюз при помощи SSH:

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

Убедиться в этом можно на мобильном клиенте, выбрав предложение Show SA Information (Рисунок 6), (Рисунок 7):

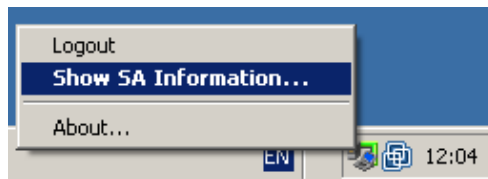


Рисунок 6

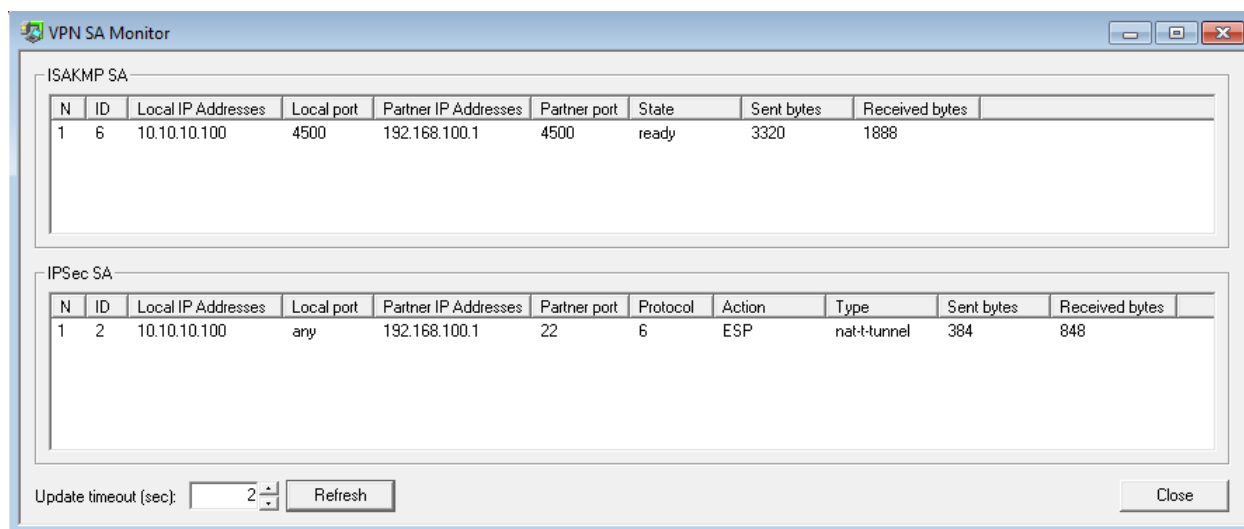


Рисунок 7

Таким образом был создан доверенный сеанс, по которому администратор может удаленно настраивать шлюз безопасности.

Способы создания политики безопасности

Настроить шлюз безопасности CSP VPN Gate или создать политику безопасности для шлюза возможно:

- с помощью команд интерфейса командной строки локально или удаленно с использованием протокола SSH, описанных в документе «[Cisco-like команды](#)» (такую конфигурацию будем называть «cisco-like конфигурацией»). Написанные команды являются родственными Cisco IOS 12.4 (13a)
- создание текстового конфигурационного файла и его последующая загрузка с помощью Специализированных команд на ПАК или модуль NME-RVPN (MCM). Создание такого файла описано в документе «[Создание конфигурационного файла](#)» (такую конфигурацию будем называть «native конфигурацией» или «LSP-конфигурацией»)
- создание политики безопасности удаленно с помощью Web-based графического интерфейса управления (GUI), описано в документе «[Web-based интерфейс управления: инструкция по установке и использованию](#)»
- с помощью CiscoWorks Router Management Center (далее по тексту Router MC) - удаленная централизованная настройка шлюзов, которая описана в документе «[Настройка с помощью CiscoWorks](#)».
- с помощью графического интерфейса Cisco Security Manager (CSM) - удаленная централизованная настройка шлюзов, описана в документе «[Настройка с помощью Cisco Security Manager](#)»

Перед созданием политики безопасности шлюза посмотрите «[Типовые сценарии](#)» и «[Примеры дополнительных возможностей продуктов](#)», размещенных на сайте компании «С-Терра СиЭсПи» по адресу <http://www.s-terra.com/support/>.

Загрузка политики безопасности

Созданную политику безопасности необходимо загрузить на шлюз.

Cisco-like конфигурация сама загружается на шлюз после выхода из конфигурационного режима при помощи команды `exit`, при этом она будет интерпретирована конвертером в LSP-конфигурацию.

LSP-конфигурацию, созданную в виде текстового конфигурационного файла нужно загрузить специализированной командой `lsp_mgr load` с указанием полного пути к файлу конфигурации.

Политики безопасности, созданные с использованием остальных платформ управления - CiscoWorks, CSM, GUI, также конвертируются в LSP-конфигурацию во время загрузки на шлюз.

Для просмотра загруженной конфигурации используется команда `lsp_mgr show`.

Конвертирование

При завершении настройки, вызывается конвертор, который преобразует cisco-like конфигурацию в LSP-конфигурацию. Конвертор работает в рамках программы cs_console.

Если конвертирование конфигурации завершается с ошибкой; то на консоль выдается сообщение об ошибке: "LSP conversion failed. You can use the "show load-message" command to obtain the additional information." ("Конвертирование LSP завершилось с ошибкой. Вы можете использовать команду [show load-message](#) для получения дополнительной информации").

Далее происходит попытка загрузки LSP-конфигурации на шлюз безопасности. Если по каким-либо причинам произошла ошибка при загрузке, LSP-конфигурация записывается в файл erroneous_lsp.txt, расположенный в каталоге шлюза безопасности. В конце работы конвертора выдается результат (успех/неуспех) обратно в cs_console.

При конвертировании cisco-like конфигурации прописываются фильтры для каждого интерфейса в отдельности.

Если после конвертирования cisco-like конфигурации на шлюзе безопасности будет зарегистрирован новый интерфейс с помощью команды [if_mgr add](#), то для него будет выполняться неявное правило Drop All. При следующем конвертировании cisco-like конфигурации новый интерфейс будет добавлен в эту конфигурацию, и для него будут действовать общие правила, как и для остальных интерфейсов.

Во время работы конвертора используются настройки конвертора, некоторые из которых могут редактироваться пользователем. Подробно работа конвертора описана в документе [«Шлюз безопасности CSP VPN Gate. Приложение»](#) в разделе «Конвертор».

Приложение

Управление службой vpngate

в ОС Solaris 10

Для управления службой vpngate в ОС Solaris 10 используются следующие команды SMF (Service Management Facility):

запуск:

```
svcadm enable vpngate
```

остановка:

```
svcadm disable vpngate
```

перезапуск:

```
svcadm restart vpngate.
```

Опция `-t` может быть применена к командам `svcadm enable` и `svcadm disable`. Эта опция говорит что служба запускается/останавливается временно (до перезагрузки). То есть, чтобы прекратить загружать службу при старте системы нужно выполнить `svcadm disable`. Чтобы загружать при каждом старте – `svcadm enable`. Разовая остановка – `svcadm disable -t`. Разовый запуск – `svcadm enable -t`.

Про штатное управление службами SMF в Solaris 10 можно почитать на английском языке – <http://www.sun.com/software/solaris/howtoguides/servicemgmthowto.jsp>, на русском – <http://www.intuit.ru/departament/os/sysadmsolaris10/13/1.html>.

Для управления службой vpngate можно также воспользоваться специальным скриптом `/etc/init.d/vpngate`.

Команда для запуска:

```
/etc/init.d/vpngate start
```

В результате выполнения данной команды в консоли может появиться сообщение: `Warning: IPsec daemon was in maintenance state.`

Оно означает, что при прошлом запуске `vpnsvc` произошла ошибка, и служба была переведена в `maintenance`-режим (состояние, когда служба завершилась аварийно и не может быть запущена без административного вмешательства). Описываемый скрипт перед запуском службы автоматически выводит ее из этого состояния, однако, если ошибка не устранена, то `vpnsvc` не запустится и снова войдет в данный режим.

Команда для остановки:

```
/etc/init.d/vpngate stop
```

Команда для перезапуска:

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

Текст cisco-like конфигурации для устройства GW1

```

version 12.4
no service password-encryption
!
crypto ipsec df-bit copy
crypto isakmp identity dn
username cscons privilege 15 secret 5 Q1W2E3r4t5y6!
hostname GW1
enable password Q1W2E3r4t5y6!
!
!
!
!
crypto identity my_Admin
  dn C=RU,L=Moscow,O=S-Terra CSP,OU=Presale,CN=Admin_host
!
crypto isakmp policy 1
  hash md5
  encr des
  group vko
!
ip local pool POOL 192.168.2.1 192.168.2.254
!
crypto ipsec transform-set TSET esp-des esp-md5-hmac
!
ip access-list extended LIST
  permit tcp host 192.168.100.1 eq 22 any
!
!
crypto dynamic-map DMAP 1
  match address LIST
  set transform-set TSET
  set pool POOL
  set identity my_Admin
  reverse-route
!
crypto map CMAP 1 ipsec-isakmp dynamic DMAP
!
!
!
interface FastEthernet0/0
  ip address 192.168.100.1 255.255.255.0
  crypto map CMAP
!
ip route 0.0.0.0 0.0.0.0 192.168.100.2

!
!
crypto pki trustpoint s-terra_technological_trustpoint
  revocation-check none
crypto pki certificate chain s-terra_technological_trustpoint
certificate 59F65F39AC60428047034A65FDD30818
308201E930820198A003020102021059F65F39AC60428047034A65FDD3081830
0806062A85030202033015311330110603550403130A532D5465727261204341
301E170D3132303331313136333732315A170D3137303331313136333732315A
3015311330110603550403130A532D54657272612043413063301C06062A8503
020213301206072A85030202230106072A850302021E0103430004403FF1E720
60D8CC17C473DB1AB2038D84A5F36CBA6C118ABDEEE5A950B1D1A5249FB91C7F
04BA36E0DE7D650C51D8DF8C03087B59BA48C2E4B71E096C7D5D6654A381C130
81BE300B0603551D0F040403020186300F0603551D130101FF040530030101FF
301D0603551D0E04160414EB69F259436E3ED325BB0295A60272D1C185F60E30
6D0603551D1F046630643062A060A05E862D687474703A2F2F77696E32303033
63736D2F43657274456E726F6C6C2F532D546572726125323043412E63726C86
2D66696C653A2F2F5C5C77696E3230303363736D5C43657274456E726F6C6C5C
532D54657272612043412E63726C301006092B06010401823715010403020100

```



```
300806062A850302020303410076E93DA00CD049C2AE59B528C4D3274B388AB1
EE09D7033CED268B1D6F3BDC1849B633316983BE9BC30BCF49A0A1CE60DE34F5
9A285694A97C223D4D01E24DD2
```

```
quit
!
end
```

Текст LSP для устройства GW1

```
# This is automatically generated LSP
#
# Conversion Date/Time: Tue Mar 13 13:03:12 2012

GlobalParameters(
    Title = "This LSP was automatically generated by
CSP Converter at Tue Mar 13 13:03:12 2012"
    Version = "3.1"
    CRLHandlingMode = OPTIONAL
    LDAPLogMessageLevel = INFO
    SystemLogMessageLevel = INFO
    PolicyLogMessageLevel = INFO
    CertificatesLogMessageLevel = INFO
)

SyslogSettings(
    Server = 127.0.0.1
    Facility = LOG_LOCAL7
)

RoutingTable(
    Routes =
        Route(
            Destination = 0.0.0.0/0
            Gateway = 192.168.100.2
        )
)

IKETransform IKETransform_1
(
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= VKO_1B
    LifetimeSeconds = 86400
)

ESPProposal ESP_TSET
(
    Transform* = ESPTransform
    (
        IntegrityAlg* = "GR341194CPR01-H96-HMAC-65534"
        CipherAlg* = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
)

CertDescription ca
(
    Issuer *= 1.2.840.113549.1.9.1=test@s-
terra.com,C=RU,L=Moscow,O=S-Terra CSP,CN=S-Terra CSP CA
    SerialNumber = "59f65f39ac60428047034a65fdd30818"
    Subject *= "1.2.840.113549.1.9.1= presale@s-
terra.com,C=RU,L=Moscow,O=S-Terra CSP,OU=Presale,CN=PresaleCA"
)
```

```
AuthMethodGOSTSign auth_ca
(
    LocalID          = IdentityEntry( DistinguishedName* = USER_SPECIFIC_DATA
)
    RemoteID          = IdentityEntry(
        DistinguishedName* = CertDescription(
            Subject *= TEMPLATE, "C=RU,L=Moscow,O=S-Terra
CSP,O=Presale,CN=Admin_host"
        )
    )
    AcceptCredentialFrom *= ca
    SendRequestMode      = ALWAYS
    SendCertMode         = ALWAYS
)

AddressPool POOL
(
    IPAddresses *= 192.168.2.1..192.168.2.254
)

IKERule IKE_DMAP_1
(
    Transform* = IKETransform_1
    AggrModeAuthMethod *= auth_ca
    MainModeAuthMethod *= auth_ca
    DoAutopass      = TRUE
    IKECFGPool      *= POOL
    DoNotUseDPD     = TRUE
)

IPsecAction DMAP_1
(
    TunnelingParameters *= TunnelEntry(
        DFHandling=COPY
    )
    ContainedProposals *= ( ESP_TSET )
    ReverseRoute = TRUE
    IKERule = IKE_DMAP_1
)

FilteringRule Filter_nil_acl_DMAP_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 192.168.100.1 ProtocolID *= 6
Port *= 22 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
ProtocolID *= 6 )
    NetworkInterfaces *= "eth0"
    Action *= ( DMAP_1 )
)

FilteringRule Filter_nil_acl
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth0"
    Action *= ( PASS )
)

FilteringRule Filter_nil_acl_1
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    NetworkInterfaces *= "eth1"
    Action *= ( PASS )
)
```

Текст LSP для устройства AdminHost

```
GlobalParameters (
    Title = "This LSP was automatically generated by CSP VPN Client AdminTool
(cp) at 2012.03.13 11:58:39"
    Version = "3.1"
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
    DistinguishedName *= CertDescription(
        Subject *= COMPLETE, "C=RU,L=Moscow,O=S-Terra
CSP,OU=Presale,CN=Admin_host"
    )
)
CertDescription local_cert_dsc_01(
    Subject *= COMPLETE, "C=RU,L=Moscow,O=S-Terra
CSP,OU=Presale,CN=Admin_host"
)
CertDescription partner_cert_dsc_01(
)
AuthMethodGOSTSign auth_method_01(
    LocalID = auth_identity_01
    LocalCredential = local_cert_dsc_01
    RemoteCredential = partner_cert_dsc_01
    SendRequestMode = AUTO
    SendCertMode = AUTO
)
IKEParameters (
    DefaultPort = 500
    SendRetries = 5
    RetryTimeBase = 1
    RetryTimeMax = 30
    SACreationTimeMax = 60
    InitiatorSessionsMax = 30
    ResponderSessionsMax = 20
    BlacklogSessionsMax = 16
    BlacklogSessionsMin = 0
    BlacklogSilentSessions = 4
    BlacklogRelaxTime = 120
)
IKETransform ike_trf_01(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= VKO_1B
)
IKETransform ike_trf_02(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_1536
)
IKETransform ike_trf_03(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_1024
)
IKETransform ike_trf_04(
    LifetimeSeconds = 28800
    CipherAlg *= "G2814789CPR01-K256-CBC-65534"
    HashAlg *= "GR341194CPR01-65534"
    GroupID *= MODP_768
)
```

```

)
ESPTransform esp_trf_01(
    IntegrityAlg *= "GR341194CPR01-H96-HMAC-65534"
    CipherAlg *= "G2814789CPR01-K256-CBC-254"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_01(
    Transform *=esp_trf_01
)
ESPTransform esp_trf_02(
    IntegrityAlg *= "GR341194CPR01-H96-HMAC-65534"
    CipherAlg *= "NULL"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_02(
    Transform *=esp_trf_02
)
ESPTransform esp_trf_03(
    CipherAlg *= "G2814789CPR01-K256-CBC-254"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000
)
ESPProposal esp_proposal_03(
    Transform *=esp_trf_03
)
IKERule ike_rule(
    DoNotUseDPD = FALSE
    DPDIdleDuration = 60
    DPDResponseDuration = 5
    DPDRetries = 3
    MainModeAuthMethod *= auth_method_01
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03,ike_trf_04
    IKECFGRequestAddress = TRUE
    DoAutopass = TRUE
)
IPsecAction ipsec_action_01(
    TunnelingParameters *=
        TunnelEntry(
            PeerIPAddress = 192.168.100.1
        )
    ContainedProposals *=
        (esp_proposal_01),(esp_proposal_02),(esp_proposal_03)
    IKERule = ike_rule
)
FilterEntry local_entry_00_00(
    ProtocolID *= 6
)
FilterEntry remote_entry_00_00(
    IPAddress *= 192.168.100.1
    ProtocolID *= 6
    Port *= 22
)
FilteringRule filter_rule_00_00(
    LocalIPFilter *= local_entry_00_00
    PeerIPFilter *= remote_entry_00_00
    Action *= (ipsec_action_01)
    RefuseTCPPeerInit = FALSE
)
FilterEntry local_entry_00_01(
    ProtocolID *= 17
)
FilterEntry remote_entry_00_01(
    IPAddress *= 192.168.100.1
    ProtocolID *= 17
    Port *= 22
)
FilteringRule filter_rule_00_01(
    LocalIPFilter *= local_entry_00_01

```

```
    PeerIPFilter *= remote_entry_00_01
    Action *= (ipsec_action_01)
    RefuseTCPPeerInit = FALSE
)
FilterEntry local_entry_01_00(
)
FilterEntry remote_entry_01_00(
)
FilteringRule filter_rule_01_00(
    LocalIPFilter *= local_entry_01_00
    PeerIPFilter *= remote_entry_01_00
    Action *= (PASS)
)
```