

**Программные комплексы  
"Шлюз безопасности  
CSP VPN Gate. Версия 3.0"  
и  
"Шлюз безопасности  
CSP RVPN. Версия 3.0"**

**Руководство  
администратора**

# Общие настройки

<b>ОБЩИЕ НАСТРОЙКИ</b> .....	<b>2</b>
<b>РЕГИСТРАЦИЯ ЛИЦЕНЗИЙ ПОСЛЕ ИНСТАЛЛЯЦИИ</b> .....	<b>4</b>
<b>РЕГИСТРАЦИЯ ЛИЦЕНЗИИ НА CSP VPN GATE</b> .....	<b>4</b>
<b>РЕГИСТРАЦИЯ ЛИЦЕНЗИИ НА КРИПТОПРО CSP 2.0</b> .....	<b>4</b>
<b>РЕГИСТРАЦИЯ ЛИЦЕНЗИИ НА КРИПТОПРО CSP 3.0</b> .....	<b>4</b>
<b>НАЗНАЧЕНИЕ IP-АДРЕСОВ ИНТЕРФЕЙСАМ</b> .....	<b>6</b>
<b>СКРИПТ IPSETUP</b> .....	<b>6</b>
<b>РЕДАКТИРОВАНИЕ КОНФИГУРАЦИОННЫХ ФАЙЛОВ</b> .....	<b>6</b>
<b>НАЗНАЧЕНИЕ НЕСКОЛЬКИХ IP-АДРЕСОВ ОДНОМУ ИНТЕРФЕЙСУ</b> .....	<b>8</b>
<b>УСТАНОВКА/СНЯТИЕ ДРАЙВЕРА ПРОДУКТА НА ИНТЕРФЕЙС В ОС SOLARIS</b> .....	<b>10</b>
<b>УСТАНОВКА/СНЯТИЕ ДРАЙВЕРА ПРОДУКТА НА ИНТЕРФЕЙС В ОС LINUX</b> .....	<b>11</b>
<b>ПЕРЕЗАГРУЗКА LSP ПРИ ИЗМЕНЕНИИ СОСТОЯНИЯ ИНТЕРФЕЙСОВ</b> .....	<b>12</b>
<b>ДОБАВЛЕНИЕ СЕТЕВЫХ ИНТЕРФЕЙСОВ</b> .....	<b>13</b>
<b>ДОБАВЛЕНИЕ СЕТЕВЫХ ИНТЕРФЕЙСОВ, ПОДДЕРЖИВАЮЩИХ 802.1Q, В ОС RED HAT LINUX 9</b> .....	<b>14</b>
<b>НАСТРОЙКА ПАРАМЕТРОВ МНОГОПРОЦЕССОРНОЙ ОБРАБОТКИ ТРАФИКА В ОС SOLARIS</b> .....	<b>15</b>
<b>НАСТРОЙКА ПАРАМЕТРОВ МНОГОПРОЦЕССОРНОЙ ОБРАБОТКИ ТРАФИКА В ОС LINUX</b> .....	<b>15</b>
<b>ИЗМЕНЕНИЕ ПАРОЛЕЙ</b> .....	<b>17</b>
<b>СОЗДАНИЕ И РЕГИСТРАЦИЯ ПРЕОПРЕДЕЛЕННЫХ КЛЮЧЕЙ (PRESHARED KEYS)</b>	<b>18</b>
<b>РЕГИСТРАЦИЯ СЕРТИФИКАТОВ</b> .....	<b>19</b>
<b>РЕГИСТРАЦИЯ ЛОКАЛЬНЫХ СЕРТИФИКАТОВ</b> .....	<b>19</b>
<b>РЕГИСТРАЦИЯ CA СЕРТИФИКАТОВ</b> .....	<b>19</b>
<b>РАСШИРЕНИЯ СЕРТИФИКАТА (CERTIFICATE EXTENSIONS)</b> .....	<b>20</b>
<b>НАСТРОЙКА КОЛИЧЕСТВА IPSEC СОЕДИНЕНИЙ</b> .....	<b>21</b>
<b>ОПИСАНИЕ ПРОБЛЕМ</b> .....	<b>21</b>
<b>УСТРАНЕНИЕ ПРОБЛЕМ</b> .....	<b>21</b>
<b>НАСТРОЙКА ПЕРЕМЕННЫХ ОКРУЖЕНИЯ</b> .....	<b>23</b>

Настройка шлюзов безопасности CSP VPN Gate и CSP RVPN производится одинаково, выполняют они одни и те же функции, поэтому в дальнейшем будем использовать только одно наименование – шлюз безопасности CSP VPN Gate или Продукт CSP VPN Gate, или Продукт.

После инсталляции Продукта CSP VPN Gate проводятся следующие настройки программно-аппаратного комплекса и сетевого модуля NME- RVPN:

- Если планируется проводить настройки и управлять локальной политикой безопасности шлюза при помощи консоли удаленно по протоколу SSH1, то после инсталляции CSP VPN Gate рекомендуется загрузить начальную конфигурацию, которая позволит в дальнейшем создать защищенный канал для настройки политики безопасности. Создание начальной конфигурации описано в разделе «Начальная конфигурация для удаленного управления шлюзом» документа [«Шлюзы безопасности CSP VPN Gate и CSP RVPN. Приложение»](#). При использовании протокола SSH2 загрузка начальной конфигурации не нужна
- [Регистрация Лицензий](#) на Продукт CSP VPN Gate и КриптоПро CSP 2.0 или КриптоПро CSP 3.0, 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 Red Hat Linux 9, 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 количества IPsec соединений](#), если используется СКЗИ “КриптоПро CSP 3.0” (**build 3303**) в ОС Solaris 9
- [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 CSP VPN Gate

Если в процессе инсталляции не была зарегистрирована Лицензия на Продукт CSP VPN Gate, то регистрация Лицензии после инсталляции в ОС Solaris осуществляется по одному из вариантов:

- запуск команды `/opt/VPNagent/bin/lic_mgr set`
- запуск скрипта `/opt/cspvpn/scripts/license_req.sh`.

В ОС Red Hat Linux 9 регистрация Лицензии на CSP VPN Gate после инсталляции производится только 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 КриптоПро CSP 2.0

Если установленное СКЗИ "КриптоПро CSP 2.0" не было зарегистрировано во время инсталляции, то его следует зарегистрировать по одному из двух вариантов:

- командой, введя серийный номер и ключ активации с бланка Лицензии на этот Продукт:  
`/opt/CPROcsp/bin/licman <Serial number> <Activation Key>`
- запустить скрипт, введя серийный номер и ключ активации по запросу скрипта:  
`/opt/cspvpn/scripts/license_req_cprocsp.sh`

После регистрации Лицензии следует перезапустить `vpn`-демона, выполнив команды:

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

### Регистрация Лицензии на КриптоПро CSP 3.0

#### ОС Solaris 9

Если установленное СКЗИ "КриптоПро CSP 3.0" не было зарегистрировано во время инсталляции, то его следует зарегистрировать для приложений, запустив утилиту:

```
/opt/CPROcsp/sbin/cpconfig -license -set xxxxxxxx,
```

где `xxxxxxx` – серийный номер продукта "КриптоПро CSP 3.0".

Для регистрации драйверной части лицензии выполните команду:

```
/opt/CPROcsp/sbin/set_driver_license.sh
```

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

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

## ОС Red Hat Linux 9

Если установленное СКЗИ **"КриптоПро CSP 3.0"** не было зарегистрировано во время инсталляции, то его следует зарегистрировать для приложений, запустив утилиту:

```
/usr/CPROcsp/sbin/cpconfig -license -set xxxxxxxx,
```

где xxxxxxxx – серийный номер продукта "КриптоПро CSP 3.0".

Для регистрации драйверной части лицензии выполните команду:

```
/usr/CPROcsp/sbin/set_driver_license.sh
```

После регистрации Лицензии следует перезапустить vpn-демона, выполнив команды:

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

## 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 CSP 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.

### ОС Solaris 8 и Solaris 9

В ОС Solaris 8 и Solaris 9 изменить IP-адрес интерфейса можно, отредактировав файлы `/etc/hosts` и `/etc/netmasks`.

Для обновления конфигурации сетевого интерфейса перезагрузите шлюз безопасности.

Изменить настройки интерфейса можно и на одну сессию командой `ifconfig`. После перезагрузки шлюза безопасности эти настройки исчезнут.

# Назначение нескольких IP-адресов одному интерфейсу

## ОС Solaris 8 и Solaris 9

Существует несколько вариантов создания виртуального интерфейса.

### Вариант 1

Для добавления постоянного виртуального интерфейса следует:

- в файле `/etc/hosts` - добавить адрес и имя хоста
- в файле `/etc/hostname.имя_интерфейса:n` - добавить имя хоста
- в файле `/etc/netmasks` - добавить маску подсети
- перезагрузить шлюз безопасности.

### Вариант 2

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

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

сначала создаем виртуальный интерфейс:

```
ifconfig имя_интерфейса:1 plumb  
ifconfig имя_интерфейса:2 plumb
```

затем присваиваем ему IP-адрес:

```
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).

## 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 Solaris

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

Если нужно снять или установить драйвер Продукта на какой-либо интерфейс, то сделать это можно по одному из следующих сценариев:

**отключение обработки трафика встроенными средствами CSP VPN Gate.**

- для этого необходимо с помощью утилиты `if_mgr remove` удалить 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

**снятие драйвера Продукта с сетевого интерфейса (вариант 1):**

- выполните команду `"ifconfig <имя_интерфейса> modlist"`.
- найдите слово `"vpndrvr"` в выводе утилиты. Перед этим словом будет указано число - позиция драйвера в стеке (`<pos>`).
- далее выполните команду `"ifconfig <имя_интерфейса> modremove vpndrvr@<pos>"`. Драйвер будет удален с сетевого интерфейса до пересоздания этого интерфейса (`ifconfig unplumb/ifconfig plumb` или перезагрузки компьютера).

**снятие драйвера Продукта с сетевого интерфейса (вариант 2):**

- 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.
- выполните команды:  
`autopush -r -M <major> -m 0`  
`ifconfig <имя_интерфейса> unplumb plumb <конфигурационные параметры...>`,  
 где `<конфигурационные параметры...>` - 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:**

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

Для установки (восстановления) драйвера Продукта на сетевом интерфейсе (после снятия драйвера вышеописанными методами):

- верните измененные строки в файле `/etc/iu.ap`.
- перезагрузите компьютер или выполните команду `"autopush -f /etc/iu.ap"`
- пересоздайте сетевые интерфейсы (`ifconfig unplumb plumb ...`).

Для установки драйвера Продукта на сетевом интерфейсе нового типа необходимо:

- добавить строку в файл `/etc/iu.ap` с именем драйвера нового интерфейса (по аналогии с уже существующими)
- выполнить команду `"autopush -f /etc/iu.ap"`

- перезагрузиться или создать (пересоздать) новый сетевой интерфейс.
- зарегистрировать интерфейс в CSP VPN Gate с помощью утилиты `if_mgr add`.

## 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 CSP 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 операцию:

- 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 (vrnsvc) 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
```

## ОС Solaris 8 и Solaris 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 файле `/etc/hosts`.
2. Создать файл `/etc/hostname.имя_интерфейса`, где `имя_интерфейса` - имя нового сетевого интерфейса, например, `iprb1`.
3. В файл `/etc/hostname.имя_интерфейса` записать имя хоста, прописанное на первом шаге в файле `/etc/hosts`. Все это можно сделать командой:

```
echo имя_интерфейса > /etc/hostname.имя_интерфейса
```

4. Если необходимо, добавить соответствие адреса подсети маске в файле `/etc/netmasks`
5. Перезагрузить шлюз (или поднять интерфейс вручную командой `ifconfig`).
6. Зарегистрировать интерфейс в продукте 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 настраиваются и работают в Продукте также, как и другие интерфейсы.

## Настройка параметров многопроцессорной обработки трафика в ОС Solaris

Если программно-аппаратная платформа имеет более одного процессора, то для достижения наилучшей производительности шлюза безопасности CSP VPN Gate в ОС Solaris выполните следующие действия:

- установите количество криптоконтекстов на один SA равным количеству ядер процессоров (NNN):
  - 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 ядер процессоров (NNN):
  - в файле `/etc/system` добавьте строку `set vpndrvr:pcap_nthreads = NNN`
- установите размер внутренней очереди пакетов равным YYY, где YYY лежит в диапазоне между NNN+1 и 2\*NNN включительно:
  - в файле `/etc/system` добавьте строку `set vpndrvr:pcap_pkt_q_size = YYY`

## Настройка параметров многопроцессорной обработки трафика в ОС Linux

Если программно-аппаратная платформа имеет более одного процессора, то для достижения наилучшей производительности шлюза безопасности CSP 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.

Для однопроцессорных платформ Gate100/Gate100B и для модуля RVPN 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.



## 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 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**.

## 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»](#).

## Расширения сертификата (Certificate Extensions)

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате будут присутствовать другие расширения, не указанные в таблице и заданные как критичные, то такой сертификат не может быть использован. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, и сертификат используется.

Name	OID value
Subject Key Identifier	2.5.29.14
Key Usage	2.5.29.15
Subject Alternative Name	2.5.29.17
Issuer Alternative Name	2.5.29.18
Basic Constraints	2.5.29.19
Name Constraints	2.5.29.30
CRL Distribution Points	2.5.29.31
Authority Key Identifier	2.5.29.35

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (<http://tools.ietf.org/html/rfc5280#section-4.2>).

# Настройка количества IPsec соединений

## Описание проблем

При использовании CSP VPN Gate на ОС Solaris 9 с СКЗИ “КриптоПро CSP 3.0” возможно возникновение следующих проблем:

**Проблема 1:** при создании большого количества IPsec соединений может происходить ошибка, причиной которой является ошибка в КриптоПро CSP, препятствующая дальнейшему созданию IPsec соединений и сопровождаемая сообщениями в системном лог следующего вида:

```
NOTICE: drvccsp: AllocMemory: 111: Too big memory  
alloc 140000
```

```
NOTICE: drvccsp: AllocMemory: 129: NTE_NO_MEMORY.
```

**Проблема 2:** при старте ОС возможно появление в системном лог сообщений вида:

```
WARNING: drvccsp: cannot read license.
```

Эта проблема не влияет на работу продукта, и других проявлений не наблюдается, кроме этого сообщения.

## Устранение проблем

При использовании СКЗИ “КриптоПро CSP 3.0” (build 3303) в Solaris 9 (для “КриптоПро CSP 3.0” других модификаций (в частности - **build 3293**) рекомендации, изложенные здесь, не подходят) для смягчения Проблемы 1 и устранения Проблемы 2 выполните следующие действия:

Для изменения количества доступных контекстов допишите в конфигурационный файл `/usr/kernel/drv/drvccsp.conf` строку:

```
maxhandles=N;
```

где `N` – желаемое количество контекстов криптопровайдера.

Если эта строка присутствует в файле, то измените значение `N` на нужное.

Число `N` должно удовлетворять следующим условиям:

- число `N` должно быть целой степенью двойки, при выборе другого числа – оно будет округлено в большую сторону до ближайшей целой степени двойки
- число `N` может быть вычислено следующим образом:  
при объёме физической памяти `X` мегабайтов значение `N` может равняться  $N_w = 2^{\lceil \log_2(X) + 8 \rceil}$  или  $N_m = 2^{\lceil \log_2(X) + 9 \rceil}$ .  
Значение `Nm` является теоретическим максимумом и недостижимо, поскольку на пути к нему физическая память будет исчерпана, что приведёт к зависанию ОС.  
Значение `Nw` – рабочее значение и к зависанию ОС с большой вероятностью не приведёт, но позволит использовать продуктивно только около половины доступного объёма памяти. Поэтому значение `Nm` рекомендуется выбирать только в тех случаях, когда `Nw` недостаточно, учитывая при этом опасность зависания.

Примеры вычислений:

Объём памяти	128М	Nw=32768	Nm=65536
Объём памяти	192М	Nw=32768	Nm=65536
Объём памяти	256М	Nw=65536	Nm=131072

Примечания

Ниже в таблице представлена зависимость количества технически доступных IPSec SA от режимов применения протоколов IPsec, без учёта возможных лицензионных ограничений и при количестве контекстов криптопровайдера “КриптоПро CSP 3.0” по умолчанию (65536). Значения приведены для случая, когда количество криптоконтекстов на SA равно 1 (значение по умолчанию). Для другого количества криптоконтекстов на SA нижеприведенные значения в таблице следует разделить на это количество.

	ESP-cipher	АН или ESP-integrity	ESP-cipher (ESP-integrity или АН)
<b>ОС Solaris</b>	4096	1638	1170

Количество криптоконтекстов для одного SA задается атрибутом `CryptoContextsPerIPSecSA` в структуре `IPsecAction` локальной политики устройства. Если этот атрибут отсутствует, то используется значение поля `DefaultCryptoContextsPerIPSecSA` из файла `agent.ini`, иначе, значение по умолчанию принимается равным 1.

## 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 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 (re)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.

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:

$$90\% * (x \text{ соединений} - 20 \text{ соединений}) / (y\% - 20\%).$$

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 wrp-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 wrp-демон сам аварийно завершает свою работу и создает core-файл.

Механизм слежения за зависанием wrp-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 wrp-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.