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

Инициализация CSP VPN Gate при использовании СКЗИ "Крипто-КОМ 3.2"

РЛКЕ.00005-01 90 03

24.11.2011

Содержание

Инициализация CSP VPN Gate при использовании СКЗИ "Крипто-КОМ 3.2"

В этом документе описана инициализация программного комплекса CSP VPN Gate, установленного на аппаратные платформы. Инициализация программного комплекса CSP VPN Gate на модуле MCM, установленный в маршрутизатор Cisco, описана в отдельном документе «Руководство по установке и настройке NME-RVPN модуля (MCM)».

Подготовка программно-аппаратного комплекса к инициализации

В качестве терминала для аппаратной платформы (АП), на которой установлен Продукт CSP VPN Gate, можно использовать:

- компьютер, подключенный к последовательному порту АП
- монитор и клавиатуру, подключенные к разъемам АП.

Но изначально заданы определенные настройки.

Шаг 1: К АП с установленным Продуктом CSP VPN Gate 3000/7000 подключите к разъемам монитор и клавиатуру в качестве терминала, и перейдите к Шагу 2.

К АП с установленным Продуктом CSP VPN Gate 100/100B/100V/1000/1000V подключите к последовательному порту компьютер в качестве терминала. Для АП TONK 1800 подключить следует к COM2-порту, для остальных АП – к COM1-порту, используя нуль-модемный кабель (5 проводов). На компьютере используйте терминальную программу, например, Windows HyperTerminal. В программе HyperTerminal выполните настройки:

```
File-> Properties-> Settings-> Emulation-> VT100
```

Во вкладке `Connect To` нажмите кнопку Configure и выполните следующие настройки `COM`-порта:

```
Bits per second: 115200
Data bits: 8
Parity: None
Stop bits: 1
Flow control: None
```

Шаг 2: Включите шнур питания в сеть переменного тока и нажмите кнопку питания на аппаратной платформе.

Шаг 3: После загрузки ОС войдите в систему пользователем "`root`" и пустым паролем.

Шаг 4: При необходимости переключить ввод/вывод с последовательного порта на монитор и клавиатуру или наоборот, воспользуйтесь скриптом `consoleswitch`, описанным в разделе «Переключение консоли на последовательный порт или монитор и клавиатуру». После этого выключите питание платформы командой:

```
cspgate:~# poweroff
```

Дождитесь окончания выполнения команды. Отсоедините шнур питания от сети переменного тока. Выполните необходимые переключения оборудования в качестве терминала. Включите шнур питания в сеть переменного тока. Нажмите кнопку питания на передней панели АП. После загрузки ОС войдите в систему пользователем "`root`" и пустым паролем.

Шаг 5: Выполните процедуру инициализации программного комплекса CSP VPN Gate, описанную в разделе «Инициализация CSP VPN Gate при первом старте».

Инициализация CSP VPN Gate при первом старте

Программно-аппаратный комплекс поставляется в инсталлированном состоянии: установлена ОС Solaris 10 или Red Hat Enterprise Linux 5 или CentOS 5, продукты CSP VPN Gate, OpenSSH, СКЗИ «Крипто-КОМ 3.2».

При первом старте программно-аппаратного комплекса после загрузки ОС появляется предупреждение "System is not initialized. Please, login as "root" and run /opt/VPNagent/bin/init.sh to start initialization procedure" и приглашение для входа в ОС.

Шаг 1: Войдите в ОС под именем "root" и пустым паролем.

Шаг 2: Запустите скрипт /opt/VPNagent/bin/init.sh для старта процедуры начальной инициализации шлюза безопасности.

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

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

Шаг 3: Далее запрашивается информация о местонахождении криптографического (RNG) контейнера, который будет использоваться для ДСЧ: "CSP VPN Agent will need cryptographic container for generating random numbers, please choose from options below to configure RNG container". RNG контейнер представляет собой каталог, поэтому имя контейнера – имя каталога. Администратору предлагается выбрать - каким контейнером воспользоваться – существующим, его копией или создать новый контейнер:

```
1. Use existing
2. Create new
3. Copy existing
4. Do not configure
```

Предлагается ввести номер выбранного пункта для RNG контейнера: "Enter menu item number [1-4]:"

- При первом старте всегда выбирайте пункт 2 – "Create new" и согласитесь с местоположением контейнера, предложенным по умолчанию.
- При выборе первого пункта "Use existing" будет предложено указать полный путь к существующему RNG контейнеру. Датчик случайных чисел при каждом использовании этого контейнера будет зачитывать из него информацию и модифицировать его.
- При выборе второго пункта "Create new" будет предложено указать полный путь к новому создаваемому контейнеру: "Enter full path to the container [/opt/sc_rng_container]:". Пользователь может ввести свой путь или нажать Enter, тогда контейнер будет создан в предложенном каталоге. Если указанного каталога не существует, то он будет создан. Также администратора попросят ввести начальную информацию для контейнера с клавиатуры, например: "Step= 1/16 Press k [6b]: " (введите символ "k" и нажмите Enter) и т.д. Таким образом, формируется начальное состояние датчика случайных чисел.
- При выборе третьего пункта "Copy existing" будет предложено указать полный путь к существующему и новому контейнерам, если каталог для нового контейнера не существует, то он будет создан. ДСЧ будет использовать информацию, которая уже была записана в этом контейнере.
- При выборе четвертого пункта "Do not configure" инициализация программного комплекса CSP VPN Gate прерывается.

Шаг 4: В процессе инициализации запрашивается лицензионная информация для CSP VPN Gate: "You have to enter license for CSP VPN Gate." Эти данные можно взять из «Лицензии на использование программного продукта компании ЗАО «С-Терра СиЭсПи», входящей в комплект поставки. Предлагаются следующие пункты для ввода:

Available product codes:

GATE100
GATE100B
GATE100V
GATE1000
GATE1000V
GATE3000
GATE7000
GATE10000
RVPN
RVPNV
BELVPN
BELVPNV
UVPN
UVPNV
KZVPN
KZVPNV

Enter product code: - введите код продукта , например, GATE1000

Enter customer code: - введите код конечного пользователя, например, GAZREESTRPROM

Enter license number: - введите номер лицензии, например, 55455

Enter license code: - введите код лицензии, например, B123456DFGH567KL

Шаг 5: Следует вопрос о корректности введенных данных:"Is the above data correct ?" После получения подтверждения инициализация продолжается без дополнительных вопросов. Если подтверждение не получено, то предлагается ввести Лицензию еще раз.

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

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

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

Драйвер Продукта CSP VPN Gate установлен на все обнаруженные сетевые интерфейсы.

Программный комплекс CSP VPN Gate установлен в каталог **/opt/VPNagent**.

Файл keygen версии 1.4.0.0, полученный от компании «Сигнал-КОМ», размещается в каталоге /opt/Signal-COM/bin. (Утилита keygen используется для генерации ключевой пары и запроса на сертификат, описана в документе «Шлюз безопасности CSP VPN Gate. Приложение».

При инициализации CSP VPN Gate устанавливается политика
Default Driver Policy = Passdhcp, при которой интерфейсы шлюза безопасности пропускают только пакеты DHCP и в незащищенном виде.

Для входа в Cisco-like интерфейс командной строки нужно использовать имя пользователя "cscons" (начальный пароль "csp"). А для входа в ОС предназначено имя "root" (изначально без пароля).

Графический интерфейс Web-based GUI не был установлен вместе с CSP VPN Gate. Инсталляция графического интерфейса описана в документе «Web-based интерфейс управления: инструкция по установке и использованию».

После инициализации программного комплекса CSP VPN Gate перейдите к его настройке, описанной в документе «Настройка шлюза».

Переключение консоли на последовательный порт или монитор и клавиатуру

Для переключения вывода консоли рекомендуется использовать скрипт `consoleswitch`, а не редактировать соответствующие конфигурационные файлы ОС.

Для настройки вывода консоли на монитор и клавиатуру выполните команду:

```
consoleswitch keyboard
```

Для настройки вывода консоли в последовательный порт выполните команду:

```
consoleswitch serial [baud[,parity[,bits]]]
```

где

дополнительными настройками порта являются (через запятую, без пробелов):

`baud` – скорость

`parity` – четность

`bits` – биты данных.

По умолчанию установлены следующие значения – 115200,`n`,`8`.

На какой именно последовательный порт происходит переключение, зависит от настройки ОС:

- в Solaris 10 – `ttya` для `COM1`, `ttyb` для `COM2` и т.д.
- в Red Hat Enterprise Linux 5 (CentOS 5) – `ttyS0` для `COM1`, `ttyS1` для `COM2` и т.д.

При вызове без параметров или с неверными параметрами, скрипт выводит краткое описание параметров запуска.

При возникновении ошибки, скрипт выдает сообщение:

```
error: can not set system console.
```

После выполнения команды consoleswitch выключите систему, переключите оборудование, запустите систему.

