

ЗАО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, проезд 4806, д.5, стр.20
Телефон: +7 (499) 720-6928
Факс: +7 (499) 720-6928
Эл.почта: information@s-terra.com
Сайт: <http://www.s-terra.com>



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

**Руководство
администратора**

Сценарии конфигурирования

РЛКЕ.00005-01 90 03

18.11.2011

Содержание

Создание правил пакетной фильтрации	3
Создание защищенных VPN туннелей	3
Настройка маршрутизации	5
Настройка Syslog-клиента	5
Настройка SNMP	6
Настройка NAT на шлюзе безопасности	6
NAT на внешнем устройстве	7
Загрузка политики безопасности	7
Работа с сертификатами	8

Сценарии конфигурирования

В этом документе описаны команды интерфейса командной строки и структуры текстового конфигурационного файла, которые используются для тех или иных целей при создании локальной политики безопасности шлюза.

На странице Технической поддержки <http://www.s-terra.com/support/> сайта нашей компании приведены примеры Типовых сценариев и Примеры дополнительных возможностей продуктов.

Создание правил пакетной фильтрации

Создание правил пакетной фильтрации состоит из формирования списков доступа и привязывания их к конкретным интерфейсам аппаратной платформы CSP VPN Gate или сетевого модуля NME-RVPN (MCM).

В интерфейсе командной строки с помощью команды ***ip access-list*** создаются листы доступа.

Команда ***ip access-list*** с параметром ***standard*** осуществляет вход в режим редактирования стандартных списков доступа. В этом режиме с помощью команд ***permit*** и ***deny*** формируются списки доступа.

В конфигурационном файле правила пакетной фильтрации создаются в структуре ***FilteringRule***.

Создание защищенных VPN туннелей

Создание политики IKE

Для создания защищенного канала, который будет обеспечивать защиту части обменов информацией первой фазы и все обмены второй фазы IKE, создаются ISAKMP политики (или одна политика) с разными приоритетами, которые будут предложены партнеру для согласования. В политиках описываются желаемые алгоритмы и параметры защищенного канала.

В интерфейсе командной строки с помощью команды ***crypto isakmp policy*** задаются IKE политики (или одна политика) с различными приоритетами, которые будут предложены партнеру для согласования. Перед созданием ISAKMP SA должны быть выбраны параметры, которые будут использоваться сторонами для защиты части обменов первой фазы и второй фазы IKE. Выполнение этой команды осуществляет вход в режим ISAKMP policy configuration, в котором предлагаются параметры для согласования.

С помощью команды ***authentication*** указывается метод аутентификации (с использованием электронной подписи или предопределенных ключей).

С помощью команды ***encryption*** указывается алгоритм шифрования, используемый в рамках протокола IKE.

С помощью команды ***hash*** указывается хэш-алгоритм, используемый в рамках протокола IKE.

С помощью команды ***lifetime*** устанавливается время жизни ISAKMP SA.

С помощью команды **group** указывается алгоритм, который будет использоваться в рамках протокола IKE для получения ключевого материала.

В конфигурационном файле в структуре **IKERule** задается метод аутентификации сторон, режим для первой фазы IKE, а также предлагается для согласования с партнером политика защиты первой и второй фазы IKE, которая описывается в структуре **IKETransform**. Структура **IKEParameters** описывает глобальные настройки протокола IKE.

Создание IPsec наборов преобразований

Далее нужно предложить партнеру для согласования наборы преобразований, которые будут использоваться для создания защищенного виртуального соединения (IPsec SA). IPsec SA – это однонаправленное логическое соединение, поэтому при двустороннем обмене данными нужно установить два IPsec SA.

В интерфейсе командной строки с помощью команды **crypto ipsec transform-set** описать параметры IPsec наборов преобразований (или одного набора преобразований). Можно указать до трех наборов преобразований.

С помощью команды **mode** указать режим использования (туннельный или транспортный).

В конфигурационном файле структура **IPsecAction** определяет режим использования IPsec, список предлагаемых наборов преобразований IPsec. Каждое преобразование описывается в структурах **AHTransform** и **ESPTTransform**.

Создание списков доступа

В интерфейсе командной строки с помощью команды **ip access-list** указываются списки доступа, в которых задается трафик, который будет потом просто пропускаться, защищаться или запрещаться. Для создания защищенных туннелей используются только расширенные списки доступа.

Команда **ip access-list** с параметром **extended** осуществляет вход в режим **config-ext-nacl** (режим редактирования расширенных списков доступа). В этом режиме с помощью команд **permit** и **deny** формируются списки доступа.

В конфигурационном файле списками доступа являются правила фильтрации, описываемые структурой **FilteringRule**.

Создание криптографических карт

В интерфейсе командной строки создание политики IPsec выполняется с помощью команды **crypto map**, которая осуществляет переход в режим настройки криптографических карт.

Командой **match address** осуществляем привязку списка доступа к записи криптографической карты.

Командой **set peer** определяем партнера, с которым будем устанавливать туннель.

Командой **set pfs** задаем режим pfs, позволяющий повысить уровень защищенности трафика.

Командой **set pool** указываем имя пула адресов для криптографической карты.

Командой **set identity** задаем идентификатор для криптографической карты

Командой **set security-association lifetime** устанавливаем время жизни IPsec SA.

Командой **set transform-set** даем ссылку на ранее созданный трансформ или трансформы (определяем параметры туннеля)

Создание набора динамических криптографических карт в интерфейсе командной строки осуществляется командой **crypto dynamic map**.

В конфигурационном файле политика IPsec задается в структуре **IPsecAction**.

Привязка криптографической карты к интерфейсу

В интерфейсе командной строки на последнем этапе производится привязка листов доступа и криптографических карт к конкретным интерфейсам аппаратной платформы. Эти операции производятся в режиме настройки интерфейсов.

Команда **interface** с указанием логического имени интерфейса осуществляет переход в режим настройки данного интерфейса.

В этом режиме командой **ip access-group** указываем список доступа для правил пакетной фильтрации, которые будут использоваться на этом интерфейсе.

Командой **crypto map** указываем криптографическую карту, с помощью которой будут создаваться VPN туннели.

В конфигурационном файле для привязки правила фильтрации к интерфейсу аппаратной платформы используется атрибут **NetworkInterfaces** в структуре **FilteringRule**. Но если атрибут **NetworkInterfaces** не указан, то привязка правила фильтрации производится на все зарегистрированные сетевые интерфейсы.

Настройка маршрутизации

Добавление строки в таблицу маршрутизации в интерфейсе командной строки задается командой **ip route** с указанием адреса и маски подсети назначения пакета, IP-адреса следующего маршрутизатора либо выходного интерфейса локального устройства, на который нужно передать пакет для передачи его далее по сети к получателю пакета.

В конфигурационном файле создание таблицы маршрутизации осуществляется структурой **RoutingTable**. Строка, которая добавляется в таблицу маршрутизации, задается в структуре **Route**. Эта строка задает маршрут, указывая адрес назначения, выходной интерфейс либо IP-адрес следующего маршрутизатора и метрику маршрута.

Настройка Syslog-клиента

Настройка Syslog-клиента в cisco-like конфигурации и LSP-конфигурации подробно описана в документе «[Протоколирование событий](#)».

Настройка SNMP

Для задания настроек по выдаче информации SNMP-агентом по протоколу SNMP в интерфейсе командной строки используются три команды. Команда **`snmp-server community`** задает строку, которая играет роль пароля при аутентификации сообщений SNMP и разрешает SNMP-менеджеру чтение статистики из базы управления SNMP-агента. Команда **`snmp-server location`** содержит информацию о физическом расположении SNMP-агента. В команде **`snmp-server contact`** указывается лицо, ответственное за работу SNMP-агента.

В конфигурационном файле задание настроек SNMP-агента осуществляется в структуре **`SNMPPollSettings`**. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, а также строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо. В документе «Мониторинг» описаны переменные, которые могут быть запрошены у SNMP-агента.

А отсылки трапов настройки SNMP-агента производятся в структурах **`SNMPTrapSettings`** и **`TrapReceiver`**. В этих структурах указывается IP-адрес и порт, на который отсылаются трап-сообщения, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

Настройка NAT на шлюзе безопасности

Обработка трафика шлюзом безопасности осуществляется в той же последовательности, что и у Cisco – исходящие пакеты проходят через NAT (Network Address Translation), потом шифруются (если необходимо), входящие пакеты расшифровываются (если необходимо) и над ними осуществляется трансляция адресов.

Управление настройками NAT на шлюзе безопасности осуществляется средствами ОС.

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

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 включает следующие сценарии:

- 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 сценариях поддерживается работа по протоколу FTP.

NAT на внешнем устройстве

В случае, если IPsec-соединение между партнерами устанавливается через внешний маршрутизатор, на котором включен NAT, рекомендуется:

- при построении IPsec туннеля в наборах преобразований использовать только протокол ESP для проверки целостности и шифрования трафика
- использовать туннельный режим, а не транспортный
- использовать IKECFG
- не использовать адрес в качестве типа идентификатора.IKE.

Загрузка политики безопасности

Загрузка политики безопасности в cisco-like конфигурации (в интерфейсе командной строки):

После выхода из конфигурационного режима при помощи команды `exit`, созданная cisco-like конфигурация будет интерпретирована конвертером и загружена на шлюз безопасности.

Cisco-like конфигурация, а также созданная на платформе управления CiscoWorks, конвертируется в LSP-конфигурацию. Для просмотра загруженной конфигурации используется команда `lsp_mgr show`.

Загрузка политики безопасности в LSP-конфигурации (конфигурационный файл):

Политика безопасности в виде текстового конфигурационного файла загружается специализированной командой `lsp_mgr load` с указанием полного пути к файлу конфигурации.

Конвертирование

При завершении настройки, кроме создания текстового конфигурационного файла, вызывается конвертор, который преобразует cisco-like конфигурацию в native-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 native-конфигурации на шлюз безопасности. Если по каким-либо причинам произошла ошибка при загрузке, native-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».

Работа с сертификатами

Регистрация CA сертификата

Зарегистрировать CA сертификат в базе Продукта можно двумя способами:

- с помощью утилиты командной строки ***cert_mgr import***
- через ***cs_console*** командами ***crypto pki trustpoint*** и ***crypto pki certificate chain***.

При регистрации сертификата первым способом при первом старте консоли после добавления сертификатов, добавленные сертификаты будут доступны для использования в cisco-like конфигурации. Для них будет создан *trustpoint* с именем *s-terra technological trustpoint*.

Для регистрации CA сертификата через ***cs_console*** используются команды:

- ***crypto pki trustpoint name*** – для объявления имени CA и входа в режим *ca trustpoint configuration*:

можно задать несколько таких команд для объявления разных *trustpoint*

в режиме этой команды можно указать адрес LDAP-сервера и режимы использования CRL при проверке сертификатов:

- ***crl query ldap://IP-адрес(:порт)*** – задает адрес LDAP-сервера. При обращении к LDAP-серверу шлюз безопасности сначала смотрит поле CDP сертификата, если в этом поле прописанный путь к LDAP-серверу является неполным, то добавляются данные (IP-адрес и порт) из команды *crl query*. Если CDP содержит полный путь, *crl query* не используется. Если в сертификате нет поля CDP, то используется эта команда для задания *url* LDAP.
- ***revocation-check method1 [method2]***
 - *method1* – параметр, принимающий одно из двух значений:
crl – при проверке сертификата обязателен действующий CRL. Если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат не принимается
none – при проверке сертификата действующий CRL используется, если он предустановлен в базе продукта или получен в процессе IKE обмена. Если это не так, то попытка получить CRL по протоколу LDAP не предпринимается и сертификат принимается.
 - *method2* – параметр необязательный, имеет одно значение:
none – если действующий CRL не найден в базе продукта и его не удалось получить по протоколу LDAP, то сертификат принимается. Используется только тогда, когда *method1=crl*.
- ***crypto pki certificate chain name*** – для входа в режим настройки цепочки сертификатов CA:
- ***certificate*** – для добавления CA сертификата (в шестнадцатеричном представлении) в базу Продукта:
- можно задать несколько таких команд для добавления либо промежуточных CA сертификатов, либо любых CA сертификатов.

В отличие от Cisco наш Продукт не проверяет являются ли добавляемые сертификаты из одной цепочки. Поэтому, можно добавлять в один *trustpoint* не только промежуточные CA сертификаты, но вообще любые CA сертификаты.

При добавлении CA сертификата в *trustpoint* командой *crypto pki certificate chain* он автоматически добавляется в базу Продукта.

При старте `cs_console` при поиске сертификата проверяются все существующие *trustpoint's* в базе Продукта. В случае отсутствия соответствующего CA сертификата в базе Продукта, *trustpoint* автоматически удаляется из *cisco-like* конфигурации и, следовательно, удаляются все CA сертификаты, зарегистрированные в этом *trustpoint*. При этом выдается соответствующее сообщение в лог.

Создание ключевой пары и запроса на локальный сертификат

Создать ключевую пару и запрос на локальный сертификат для шлюза безопасности можно двумя путями:

- локально с помощью утилиты `/opt/VPNagent/bin/cert_mgr create`
- на отдельном компьютере с помощью средств MS Windows и СКЗИ, как описано в документе [«Шлюз безопасности CSP VPN Gate. Приложение»](#).

Регистрация локального сертификата

Для регистрации локального сертификата в базе Продукта используется утилита командной строки `cert_mgr import`.

Удаление сертификатов

Удалять сертификаты из базы Продукта можно двумя способами:

- с помощью утилиты командной строки `cert_mgr remove`
- через `cs_console` командой `no crypto pki trustpoint`.

При удалении *trustpoint* с указанным именем, все CA сертификаты из этого *trustpoint* удаляются из текущей конфигурации, базы Продукта и *cisco-like* конфигурации.

Если в `cs_console` добавить сертификат в *trustpoint*, а потом, выйдя из консоли, удалить добавленный сертификат с помощью `cert_mgr remove`, то при следующем старте консоли *trustpoint* с сертификатом удалится и оттуда.

Удалить CRL из базы Продукта помощью утилиты командной строки `cert_mgr remove` невозможно. Если в команде указать номер (индекс) CRL, то будет выведено сообщение об ошибке о недопустимом индексе.

Просмотр сертификатов в базе Продукта

Для просмотра сертификатов в базе Продукта используйте команду `cert_mgr show`.

Отсылка локального сертификата

Для отсылки локального сертификата партнеру по протоколу IKE:

в LSP-конфигурации (конфигурационный файл):

Для отсылки локального сертификата партнеру по протоколу IKE в LSP, в структуре **AuthMethodGOSTSign** задать атрибут **SendCertMode** со значением:

- **ALWAYS** – всегда отсылать локальный сертификат
- **CHAIN** – всегда отсылать локальный сертификат, CA сертификат и промежуточные CA сертификаты.

в cisco-like конфигурации (в интерфейсе командной строки):

при создании политики IKE, параметры которой согласовываются с партнером, в режиме команды **crypto isakmp policy** задать метод аутентификации сторон с использованием сертификатов командой

authentication rsa-sig

В файле настроек конвертора **cs_conv.ini** параметру **send_cert** присвоено значение **ALWAYS**, и поэтому по умолчанию партнеру всегда будет отсылаться локальный сертификат по протоколу IKE.

Получение сертификата партнера

Сертификат партнера можно получить либо по протоколу IKE, либо по протоколу LDAP.

Сначала шлюз безопасности пытается получить сертификат партнера по IKE. Если партнер не прислал сертификат, а прислал свой идентификатор, то шлюз безопасности по этому идентификатору ищет сертификат партнера сначала в своей базе Продукта, если не нашел, то продолжает поиск на LDAP-сервере.

Получение сертификата партнера по IKE

Для получения сертификата партнера по протоколу IKE нужно:

в LSP-конфигурации:

- в локальной конфигурации в структуре **AuthMethodGOSTSign** задать атрибут **SendRequestMode** со значением **ALWAYS** – всегда запрашивать сертификат партнера
- в конфигурации партнера в структуре **AuthMethodGOSTSign** задать атрибут **SendCertMode** со значением:
 - **ALWAYS** – высылать сертификат
 - **CHAIN** – высылать локальный сертификат, CA сертификат с цепочкой промежуточных CA.

в cisco-like конфигурации:

в режиме команды **crypto isakmp policy** задать метод аутентификации сторон с использованием сертификатов командой

authentication rsa-sig

В файле настроек конвертора **cs_conv.ini** параметру **send_request** присвоено значение **ALWAYS**, и поэтому по умолчанию у партнера всегда будет запрашиваться локальный сертификат по протоколу IKE.

Получение сертификата партнера по LDAP

Получение сертификата партнера на LDAP-сервере. В этом случае партнер присылает свой идентификатор, а шлюз безопасности по значению Subject будет искать сертификат партнера

на LDAP-сервере. Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответствующий фильтр.

В LSP-конфигурации:

в локальной конфигурации задать структуру **LDAPSettings** с IP-адресом LDAP-сервера и также:

- если прислан идентификатор типа DN:
 - шлюз безопасности по Subject ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере
- если прислан идентификатор другого типа:
 - для получения Subject в локальной конфигурации задаются атрибуты *RemoteID*, *RemoteCredential*, *DoNotMapRemoteIDToCert*
 - если *DoNotMapRemoteIDToCert* = *TRUE*, то Subject будет состояться из *RemoteCredential*
 - если *DoNotMapRemoteIDToCert* = *FALSE*, то Subject будет состояться из *RemoteCredential* и *RemoteID*.
 - по составленному значению Subject шлюз безопасности ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере.

В cisco-like конфигурации:

если партнер не прислал свой сертификат по протоколу IKE, и в базе Продукта его нет, то шлюз безопасности посылает запрос на заданный LDAP-сервер в команде ***crl query*** для получения сертификата партнера. По полученному идентификатору типа *dn* от партнера будет осуществляться поиск сертификата. Если получен идентификатор другого типа – запрос на LDAP-сервер не посылается. Если отредактировать сконвертированную native-конфигурацию для работы с идентификаторами другого типа, как описано в предыдущем пункте, то сертификат партнера можно получить по LDAP.

Проверка сертификата по CRL

Для проверки сертификата партнера по списку отозванных сертификатов (CRL) нужно:

в LSP-конфигурации:

в структуре **GlobalParameters** задать атрибут ***CRLHandlingMode***, при значениях этого атрибута:

- *optional* – используется действующий CRL из базы Продукта
- *enable* и *best_effort* – действующий CRL может быть получен по LDAP.

Для получения CRL с LDAP-сервера сначала проверяется поле CDP в проверяемом сертификате, если поле CDP отсутствует, то в конфигурации должна быть задана структура **LDAPSettings** с адресом LDAP-сервера. В базу Продукта с LDAP-сервера загружается действующий CRL и по нему проверяется сертификат партнера.

Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответствующий фильтр.

в cisco-like конфигурации:

в режиме команды *crypto pki trustpoint* командой ***revocation-check*** задается режим использования CRL.

Несколько локальных и СА сертификатов

Иногда при работе с разными партнерами аутентификация осуществляется с использованием разных локальных сертификатов, подписанных разными УЦ, соответственно и СА сертификаты разные.

В cisco-like конфигурации:

в командной строке нет команд для указания соответствия между идентификатором партнера, локальным сертификатом и СА сертификатом. Поэтому после конвертирования cisco-like конфигурации в LSP конфигурацию последнюю необходимо отредактировать.

В LSP-конфигурации:

в структуре *AuthMethodGOSTSign* существуют атрибуты, которые позволяют задать соответствие между локальным, партнерским и СА сертификатами, локальным и партнерским идентификаторами.

Пример работы с сертификатами, выпущенными разными УЦ, опубликован на сайте компании <http://www.s-terra.com/CSP/RU/support/support.htm> в разделе «Типовые сценарии» – «Построение VPN туннеля в топологии «звезда» с использованием сертификатов, выпущенных разными УЦ».

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>).