27.10.2009

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

Руководство администратора

Сценарии конфигурирования

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

 Copyright © S-Terra CSP 2003 -2009

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. Под шлюзом безопасности в данном документе подразумевается как «Шлюз безопасности CSP VPN Gate», так и «Шлюз безопасности CSP RVPN».

В документе «Примеры конфигураций в различных сценариях» приведены примеры локальных политик безопасности шлюзов в двух сценариях.

На странице Технической поддержки http://www.s-terra.com/CSP/RU/support/scn.htm 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 RVPN.

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

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 IKE 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 (RSA подпись, RSA шифрование или аутентификация на предопределенных ключах).

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 IKE SA.

С помощью команды **group** указывается Diffie-Hellman группа, которая будет использоваться в рамках протокола IKE.

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.

Copyright © S-Terra CSP 2003 -2009

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.

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 **ESPTransform**.

Создание списков доступа

Списки доступа в интерфейсе командной строки создаются с помощью команды **ip access-list** для определения защищать или нет трафик. 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 фильтрования, 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 и группу Diffie-Hellman.

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)

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

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

Copyright © S-Terra CSP 2003 -2009

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 фильтрования к интерфейсу аппаратной платформы используется **атрибут Networkinterfaces в структуре FilteringRule.** Но если атрибут **Networkinterfaces** не указан, то привязка правила фильтрования 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,

 Copyright © S-Terra CSP 2003 -2009

на который отсылаются трап-сообщения, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

Работа через NAT

При создании защищенных соединений между партнерами при использовании NAT рекомендуется:

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

Загрузка политики безопасности

После выхода из режима настройки в интерфейсе командной строки созданная cisco-like конфигурация будет интерпретирована конвертером и загружена на шлюз безопасности.

Независимо от способа создания конфигурации – в интерфейсе командной строки, платформе управления CiscoWorks – при загрузке на шлюз безопасности, cisco-like конфигурация конвертируется в native-конфигурацию. Для просмотра загруженной конфигурации используется команда **`lsp_mgr show`**.

Политика безопасности, созданная 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-Приложении - "CSP_VPN_Appendix.pdf".

Copyright © S-Terra CSP 2003 -2009

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.

 Copyright © S-Terra CSP 2003 -2009

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, следовательно и удаляются все CA сертификаты, зарегистрированные в этом `trustpoint`. При этом выдается соответствующее сообщение в лог.

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.

Регистрация локального сертификата

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

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 IKE:

в LSP-конфигурации (конфигурационный файл):

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.

 Copyright © S-Terra CSP 2003 -2009

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

создается политика, параметры которой согласовываются в процессе установления соединения, в том числе и метод аутентификации сторон, командой

- **`crypto isakmp policy`**
- **`authentication rsa-sig`** – при выборе этого метода локальный сертификат всегда отсылается партнеру по протоколу IKE.

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 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:

партнеру предлагается политика, параметры которой согласовываются в процессе установления соединения, в том числе и метод аутентификации сторон, командой:

- **`crypto isakmp policy`**
- **`authentication rsa-sig`** – при выборе этого метода всегда будет запрашиватся сертификат партнера 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 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:

- 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:

 Copyright © S-Terra CSP 2003 -2009

- для получения Subject в локальной конфигурации задаются атрибуты **RemoteID, RemoteCredential, DoNotMapRemoteIDToCert**
- если DoNotMapPeerIDToCert = TRUE, то Subject будет составляться из RemoteCredential
- если DoNotMapPeerIDToCert = FALSE, то Subject будет составляться из RemoteCredential и RemoteID.
- по составленному 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 IKE и в базе Продукта его нет, то шлюз безопасности пошлет запрос для получения сертификата партнера на заданный LDAP-сервер в команде **`crl query`**. 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 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.

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

 Copyright © S-Terra CSP 2003 -2009

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).

Copyright © S-Terra CSP 2003 -2009