28.08.2009

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

Руководство администратора

Введение

Комплекты поставки Программных комплексов -

Программный комплекс “Шлюз безопасности CSP VPN Gate. Версия 3.0” (далее - Продукт CSP VPN Gate 3.0) предназначен для использования на:

- аппаратных платформах, работающих под управлением ОС Sun Solaris 8 или ОС Sun Solaris 9
- аппаратных платформах, работающих под управлением ОС Red Hat Linux 9
- сетевом модуле NME-RVPN, устанавливаемом в маршрутизаторы Cisco, и работающем под управлением ОС Red Hat Linux 9.

Программный комплекс “Шлюз безопасности **CSP RVPN**. Версия 3.0” (далее - модуль CSP RVPN) поставляется в следующей комплектации:

- сетевой модуль RVPN с установленной в нем компакт-флеш картой, которая содержит:
  - установленную ОС Red Hat Linux 9 (SP4, нужен при использовании СКЗИ "КриптоПро CSP 3.0") с OpenSSH
  - подготовленный к инсталляции дистрибутив Продукта CSP VPN Gate 3.0 со встроенным криптоядром:
    - СКЗИ "Крипто-КОМ 3.2"
    - либо СКЗИ "LirSSL"
  - либо подготовленные к инсталляции дистрибутивы Продуктов CSP VPN Gate 3.0 и СКЗИ "КриптоПро CSP 3.0"
- в комплект поставки CSP RVPN входят 3 диска:
  - компакт-диск с дистрибутивом CSP VPN Gate 3.0
  - компакт-диск с Live CD Linux (Slax), образом компакт-флеш карты (CF), скриптами
  - компакт-диск с документацией.

.

Программный комплекс “Шлюз безопасности **CSP VPN Gate**. Версия 3.0” при использовании:

ОС Sun Solaris 8 или ОС Sun Solaris 9 и **СКЗИ "КриптоПро CSP 2.0" или СКЗИ "КриптоПро CSP 3.0"**

поставляется в следующей комплектации:

- аппаратная платформа, жесткий диск которой содержит:
  - установленную операционную систему Sun Solaris 8 или Sun Solaris 9 (SP4) с OpenSSH
  - подготовленные к инсталляции дистрибутивы Продуктов:
    - CSP VPN Gate 3.0
    - КриптоПро CSP 2.0 или КриптоПро CSP 3.0
    - OpenSSH (только для ОС Solaris 8)
- 4 компакт-диска:
  - с дистрибутивом Продукта CSP VPN Gate 3.0

- с вспомогательным ПО для восстановления образа диска и Инструкцией по восстановлению ПАК
- с образом жесткого диска и Приложением к Инструкции по восстановлению ПАК
- с документацией.

Программный комплекс “Шлюз безопасности **CSP VPN Gate**. Версия 3.0” при использовании

ОС Sun Solaris 9 или ОС Red Hat Linux 9 с OpenSSH и **СКЗИ "Крипто-КОМ 3.2"**

поставляется в следующей комплектации:

- аппаратная платформа, жесткий диск которой содержит:
  - установленную операционную систему
  - подготовленный к инсталляции дистрибутив Продукта CSP VPN Gate 3.0 со встроенным криптоядром СКЗИ "Крипто-КОМ 3.2"
- 4 компакт-диска:
  - с дистрибутивом Продукта CSP VPN Gate 3.0
  - с вспомогательным ПО для восстановления образа диска и Инструкцией по восстановлению ПАК
  - с образом жесткого диска и Приложением к Инструкции по восстановлению ПАК
  - с документацией.

Программный комплекс “Шлюз безопасности **CSP VPN Gate**. Версия 3.0” при использовании

ОС Sun Solaris 9 или ОС Red Hat Linux 9 с OpenSSH и **СКЗИ "LirSSL"**

поставляется в следующей комплектации:

- аппаратная платформа, жесткий диск которой содержит:
  - установленную операционную систему
  - подготовленный к инсталляции дистрибутив Продукта CSP VPN Gate 3.0 со встроенным криптоядром СКЗИ "LirSSL"
- 4 компакт-диска:
  - с дистрибутивом Продукта CSP VPN Gate 3.0
  - с вспомогательным ПО для восстановления образа диска и Инструкцией по восстановлению ПАК
  - с образом жесткого диска и Приложением к Инструкции по восстановлению ПАК
  - с документацией.

Список поставляемых HTTP-серверов в составе операционных систем

В состав поставляемых операционных систем входит HTTP-сервер:

- в ОС Solaris 8 – Apache Web-Server версии 1.3.12 с установленными рекомендуемыми производителем патчами, в том числе 116974-05
- в ОС Solaris 9 – Apache Web-Server версии 1.3.29 с установленными рекомендуемыми производителем патчами
- в ОС Red Hat Linux 9 - Apache Web-Server версии 2.0.40.

Назначение и функции Продукта

Программный комплекс “Шлюз безопасности CSP VPN Gate. Версия 3.0” и Программный комплекс “Шлюз безопасности CSP RVPN. Версия 3.0” обеспечивают защиту транзитного трафика между различными узлами сети, защиту трафика самого шлюза безопасности, а также пакетную фильтрацию трафика.

Управление шлюзами безопасности осуществляется:

- централизованно посредством графического интерфейса центра управления CiscoWorks VPN/Security Management Solution v.2.3 – CiscoWorks Router Management Center (Router MC)
- централизованно удаленно посредством графического интерфейса Cisco Security Manager версии 3.2
- локально и удаленно по протоколу SSH с помощью интерфейса командной строки. В интерфейсе командной строки в основном используются команды Cisco, что облегчает управление администраторам, имеющим опыт конфигурирования шлюзов безопасности и межсетевых экранов Cisco Systems
- созданием политики безопасности в виде конфигурационного текстового файла и последующей его загрузки на шлюз.
- удаленно с помощью Web-based графического интерфейса управления (GUI).

Защита трафика шлюзов безопасности осуществляется в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) - RFC2407.

Шлюзы безопасности обеспечивают:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней:
  - на сетевом уровне – по IPv4 адресам и/или полю 'протокол' IP-заголовка
  - на транспортном уровне – по направлению установления TCP – соединений и составу сервисов (сервисных протоколов)
- загрузку политики из внешнего файла
- различные наборы правил обработки трафика на различных интерфейсах
- получение сертификатов открытых ключей по протоколу LDAP
- событийное протоколирование
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика
- маскировку топологии защищаемого сегмента сети (туннелирование трафика).

Продукты CSP VPN Gate и CSP RVPN используют в качестве внешней криптографической библиотеки одно из средств криптографической защиты информации (СКЗИ):

- СКЗИ "КриптоПро CSP 2.0" или "КриптоПро CSP 3.0", разработанное компанией "Крипто-Про"
- СКЗИ "Крипто-КОМ 3.2", разработанное компанией "Сигнал-КОМ"
- СКЗИ “LirSSL”, разработанное компанией “ЛИССИ”.

СКЗИ "КриптоПро CSP 2.0", "КриптоПро CSP 3.0", СКЗИ "Крипто-КОМ 3.2" и СКЗИ “LirSSL” реализуют российские криптографические алгоритмы:

- ГОСТ 28147-89 - шифрование/расшифрование данных
- ГОСТ Р 34.11-94 HMAC - целостность данных
- ГОСТ Р 34.11-94 – функция хэширования
- ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001- формирование и проверка электронно-цифровой подписи (ЭЦП)
- генерацию случайных чисел.

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.

Требования на аппаратные платформы

Продукт CSP VPN Gate работает под управлением:

- ОС Sun Solaris 8
- ОС Sun Solaris 9
- ОС Red Hat Linux 9.

На поставляемой аппаратной платформе ОС настраивается в соответствии с внутренними стандартами компании “С-Терра СиЭсПи” и администратору безопасности запрещается изменение среды функционирования, а именно:

- модернизация ОС, включая установку штатных обновлений
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки Изделия)
- установка дополнительных приложений
- самостоятельное добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Архитектура CSP VPN Gate

Функциональность шлюзов безопасности CSP VPN Gate и CSP RVPN состоит из следующих основных частей:

- VPN daemon (демон)
- VPN driver (драйвер)
- Cisco-like console (CLI консоль)
- Command Line Utilities (утилиты)
- Web-based Graphic User Interface (GUI).

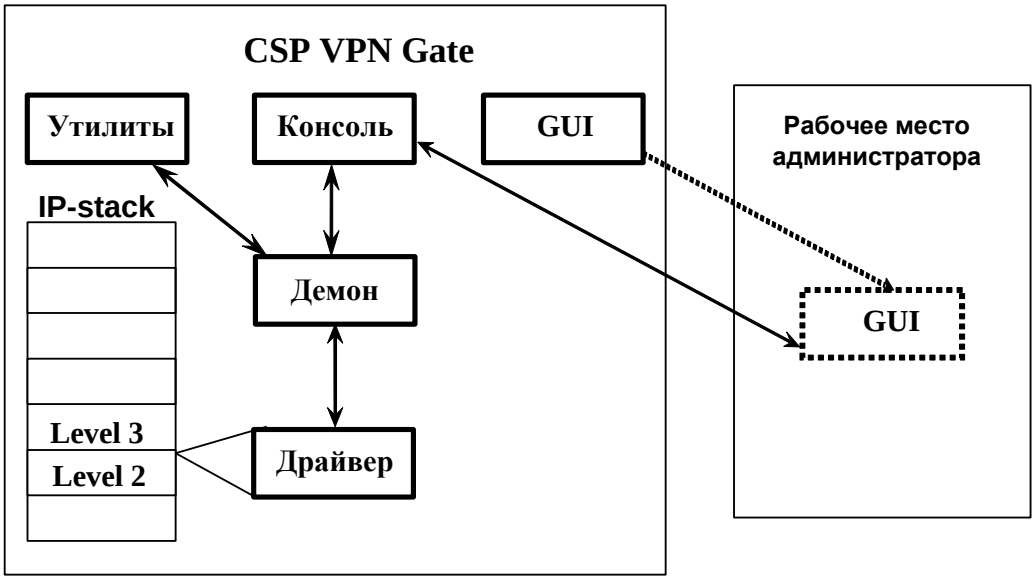

Рисунок 1

Рассмотрим основные части.

Демон (vpnsvc) - основная часть Продукта, которая реализует протокол IKE, обеспечивает работу с базой IPsec SA, взаимодействует с драйвером, загружая в него конфигурационную информацию и обрабатывая его запросы на создание SA. Кроме этого, в демоне выполняется вся работа с сертификатами, событийное протоколирование, сбор статистики и реализована поддержка протоколов SNMP, LDAP, SYSLOG.

Работой демона управляет специальное описание – Local Security Policy (LSP). LSP (или “native configuration”) имеет текстовое представление и может быть загружена в демон пользователем консоли или при помощи утилит. При загрузке новой LSP все существующие SA уничтожаются.

Основная задача **драйвера** – перехват, фильтрация и обработка пакетов. Перехватив пакет, драйвер сравнивает его со списком фильтров и при совпадении параметров пакета (адреса, порты, протокол) с параметрами фильтра либо выполняет обработку пакета, либо пропускает его дальше без обработки, либо уничтожает пакет.

При загрузке LSP параметры фильтров и описание действия, которое необходимо выполнить с пакетом, загружаются демоном в драйвер.

Консоль (CLI) предоставляет пользователю интерфейс в стиле командной строки Cisco IOS. Набор команд консоли является подмножеством команд IOS с некоторыми ограничениями функциональности и небольшими дополнительными возможностями. Как и у IOS, у консоли есть привилегированный и конфигурационный режимы (configure terminal). Однако, следует отметить, что (в отличие от IOS) изменения настроек вступают в действие не сразу, а только после выхода из конфигурационного режима. В этот момент Cisco-like конфигурация автоматически конвертируется в native-конфигурацию и загружается в `vpnsvc`. Таким образом, включает в себя:

- интерфейс командной строки для ввода команд конфигурации
- интерпретатор команд, родственных Cisco
- обработчик конфигурации. Формирует и обрабатывает конфигурацию из команд консоли и передает ее конвертору.

CLI консоль, на самом деле, является специальным shell-ом по умолчанию для предопределенного пользователя «`cscons`» и всех пользователей, которые создаются в CLI конфигурации. Остальные пользователи, например «`root`», при входе попадают в ОС.

Утилиты служат для общего управления Продуктом. Они позволяют загружать и просматривать LSP, регистрировать в Продукте сертификаты и ключи, получать различную информацию о текущем состоянии Продукта.

Утилиты могут быть вызваны из CLI консоли с использованием специальной команды `run`.

GUI является еще одним средством настройки шлюза безопасности. В состав ОС входит Web-сервер и SSH-сервер, а GUI представляет из себя Java-applet, который может быть загружен по протоколу HTTP администратором и запущен на его рабочем компьютере. После запуска GUI взаимодействует с консолью по протоколу SSH. Внешне GUI выполнен в стиле Cisco CDM с существенным сокращением функциональности. Он позволяет пользователю редактировать Cisco-like policy, представленную в виде набора связанных таблиц. После внесения необходимых изменений они по специальной команде пользователя в виде набора команд конфигурационного режима передаются консоли.

База Продукта – в ней хранятся сертификаты, предопределенные ключи, список интерфейсов, локальные настройки различных модулей, локальная политика безопасности и др.

Примеры взаимодействия описанных компонент

Перед созданием конфигурации с помощью интерфейса командной строки нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. Затем запустить консоль и создать в ней конфигурацию, при выходе из конфигурационного режима консоли конфигурация конвертируется, загружается в Агента и хранится в базе Продукта. Используя утилиту, конфигурацию можно выгрузить из Агента и при этом загрузится политика DDP. Выгруженную конфигурацию можно опять загрузить в Агента.

Перед созданием конфигурации с помощью графического Web-based интерфейса нужно зарегистрировать локальный сертификат в базе Продукта, используя утилиту. При запуске GUI вызывается Java-апплет, который использует консоль. В ней создается конфигурация, при доставке на Агента она конвертируется и загружается, а также хранится в базе Продукта.

Способы создания политики безопасности

Создание политики безопасности для CSP VPN Gate возможно осуществить следующими способами:

- 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 программно-аппаратный комплекс или сетевой модуль RVPN. Создание такого файла описано в документе «Создание конфигурационного файла» (такую конфигурацию будем называть «native 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), которое описано в документе «Конфигурирование с помощью CiscoWorks».
- удаленное создание политики безопасности с помощью графического интерфейса Cisco Security Manager (CSM), описанного в документе «Управление CSP VPN Gate с помощью Cisco Security Manager»

Далее перейдите к инсталляции Продукта CSP VPN Gate 3.0 на программно-аппаратный комплекс, которая описана в документах «Инсталляция CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 2.0» или «КриптоПро CSP 3.0», «Инсталляция CSP VPN Gate при использовании СКЗИ «Крипто-КОМ 3.2», «Инсталляция CSP VPN Gate при использовании СКЗИ «LirSSL» или на модуль NME-RVPN «Инсталляция CSP VPN Gate на модуль».

Требования к внешним мерам безопасности

Физические меры безопасности

Помещения предприятия должны удовлетворять следующим требованиям:

- Обеспечение круглосуточной охраны корпусов предприятия;
- Обеспечение контроля внешнего периметра и внутренних помещений (видеонаблюдение);
- Обеспечение пропускного режима;
- Рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб;
- Двери должны быть прочными и оборудованы надежными механическими замками;
- Оборудование помещений системой пожарной сигнализации;
- Ведение Журнала выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника взявшего или сдавшего ключ дежурному вахтеру по зданию;
- Наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с продуктом, другой конфиденциальной информации. Для сейфа должно быть два ключа - основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат в опечатанном его личной печатью пенале в сейфе Генерального директора.

Процедурные меры безопасности

К безопасной эксплуатации продукта и обращения с СКЗИ предъявляются следующие требования:

- При приеме на работу сотрудники подписывают Обязательство о неразглашении сведений, составляющих коммерческую тайну организации
- Перечень сведений, составляющих коммерческую тайну организации, утверждается Генеральным директором;
- На предприятии должна быть разработана Инструкция по обращению с сертифицированными ФСБ/ФАПСИ шифровальными средствами (средствами криптографической защиты информации);
- Ведение Журнала учета СКЗИ, тестовых ключей на предприятии;
- Ведение Журнала учета обращения эталонных CD дисков на предприятии.

Технические меры безопасности

К техническим мерам безопасности предъявляются следующие требования:

- На поставляемой программно-аппаратной платформе ОС настраивается в соответствии с внутренними стандартами «С-Терра CSP” и администратору запрещается изменение среды функционирования, а именно:
  - модернизация ОС, включая установку штатных обновлений
  - добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки Изделия)

  - установка дополнительных приложений
  - самостоятельное добавление/удаление аппаратных компонент (в том числе сетевых карты, жестких дисков и т.п.).
- Доступ к персональным компьютерам и программно-аппаратным комплексам осуществляется на основе логического имени и пароля администратора в рамках операционных систем;
- Инсталляция, настройка и управление политикой безопасности комплекса осуществляется только администратором в соответствии с политикой безопасности предприятия;
- Администратор должен быть аутентифицирован и идентифицирован перед доступом к продукту с целью администрирования. Аутентификация осуществляется на основе пароля, вводимого с клавиатуры, не отображаясь на экране монитора, и выполняется операционной системой;
- Доставка контейнера с криптографическим ключом локального сертификата осуществляется только по доверенному каналу связи.

