УТВЕРЖДЕНО

BY.PTHK.00001-03.01 34 01-3-ЛУ

Программно-аппаратный комплекс

«Шлюз безопасности Bel VPN Gate 3.0.1»

РУКОВОДСТВО ОПЕРАТОРА

Руководство администратора

Введение

BY.PTHK.00001-03.01 34 01-3

Листов 11

Подп. и дата	
Инв. № дубл.	
Взам. инд. №	
Подп. и дата	
Инд. № подл.	

2012

Введение

.

Комплект поставки программно-аппаратного комплекса Bel VPN Gate 3.0.1

Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» включает:

– программный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1», содержащий программное средство ЭЦП и шифрования «AvCrypt ver 5.1» (РБ.ЮСКИ.09000-02, производитель ЗАО «Авест»), а также программные криптомодули «Криптоплагин», «Утилита для работы с контейнером»» для вызова криптографических процедур из «AvCrypt ver 5.1»;

– ОС Red Hat Linux 9;

– аппаратную платформу (сервер, терминал, ПЭВМ) с архитектурой Intel x86;

– внешнее устройство хранения информации (USB-носитель), совместимое с «AvCrypt ver 5.1» – по усмотрению пользователя;

– комплект программной документации.

Программно-аппаратный комплекс Bel VPN Gate 3.0.1 поставляется в следующей комплектации:

- аппаратная платформа, жесткий диск/энергонезависимая память которой содержит:
  - установленную операционную систему Red Hat Linux 9 с OpenSSH
  - предварительно инсталлированный и готовый к настройке программный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1» со встроенными криптографическими библиотеками программного средства электронной цифровой подписи и шифрования «AvCrypt ver. 5.1» (РБ.ЮСКИ.09000-02)
  - внешнее устройство хранения информации (USB-носитель), совместимый с «AvCrypt ver. 5.1» – по усмотрению пользователя;
- 3 компакт-диска:
  - с образом жесткого диска и Приложением к Инструкции по восстановлению ПАК
  - с вспомогательным ПО для восстановления образа диска и Инструкцией по восстановлению ПАК
  - с документацией.

Назначение и функции

Bel VPN Gate обеспечивает защиту транзитного трафика между различными узлами вычислительной сети, защиту трафика самого шлюза безопасности, а также пакетную фильтрацию трафика.

Управление шлюзом безопасности Bel VPN Gate 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.

Защита трафика Bel VPN Gate 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.

Шлюз безопасности Bel VPN Gate обеспечивает:

- 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).

ПАК Bel VPN Gate 3.0.1 использует криптографические библиотеки программного средства электронной цифровой подписи и шифрования «AvCrypt ver. 5.1» (РБ.ЮСКИ.09000-02), разработанного ЗАО "Авест".

«AvCrypt ver. 5.1» реализует криптографические алгоритмы в соответствии со стандартами Республики Беларусь:

- алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89;
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99;
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011;
- процедура выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99;
- процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».

Требования на базовые платформы

ПАК Bel VPN Gate 3.0.1 функционирует на аппаратных платформах с архитектурой Intel x86 под управлением ОС Red Hat Linux 9.

ПАК Bel VPN Gate 3.0.1 поставляется с настроенной операционной системой и инсталлированным программным комплексом (ПК) Bel VPN Gate 3.0.1. При этом администратору безопасности запрещается несанкционированное 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
- внесение изменений в ПО
- модификация файлов, содержащих исполняемые коды, при их хранении на жестком диске
- самостоятельное добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Нарушение этих ограничений рассматривается как нарушение целостности ПАК, заявленной функциональности и является основанием для отказа в гарантийном и дополнительном техническом сопровождении ПАК.

Архитектура Bel VPN Gate

Функциональность программно-аппаратного комплекса обеспечивает программный комплекс Bel VPN Gate (далее – Продукт), который состоит из следующих основных частей:

- VPN daemon (демон)
- VPN driver (драйвер)
- Cisco-like console (CLI консоль)
- Command Line Utilities (утилиты).

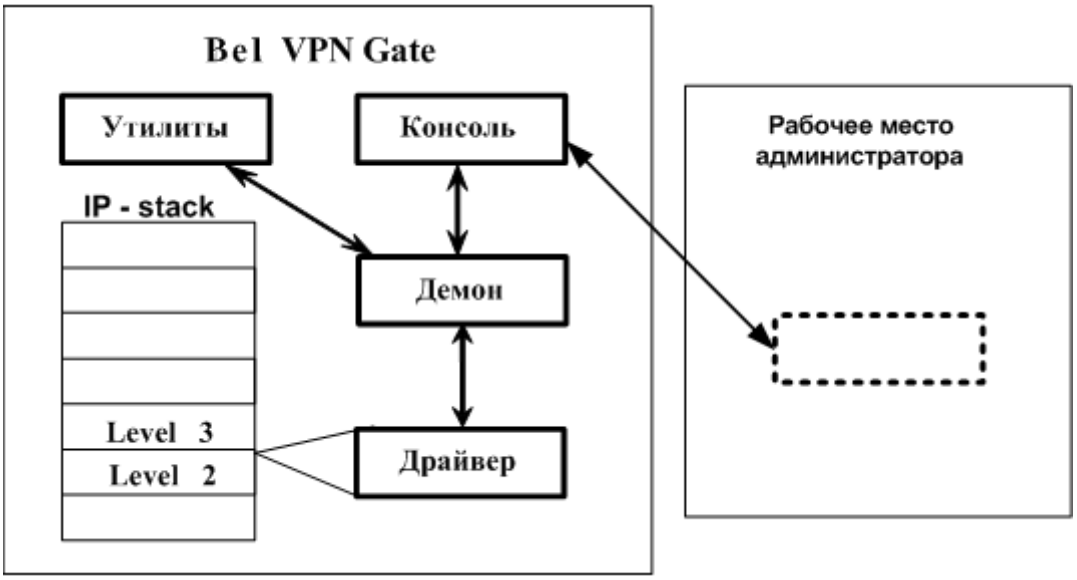

Рисунок 1

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`.

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.

Способы создания политики безопасности

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

- конфигурирование 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. Создание такого файла описано в документе «Создание конфигурационного файла» (такую конфигурацию будем называть «native конфигурацией»)
- конфигурирование 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 Bel VPN Gate с помощью Cisco Security Manager»

Далее перейдите к инсталляции Продукта Bel VPN Gate 3.0.1 на аппаратный комплекс, которая описана в документе «Инсталляция Bel VPN Gate при использовании «AvCrypt ver. 5.1».

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;
- принять меры по исключению несанкционированного доступа в помещения, в которых размещены ПК с установленным СКЗИ, посторонних лиц, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях, должен быть обеспечен контроль и обеспечена невозможность каких-либо действий с их стороны на ПК
- 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 руководителя.

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 служебную информацию/коммерческую тайну организации
- Перечень сведений, составляющих служебную информацию/коммерческую тайну организации, утверждается руководителем;
- На предприятии должна быть разработана Инструкция по обращению с сертифицированными 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 и защиты от НСД

К техническим мерам безопасности предъявляются следующие требования:

- На поставляемой программно-аппаратной платформе ОС настраивается в необходимой конфигурации 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;
- Не реже 1 раза в месяц проводится периодическое тестирование работоспособности комплекса, и контроль целостности программной части ПАК Bel VPN Gate;
- Право доступа к режиму управления комплексом (пользовательскому интерфейсу ПАК) имеет только администратор;
- Настройка ПАК (назначение IP-адресов интерфейсам, создание политики безопасности, регистрацию сертификатов, другие дополнительные настройки) осуществляется только администратором безопасности в соответствии с Руководством администратора ПАК Bel VPN Gate 3.0.1;
- Администратором организуется система протоколирования и аудита, ведется регулярный анализ результатов аудита с целью выявления нарушений несанкционированного доступа к ПАК.

Деятельность администратора на предприятиях с информацией ограниченного распространения регламентируется также Инструкцией по установке, настройке и эксплуатации ПАК Bel VPN Gate 3.0.1, предоставляемой дополнительно.

ЗАПРЕЩАЕТСЯ:

- осуществлять несанкционированное вскрытие ПАК;
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием ПАК;
- записывать на ключевые носители постороннюю информацию;
- защита ПАК и ключевой информации от НСД должна обеспечиваться не только в режиме функционирования, но и при проведении ремонтных и регламентных работ.