«Инфосистемы Джет»

Межсетевой экран Z-2

Описание состава и функциональных возможностей

Москва

2002 г.

Оглавление

Общие сведения о продукте

Назначение межсетевого экрана Z-2

Межсетевой экран (МЭ) Z-2 представляет собой программно-аппаратное средство управления доступом субъектов из одной сети или ее сегмента к объектам другой сети (сетевого сегмента).

МЭ Z-2 устанавливается на границе между защищаемой сетью Компании и внешними «открытыми» сетями, либо между сегментами защищаемой корпоративной сети и осуществляет полный контроль входящих/исходящих информационных на основе заданных правил управления доступом.

Типовая схема подключения Z-2 представлена на Рис. 1.

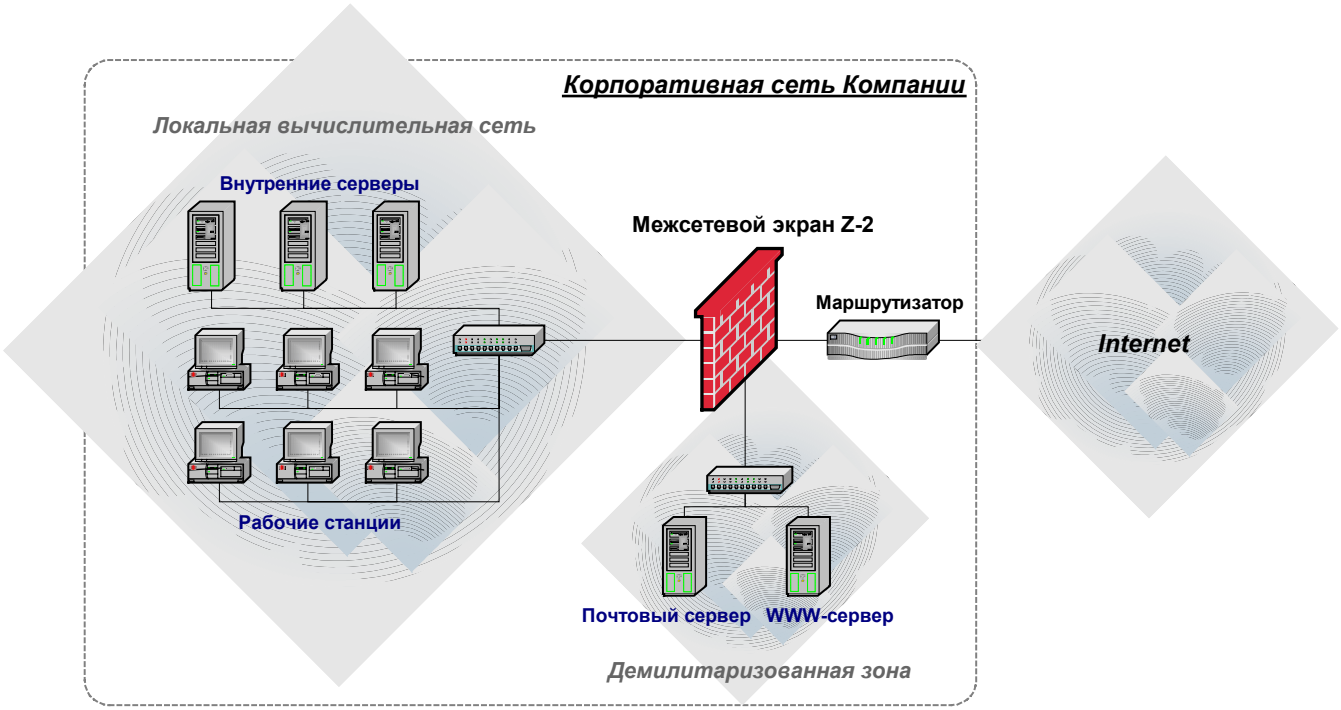

Рис. 1. Общая схема подключения межсетевого экрана Z-2

Контроль поступающей/исходящей информации и защита корпоративной сети обеспечивается путем фильтрации данных, т. е. их анализа по совокупности критериев и принятия решения о дальнейшем распространении информации в (из) корпоративной системы.

Основные функциональные возможности

МЭ Z-2 реализует разделение входящих/исходящих информационных потоков как на сетевом и сеансном уровнях модели информационного обмена ISO/OSI (пакетный фильтр), так и на уровне приложений, обеспечивая таким образом необходимую степень защиты внутреннего информационного пространства.

На сетевом и транспортном уровне МЭ обеспечивает фильтрацию соединений на основе транспортных адресов отправителя и получателя. Также осуществляется контроль доступа к сетевым сервисам в соответствии с установленными правилами доступа к сетевым ресурсам.

На уровне приложений МЭ обеспечивает фильтрацию запросов к прикладным сервисам с использованием шлюзов прикладного уровня, обеспечивающих возможность фильтрации по дате и времени запроса, типу протокола и набору разрешенных для данного протокола команд. Эти сервисы осуществляют передачу информации между сторонами, взаимодействующими через МЭ, что позволяет избежать прямого взаимодействия между внутренней сетью и внешними ресурсами. При этом обеспечивается полный анализ состояния TCP-соединения и анализ сетевого пакета.

Фильтрация осуществляется:

- при получении информации от субъектов внешнего информационного пространства.
- при выдаче информации субъектам внешнего информационного пространства.
- при информационном обмене МЭ Z-2 с субъектами внутреннего и внешнего информационного пространства для проведения аутентификации и обеспечения работы служебных сервисов управления и диагностики работы сетевых устройств.

Правила фильтрации МЭ Z-2 задаются администратором МЭ на основе принятых в Компании (подразделении) регламентов политики безопасности. Параметрами фильтрации являются служебные поля информационных пакетов, содержащие сетевой адрес источника запроса и адрес приемника, адреса сетевых интерфейсов, идентификаторы портов и сервисов.

МЭ позволяет проводить трансляцию сетевых адресов, в связи с чем внешний субъект не имеет возможности установить структуру внутренней сети.

Надежность работы МЭ обеспечивается комплексом мер по внутреннему аудиту системы, протоколированием всех соединений, протоколированием событий блокировки сетевых соединений и своевременным оповещением администратора МЭ о попытках несанкционированного доступа в систему.

Развитые средства администрирования межсетевого экрана делают удобной и практичной защиту сети любого масштаба, позволяют наращивать механизмы безопасности параллельно с развитием корпоративной информационной системы.

Комплекс МЭ обеспечивает возможность резервного копирования как файлов протоколирования, так и всей системы в целом с целью быстрого восстановления системы при тех или иных сбоях программно-аппаратного обеспечения.

Состав МЭ Z-2

МЭ Z-2 представляет собой программный комплекс.

В состав комплекса МЭ Z-2 входят следующие программные компоненты:

- фильтр сетевых пакетов;
- шлюзы прикладного уровня;
- средства идентификации и аутентификации пользователей;
- средства регистрации и учета запрашиваемых сервисов;
- средства оповещения и сигнализации о попытках нарушения правил фильтрации;
- средства контроля целостности;
- средства управления программным комплексом МЭ.

Схема взаимодействия основных компонент МЭ Z-2 представлена на Рис. 2.

IP-пакет, поступивший на один из сетевых интерфейсов МЭ Z-2, первоначально обрабатывается пакетным фильтром, после чего, если в результате анализа принимается решение о дальнейшей обработке пакета, он, если необходимо, передается одному из шлюзов прикладного уровня.

Шлюзы приложений могут анализировать сеансы взаимодействия в рамках конкретного протокола и производить фильтрацию по отдельным командам и другим атрибутам, характерным для данного протокола. Шлюз приложений может производить аутентификацию пользователей при запросах на установление соединения на сервере аутентификации и авторизации.

Кроме того, в состав межсетевого экрана Z-2 входят подсистема контроля целостности программной и информационной среды МЭ и подсистема восстановления в случае сбоев и отказов оборудования.

Управление всем программным комплексом МЭ осуществляется при помощи графического интерфейса.

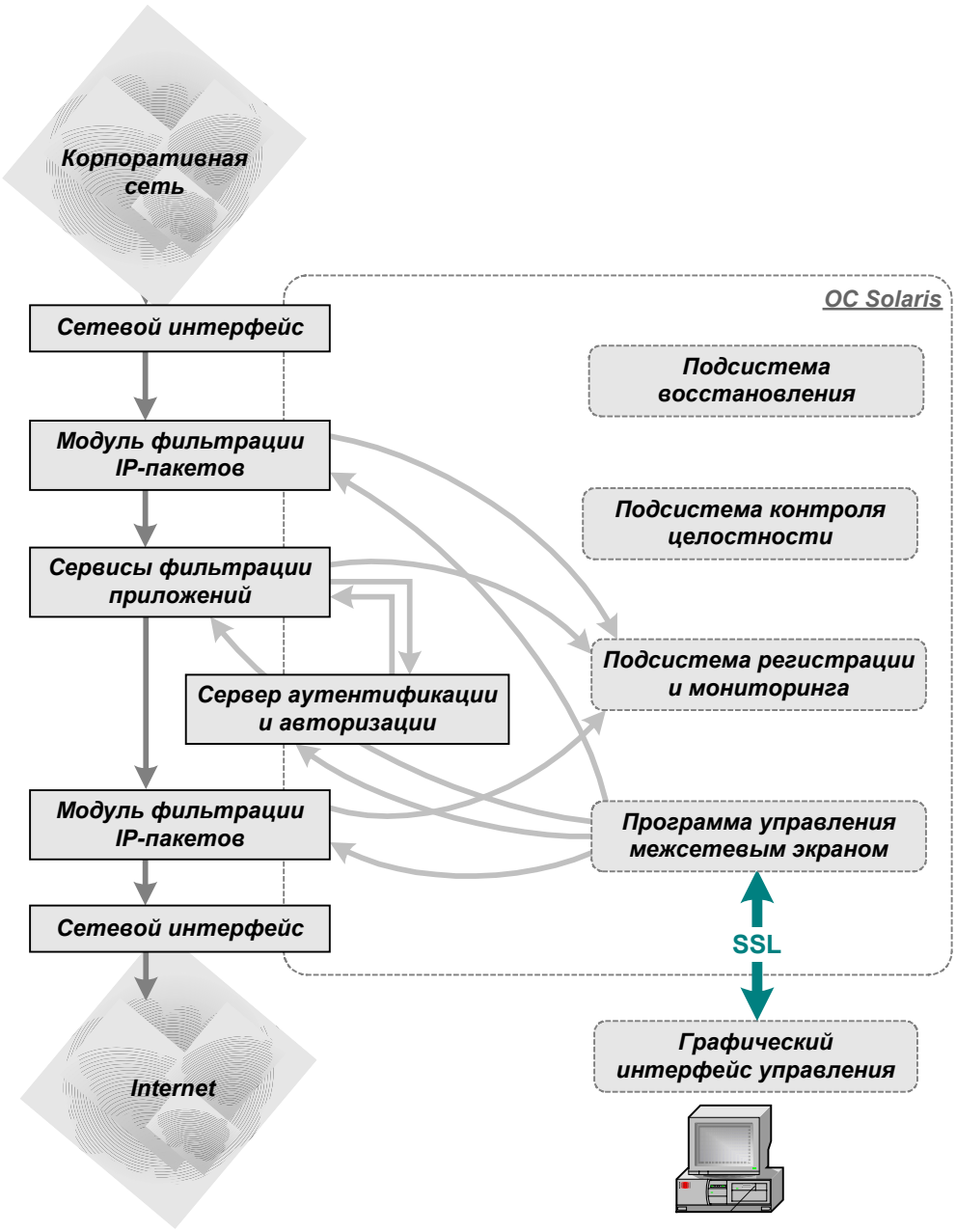

Рис. 2. Схема взаимодействия основных компонент межсетевого экрана Z-2

Правила фильтрации

Фильтрация информационных потоков МЭ Z-2 осуществляется двумя модулями - пакетным фильтром (на сетевом и транспортном уровнях) и набором шлюзов приложений (на прикладном уровне).

Фильтрация IP-пакетов

Модуль фильтрации IP-пакетов

Модуль ядерной фильтрации IP-пакетов МЭ Z-2 (**ipfilter**) представляет собой компоненту МЭ Z-2, предназначенную для фильтрации трафика на уровне IP-пакетов. Данный модуль обеспечивает:

- возможности фильтрации по следующим параметрам:
  - направлению движения пакета - входящий/исходящий (по интерфейсам);
  - IP адресам отправителя и получателя пакета;
  - портам отправителя и получателя пакета;
  - сетям;
  - любым IP протоколам;
  - опциям IP пакетов;
- фильтрацию фрагментированных IP пакетов;
- фильтрацию с сохранением состояния сессии;
- работу шлюзов приложений в «прозрачном» режиме;
- трансляцию сетевых адресов;
- протоколирование событий, получение и сохранение статистики работы по различным критериям.

Правила фильтрации IP-пакетов

Для управления трафиком IP-пакетов модуль пакетной фильтрации использует структуру данных, называемую правилом фильтрации. Пакетный фильтр применяет последовательность правил для каждого пакета. Если пакет отвечает правилу, то он может быть отправлен получателю (в т. ч. с занесением в журнал) или отброшен.

Создание и редактирование правил производится с помощью графического интерфейса. Правила обрабатываются МЭ Z-2 в порядке их записи.

Правило состоит из следующих элементов:

- направление движения пакетов: входящие в интерфейс, исходящие из интерфейса.
- IP-адреса или доменные имена отправителей пакетов.
- номера портов отправителей пакетов.
- IP-адреса или доменные имена получателей пакетов.
- номера портов получателей пакетов.
- действие, применяемое к пакету, отвечающему заданным условиям:
  - запретить прохождение пакета,
  - разрешить прохождение пакета,
  - разрешить прохождение пакета, вычислить количество переданных байт.
- способ протоколирования событий.
- признак сохранения состояния сессии:
  - сохранять состояние,
  - не сохранять состояние.
- дополнительные текстовые строки, которые добавляются к правилу в процессе его трансляции. Для их задание используется ниспадающие списки шаблонов.
- имя интерфейса, к которому применяется данное правило, из сформированного МЭ списка.

Трансляция сетевых адресов

Помимо фильтрации трафика пакетный фильтр включает систему трансляции IP-адресов (Network Address Translation, NAT). Основой для ее функционирования является набор правил трансляции, задание, редактирование и изменение порядка следования которых производится с помощью графического интерфейса.

Фильтрация на уровне приложений

Фильтрация на прикладном уровне МЭ Z-2 осуществляется средствами нескольких сервисов – шлюзов приложений, каждый из которых отвечает за управление обменом информацией по одному отдельному протоколу и между одним отдельным типом приложений. Например, прикладной шлюз FTP поддерживает протокол FTP и обслуживает запросы на передачу FTP-трафика через МЭ.

МЭ также включает в себя прикладные шлюзы общего назначения, которые называются подключаемыми шлюзами. Они поддерживают протоколы TCP и UDP и могут взаимодействовать с различными типами приложений.

Правила фильтрации на уровне приложений

Различные шлюзы приложений используют отличающиеся правила в зависимости от свойств конкретного сетевого протокола. Фильтры приложений конкретных протоколов позволяют избирательно разрешать или запрещать различные команды данного протокола.

Для каждого шлюза прикладного уровня существует набор параметров, определяющих его конфигурацию. Любой прикладной шлюз может быть заблокирован или разблокирован администратором МЭ. Это позволяет указать посреднику на то, следует ли ему предоставлять клиентам определенный тип сервиса.

Может возникнуть необходимость в создании нескольких конфигураций для одного шлюза прикладного уровня. Например, одним из требований политики безопасности может быть ограничение числа узлов WWW, доступных группе пользователей локальной сети. Администратор может модифицировать конфигурацию шлюза протокола HTTP с целью ограничения доступа к некоторым узлам WWW. Однако, это изменение коснется всех систем, находящихся в достоверной локальной сети, а не только этих пользователей. Вместо этого, можно иметь две различные конфигурации: конфигурацию для этой группы пользователей и конфигурацию для всех остальных пользователей локальной сети.

МЭ позволяет создавать для некоторых шлюзов прикладного уровня множественные конфигурационные наборы. Они дают возможность иметь несколько различных конфигураций для одного прикладного шлюза. Конфигурационные наборы могут быть добавлены в различные группы сервисов, для которых могут быть созданы различные правила их использования.

Модуль фильтрации на уровне приложений

Модуль фильтрации прикладного уровня МЭ Z-2 включает в себя следующие шлюзы:

- HTTP;
- FTP;
- SMTP;
- Telnet;
- Generic TCP/UDP;
- SNMP.

Прикладной шлюз протокола HTTP

Прикладной шлюз протокола HTTP (**http-gw**) осуществляет следующие функции:

- Фильтрация запросов на установление соединения по протоколу HTTP и ответов на запросы. В качестве критериев фильтрации могут выступать:
  - IP-адрес.
  - Метод протокола HTTP.
  - Запрашиваемый ресурс (URI).
  - MIME-тип ответа.
- Аутентификации запросов с помощью сервера аутентификации.
- Трансляции заблокированных ответов.

Независимо от режима работы прикладного шлюза HTTP, для заданных IP-адресов может быть задействован режим аутентификации. При этом до установления соединения HTTP-шлюз производит запрос сервера аутентификации по заданным адресу и порту.

HTTP-шлюз поддерживает два режима фильтрации запросов: "сильный" и "слабый".

В "сильном" режиме недопустимые запросы отвергаются, а в качестве ответа отправляется стандартная HTML-форма с сообщением об ошибке.

В "слабом" режиме осуществляются запросы даже на недопустимые URI, но ответы подвергаются фильтрации, в процессе которой происходит замена заблокированных MIME-типов на соответствующие файлы-заглушки.

Структура правил фильтрации запросов протокола HTTP более сложная, чем у других шлюзов приложений. В нее входят:

- Диапазон IP-адресов и портов, с которых запрос разрешен.
- Диапазон IP-адресов и портов, с которых запрос запрещен.
- Список заблокированных методов протокола HTTP.
- Список заблокированных URI.
- Таблица трансляции различных типов заблокированных ответов в файлы-заглушки.

МЭ Z-2 может включать в свой состав несколько шлюзов HTTP.

Настройка правил доступа к шлюзам HTTP производится с помощью графического интерфейса, с помощью которого указываются IP-адреса и порты с которых разрешен/запрещен доступ к шлюзам HTTP, а также необходимость выполнения процедуры аутентификации.

Как и все остальные шлюзы приложений, **http-gw** осуществляет протоколирование происходящих событий при помощи системного сервиса **syslogd**.

Прикладной шлюз протокола SMTP

Шлюз протокола SMTP МЭ Z-2 предназначен для разграничения и фильтрации почтового обмена между внешними и внутренними сетями (обрабатывается трафик SMTP). Шлюз SMTP представляет собой два взаимодействующих между собой процесса.

Первый из них - smtp-gw - производит прием почтового трафика из внешних и внутренних сетей и фильтрацию попыток установления соединения по следующим критериям:

1. Запрос должен исходить с разрешенного IP-адреса и порта.
2. При запросе должны использоваться только разрешенные команды протокола SMTP.

Если запрос соответствует обоим критериям, то между почтовым сервером и smtp-gw устанавливается соединение. Весь дальнейший обмен подвергается фильтрации, критериями которой будут являться:

1. Адрес электронной почты отправителя в поле MAIL FROM конверта почтового сообщения.
2. Адреса электронной почты получателя в поле RCPT TO конверта почтового сообщения.
3. IP-адрес отправителя (с которого был послан запрос на установление smtp-соединения).

Почтовые сообщения, отвечающие всем критериям, принимаются и записываются в специальный каталог. Прием всех остальных сообщений не производится, а серверу направляется уведомление об отказе. smtp-gw имеет встроенные возможности для обращения к базам данных, содержащих "спамерские" адреса, и осуществления фильтрации с использованием полученных данных.

Для задания критериев фильтрации используется специальная база данных. Кроме того, IP-адрес проходит дополнительную проверку на наличие в специализированной общедоступной базе данных, http://www.orbs.org, куда заносятся сведения об адресах почтовых серверов, используемых для рассылки нежелательных почтовых сообщений и "спама". Если почтовое сообщение поступило с такого адреса, то smtp-gw может заблокировать его или пропустить, добавив в заголовок письма запись Warning: Possible SPAM.

Еще одним критерием фильтрации smtp-gw является размер почтового сообщения. Если почтовое сообщение превышает установленный лимит, тело письма "отрезается" до установленного размера, а в конец сообщения добавляется запись Message exceeds maximum size, truncated by smtp proxy.

Второй процесс, называемый smtp-fwdr, запускается с определенной периодичностью и производит дополнительную фильтрацию сообщений, записанных процессом smtp-gw, и затем передает прошедшие фильтрацию почтовые сообщения почтовому серверу. Критерием фильтрации в данном случае будет является только корректность задания заголовков в теле почтового сообщения (From, To, Sender, Resent-Reply-To и др.)

Почтовые сообщения, не прошедшие фильтрацию или отвергнутые почтовым сервером, записываются в специальный каталог "некорректной" информации.

smtp-gw представляет собой резидентный процесс и функционирует постоянно. smtp-fwdr, напротив, должен запускаться периодически из планировщика задач cron. Все необходимые настройки выполняются автоматически во время инсталляции системы.

Управление обоими процессами осуществляется при помощи графического интерфейса.

Для хранения правил фильтрации предназначена специализированная база данных.

Настройка правил доступа к smtp-gw производится с помощью раздела Access Control Lists (ACL). Для него определяются значения следующих параметров:

1. Диапазон IP-адресов и портов, запрос с которых является разрешенным. Для этого необходимо с определить значения полей: action, class, alias, ports. Значения устанавливаются с помощью ниспадающих списков.
2. Список команд протокола SMTP, которые будут регистрироваться в протоколах работы МЭ Z-2. Для редактирования списка предназначен раздел log.
3. Список команд протокола SMTP, использование которых запрещено. Для этого предназначен раздел deny. Порядок редактирования списка такой же как и в предыдущем случае.

Прикладной шлюз протокола FTP

Прикладной шлюз протокола FTP (ftp-gw) предназначен для предотвращения прямого взаимодействия между внутренними и внешними информационными сетями по протоколу FTP и выполняет функции посредника.

ftp-gw предоставляет следующие возможности:

1. фильтрация входящих и исходящих запросов на установление FTP-соединения по. Критериями фильтрации являются IP-адрес и порт отправителя запроса, а также IP-адрес и порт узла, на который запрос направлен.
2. аутентификация входящих запросов на установление ftp-соединения на сервере авторизации.
3. фильтрация и протоколирование отдельных команд протокола FTP.

Все настройки ftp-gw, в том числе правил фильтрации, выполняются с помощью графического интерфейса.

Для каждого правила определяются значения следующих параметров:

1. Выполнение аутентификации через сервер.
2. Диапазон IP-адресов и портов, запрос с которых является разрешенным.
3. Список команд протокола FTP, которые будут регистрироваться.
4. Список команд протокола FTP, использование которых запрещено.

Прикладной шлюз протокола TELNET

Прикладной шлюз протокола TELNET предназначен для:

1. Фильтрации входящих и исходящих запросов на установление соединения протоколом TELNET по сетевым адресам источника и приемника запроса;
2. Аутентификации входящих запросов на установление соединения протоколом TELNET через сервер аутентификации.

Режимы работы прикладных шлюзов

Каждый из шлюзов прикладного уровня может работать в одном из двух режимов - "прозрачном" и "непрозрачном".

В "непрозрачном" режиме пользователь устанавливает соединение по соответствующему протоколу с МЭ Z-2 на заранее известный порт. На основании заданных правил фильтрации шлюз прикладного уровня разрешает или отвергает запрос на установление соединения. Если установление соединения данного

пользователя разрешено, шлюз прикладного уровня позволяет пользователю перейти в режим соединения с удаленным сервером по соответствующему протоколу. При необходимости производится также авторизация пользователя.

В "прозрачном" режиме пользователь устанавливает соединение по соответствующему протоколу напрямую с требуемым сервером, МЭ перехватывает запрос и передает его на обработку соответствующему шлюзу прикладного уровня, который на основании правил фильтрации разрешает или отвергает установление соединения, однако, в этом режиме работа МЭ полностью прозрачна для пользователя.

"Прозрачный" режим функционирования не предполагает наличие маршрутизации между рабочим местом пользователя и удаленным сервером.

Данный режим работы прикладных шлюзов реализуется только совместно с модулем фильтрации IP-пакетов. Для этого модуль фильтрации IP-пакетов должен быть соответствующим образом настроен.

Верификация правил фильтрации

Для верификации правил фильтрации, загружаемых в модуль фильтрации, в состав МЭ Z-2 включена специальная утилита checkipf.

Данная утилита проводит проверку списка правил, загружаемых в модуль фильтрации, на избыточность (пересечение по адресам, портам и протоколам в спецификации источника или точки назначения пакета) и непротиворечивость.

Идентификация и аутентификация пользователей МЭ Z-2

Аутентификация и проверка прав доступа пользователей МЭ Z-2 при их обращении к прикладным сервисам реализуется с помощью сервера аутентификации и требует соответствующей настройки правил фильтрации шлюзов прикладного уровня. Шлюзы приложений, требующих аутентификации пользователей, обращаются для этого к серверу аутентификации. Доступ к запрашиваемому сервису может быть разрешен только в случае успешной проверки подлинности пользователя на сервере аутентификации.

Сервер аутентификации и авторизации

Аутентификация пользователей осуществляется встраиваемыми аутентификационными модулями (PAM-модулями), количество которых может быть произвольным. В комплект МЭ входят два базовых модуля, реализующих схемы аутентификации по паролю и по схеме S/key. Кроме того, совместно с МЭ Z-2 можно использовать любые PAM-модули, входящие в состав ОС Solaris, при этом не требуется изменение программного кода сервера аутентификации.

Использование технологии PAM-модулей позволяет:

- динамически добавлять новые схемы аутентификации.
- использовать различные технологии аутентификации для различных пользователей.
- осуществлять общее управление учетными записями пользователей.

Несколько МЭ Z-2 могут использовать общий сервер аутентификации. МЭ Z-2 может иметь в своем составе несколько серверов аутентификации.

Настройка сервера аутентификации и авторизации выполнятся с помощью графического интерфейса.

Сервер аутентификации и авторизации осуществляет фильтрацию входящих запросов по IP-адресам и портам, для чего в его правилах фильтрации указываются IP-адреса, с которых разрешено производить запрос на аутентификацию.

Реализация конкретных схем аутентификации может существенно различаться в зависимости от принятой политики информационной безопасности Компании. Рекомендуется ограничивать доступ к серверу аутентификации и авторизации и разрешать его только для сервисов фильтрации на уровне приложений.

Настройка правил доступа к серверу аутентификации и авторизации производится с помощью списков управления доступом (Access Control Lists).

Схемы аутентификации пользователей

В настоящее время в МЭ Z-2 реализованы следующие схемы аутентификации:

- аутентификация по паролю (plain password);
- аутентификация по схеме одноразовых паролей S/Key.

Система аутентификации S/Key обеспечивает защиту от пассивных атак, таких как прослушивание сетевого трафика и перехват паролей и идентификаторов пользователей с целью последующего осуществления попыток НСД. Т. е. информация, которая потенциально может быть использована злоумышленником, не передается по сети, а используемые для аутентификации пароли не хранятся на каком-либо компьютере.

Генерируется уникальная последовательность одноразовых паролей на основе секретного пароля клиента путем многочисленных итераций надежной однонаправленной функции. Проверка одноразового пароля сервером аутентификации осуществляется при помощи однократного применения к нему надежной однонаправленной функции и сравнения полученного результата с предыдущим одноразовым паролем.

Безопасность системы S/Key базируется на секретности ключа (пароля) и открытости алгоритма.

Механизм авторизации/аутентификации пользователя описан в базе данных пользователей. Для пользователей, отсутствующих в базе, применяются механизмы по умолчанию, а в случае отсутствия таковых - пользователям отказывается в авторизации.

Настройка и администрирование МЭ Z-2

Управление МЭ Z-2 осуществляется централизовано с рабочего места администратора с помощью графической программы, установленной и исполняемой на рабочем месте администратора. При этом реализована технология "клиент-сервер", где в качестве серверов выступают программы, исполняемые совместно с остальным программным обеспечением (mserv). Графическая программа позволяет управлять произвольным количеством серверов, на которых развернуто программное обеспечение МЭ Z-2.

Графический интерфейс управления МЭ Z-2

Графический интерфейс обеспечивает администратору МЭ Z-2 возможность управления настройками межсетевого экрана. Запуск графического интерфейса управления производится с помощью командной строки.

Программа управления МЭ Z-2 mserv обеспечивает возможность удаленного управления компонентами МЭ администратором безопасности. По командам администратора программа управления вносит изменения в конфигурацию фильтров, осуществляет их запуск и остановку, и т.д.

Программа управления функционально выполнена в виде центрального объекта, сервера управления (MgmtServer) и субъектов управления:

- **NetworkManager** - осуществляет передачу информации о конфигурации интерфейсов и других сетевых настроек в графическую управляющую программу.
- **ProxyManager** - обеспечивает чтение, запись и генерацию конфигурационных файлов, запуск и остановку сервисов фильтрации на уровне приложений и пакетного фильтра, передачу статуса работы шлюзов.
- **AuthManager** - осуществляет редактирование баз данных пользователей сервера аутентификации и авторизации.
- **LogViewer** - производит передачу информации из системных журналов в реальном времени и фильтрацию сообщений.

Программа управления выполняет следующие функции:

- обеспечивает систему именования, необходимую для доступа управляющей графической программы к объектам управления.
- аутентификацию администратора по сертификатам x509 и установление SSL-соединений, а также определение полномочий для доступа администратора к объектам управления.

Разграничение доступа к функциям администрирования МЭ

Доступ к функциям конфигурирования и администрирования МЭ Z-2 предоставляется только уполномоченному администратору. Решение о предоставлении доступа к функциям администрирования принимается по результатам аутентификации.

Конфиденциальность взаимодействия между сервером, на котором установлен МЭ Z-2, и клиентским рабочим местом администратора, а также целостность передаваемой информации обеспечивается средствами протокола SSLv3. Протокол SSL подразумевает использование несимметричной ключевой пары в качестве долговременных ключей и сертификатов открытого ключа в формате X.509.

Аутентификация администратора МЭ

Подлинность администратора МЭ Z-2 устанавливается путем проверки подлинности сертификатов, выданных корпоративным Центром сертификации.

МЭ Z-2 использует в качестве аутентификационной информации для задач администрирования МЭ сертификат открытого ключа, созданного корпоративным Центром сертификации, и пароль.

Аутентификация администратора и генерация сеансового ключа для кодирования управляющего трафика выполняется по двустороннему протоколу SSLv3, субъектами которого являются администратор безопасности и сервер МЭ Z-2.

Для инициализации протокола оба субъекта должны обладать сертификатом открытого ключа доверенного центра сертификации, собственным секретным ключом и сертификатом открытого ключа, выданным доверенным центром сертификации (наличие у одного из субъектов сертификата открытого ключа другого субъекта не требуется).

Взаимная аутентификация происходит в несколько этапов, включающих обмен реквизитами, параметрами аутентификации, сертификатами открытого ключа, их проверку у центра сертификации и генерацию сеансовых ключей для кодирования трафика.

Создание центра сертификации открытых ключей

В состав базового ПО МЭ Z-2 входят средства генерации пар секретного и открытого ключей и запросов на сертификацию открытого ключа, а так же средства сохранения и управления сформированными сертификатами. Генерация сертификатов открытого ключа производится в центре сертификации открытых ключей. Средства, встроенные в Java-машину, позволяют использовать сертификаты открытых ключей в формате X.509, сформированные большинством распространенных центров сертификации (Microsoft Sertification Authority, Verisign, KEON и др).

Если в Компании МЭ Z-2 уже существует инфраструктура открытых ключей, МЭ Z-2 сможет использовать сформированные ей сертификаты.

При отсутствии в Компании развернутой ключевой инфраструктуры, возможно организовать новую службу генерации и сертификации ключей специально для целей аутентификации администратора безопасности и кодирования служебного трафика МЭ Z-2.

Создание и формат информационных файлов

После проверки корректности передаваемых сертификатов, управляющий сервер принимает решение об установлении соединения с аутентифицированным администратором безопасности на основании специальных файлов, содержащих список имен администраторов безопасности и операторов МЭ Z-2, которым позволено управлять МЭ Z-2 или просматривать протоколы посредством управляющего сервера.

Файлы имеют текстовый формат и создаются системным администратором после того, как администратор безопасности создаст необходимый набор сертификатов.

Защита управляющей информации

Средства кодирования и взаимной аутентификации администратора и сервера протокола SSLv3 поддерживают следующие методы кодирования, электронной подписи и генерации сеансовых ключей:

Алгоритмы блочного кодирования:

- RC4 с длиной ключа 128 бит.

- DES с длиной ключа 64 бита.
- Triple DES с длиной ключа 192 бита.

Алгоритмы аутентификации и цифровой подписи:

- RSA с длиной ключа 512÷2048 бит.
- DSA с длиной ключа 512÷2048 бит.

Алгоритмы выработки сеансового ключа:

- RSA с длиной ключа 512÷2048 бит.
- процедура Диффи-Хэллмана с длиной ключа 1024 бита.

По умолчанию для кодирования управляющей информации используется алгоритм Triple DES, для аутентификации и цифровой подписи - DSA с длиной ключа 1024 бит, для выработки сеансового ключа - процедура Диффи-Хэллмана.

Для установления защищенного соединения между графической программой управления и компьютерами с установленными МЭ необходимо иметь следующие ключи и сертификаты:

- сертификат открытого ключа доверенного центра сертификации;
- секретный ключ и сертификат открытого ключа администратора безопасности;
- набор секретных ключей и сертификатов открытого ключа компьютеров с установленными МЭ (по одной паре на каждый МЭ).

Секретные ключи и сертификаты открытых ключей (свой и доверенного центра сертификации) хранятся локально на рабочем месте администратора и на компьютерах, на которых установлены МЭ.

Ключи хранятся в хранилищах ключей. Создание хранилища и помещение в него ключей выполняется средствами окружения Java-машины.

Протоколирование и аудит

Средства регистрации событий

МЭ Z-2 позволяет осуществлять регистрацию событий, относящихся к функционированию МЭ, включая события загрузки и останова системы, запуска и остановки МЭ, регистрации и выхода из системы администратора и других пользователей. Программа протоколирования syslogd осуществляет запись сообщений о событиях в специальный файл, просмотр которого осуществляется при помощи подсистемы графического интерфейса администратора.

МЭ Z-2 способен генерировать запись аудита для следующих событий:

- все запросы сервисов прикладного уровня, блокированные МЭ Z-2 .
- все запросы, адресованные непосредственно к МЭ Z-2, в том числе для получения информации об архитектуре и конфигурации МЭ Z-2.
- все попытки изменения атрибутов безопасности.
- все запросы на использование механизмов аутентификации.
- завершение обработки запроса, вызванное рядом неудачных попыток аутентификации.
- использование функций, относящихся к администрированию МЭ Z-2.
- успешные и неудачные попытки изменения параметров конфигурации МЭ Z-2.

В каждой записи аудита регистрируется следующая информация:

- дату и время события;
- тип события;
- степень значимости события;
- идентификатор субъекта;
- результат (успех или неудача) события.

МЭ Z-2 защищает хранимые записи аудита от несанкционированного удаления.

Формат регистрации событий

Сообщения в журнале регистрации событий МЭ Z-2 подразделяются на 3 вида.

- информационные сообщения, выдаваемые каждым из сервисов фильтрации прикладного уровня в следующих случаях:
  - подсоединение шлюза к удаленному ресурсу по запросу клиента.
  - рассоединение шлюза с удаленным ресурсом/клиентом.
  - передача команды протокола, протоколирование которой затребовано администратором.
- предупреждения - сообщения о запрете в обслуживании в соответствии с политикой безопасности
- сообщения об ошибках

Просмотр протоколов

МЭ Z-2 предоставляет возможность сбора и отображения информации из журнала аудита с помощью специальной подсистемы отображения протоколируемых событий в составе графического интерфейса только уполномоченному администратору. Данная подсистема производит постоянное чтение файлов записей о протоколируемых событиях и позволяет просматривать и обрабатывать записи, выполненные каждым из серверов.

Подсистема предоставляет возможность выборочного просмотра журнала аудита и задания приоритетов при отображении событий. Для этого подсистема осуществляет фильтрацию записей по задаваемым администраторам критериям с помощью шаблонов.

Шаблоны протоколируемых событий представляют собой списки правил обработки (фильтрации) записей о событиях по определенным критериям, формируемые администратором МЭ средствами графического интерфейса, позволяющие фильтровать протоколы функционирования каждого из серверов и выделять только необходимую информацию.

При появлении новой записи к ней последовательно применяются все правила текущего набора, пока не будет обнаружено соответствие, после чего сообщение, полученное в результате обработки, выводится на первую строку таблицы.

Анализ регистрационной информации

Для анализа регистрационной информации в МЭ Z-2 используется программа plog, позволяющая генерировать отчеты на основе протоколируемой информации от модуля ядерной фильтрации ipmon.

Программа генерирует два вида отчетов:

- по адресам - отправителям IP пакетов
- по адресам - получателям IP пакетов

Оповещение администратора МЭ о попытках НСД

При обнаружении заданных событий, интерпретируемых как попытка НСД, МЭ Z-2 обеспечивает следующие действия:

- локальное оповещение администратора, осуществляющего мониторинг работы МЭ.
- удаленное оповещение администратора по электронной почте.

Требование реализуется средствами графического интерфейса администратора МЭ Z-2, в который входит подсистема просмотра журнала протоколируемых событий. С ее помощью можно выделять отдельные сообщения, соответствующие задаваемым администратором критериям. Выделенные сообщения могут выводится с выделением другим цветом и в самой верхней строке. В качестве реакции на заданное событие может быть задана посылка сообщения по электронной почте.

Контроль целостности МЭ Z-2

МЭ Z-2 обеспечивает динамический контроль целостности своей программной части (исполняемых модулей, и компонент операционной системы) и информационной среды (конфигурационных файлов и баз

данных, баз данных пользователей и аутентификационной информации) с помощью подсистемы контроля целостности, которая входит в состав МЭ. Подсистема подстроена на основе программного обеспечения Tripwire. С ее помощью выполняются периодические проверки контрольных сумм конфигурационных файлов, баз данных пользователей, исполняемых файлов и т.д.

Возможность верификации целостности конфигурации и хранимого кода МЭ Z-2 предоставляется только уполномоченному администратору.

МЭ Z-2 также выполняет набор операций самотестирования при запуске, восстановлении после сбоев и при запросах уполномоченного администратора.

Средства контроля целостности

Подсистема контроля целостности МЭ Z-2 позволяет отслеживать все изменения в наборе файлов и каталогов, определенном администратором МЭ. При этом используется два вида входных данных:

- описание объекта мониторинга - файловой системы (файл конфигурации),
- предварительно сгенерированную базу контрольных сумм текущей конфигурации.

Файл конфигурации содержит список файлов и/или каталогов с ассоциированными с ними списками атрибутов, подлежащих мониторингу. База контрольных сумм, генерируемая программой Tripwire, содержит набор записей с именами файлов, значениями атрибутов, информацией о сигнатуре, избирательных масках и записях конфигурационного файла, на основе которого была сгенерирована база контрольных сумм.

Программа Tripwire функционирует в четырех режимах, списанных ниже.

Инициализация базы контрольных сумм

Производит генерацию первоначальной базы данных контрольных сумм, содержащей записи о каждом файле согласно списку файла конфигурации. Каждая запись в базе контрольных сумм содержит: имя файла, атрибуты, информацию о сигнатуре и запись о конфигурации, для которой была сгенерирована база.

Проверка целостности

Проводит считывание данных из файла конфигурации, генерацию новой базы контрольных сумм и ее сравнение с первоначальной базой данных контрольных сумм, после чего составляется список добавленных и удаленных файлов. Для измененных файлов определяется необходимость занесения информации о произошедших событиях в создаваемый отчет.

Если выявленные изменения файлов являются разрешенными, проводится обновление первоначальной базы контрольных сумм в одном из описанных ниже режимов.

Обновление базы контрольных сумм.

В этом режиме выдается список файлов или конфигурационных записей в командной строке. Для этих файлов вновь производится генерация записей базы контрольных сумм, и записывается новая база (по запросу – также на безопасный носитель).

Интерактивное обновление базы контрольных сумм.

В этом режиме выводится список всех изменений, полученных в режиме проверки целостности. Для каждого изменения производится запрос системного администратора об обновлении соответствующего файла или записи.

Выполнение процедур контроля целостности

Для обеспечения контроля целостности программной и информационной части МЭ Z-2 программу контроля целостности необходимо запускать с периодичностью как минимум раз в сутки, проверяя тем самым возможные изменения в критичных с точки зрения информационной безопасности файлах операционной системы и межсетевого экрана. Запуск может производиться системным планировщиком cron.

Результатом работы является список всех изменений в установленном наборе файлов, включая удаление и добавление файлов, со времени инсталляции или последнего обновления базы данных контрольных

сумм, что позволяет гарантировать целостность программной и информационной части МЭ Z-2, а также своевременную реакцию на возможные попытки несанкционированного доступа.

Резервное копирование и восстановление МЭ

Если в результате сбоя или прерывания в обслуживании невозможно автоматическое восстановление, МЭ Z-2 переходит в режим обслуживания, который предоставляет возможность его возвращения в штатное состояние.

Выход из строя любого сервиса фильтрации уровня приложений или модуля ядерной фильтрации IP-пакетов приводит к приостановке связи по соответствующему протоколу. После этого любой доступ извне к ресурсам внутреннего информационного пространства становится невозможен.

Меры обеспечения надежности работы включают обязательное резервное копирование конфигурационных файлов и других данных, изменяемых в процессе работы.

МЭ Z-2 имеет возможность оперативного восстановления работоспособности после сбоев и отказов оборудования. Основным методом повышения надежности и обеспечения восстановления является периодическое проведение процедуры резервирования всей системы межсетевого экрана или ее критических участков и восстановления в случае сбоев. Для этих процедур используются штатные средства ОС Solaris: ufsdump и ufsrestore.

Создание резервных копий

Для выполнения процедуры резервного копирования всей файловой системы или отдельных файлов на магнитную ленту, жесткий диск или дискеты используется программный модуль ufsdump.

При минимальном объеме резервного копирования достаточно ограничиться сохранением всех файлов в указанных каталогах.

Резервному копированию подлежат:

- конфигурация пакетного фильтра;
- конфигурация шлюзов прикладного уровня.

Системные требования к аппаратной части МЭ

МЭ Z-2 работает под управлением операционной системы Solaris 8.0 компании Sun Microsystems на аппаратной платформе на базе процессора SPARC или Intel, что позволяет подбирать оптимальные по производительности и цене конфигурации.

Минимальные системные требования для платформы Solaris/Sparc:

- CPU: UltraSPARC IIe
- RAM: 128 Мбайт
- HDD: 8 Гбайт
- 2 Network Ethernet card

Минимальные системные требования для платформы Solaris/Intel:

- CPU: Intel Pentium 350 МГц
- RAM: 128 Мбайт
- HDD: 8 Гбайт
- 2 Network Ethernet card
- Цветной монитор 15"
- Клавиатура и мышь