==========

Z-2 – универсальный межсетевой экран высшего уровня защиты

==========

Практически все современные корпоративные информационные системы используют сети общего пользования для получения доступа к внешним ресурсам, предоставления собственных ресурсов внешним пользователям, а зачастую используют публичные сети как средство организации информационного взаимодействия территориально-распределенных участков корпоративной сети.

В такой ситуации с одной стороны возникает необходимость ***обеспечения доступности части корпоративных информационных ресурсов извне***, а также ресурсов внешних открытых сетей для внутренних пользователей Компании, с другой – остро встает ***проблема контроля информационного взаимодействия*** с внешним миром и ***обеспечения защиты корпоративной информационной системы от угроз*** информационной безопасности извне.

Для разграничения доступа к ресурсам и контроля информационных потоков между защищаемой сетью Компании и внешними сетями, а также между сегментами корпоративной сети, необходимо использовать ***специальные средства защиты – межсетевые экраны***.

Межсетевой экран Z-2

Межсетевой экран (МЭ) Z-2 предназначен для защиты внутреннего информационного пространства корпоративных информационных систем (в том числе территориально-распределенных) при информационном взаимодействии с внешним миром в соответствии с принятой в Компании политикой информационной безопасности.

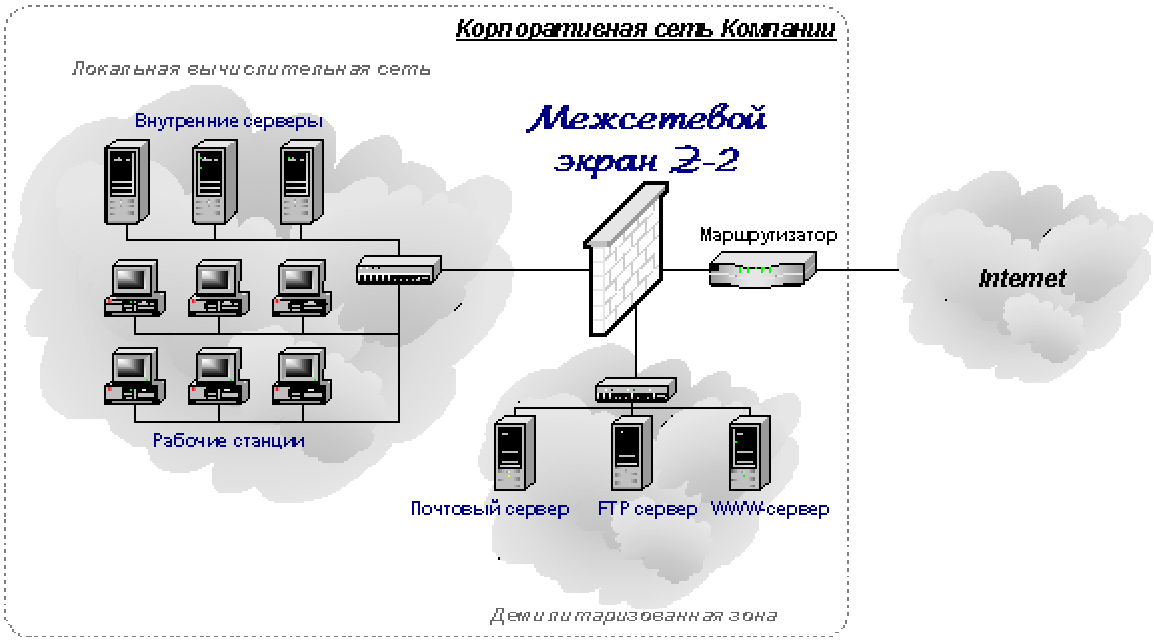
МЭ Z-2 устанавливается на границе между защищаемой сетью Компании и внешними «открытыми» сетями либо между сегментами защищаемой сети (разного уровня конфиденциальности или служащих для решения различных задач и потому требующих изоляции) и осуществляет контроль входящих/исходящих информационных потоков на основе заданных правил управления доступом.

Основные функциональные возможности

Основные возможности МЭ Z-2 по обеспечению информационной безопасности корпоративной информационной системы включают:

- **Контроль входящих/исходящих информационных потоков на нескольких уровнях модели информационного обмена OSI/ISO;**
- **Идентификацию и аутентификацию пользователей с защитой от прослушивания сетевого трафика;**
- **Трансляцию сетевых адресов и сокрытие структуры защищаемой сети;**
- **Обеспечение доступности сетевых сервисов;**
- **Регистрацию запросов на доступ к ресурсам и результатов их выполнения;**
- **Обнаружение и реагирование на нарушения политики информационной безопасности.**

Рисунок 1: Схема подключения межсетевого экрана Z-2



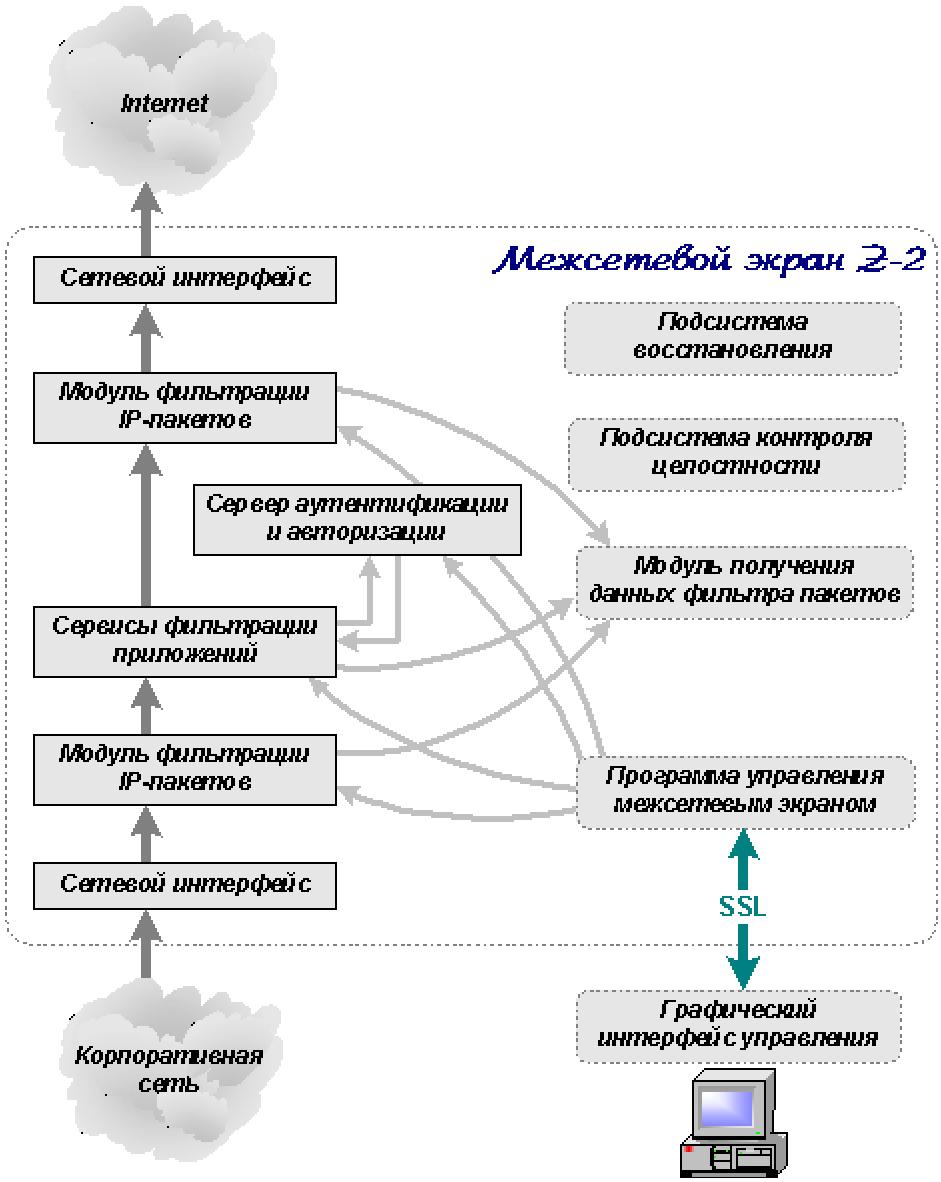
Состав МЭ Z-2

МЭ Z-2 представляет собой программный комплекс, функционирующий под управлением операционной системы Solaris компании Sun Microsystems на аппаратной платформе SPARC или Intel, что позволяет подбирать оптимальную конфигурацию по производительности и цене.

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 случаях нарушения правил фильтрации;
- Средства динамического контроля целостности программной и информационной среды МЭ;
- Средства управления программным комплексом МЭ.

Рисунок 2: Состав межсетевого экрана Z-2



Функционирование МЭ Z-2

Фильтрация информационных потоков

Разграничение доступа и контроль входящих/исходящих информационных потоков осуществляется путем фильтрации данных, т.е. их анализа по совокупности критериев и принятия решения об их распространении в (из) защищаемой сети или сегмента.

Фильтрация производится на основе правил, задаваемых администратором, в соответствии с принятой в Компании политикой информационной безопасности.

На сетевом и транспортном уровнях фильтрация соединений осуществляется пакетным фильтром на основе транспортных адресов отправителя и получателя с сохранением состояния сессии. При этом осуществляется контроль доступа в соответствии с установленными правилами разграничения доступа к сетевым ресурсам и сервисам.

Фильтрация на уровне приложений осуществляется набором фильтров прикладного уровня, каждый из которых отвечает за фильтрацию информационного обмена по одному отдельному протоколу и между одним определенным типом приложений. Фильтрация осуществляется по дате и времени запроса, IP-адресам источников запроса, типу протокола, отдельным командам и другим атрибутам, характерным для данного протокола.

МЭ Z-2 включает шлюзы прикладного уровня для протоколов HTTP, FTP, SMTP, TELNET и SNMP.

МЭ также включает в себя прикладные шлюзы общего назначения, которые являются нейтральными по отношению к содержимому протокола и могут быть использованы для различных типов приложений, применяющих в качестве транспорта протоколы TCP и UDP. Универсальные шлюзы Generic TCP и Generic UDP обеспечивают фильтрацию по сетевым адресам и портам источника и получателя запроса и протоколирование соединений.

Шлюзы приложений могут также производить аутентификацию запроса на установление соединения на сервере аутентификации и авторизации.

МЭ может также проводить фильтрацию запросов к прикладным сервисам путем создания шлюзов приложений на уровне ядра ОС, для чего в его состав входят шлюзы приложений на уровне ядра ОС. Основная их задача – пропустить протокол, который они обслуживают, через МЭ на уровне пакетного фильтра, что позволяет существенно повысить быстродействие МЭ. В состав МЭ Z-2 входят шлюзы приложений на уровне ядра для протоколов FTP, Rlogin/Rsh и RealAudio (протокол PNA).

Разграничение доступа к шлюзам приложений производится с помощью списков управления доступом (Access Control Lists) на основании заданного диапазона IP-адресов и портов разрешенных источников запросов.

Верификация правил фильтрации

Для проверки списка правил фильтрации на избыточность и непротиворечивость МЭ Z-2 включает в состав средства проверки правил по адресам, портам и протоколам источника или точки назначения пакета.

Трансляция сетевых адресов

Помимо фильтрации информационных потоков МЭ Z-2 позволяет проводить трансляцию сетевых адресов (Network Address Translation, NAT) на основании заданного набора правил. Это позволяет скрыть структуру внутренней сети от внешних субъектов и расширить возможность использования произвольных внутренних IP-адресов.

Обеспечение доступности ресурсов

Для предотвращения угроз доступности сервисов внешнего информационного обмена МЭ Z-2 осуществляет управление информационными потоками. В качестве атрибутов безопасности выступает количество одновременно обрабатываемых запросов на предоставление сервисов в зависимости от приоритета сервиса, определенного политикой безопасности компании.

Идентификация и аутентификация пользователей МЭ Z-2

МЭ Z-2 включает две схемы аутентификации пользователей – по простому паролю и паролю временного действия. Использование временных паролей позволяет обеспечить защиту от пассивных атак, таких как прослушивание сетевого трафика и перехват идентификаторов и паролей пользователей, т.к. информация, которая потенциально может быть использована для попыток получения несанкционированного доступа, не передается по сети, а используемые для аутентификации пароли не хранятся на каком-либо компьютере.

Аутентификация и проверка прав доступа пользователей при обращении к прикладным сервисам реализуется с помощью сервера аутентификации и авторизации, к которому обращаются шлюзы приложений МЭ Z-2. Доступ к запрашиваемому сервису может быть разрешен только в случае успешной проверки подлинности на сервере аутентификации.

Схема аутентификации каждого конкретного пользователя и иная необходимая информация хранится в базе данных пользователей на сервере аутентификации и авторизации МЭ Z-2.

Благодаря использованию встраиваемых модулей аутентификации (PAM-модулей), МЭ Z-2 допускает подключение других схем аутентификации без изменения программного кода сервера аутентификации и авторизации межсетевого экрана.

Доступ к серверу аутентификации разрешен только шлюзам приложений в соответствии со списками управления доступом на основании IP-адресов и портов разрешенных источников запросов на аутентификацию.

Настройка и администрирование МЭ Z-2

Средства управления

Управление компонентами одного или нескольких межсетевых экранов Z-2 осуществляется централизованно с рабочего места Администратора на основе технологии «клиент-сервер», где в качестве сервера выступает программа управления, запускаемая на МЭ Z-2, а в качестве клиента – графический интерфейс управления МЭ Z-2, установленный на рабочем месте Администратора.

Графический интерфейс и программа управления написаны на языке Java, что обеспечивает многоплатформенность интерфейса управления МЭ.

Графический интерфейс управления позволяет:

- Производить настройку фильтра сетевых пакетов МЭ;
- Проводить настройки сервисов фильтрации, осуществлять их запуск и остановку, а также передачу статуса их работы;
- Редактировать базы данных пользователей сервера аутентификации;
- Производить полный или выборочный просмотр системных журналов в реальном времени;
- Производить настройку системного планировщика задач (cron).

Разграничение доступа и защита функций администрирования МЭ

Доступ к функциям конфигурирования и администрирования МЭ Z-2 предоставляется только уполномоченному Администратору, который должен пройти процедуру проверки подлинности.

Кроме того, осуществляется защита данных и команд управления, передаваемых между МЭ Z-2 и рабочим местом Администратора.

В качестве аутентификационной информации для задач администрирования МЭ Z-2 используется сертификат открытого ключа X.509 и одноразовый пароль S/key. Конфиденциальность и целостность информации управления обеспечивается средствами протокола SSLv3.

Обеспечение надежности функционирования МЭ

Надежность работы МЭ Z-2 обеспечивается комплексом мер по внутреннему аудиту, регистрацией событий и своевременным оповещением Администратора МЭ о нарушениях политики безопасности, а также средствами контроля целостности компонентов, резервного копирования и восстановления МЭ в случае сбоев.

Регистрация событий

МЭ Z-2 осуществляет регистрацию событий, связанных с его функционированием, включая все виды входящих/исходящих запросов и процессов их обработки, изменения конфигурации МЭ и прочие административные действия, события загрузки и останова МЭ, регистрации и выхода из системы Администратора и других пользователей. При этом обеспечивается защита хранимых данных аудита от несанкционированного удаления.

Полный или выборочный просмотр протоколов регистрации осуществляется только уполномоченным Администратором.

МЭ Z-2 включает также средства анализа регистрационной информации и генерации отчетов на ее основе.

Оповещение Администратора МЭ о попытках НСД

Для обеспечения оперативного реагирования на нарушения политики информационной безопасности компании при обнаружении событий, отвечающих определенным критериям (например, интерпретируемых как попытки НСД), МЭ Z-2 осуществляет одно из заданных действий, например:

- локальное оповещение Администратора, осуществляющего мониторинг работы МЭ;
- удаленное оповещение – посылка Администратору сообщения по электронной почте;
- другие настраиваемые Администратором действия.

Контроль целостности МЭ Z-2

МЭ Z-2 обеспечивает динамический контроль целостности своей программной части (исполняемых модулей и компонентов операционной системы) и информационной среды (конфигурационных файлов, баз данных пользователей и аутентификационной информации).

Возможность проверки целостности компонентов МЭ Z-2 предоставляется только уполномоченному Администратору.

Резервное копирование и восстановление МЭ

При выходе из строя компонентов фильтрации МЭ в результате сбоя или отказа происходит приостановка связи по соответствующему протоколу и прекращение доступа к защищаемым ресурсам. Тем самым реализован принцип невозможности перехода в небезопасное состояние защищаемой информационной системы.

Для быстрого возобновления выполнения функций защиты корпоративной сети в случае сбоев и отказов программно-аппаратного обеспечения МЭ Z-2 предусмотрена возможность резервного копирования компонентов самого МЭ (конфигурационных файлов, файлов протоколирования, баз данных пользователей), файловой системы (средствами операционной системы), а также оперативного восстановления работоспособности МЭ.

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

Основные особенности МЭ Z-2

Отличительными особенностями МЭ Z-2 являются:

- Гибкая система контроля информационных потоков на нескольких уровнях сетевых протоколов;
- Возможность функционирования шлюзов в специальном режиме работы на быстрых каналах связи;
- Трансляция адресов и сокрытие структуры защищаемой сети;

- Наличие встроенного расширяемого сервера аутентификации и авторизации;
- Возможность централизованного управления корпоративной политикой безопасности;
- Мультиплатформенный графический интерфейс управления произвольным количеством МЭ;
- Возможность аутентификации Администратора МЭ на основании биометрических характеристик;
- Контроль действий Администратора;
- Возможность мониторинга и автоматического реагирования на нарушения политики безопасности;
- Высокая степень собственной защищенности;
- Возможность интеграции с антивирусными решениями и системами блокировки “спам”;
- Гибкий баланс уровня защиты корпоративной сети и производительности.

Варианты поставки МЭ Z-2

В зависимости от особенностей защищаемой информационной системы компании МЭ Z-2 может быть поставлен в трех различных вариантах комплектации:

Состав программного обеспечения	**Серия «С»**	**Серия «В»**	**Серия «А»**
Модуль фильтрации IP-пакетов на уровне ядра ОС	+	+	+
Минимальный набор шлюзов приложений (HTTP, FTP, SMTP)	+	+	+
Расширенный набор шлюзов приложений (telnet, SNMP, Generic TCP/UDP)	-	+	+
Набор шлюзов приложений на уровне ядра ОС	+	+	+
Сервер аутентификации и авторизации	+	+	+
Подсистема контроля целостности	+	+	+
Графический интерфейс администратора	+	+	+
Подсистема мониторинга и регистрации событий	+	+	+
Средства обеспечения отказоустойчивости	-	-	+
Подсистема биометрической аутентификации администратора	-	-	+
Класс защищенности в соответствии с РД Гостехкомиссии[1]	3 класс	2 класс	1 класс

Заключение

Использование МЭ Z-2 для защиты корпоративной информационной системы позволит обеспечить высокий уровень безопасности внутреннего информационного пространства компании и возможность детального разграничения доступа к ресурсам и сервисам на основании корпоративной политики информационной безопасности. Развитые средства

[1] МЭ Z-2 серии «С» получил сертификат Гостехкомиссии РФ № 555 от 27.12.2001 г.

МЭ Z-2 серии «В» получил сертификат Гостехкомиссии РФ № №638 от 27.06.2002 г.

Сертификация МЭ Z-2 серии «А» проводится в настоящее время в Гостехкомиссии РФ.

управления МЭ Z-2 делают реальной и практичной защиту сети любого назначения и масштаба, позволяют наращивать механизмы безопасности параллельно с развитием корпоративной информационной системы.

========