Межсетевое экранирование

Содержание:

Цели

- изучить принципы организации межсетевого экранирования как механизма обеспечения безопасности информационных систем;
- ознакомиться с классификацией межсетевых экранов.
- ознакомиться с технологией виртуальных частных сетей и механизмом ее реализации.

- Одним из эффективных механизмов обеспечения информационной безопасности распределенных вычислительных сетях является экранирование, выполняющее функции разграничения информационных потоков на границе защищаемой сети.
- Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Межсетевой экран

- Функции экранирования выполняет **межсетевой экран** или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Принципы работы межсетевых экранов

- Существует два основных способа создания наборов правил межсетевого экрана: "включающий" и "исключающий". Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.

Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика. Безопасность может быть дополнительно повышена с использованием "межсетевого экрана с сохранением состояния". Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что оптимально для реальных применений.

Дополнительные возможности межсетевого экранирования

- антивирусный контроль "на лету";
- контроль информационного наполнения (верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);
- выполнение функций ПО промежуточного слоя;
- наличие сервисных утилит работы с правилами;
- встраиваемые системы сбора статистики и предупреждений об атаке.

1. Классификация межсетевых экранов

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети – на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов, например, при использовании сетевой операционной системы Novell Netware, следует принимать во внимание протокол SPX/IPX.

Характеристика межсетевых экранов

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Межсетевые экраны с фильтрацией пакетов

Представляют собой маршрутизаторы или работающие на сервере программы, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Поэтому такие экраны называют иногда пакетными фильтрами. Фильтрация осуществляется путем анализа IP-адреса источника и приемника, а также портов входящих TCP- и UDP-пакетов и сравнением их со сконфигурированной таблицей правил. Эти межсетевые экраны просты в использовании, дешевы, оказывают минимальное влияние на производительность вычислительной системы. Основным недостатком является их уязвимость при подмене адресов IP. Кроме того, они сложны при конфигурировании: для их установки требуется знание сетевых, транспортных и прикладных протоколов.

Шлюзы сеансового уровня

Контролируют допустимость сеанса связи. Они следят за подтверждением связи между авторизованным клиентом и внешним хостом (и наоборот), определяя, является ли запрашиваемый сеанс связи допустимым. При фильтрации пакетов шлюз сеансового уровня основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола TCP, т. е. функционирует на два уровня выше, чем межсетевой экран с фильтрацией пакетов. Кроме того, указанные системы обычно имеют функцию трансляции сетевых адресов, которая скрывает внутренние IP-адреса, тем самым, исключая подмену IP-адреса. Однако в таких межсетевых экранах отсутствует контроль содержимого пакетов, генерируемых различными службами. Для исключения указанного недостатка применяются шлюзы прикладного уровня.

Шлюзы прикладного уровня

- проверяют содержимое каждого проходящего через шлюз пакета и могут фильтровать отдельные виды команд или информации в протоколах прикладного уровня, которые им поручено обслуживать. Это более совершенный и надежный тип межсетевого экрана, использующий программы-посредники (proxies) прикладного уровня или агенты. Агенты составляются для конкретных служб сети Интернет (HTTP, FTP, Telnet и т. д.) и служат для проверки сетевых пакетов на наличие достоверных данных.

Межсетевые экраны экспертного уровня.

- Наиболее сложные межсетевые экраны, сочетающие в себе элементы всех трёх приведённых выше категорий. Вместо прокси-сервисов в таких экранах используются алгоритмы распознавания и обработки данных на уровне приложений.

Вопросы безопасности применения межсетевого экранирования

Наиболее очевидным недостатком МЭ является большая вероятность того, что он может заблокировать некоторые необходимые пользователю службы, такие как Telnet, FTP, XWindow, NFS и т. д. Некоторые объекты могут обладать топологией, не предназначенной для использования МЭ, или использовать службы (сервисы) таким образом, что его использование потребовало бы полной реорганизации локальной сети.

МЭ, как правило, не обеспечивает защиту от внутренних угроз. С одной стороны, МЭ можно разработать так, чтобы предотвратить получение конфиденциальной информации злоумышленниками из внешней сети, однако, МЭ не запрещает пользователям внутренней сети копировать информацию на магнитные носители или выводить ее на печатающее устройство. Таким образом, было бы ошибкой полагать, что наличие МЭ обеспечивает защиту от внутренних атак или вообще атак, для которых не требуется использование МЭ.

В заключение стоит отметить, что межсетевые экраны являются необходимым, но явно недостаточным средством обеспечения информационной безопасности. Они обеспечивают лишь первую линию обороны.