Администрирование информационных систем

Межсетевой экран

Основные определения

- Межсетевой экран (брандмауэр, файрвол) – программный или программно-аппаратный комплекс, основной функцией которого является разделение глобальной и локальной сетей, а также защита последней от несанкционированного доступа и вредоносных программ.
- Туннелирование – процесс, в ходе которого создаётся логическое соединение между двумя конечными точками посредством инкапсуляции (вкладывания) различных протоколов друг в друга; часто применяется шифрование.
- Интранет – внутренняя частная сеть организации с использованием всех технологий Веб для организации своей работы (протоколы и тд), наличие в ней подсетей с различным уровнем доступа. «Интернет в миниатюре».

Функции сетевого экрана

Основные функции сетевого экрана выглядят так:

- скрытие информации о внутренней сети (имена систем, топология сети, типы сетевых устройств и внутренние идентификаторы пользователей, другое);
- скрытие уязвимых мест системы, защита от атак;
- перенаправление входного трафика к требуемым внутренним системам и/или подсетям;
- протоколирование трафика в/из внутренней сети;
- блокировка нежелательного или недостоверного трафика;
- обеспечение аутентификации пользователей.

Классификация сетевых экранов

Сетевые экраны могут работать на таких уровнях модели OSI:

- канальном (управляемые коммутаторы) – фильтруют трафик, используя низкоуровневую информацию, например, MAC-адрес; эффективность низкая, применение в основном между узлами сети или подсетями;
- сетевом (пакетные фильтры) – фильтрация использует данные из заголовка пакета, такие, как IP-адрес, порт и др.; быстрые, эффективные, часто используются на границах системы, но не обладают свойством анализа получаемой информации и уязвимы к подменам адресов/данных в пакете;
- сеансовом (шлюзы и посредники) – исключают прямой доступ ко внутренним узлам сети; присутствует детальный анализ поступающей информации по типу, источнику, способу доставки и др.

Классификация сетевых экранов

Сетевые экраны могут быть реализованы:

- программно – специальное ПО, которое необходимо установить на один из ПК сети и настроить; условно дешевая и простая реализация (при наличии свободного устройства и грамотного администратора);
- программно-аппаратно – зачастую это уже готовое устройство с предварительно установленным и настроенным ПО, выполняющее указанные функции; более просты в эксплуатации и высокоэффективны, однако имеют ряд ограничений в работе и модернизации;
- гибридная реализация – совместное использование перечисленных выше вариантов в комплексе с рядом дополнений позволяет устранить недостатки и повысить эффективность работы системы.

Сетевые экраны – архитектура системы

Существует несколько вариантов конфигурации архитектуры сетевого экрана и архитектурных защитных решений:

- Хост на два сегмента сети – это устройство с двумя сетевыми картами на два выхода, во внутреннюю и внешнюю сети. Маршрутизация отключена, прямая связь блокируется. Брандмауэр – обязательное промежуточное звено. Простой и недорогой вариант.
- Экранированный хост (хост-бастион) – это один из хостов сети с повышенными параметрами защищенности. Маршрутизация настраивается так, что все **входящие** запросы обязательно проходят исключительно через бастион, а уже потом на узлы внутренней сети.
- Экранированная подсеть – дополнение бастиона малой внешней сетью-периметром с дополнительной экранированной точкой доступа во внутреннюю сеть. Появляются дополнительные «линии обороны», препятствующие несанкционированному доступу в сеть – шлюз-бастион-периметр-внутр.шлюз.

Сетевые экраны – факторы администрирования

При администрировании сетевых экранов существенную роль могут сыграть такие факторы как:

- уровень угрозы для сети и «необходимый уровень паранойи» для защиты сети от атак;
- необходимость реализации интранета и разграничения доступа пользователей к различным сегментам сети предприятия;
- необходимость удаленного доступа к системе защиты и удаленного администрирования сетевого экрана;
- количество зарегистрированных пользователей экрана и система его резервирования;
- наличие доверительных линий (с другими проверенными сетями и/или между частями большой распределенной сети);
- применение туннелирования и технологии VPN.