Призначення, можливості і основні захисні механізми міжмережевих екранів (брандмауерів). Переваги та недоліки брандмауерів. Основні захисні механізми: фільтрація пакетів, трансляція мережевих адрес, проміжна аутентифікація, відхилення скриптів, перевірка пошти, віртуальні приватні мережі, протидія атакам, націленим на порушення роботи мережевих служб, додаткові функції. Політика безпеки при доступі до мережі загального користування.

Міжмережевий екран (МЕ) називають локальний або функціонально розподілений програмний (програмно—апаратний) засіб (комплекс), який реалізує контроль за інформацією, що надходить в автоматизовану систему і/або виходить з автоматизованої системи. Також зустрічаються загальноприйняті назви брандмауер і firewall (англ. вогняна стіна).

МЕ виконують такі функції:

1. фізичне відділення робочих станцій і серверів внутрішнього сегмента мережі від зовнішніх каналів зв’язку;
2. багатоетапну ідентифікацію запитів, що надходять в мережу;
3. перевірку повноважень і прав доступу користувача до внутрішніх ресурсів мережі;
4. реєстрацію всіх запитів до компонентів внутрішньої підмережі ззовні;
5. контроль цілісності програмного забезпечення і даних;
6. економію адресного простору мережі;
7. приховування IP—адреси внутрішніх серверів з метою захисту від хакерів.

Фільтрація інформаційних потоків здійснюється міжмережевими екранами на основі набору правил, що є вираженням мережевих аспектів політики безпеки організації. У цих правилах, крім Інформації, яка зберігається у фільтрованих потоках, можуть фігурувати дані, отримані з оточення, наприклад, поточний час, кількість активних з'єднань, порт, через який надійшов мережевий запит і т.д. Таким чином, у міжмережевих екранах використовується дуже потужний логічний підхід до розмежування доступу.

Існує три типи firewall: мережного рівня, прикладного рівня і рівня з'єднання. Кожен з цих трьох типів використовує свій, відмінний від інших підхід до захисту мережі.

- **Firewall мережного рівня** представлений екрануючим маршрутизатором. Він контролює лише дані мережевого і транспортного рівнів (див.Модель OSI) службової інформації пакетів. Мінусом таких маршрутизаторів є те, що ще п'ять рівнів залишаються неконтрольованими. Нарешті, адміністратори, які працюють з екрануючими маршрутизаторами, повинні пам'ятати, що у більшості приладів, що здійснюють фільтрацію пакетів, відсутні механізми аудиту та подачі сигналу

тривоги. Іншими словами, маршрутизатори можуть піддаватися атакам і відбивати велику їх кількість, а адміністратори навіть не будуть проінформовані.

- **Firewall прикладного рівня** також відомий як проксі-сервер (сервер-посередник).Фаєрволи прикладного рівня встановлюють певний фізичний поділ між локальною мережею і Internet,тому вони відповідають найвищим вимогам безпеки. Проте, оскільки програма повинна аналізувати пакети і приймати рішення щодо контролю доступу до них, фаєрволи прикладного рівня неминуче зменшують продуктивність мережі, тому в якості сервера-посередника використовуються більш швидкі комп'ютери.

- **Фаєрвол рівня з'єднання** схожий на фаєрвол прикладного рівня тим, що обидва вони являються серверами-посередниками. Відмінність полягає в тому, що firewall прикладного рівня вимагають спеціального програмного забезпечення для кожної мережевої служби на зразок FTP або HTTP. Натомість, firewall рівня з'єднання обслуговують велику кількість протоколів.

Недоліки брандмауерів

Обмеження в доступі до потрібних службам

Самим очевидним недоліком брандмауера є те, що він може блокувати ряд служб, які використовують користувачі, такі як TELNET, FTP, X Windows, NFS і ін Тим не менше, ці недоліки не властиві тільки брандмауерів; мережевий доступ також може обмежуватися при захисті на рівні хостів у відповідності з політикою безпеки.

Велика кількість залишених вразливих місць

Брандмауери не захищають від чорних входів (люків) у мережі. Наприклад, якщо можна здійснити необмежений доступ по модему в мережу, захищену брандмауером, атакуючі можуть ефективно обійти брандмауер.

Погана захист від атак своїх співробітників

Брандмауери зазвичай не забезпечують захисту від внутрішніх загроз. Хоча брандмауер може захищати від отримання сторонніми особами критичних даних, він не захищає від копіювання своїми співробітниками даних на стрічку або дискету і виносу її за межі мережі. Тому, було б помилкою думати, що наявність брандмауера захищає від атак зсередини або атак, для захисту від яких потрібен не брандмауер.