Firewall

Михаил Радев

Предназначение

- Това е система за мрежова сигурност, която контролира входящия и изходящия мрежови трафик на базата на съвкупност от правила. Установява препятствие между сигурната вътрешна мрежа и други мрежи (напр.Интернет).

Класификация

- host-based – инсталира се на клиентските машини върху ОС и защитава конкретната машина. Използва се в домашни условия или в мрежова среда като допълнително средство за безопасност.
- Network firewall – защитава цялата мрежа и обикновено е шлюз за тази мрежа. Подразделя се на:
  - ASIC-accelerated - ASIC – application-specific integrated circuit. - машини, в които функционалността на firewall-а се изпълнява на апаратно ниво. Скъпи са, използват се от ISP и големи организации
  - PC-based – на база на обикновен компютър. Това са всички не-ASIC, т.е всички останали

Видове pc-based firewall

- Делят се на 2 вида:
  - Дистрибутиви – предимства: може да разполагате с хардуер, или да купите сървър на добра цена; да се премести на нов компютър; по-малка е зависимостта от доставчика на firewall решението. И те се разделят на такива с отворен и затворен код.
  - appliances (кутии) – оптимизирани, тествани, пропуска се избора на сървърен хардуер и съвместимостта на софтуера с него

Функционалности на firewall-те

- UTM – Unified Threat Management. Това е PC-based firewall с допълнителни функционалности - IDS/IPS, VPN, load-balancing, routing, content filtering, antivirus, anti-spam… Подходящи са за малки организации с малък бюджет.
- IDS/IPS анализатор на трафика, работещ на база подписи и опитващ се да открие аномалии.
  - IDS (intrusion detection system) опитват се да открият аномалии
  - IPS (intrusion prevention system) опитват се да спрат аномалиите
- Layer 7 firewall – IDS/IPS не разбират протоколите и затова е нужен layer 7 firewall.

Разновидности

- Платен/безплатен
- Софтуерен/хардуерен
- С отворен код / затворен код

Мрежови профили/Network Profiles

- Home network (Private)
  - доверяваме се на компютрите в home network
  - позволено е Network Discovery
  - компютърът може да е член на HomeGroup
- Work Network (Private)
  - доверяваме се на компютрите в work network
  - позволено е Network Discovery
  - компютърът не може да е член на HomeGroup
- Domain Network
  - Компютърът е присъединен към Active Directory домейн
  - Компютърът не може да е член на HomeGroup
- Public Network

Мрежови профили/Network Profiles

- Мрежовите профили позволяват прецизно задаване на политики на база на типа на мрежата, към която компютърът се свързва
- Firewall може да бъде включен или изключен за конкретния вид мрежа
  - Изключен, когато компютърът е свързан към домейн и включен, когато същия се включи към public мрежа
- Различни профили могат да се активират едновременно, ако комютърът е свързан към множество мрежи

Windows Firewall – цели и възможности

- Защитава компютрите като спира/разрешава определен мрежови трафик
- Може да блокира и входящия /incoming/ и изходящия /outgoing/ трафик
- Според избрания Network profile се включват определени firewall правила /rules/

Позволяване на достъп на програми

- Когато се инсталира нова програма, тя се нуждае от достъп до мрежата
- Този достъп може да се зададе за конкретната програма или да се конфигурират мрежови портове, които тя ползва
  - Firewall exception – да позволим ICMP / Ping
    - GUI метод
    - От командния ред
      - Netsh advfirewall firewall add rule name=PING4 protocol=icmpv4:any,any dir=in action=allow
- Rules/exceptions могат да се добавят за конкретен профил

Управление на Firewall

- Конфигуриране на firewall notification settings
  - Могат да се конфигурират според мрежовия профил
- Връщане на Windows Firewall до Defaults
  - GUI
    - Restore defaults от контролния панел - Windows Firewall
  - От командния ред
    - Netsh advfirewall reset

Run as

- Позволява стартирането на програма чрез използване на различни от текущите потребителски пълномощия
- Runas /user:DOMAIN\USER “program” /параметри

- Runas /user:magna\kolev “mspaint”

- Runas /user:pc1\kolev “mspaint”

Въпроси?