Obranné valy (Firewalls)

- Provádí ochranu sítě před napadením (ochrana počítačů nestačí)
- Odděluje uživatele (prvek nespolehlivosti) od prvků ochrany

Vlastnosti

- Filtrování paketů a vlastnost odstínění
- Různé úrovně ověřování
- Přihlašování (registrace) a účtování
- Transparentnost a přizpůsobení uživatelům
- Ovladatelnost (management)
- Rozlišení požadavků dle klientů nebo sítí

Realizace obranných valů

- Komerční produkty
- Vlastní realizace

Nechráněná síť

- Jednotlivé hostitelské systémy mohou být dosažitelné z libovolných systémů Internetu
    - Je třeba chránit interní hostitelské systémy
    - Tato situace je nezvládnutelná prostředky operačního systému a není bezpečná

Chráněná síť

- Spojení mezi vnitřními a vnějšími hostitelskými systémy je filtrováno a chráněno odděleným systémem – obranným valem.
    - Jeden silný bod ochrany
    - Daleko ovladatelnější a bezpečnější

Základní typy obranných valů

- Kombinace technických a programových prostředků
    - Technické prostředky – směrovač a/nebo počítač (UNIX)
    - Programové prostředky – přístupový seznam ve směrovači, specializovaný oddělovací program

Základní rozdělení podle úrovně filtrování

- Filtrování na síťové úrovni (IP filtrování)
- Filtrování na transportní úrovni (úroveň spojení)
- Filtrování na aplikační úrovni (aplikační filtry)

V praxi kombinace výše uvedených

- Založeno na podpoře klientů v hostitelských počítačích
- Založeno na službách podporovaných obranným valem pro „své“ klienty

- Založeno na podmínkách závislých na bezpečnosti, pružnosti a transparentnosti

Principy filtrování na IP úrovni

- Jednotlivé pakety jsou analyzovány a filtrovány (blokovány nebo propouštěny)
- Filtrovací kritéria
    - IP adresa (zdrojová, cílová, obě)
    - Port (zdrojový, cílový, oba)
    - Typ paketu (IP, jiný)
- Nejsou filtrována žádná aplikační data
- Obecně bezestavové filtrování
    - Nejsou k dispozici žádné znalosti o spojení klient/server
    - Nezávisle filtruje přicházející a odcházející pakety

- Výhody
    - Transparentní vzhledem k účastníkům, jednoduše přizpůsobitelné
        - Podporuje libovolný protokol klient/server
        - Není třeba modifikovat ani server, ani klienta
    - Jednoduché levné odstínění (směrovač)
    - Vysoká propustnost
- Nevýhody
    - Méně bezpečné
        - Bezestavový charakter
        - Založeno na omezeném filtrování
        - Využívá implicitní předpoklady
        - Slabé ověřování (IP adresa)
        - Nebrání „prosakování“ IP paketů
    - Není filtrován vlastní protokol server/klient
    - Neumožňuje (nebo jen omezeně) logování a účtování
    - Pravidla filtrování mohou být složitá a náchylná k chybám
    - Může se stát ne-managementovatelný
- Závěr
    - Jednoduché a laciné filtrování na IP úrovni je bezpečné pouze pro
        - Blokování všech paketů (deny)
        - Propouštění všech paketů (allow)

Typy filtrů

- Filtry pro konkrétní služby
- Filtry nezávislé na službách

Filtry pro služby

- Specifikace pro konkrétní port
- Filtrování standardních služeb (Telnet, SMTP, FTP, http, Gopher, DNS)
- Filtrování podle směru navazovaného spojení

Filtry nezávislé na službách

- Poskytují ochranu proti útokům založeným na vlastnostech TCP

    - Source IP spoofing attack
    - Pakety s IP volitelnými parametry (source routing …)
    - Tunelování IP over IP
    - Pokusy o degradaci služeb pomocí ICMP zpráv

Další komplikace filtrování na IP úrovni

- Interní adresy jsou viditelné na Internetu
- Interní klienti jsou schopni předávat externí resoluce jméno/adresa (DNS běžící na interní síti může kooperovat s vnějším DNS.

Principy filtrování na aplikační úrovni

- Hlavní princip – vnitřní pakety nesmí přecházet přímo do vnější sítě a naopak
- Klient se spojuje s obranným valem, ne přímo se serverem
- Na obranném valu je umístěn proxy (zástupce), který přijímá pakety, kontroluje je a rozhoduje o tom, má-li být paket propuštěn nebo zachycen
- Lze provádět ověřování klienta v širokém rozsahu
    - Od IP zdrojové adresy
    - K přísným ověřovacím technikám typu výzva/odpověď
- Může být filtrován i protokol server/klient

Výhody:

- Zvýšená bezpečnost
    - Předcházení problémům s bezpečností na IP úrovni
    - Má informaci o stavu spojení (filtrování na aplikační úrovni může být stavové)
    - Použití ověřovacích technik
    - Filtrace protokolu server/klient
- Umožňuje rozšířené logování a účtování
- V zásadě méně složitá pravidla filtrování, méně náchylná k chybám, jednodušší ovládání
- Interní DNS nemusí spolupracovat s externím DNS
- Je možné rozšířit proxy o cache – zachycování často požadovaných dat

Nevýhody:

- Méně transparentní a přizpůsobivé
    - Klient si může proxy uvědomit
    - Podpora jednoduchých klientů nebo proxy klientů
    - Omezený počet proxy, pro každý protokol musí existovat proxy
    - Vyžaduje vyhrazený počítač

Principy filtrování na úrovni spojení

- V zásadě vypadá jako filtrování na aplikační úrovni
    - Generické proxy na úrovni spojení pracuje na obranném valu
    - Klienti se spojují s proxy na úrovni spojových služeb (TCP)
    - Proxy ověřuje klienty na úrovni tohoto spojení

    - Spojení mezi proxy a serverem je pak transparentní
- Od filtrování na aplikační úrovni se liší
    - Slabším ověřováním
    - Nezajišťuje filtrování protokolu na úrovni aplikace klient/server
- Realizace
    - Realizace vyžaduje zásah do programového vybavení klienta
    - Systémové volání na nižší úrovni v klientu nahrazeno spojkami (connect)
    - Spojka spojuje klienta a spojované proxy
    - S použitím speciálního protokolu posílá adresu a port cílového počítače.

Vlastnosti

- Bezpečnost mezi IP úrovní a aplikační úrovní
- Transparentnost mezi IP úrovní a aplikační úrovní
- Zahrnuje logování a účtování
- Programové vybavení klienta musí být přizpůsobeno

Výhody

- Doplnění programu o spojku je jednodušší než zavedení proxy
- Je však nutné mít zdrojový kód, knihovny, …

Socks

- Představuje programové vybavení spojky pro realizaci proxy na úrovni spojení
- Navrženo pro aplikace typu klient/server
- Klient naváže spojení se socks, přenese adresu cíle, port cíle, typ spojení a identitu uživatele
- Socks vytvoří vlastní komunikační kanál, kterým posílá data klienta do serveru
- Během vytváření spojení lze provádět doplňkové funkce (ověřování, vyjednávání o bezpečnosti, …)

Model socks

- Zahrnuje 3 základní operace
    - Požadavek na spojení
    - Nastavení proxy spojení
    - Přepínání aplikačních dat
    - Ověřování

Typy obranných valů

Filtrující směrovač (Screening Router)

- Provádí filtraci paketů podle směru přenosu, IP adresy a čísla portu

Opevněný počítač (Bastion Host)

- Používá se při realizaci důležitých serverů, které mají být navíc velmi bezpečné. Např. SMTP, FTP, DNS, HTTP, atd.

Brána se dvěma vstupy (Dual Homed Gateway)

- Úplně odděluje vnitřní a vnější síť. Služby musí být umístěny na této bráně a jsou přístupné jak z vnitřní sítě, tak i z vnější sítě.

Screened Host Gateway

- Vnitřní síť je chráněna filtrujícím směrovačem, který propouští pouze pakety určené pro vybraný počítač (Bastion Host). Pakty mohou být filtrovány nejen podle IP adresy, ale i podle portu (přístup k určitým službám).

Screened Subnet

- Pomocí dvou filtrujících směrovačů se vytvoří oblast mezi vnitřní a vnější sítí, nazývaná demilitarizovaná zóna. Do této subsítě se připojí Bastion Hosts, nesoucí služby, které mají být přístupné jak z vnější, tak i z vnitřní sítě. Filtrujícími směrovači lze dosáhnout toho, že pakety s vnějšími adresami nejsou přenášeny do vnitřní sítě a naopak pakety s adresami vnitřní sítě nejsou přenášeny do sítě vnější.

Brána aplikační úrovně

- Pomocí filtrujícího směrovače jsou propouštěny pouze pakety určené aplikační bráně. Zde jsou instalovány aplikační proxy, které umožní komunikaci a klienty ve vnitřní síti.