Firewall - Principy fungování, typy firewallů (stateful, stateless, aplikační), konfigurace pravidel, NAT, DMZ, VPN

Firewall

Firewall je predstavuje bezpecnosti system, ktery kontroluje sitovy provoz a chrani pocitace pred nezadoucim pristupem. Vpodstate funguje jako bezpecnosti brana v privatni siti pred vnejdim internetem - hackeri a dalsi nejakej malicious kod.

Hlavni funkci je filtrovani provozu podle predem definovanych pravidel. Tato pravidla urcuji, ktery provoz je povoleny a bezpecny a ktery je potencialne nebezpecny a nepovolony

Firewall funguje na ruznych vrstvach OSI modelu. Na OSI 3 sitove vrstve kontroluje ip adresy, na OSI 4 transportni vrstve kontroluje porty a protokoly a na OSI 5-7 aplikacni vrstve kontroluje obsah datovych paketu.

Typy firewallu

Stateless firewall

Zakladni typ, ktery pracuje na principu paketove filtrace. Kazdy prochazejici paket hodnoti samostatne, bez ohledu na to, jestli byl nekdy nekdy posilan. Kontroluje hlavne IP adresy, porty a protokoly, tato filtrace je zalozena na statickych pravidlech. Nema zadnou cache pamet na predchozi komunikaci. Je jednoduchy a rychly, ale je mene bezpecny a nemuze detekovat komplexnejsi utoky

Stateful firewall

Nastupce Stateless, pokrocilejsi typ, ktery si udrzuje informace o stavu spojeni. Dokaze rozeznat, zda paket patri existujicimu spojeni - udrzuje stavovou tabulku. Sleduje tak TCP handshaky jeste. Bezpecnejsi, ale slozitejsi na konfiguraci

Application firewall

Znamy jako WAF (Web Application Firewall) je nejpokrocilejsi typ. Pracuje na aplikacni vrstve a dokaze analyzovat obsah packetu. Nejvyssi uroven ochrany, detekce slozitejsich utoku. Pomerne slozity na konfiguraci

Konfigurace

Zdroj - odkud pochazi (IP)
Cil - kam smeruje
Port - jakou sluzbu vyuziva

Akce - co s provozem delat (povolit, zakazat, logovat)
Smer - prichozi nebo odchozi

Bezpecnost
Dva zakladni pristupy ke bezpecnosti:

1. Implicitni zakaz
    - veskery provoz implicitne zakazan, povoluje pouze specifiky, pouzivan v podnikovem prostredi
2. Implicitini povoleni
    - veskery provoz implicitne povolen, zakazuje pouze podzrely nebo skodlivy provoz, mene bezpecnejsi, uzivatelsky privetivejsi

NAT
Technolgoie, ktera umoznuje preklad mezi ruznymi adresnimi prostory. Nejcasteji se pouziva k tomu, aby vice zarizeni v lokalni siti mohlo sdilet jednu verejnou IP adresu.

Zarizeni v lokalni siti odesila paket na externi server mimo lokalni sit. Router s NATEM nahradi privatni zdrojovou IP adresu a nahradi ji svoji verejnou IP adresou. Tuto zmenu si ulozezi do NAT tabulky. Kdyz prijde odpoved router podle tabulky zjisti, kterem zarizeni v lokalni siti ma paket dorucit.

Typy NAT
Static

- pevne mapovani mezi privatni a verejnou IP adresou
- kazda interni adresa ma vyhrazenou verejnou adresu
- servery, ktere musi byt dostupne z internetu

Dynamic

- skupina internich adres je mapovana na skupinu verejnych ip
- preklad je tvoren dynamicky, kdyz zarizeni chce komunikovat
- pouziva se kdyz mame k dispozici vice verejnych IP, ale mene nez internetich

PAT

- nekolik internich IP je mapovano na jednu verejnou IP s ruznymi porty
- pouziva se v domacnostech

DMZ - demilitarizovana zona
Specialni sitovy segment umisteny mezi interni siti a internetem. Umoznuje externim uzivatelum pristup k urcitym sluzbam, anyz by ohrozila bezpecnost interni site. Vetsinou se napojuje na firewall nebo mezi dva firewally.

Konkrétní příklad provozu přes DMZ

Když někdo navštíví tvůj firemní web, dějí se tyto kroky:

1. **Požadavek přichází z internetu** - někdo zadá www.tvafirma.cz do prohlížeče
2. **Požadavek prochází přes vnější firewall do DMZ** - firewall zkontroluje, že jde o běžný webový požadavek, a pustí ho dál
3. **Webový server v DMZ zpracuje požadavek** - server načte webovou stránku
4. **Pokud server potřebuje data z interní sítě** - pošle požadavek přes vnitřní firewall do interní sítě
5. **Databázový server v interní síti pošle potřebná data** - např. produkty, ceny
6. **Webový server v DMZ sestaví kompletní stránku** a pošle ji zpět přes vnější firewall uživateli

VPN

Technolgoie, ktera vytvari zabezpecene, sifrovani pres internet. Hlavnim ucelem je zajsitit bezpecnou komunikaci mezi vzdalenymi sitemi nebo uzivateli a chranit prenasena data pred odposlouchavanim a manipulaci.

Funguje na OSI 2 a OSI 3 vrstvach.

Zakladni princip spociva v zapouzdreni a sifrovani puvodnich datovych packetu. Pri vyziti VPN se vytvari tunel (logicke spojeni mezi body), kterym proudi sifrovana data. tato data jsou pred odeslanim zasifrovana a na druhe strane desifrovana, coz umoznuje bezpecny prenos.

Typy VPN

1. Remot-Access VPN
- jednotlivym uzivatelum umoznuje pripojeni ke vzdalene privatni siti, typicky k firemni infrastrukture
2. Site-to-Site VPN

- propujuje cele site, nikoliv jednotlive uzivatele
- vytvari most mezi geograficky oddelenymi lokalitami

VPN protokoly

1. IPsec
    - zajišťuje šifrování a autentizaci dat přímo na síťové vrstvě IP protokolu
    - site-to-site VPN
2. SSL/TLS
    - vytváří zabezpečené spojení pomocí stejných protokolů, které zajišťují bezpečnost webových stránek
    - vzdaleny pristup zamestancu k firemnim aplikacim pres webovy prohlizec
3. Open VPN
    - open-source řešení vytvářející šifrované tunely pomocí knihovny OpenSSL a vlastního protokolu
4. WireGuard
    - moderní, minimalistický VPN protokol zaměřený na rychlost a jednoduchost implementace
    - mobilni zarizeni