Síťové prvky, přiřazení k vrstvám OSI/ISO

Joseph Soukup – P4

Firewall

- Firewall – aby se v hořícím domě oheň dál nešířil
- Síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
- Zjednodušeně se dá říct, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje
- Pravidla vždy zahrnovala
    - identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu)
    - zdrojový a cílový port
- => poměrně nedostatečné
- Modernější firewally se opírají přinejmenším o:
    - Informace o stavu spojení
    - Znalost kontrolovaných protokolů
    - Případné prvky IDS (Intrusion Detection System) - systém pro odhalení průniků (odhalení podezřelých aktivit)
- Podle umístění lze firewally dělit na:
    - Síťové:
        - Samostatné hardwarové řešení pro ochranu sítě
    - Personální:
        - Realizován na koncových stanicích (PC)

Paketové filtry

- Pravidla uvádějí, z jaké adresy a jakého portu na jakou adresu a port může být doručen procházející paket
- Kontrola se provádí na 3 (Síťová) a 4 (transportní) vrstvě síťové komunikace OSI

Aplikační filtry (Proxy Firewally)

- Na rozdíl od paketových filtrů zcela oddělily sítě, mezi které byly postaveny
- Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení:
    - Klient (iniciátor spojení) se připojí na aplikační bránu (proxy)
    - Proxy příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru
    - Tam je klientem aplikační brána

Stavové paketové filtry

- Provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních, které pak mohou využít při rozhodování, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem

Stavové paketové filtry s kontrolou známých protokolů (popř. kombinované s IDS)

- Deep Inspection a Application Intelligence
- => Firewally jsou schopny kontrolovat procházející spojení až na úroveň korektnosti procházejících dat známých protokolů i aplikací

- Mohou tak například zakázat průchod http spojení, v němž objeív indikátory, že se nejedná o požadavek na WWW server, ale tunelování jiného protokolu

Router (Síťová vrstva)

- Aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli
- Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI
- Je v každé síti to podstatné zařízení, které ji řídí
    - Umí směrovat provoz, tedy rozdělovat provoz na síti mezi více připojených zařízení
    - jednotlivým zařízením přiděluje jejich IP adresy
    - Řeší spravedlivé rozdělení celého pásma v síti tak, aby se provoz neucpal (kdyby někdo stahoval velký soubor, tak aby ostatní mohli dále pracovat) - QoS
- V domácí síti například router zprostředkovává připojení na internet a řídí domácí síť
    - Většina domácností používá WiFi router, který vše umí i bezdrátově
- Ve firemní síti se používá router buď stejně jako v domácnosti nebo pro propojení dvou stejných počítačových sítí, tedy dvou částí firemní sítě
- Routery jsou jedním z klíčových prvků celosvětové sítě internet, která je vlastně tvořena jednotlivými sítěmi, které jsou spojeny routery
- Základní funkce routerů:
    - Brána mezi lokální síti a internetem
    - DHCP server
    - NATоovaní
    - Firewall

Switch (Linková vrstva)

- Aktivní prvek v počítačové síti
- Propojuje jednotlivé prvky do hvězdicové topologie
- Obsahuje větší, či menší množství portů, na, než se připojují síťová zařízení nebo části sítě
- Switch přeposílá síťový provoz jenom do těch směrů, do kterých je to potřeba, čímž se odlišuje od jednoduššího hubu

Způsoby přeposílání rámců

Store and forward

- Rámce z jednoho rozhraní přijmou, uloží si ho do vyrovnávací paměti, prozkoumá jeho hlavičky a následně odvysílají do příslušného rozhraní

Cut-through switching

- Optimalizovaný proces
- K analýze hlaviček dochází, jakmile dorazí začátek rámce
- Ani s vysíláním do cílového rozhraní se nečeká až dorazí celý rámec, ale zahajuje se co nejrychleji, aby zpoždění rámce bylo minimální

Fragment free

- Switch začne přeposílat rámec až po přijetí 64 bitů, kdy je jisté, že na daném segmentu nevznikne kolize – v případě že je do přepínače připojen hub

Adaptive switching

- Automatické přepínání mezi metodami cut-through switching a store and forward

LAN switching

- Klasický switch (linková vrstva)
- Pokročilejší, které rozhodují o cíli přijatého rámce na základě informací z vyšších síťových vrstev a složitějších pravidel
- Pokud je rozhodnutí založena na IP adrese, označují se takové switche jako layer3 switch (síťová vrstva)
- Jeli rozhodnutí prováděno nejen podle IP adresy ale i podle čísla síťového portu, označují se jako layer4 switch (transportní vrstva)

Bridge (Linková vrstva)

- Spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI
- Je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě

Princip činnosti

- Odděluje provoz dvou segmentů sítě tak, že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí
- Leží-li příjemce ve stejném segmentu jako odesílatel, bridge rámce do jiných částí sítě neodešle
- V opačném případě je odešle do příslušného segmentu v nezměněném stavu

Transparent bridging

- Neviditelné pro koncové stanice – propojené sítě se jeví jako jedna síť
- Na začátku vůbec neví, jak jsou stanice v síti rozloženy, a musí paket přijatý na jedné síti poslat do všech ostatních připojených sítí, protože ještě neví, kde se cílová stanice nachází

Source route bridging

- V token-ring sítích
- Zde je cílem, aby bridge byla co nejjednodušší
- Každý paket musí kromě adresy odesílatele a příjemce obsahovat také posloupnost adres všech bridgů, kterými musí paket projít
- Vysílací stanice tedy, dříve než pošle první paket, musí zjistit celou cestu k cílové stanici

Bridging vs Routing

- Podobné řízení toku dat, ale pracují pomocí různých metod
- Bridging = linková vrstva
- Routing = síťová vrstva
- Most směruje rámce na základě MAC adresy (není schopen díky tomu rozlišovat sítě)
- Router rozhoduje podle IP adresy uvnitř přenášeného datagramu

Access Point (Linková vrstva)

- Přístupový bod k bezdrátové Wi-Fi síti je zařízení, ke kterému se klienti připojují.
- Klienti spolu nekomunikují přímo, ale prostřednictvím přístupového bodu, takže mohou být jednodušší a nemusejí být ve vzájemném radiovém spojení
- Centralizovaný způsob komunikace též umožňuje použití směrových antén, který zvyšují dosah radiového signálu
- Tento typ uspořádání nazýváme infrastrukturní síť
- Opakem jsou Ad-hoc sítě, kde jsou dva nebo více klienti ve vzájemném přímém rádiovém spojení (bez existence prostředníka)
- Je obvykle realizován malým jednoúčelovým zařízením, ale s potřebnou softwarovou výbavou se jim může stát i jakýkoliv počítač s bezdrátovým Wi-Fi zařízením
- Některá z těchto jednoúčelových zařízení využívají jako základ operační systém Linux

Role přístupových bodů:

- Mají několik rolí, které jsou dány nejen požadavky struktury sítě, ale i schopnostmi zařízení
    - Bridge:
        - Bezdrátová síť je součástí sítě LAN
        - Bridge odděluje síťový provoz, ale propouští lokální broadcasty
        - Není nutné konfigurovat
    - Router
        - Bezdrátová síť je samostatnou podsítí
        - Router odděluje síťový provoz a nepropouští lokální broadcasty
        - Vyžaduje konfiguraci IP adres zařízení a nastavení směrování
- Pokud je v bezdrátovém zařízení (AP) zabudována bezdrátová část dvakrát, označuje se jako **point-to-multipoint,** protože dokáže např. bezdrátový signál dálkově přijímat a zároveň ho distribuovat dalším bezdrátovým klientům v blízkém okolí.
- Takto jsou konstruovány bezdrátové přípojné body poskytovatelům internetového připojení (providerů), kteří však někdy kvůli ceně používají dvě samostatná bezdrátová zařízení
- Specifickým typem jsou **WDS** sítě (Wireless Distribution System), kdy všechny přístupové body vysílají na stejném kanálu, navzájem spolu komunikují a jeví se tak klientům jako jedna síť

Připojení k přístupovému bodu:

- Klienti se připojují, přičemž mohou být vůči nim uplatněna omezení a přístup odepřen
- Komunikace mezi klienty probíhá prostřednictvím přístupového bodu, tj. minimálně dva skoky (nejprve na přístupový bod a z něj pak na příslušnou proti stanici)
- Klient tak udržuje spojení jen s přístupovým bodem a nemusí mít cílovou stanici ani v přímém rádiovém dosah

Hub (Fyzická)

- Aktivní prvek počítačové sítě, který umožňuje její větvení a je základem sítí s hvězdicovou topologií

- Veškerá data, co přijdou na jeden z portů, zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu data náleží
- => všechny počítače v síti vidí všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým ve skutečnosti data nejsou určena
- Hub pracuje na fyzické vrstvě modelu OSI

Technické informace

- Signál, který do něj vstoupí, je obnoven a vyslán všemi ostatními porty
- => zpoždění je proto pouze 1 bit => nižší latence než switch

Použití

- Nahrazovány switchy, ale přesto mohou být užitečný:
    - Některé počítačové clustery (seskupení volně vázaných počítačů) vyžadují, aby všechny počítače v clusteru obdržely stejné packety
    - Pokud je přepínač přístupný nezkušeným nebo nedbalým uživatelům, např. konferenční místnosti, můžou ochromit celou síť tím, že propojí dva porty, čímž vytvoří smyčky

Repeater (Fyzická)

- Elektronický aktivní síťový prvek, který přijímá zkreslený, zašuměný nebo jinak poškozený signál a opravený, zesílený a správně časovaný ho vysílá dále
- => Zvýšení dosahu média bez ztráty kvality a obsahu signálu
- Opakovače patří do první (fyzické) vrstvy referenčního modelu OSI, protože pracují přímo s elektrickým signálem

Bezdrátové komunikace

- Skládá se z přijímače, zesilovačem vysílače, izolátoru a dvou antén
- Vysílač generuje signál na odlišné frekvenci od signálu na vstupu, což je nezbytné k ochraně vstupu před narušením od zesíleného signálu na výstupu

Satelitní komunikace

- Transponder přijímá signál a přeposílá jej, často na odlišných frekvencích do cílové lokace

Mobilní komunikace

- Zařízení pro posílení GSM signálu v místech, kde není dostatečně silný (sklepy, garáže, …)

Optická vlákna

- Repeater je složen z fotobuňky (přijímače), zesilovače a světlo emitující (LED) nebo infra-diody (IRED)
- Optický signál nejprve převede na elektronický a po z restaurování opět na optický, který je vysílán dále do optického vlákna

Radiotechnika

- Opakovače jsou využívány i komerčními radio stanicemi, radioamatéry k oddělení signálu v jejich frekvenčním rozsahu od jednoho přijímače k druhému