10 – Virtuální sítě

Virtuální privátní sítě (VPN)

Co to je?

- Bezpečné (autentizované a šifrované) a přitom pro uživatele zcela transparentní spojení mezi dvěma či více sítěmi.
- Pro spojení mezi uživatelem a požadovanou destinací použita veřejná síť - nejčastěji internet

Možnosti spojení

- *LAN – LAN spojení*
  - Vztah brána - brána
    - § Vyžadováno šifrování přenosu a ověření autenticity obou stran
    - § Obě brány tak mezi sebou na IP adresách třetí tranzitní sítě navážou spojení (tunel)

- *Uživatel – LAN*
  - Vztah klient - klient
    - § Každá stanice má přidělenou vlastní IP adresu
    - § Požadováno šifrování přenosu a případné ověření autentičnosti obou stran

  - Vztah klient - brána
    - § Klient = mobilní účastník ("road warrior") s dynamicky přidělenou IP adresou
    - § Vhodné mít přidělenou IP adresu dle číslovacího plánu
    - § Brána - Statická IP adresa
    - § Mobilní účastník tak obdrží veřejnou IP adresu, ale zároveň pro připojení do sítě používá svojí vnitřní IP adresu ze sítě, do které se připojuje
    - § Jeho IP adresa a veřejná IP adresa protistrany je tak využita pouze pro navázání spojení

Požadavky kladené na VPN

a) **Zajištění integrity dat**

- Pomocí jednosměrné hashovací funkce
  - Funkce generuje přesně danou velikost souboru založenou na jeho skutečné velikosti
  - Ověření je provedeno výpočtem na straně příjemce, kde dojde k výpočtu hodnoty a jejímu porovnávání s poslanou hodnotou
  - Příklady hashovacích algoritmů MD5, SHA-1 and RIPE-MD-160
- Pomocí MACs (Message-authentication codes)
  - Přiřadí klíč k hashovacím funkcím
  - Odesílatel vytvoří soubor, kde je vypočítaná MAC na základě klíče sdíleného s příjemcem a následně je tento soubor přepojen k posílanému souboru
  - Příjemce pak na základě klíče opět spočte MAC a porovná se souborem, který je přiložen
- Pomocí Digitálního podpisu
  - Odesílatel podepíše dokument s jeho privátním klíčem a příjemce ověří poté tento soubor pomocí odesílatelova veřejného klíče

b) **Autentifikace**

- Pomocí digitálního podpisu
  - (založen na standardu X.509)
  - Vydáván certifikační autoritou
  - Identita svázána s veřejným klíčem
    - Obsahuje inforamce o uživateli jako např. jméno, společnost, apod.
    - Inforamce specifické vydavateli
    - Dobu platnosti
    - a další
  - Tyto informace budou použity k vytvoření přehledu, který je pak zakódován pomocí privátního klíče Certifikační Autoritou k podepsání certifikátu

Výhody použití

- Rozšíření hranic působnosti bez nutnosti budovat další síťovou infrastrukturu
- Značné úspory proti budování vlastních WAN sítí

- Dle zvoleného řešení zaručena bezpečnost
- Možnost být stále v kontaktu s daty v lokální síti
- Škálovatelnost (rozšiřitelnost) - možnost růstu úměrně potřebám

Virtuální lokální sítě (VLAN)

Co to je?

- Slouží k logickému rozdělení sítě nezávisle na fyzickém uspořádání. Můžeme tedy naši síť segmentovat na menší sítě uvnitř fyzické struktury původní sítě. Druhým důležitým pojmem, který bude více vysvětlen později, je trunk. Jako trunk označujeme port, který je zařazen do více VLAN.
- Jednoduše řečeno pomocí VLAN můžeme dosáhnout stejného efektu, jako když máme skupinu zařízení připojených do jednoho (několika propojených) switche a druhou skupinu do jiného (jiných) switche. Jsou to dvě nezávislé sítě, které spolu nemohou komunikovat (jsou fyzicky odděleny). Pomocí VLAN můžeme takovéto dvě sítě vytvořit na jednom (nebo několika propojených) switchi.

Počítačová síť - WAN, LAN

Počítačová síť vznikne ve chvíli, kdy dva (někdy se říká minimálně tři) nebo více počítačů propojíme dohromady pomocí telekomunikačního systému za účelem sdílení zdrojů. Sítě se dále dělí podle řady parametrů na LAN, WAN, WLAN, MAN apod. V tuto chvíli nás zajímá lokální počítačová síť - LAN (Local Area Network), která se vyznačuje tím, že počítače jsou propojeny na menším geografickém území (tedy v rámci firmy, budovy, místnosti, atp.). Pro LAN se nejčastěji používá technologie Ethernet s protokolem TCP/IP a pro WAN (Wide Area Network - propojení jednotlivých LAN) technologie Frame Relay.

Podsíť - subnet

CP/IP protokol používá pro adresování zařízení IP adresy. Těchto adres je určitý rozsah, který se pro praktické použití (směrování, přidělování adres organizacím, broadcasty) dělí na menší hierarchické části, kterým se říká subnety (podsítě).

Zařízení mohou přímo komunikovat pouze s dalšími zařízeními, která jsou ve stejném subnetu. Se zařízeními z jiných subnetů komunikují typicky přes jednu adresu - gateway (bránu), která provádí routování.

Oddělení sítí

Jak jsem uvedl výše, pokud použijeme různé subnety, tak spolu zařízení nemohou komunikovat. Není to však úplně pravda, rozhodně nedojde k oddělení těchto zařízení. Pokud jsou totiž připojena na stejné médium, propojena do stejného hubu (pracuje na 1. vrstvě OSI) nebo switche (pracuje na 2. vrstvě OSI). Tak komunikace dorazí z jednoho zařízení na druhé, i když jsou v jiném subnetu. Zařízení však bude tuto komunikaci ignorovat. Je to proto, že hub (posílá všude) ani switch (používá MAC adresy) se nedívá na IP adresy procházející

komunikace. Proto se dá tato komunikace zachytávat a odposlouchávat. Pokud tedy chceme mít oddělené sítě, tak musíme použít oddělené switche.

Kdežto použitím VLAN dojde k tomu, že komunikace se posílá pouze na porty, které jsou zařazeny do stejné VLANy. Záleží tedy sice na softwaru switche, ale dá se říct, že se jedná o fyzické oddělení. Existují nějaké metody útoky na VLAN (proniknutí do jiné VLAN), ale při dobře nastavené síti by mělo být vše bezpečné.

Subnety a VLANy

Z výše uvedeného také plyne to, že pro různé VLANy bychom měli používat různé subnety. Pokud chceme mezi těmito VLANami routovat, tak je to nutné, stejně jako v případě, kdy chceme využít některé speciální funkce na switchi.

Praktické výhody VLAN

- **snížení broadcastů** - hlavní výhodou VLAN je vytvoření více, ale menších, broadcastových domén. Tedy zlepšení výkonu sítě snížením provozu (traffic).
- **zjednodušená správa** - k přesunu zařízení do jiné sítě stačí překonfigurovat zařazení do VLANy, tedy správce konfiguruje SW (zařazení do VLAN) a ne HW (fyzické přepojení)
- **zvýšení zabezpečení** - oddělení komunikace do speciální VLANy, kam není jiný přístup. Toho se dá samozřejmě dosáhnout použitím samostatných switchů, ale často se toto uvádí jako bonus VLAN.
- **oddělení speciálního provozu** - dnes se používá řada provozu, který nemusí být propojen do celé sítě, ale přesto jej potřebujeme dostat na různá místa, navíc nechceme, aby nám ovlivňoval běžný provoz. Příkladem je například IP telefonie, komunikace mezi AP v centrálně řízeném prostředí, management (zabezpečení správcovského přístupu k zařízením). Například pro IP telefonii, kde je použití VLAN naprosto běžné, nám stačí jediná zásuvka, kam přivedeme VLAN pro telefonii i VLAN s přístupem do sítě a v telefonu se komunikace rozdělí. Navíc VLANy můžeme použít spolu s QoSem pro zaručení kvality komunikace (obsazení pásma).
- **snížení HW** - samozřejmě se nám nesnižuje potřebný počet portů (až na speciální případy jako IP telefonie), ale tím, že mohou být různé podsítě na stejném switchi, jej můžeme lépe využít (například pro propojení tří zařízení nepotřebujeme speciální switch, který má minimálně 8 portů).

Zdroje: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

Zdroje: http://home.zcu.cz/~ondrous/index.php?menu=0