VXLAN (Virtual Extensible LAN)

VXLAN je technologie síťové virtualizace, která řeší problémy se škálovatelností ve velkých cloudových prostředích a datových centrech. Umožňuje vytvářet logické sítě na 2. vrstvě (L2 Ethernet) přes stávající sítě na 3. vrstvě (L3 IP).

V podstatě jde o tunelovací protokol, který „zabalí“ (enkapsuluje) klasický Ethernet rámec do UDP paketu.

Proč používáme VXLAN?

Tradiční standardy pro segmentaci sítě, jako jsou VLAN, již v moderní infrastruktuře narážejí na své limity:

- **Kapacita ID:** Klasická VLAN umožňuje pouze 4 096 unikátních sítí. **VXLAN** rozšiřuje tento prostor na více než **16 milionů** (pomocí 24bitového VNI - VXLAN Network Identifier).
- **Flexibilita:** VXLAN umožňuje, aby se virtuální servery (VM) nacházely v jedné logické síti, i když jsou fyzicky umístěny v jiných částech datového centra nebo v různých budovách propojených přes **WAN**.
- **Efektivita cesty:** Na rozdíl od VLAN se VXLAN nespoléhá na limitující protokol Spanning Tree (STP), ale využívá moderní směrovací protokoly pro využití všech dostupných cest v síti.

Klíčové komponenty

* **VTEP (VXLAN Tunnel End Point):** Zařízení (fyzický switch nebo softwarový modul v serveru), které provádí balení a rozbalování VXLAN paketů. * **VNI (VXLAN Network Identifier):** Unikátní číslo, které identifikuje konkrétní virtuální síť (obdoba VLAN ID). * **Underlay Network:** Fyzická síť (IP), po které se pakety pohybují. * **Overlay Network:** Virtuální síť, kterou vidí koncová zařízení a aplikace.

Využití v rámci IT infrastruktury

V naší společnosti nasazujeme VXLAN především v těchto oblastech:

```
1. **Multitenance:** Oddělení provozu různých oddělení (např.
**[[Marketingové oddělení|Marketing]]** vs. **[[Vývojový tým|Vývoj]]**) v
rámci sdíleného serverového clusteru.
2. **Mobilita virtuálních strojů:** Možnost přesunout běžící server z jedné
pobočky na druhou bez nutnosti měnit jeho IP adresu.
3. **Bezpečnostní segmentace:** Ve spolupráci s **[[WAF]]** a firewally
umožňuje VXLAN vytvářet mikro-segmenty pro kritické aplikace.
```

Vztah k bezpečnosti

Protože VXLAN běží nad standardním IP protokolem, v rámci naší **kybernetické bezpečnosti** dbáme na:

- **Autentizaci VTEP bodů:** Aby se do naší virtuální sítě nemohl připojit neautorizovaný switch.
- **Šifrování:** Pokud VXLAN tunely procházejí přes veřejnou **WAN**, jsou povinně zapouzdřeny do IPsec tunelu.
- **Monitoring:** Sledujeme integritu VXLAN hlaviček, abychom zabránili útokům typu spoofing.

> **Technická poznámka:** VXLAN mírně zvyšuje velikost paketu (režie o 50 bajtů). Proto je v naší síti nutné mít nastavené **Jumbo Frames** (MTU minimálně 1600 bajtů), aby nedocházelo k fragmentaci dat.

— **Související stránky:** ZIF, WAN, WLAN, Kybernetická bezpečnost, IT Podpora, Vývojový tým