Současné využívání několika internetových konektivit s ohledem na dynamické upřednostňování konkrétní linky (linek) dle aktuálního stavu

Jan Václavík, Systems Engineer CEE, Fortinet
jvaclavik@fortinet.com

Anotace

Během prezentace blíže představíme často skloňovanou problematiku poslední doby - současné využívání několika internetových konektivit s ohledem na dynamické upřednostňování konkrétní linky (linek) dle aktuálního stavu, detekované aplikace (pomocí L7 footprint) a dalších rozhodovacích parametrů. Neopomeneme zmínit také důležitost zabezpečení a inspekce provozu i s ohledem na stále narůstající množství SSL šifrované komunikace.

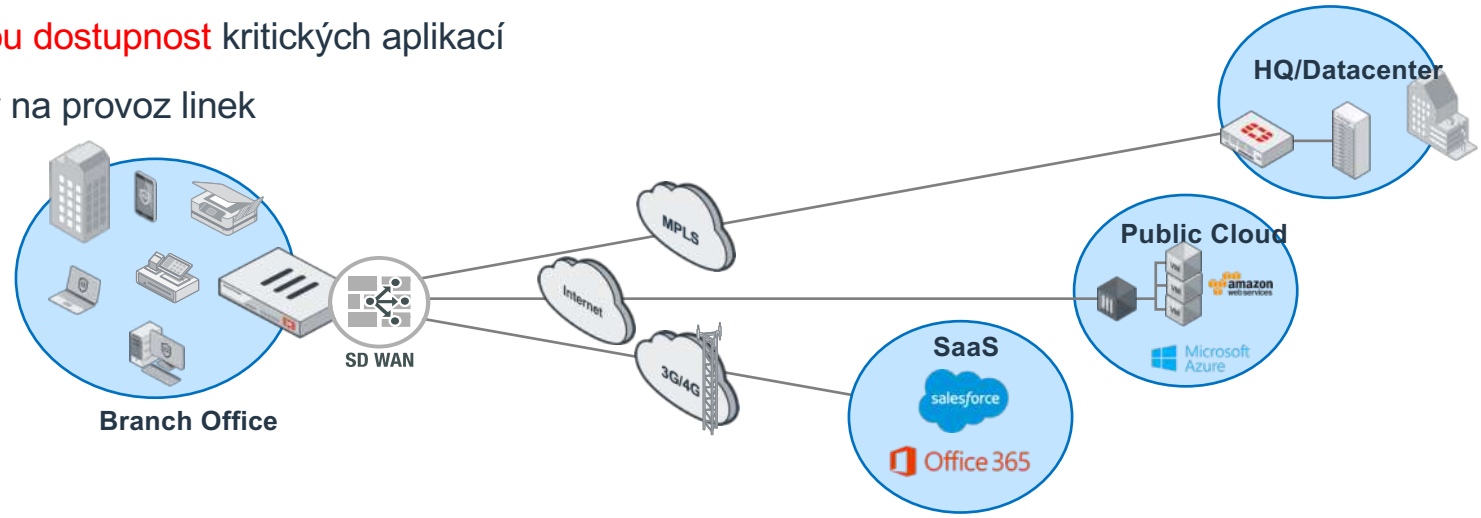
Dále představíme možnosti hw akcelerace inspekce síťového provozu na L2-L7 za účelem kontroly komunikace zařízením typu NGFW, které krom bezpečnostních funkcí může v síti zákazníka plnit i roli kontroléru pro bezdrátové přístupové body a síťové přepínače s cílem utvořit ucelený ekosystém bezpečnostních prvků s jednotnou správou, který je schopen odolat kybernetickým hrozbám. Na závěr ukážeme, že celé řešení je jednoduché na nasazení i správu a lze ho zákazníkům s výhodou nabízet jako službu.

Agenda

- Představení SD-WAN
- Možnosti inspekce sítového provozu
- Secure SD-Branch
- Orchestrace a centrální správa

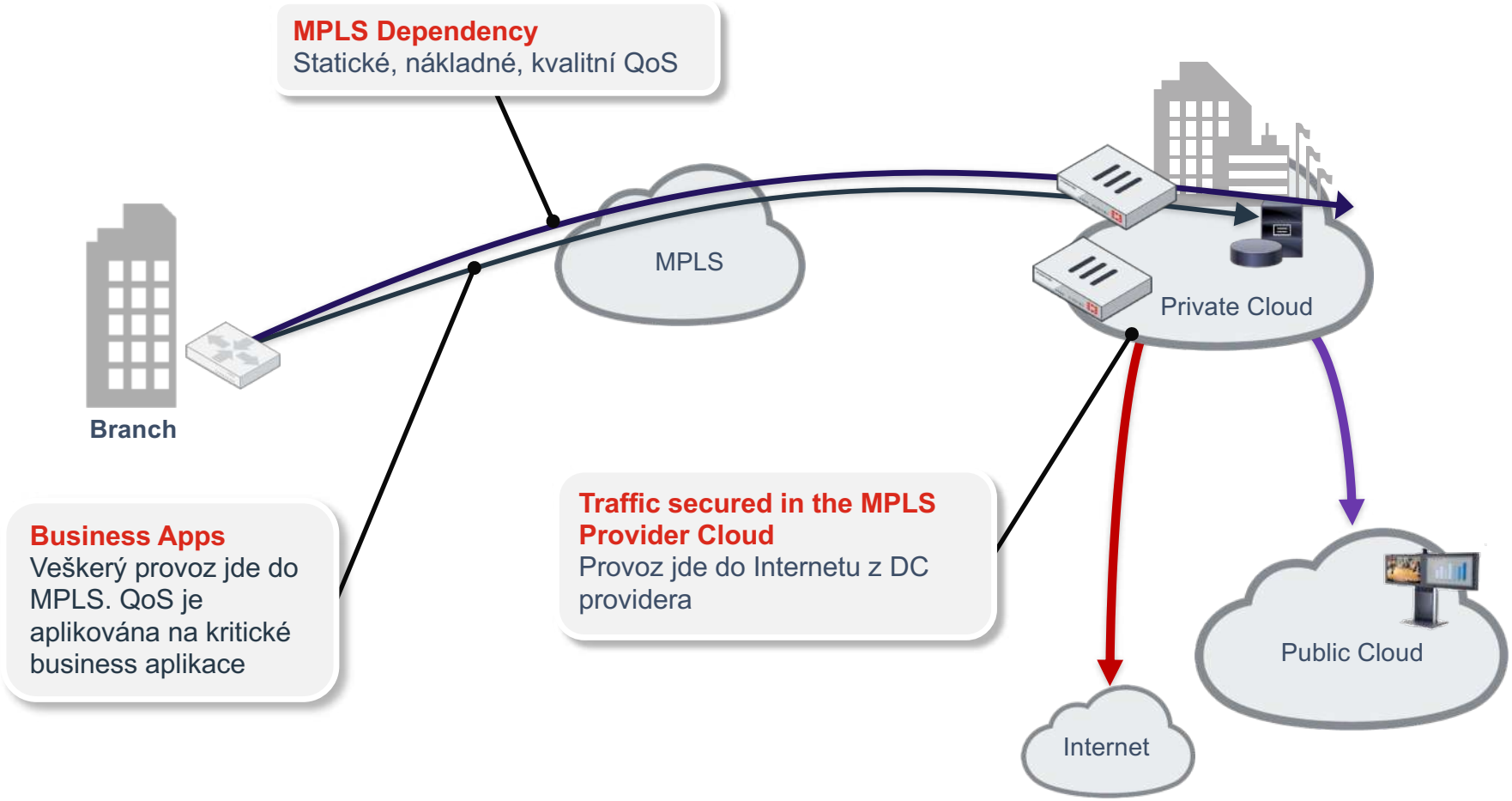
Co je to SD-WAN?

- **Virtuální interface, do kterého lze vložit různé druhy interfaců, které směřují do různých cílů**
- Poskytuje efektivní rozkládání zátěže za použití různých balancovacích algoritmů
- Umožňuje směrování do různých linek na základě statických nebo dynamických objektů, aplikací a nebo ISDB*
- Podporuje dynamické měření kvality linky
- Podporuje IPv4 i IPv6
- Umožňuje dynamické směrování provozu na základě kvality linek
- Zajistí vysokou dostupnost kritických aplikací
- Sníží náklady na provoz linek

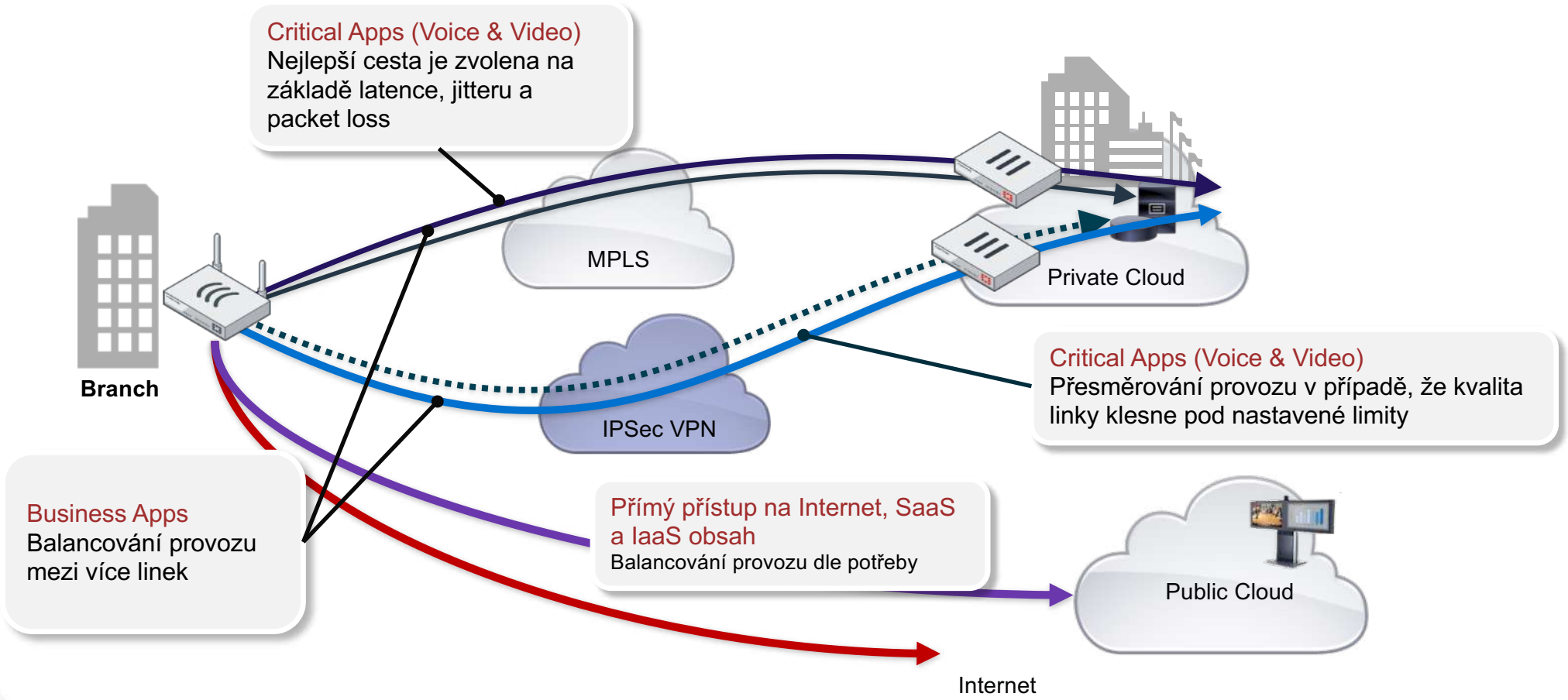


* Internet Service Database

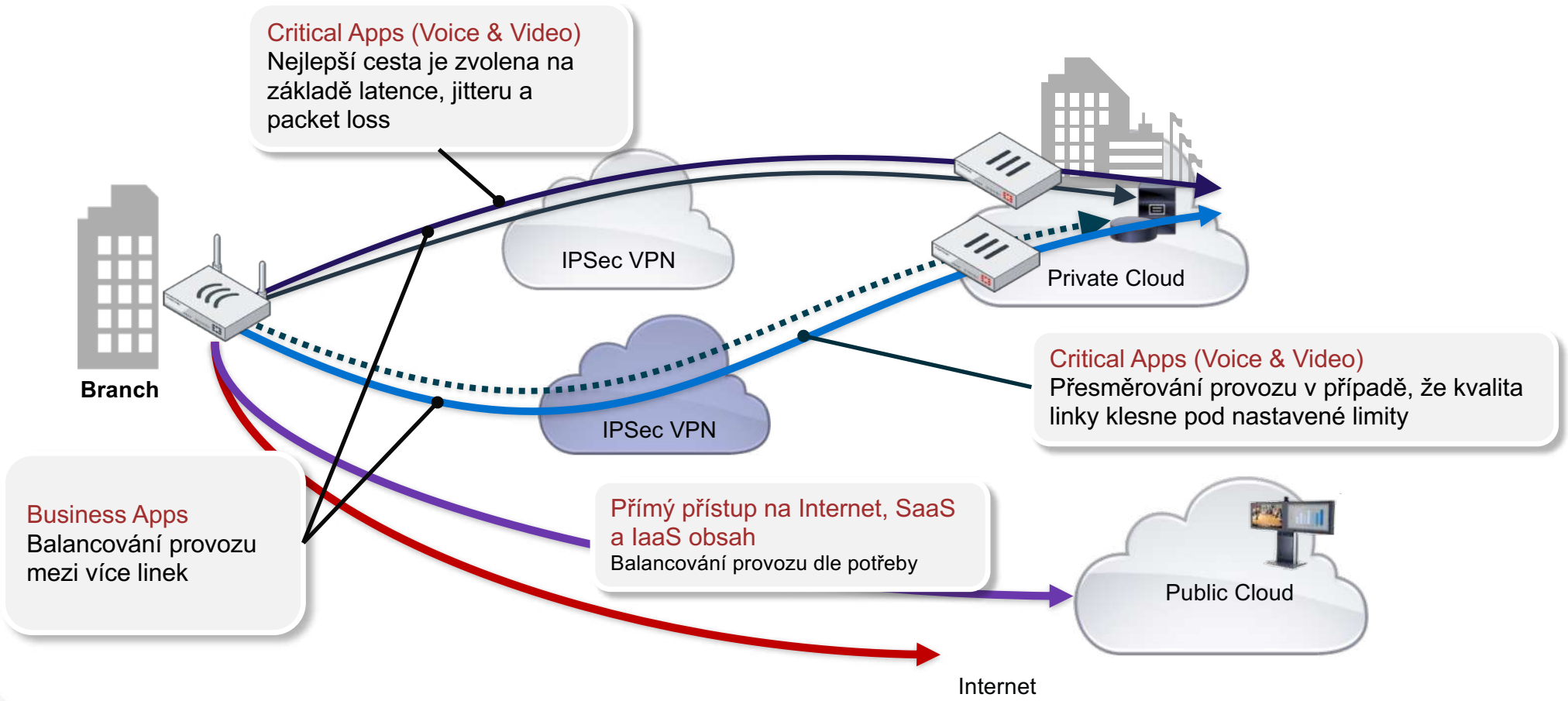
„Enterprise“ SD-WAN use case



„Enterprise“ SD-WAN use case



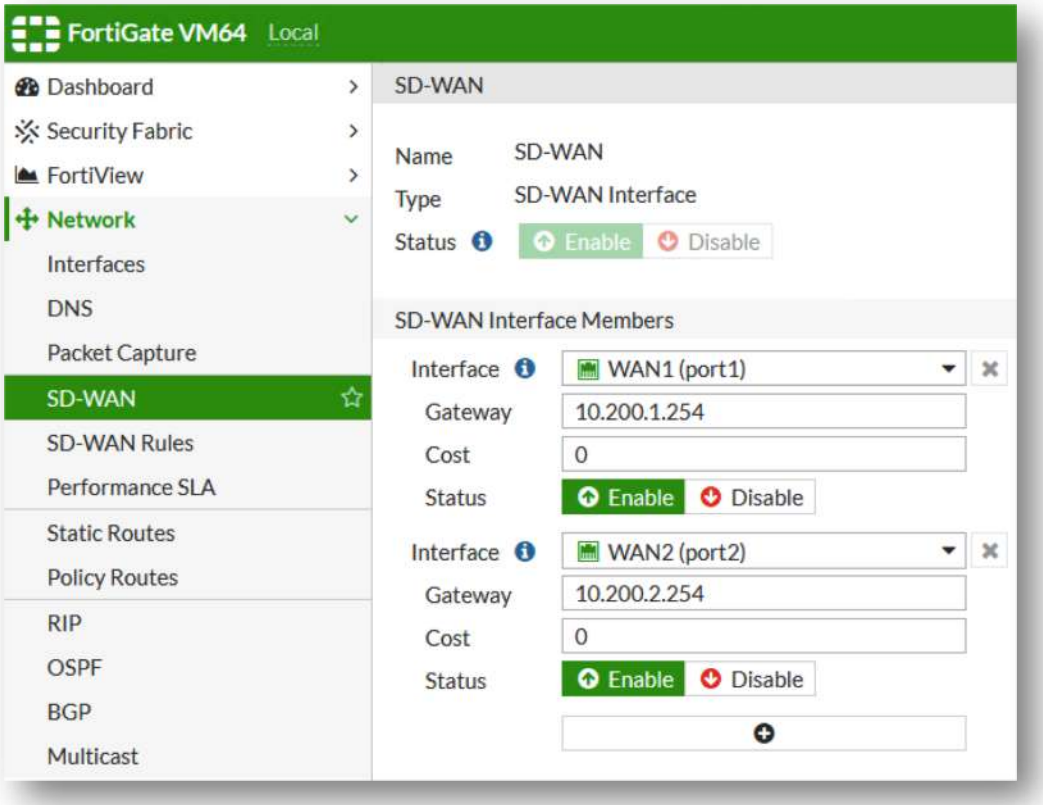
„Enterprise“ SD-WAN use case



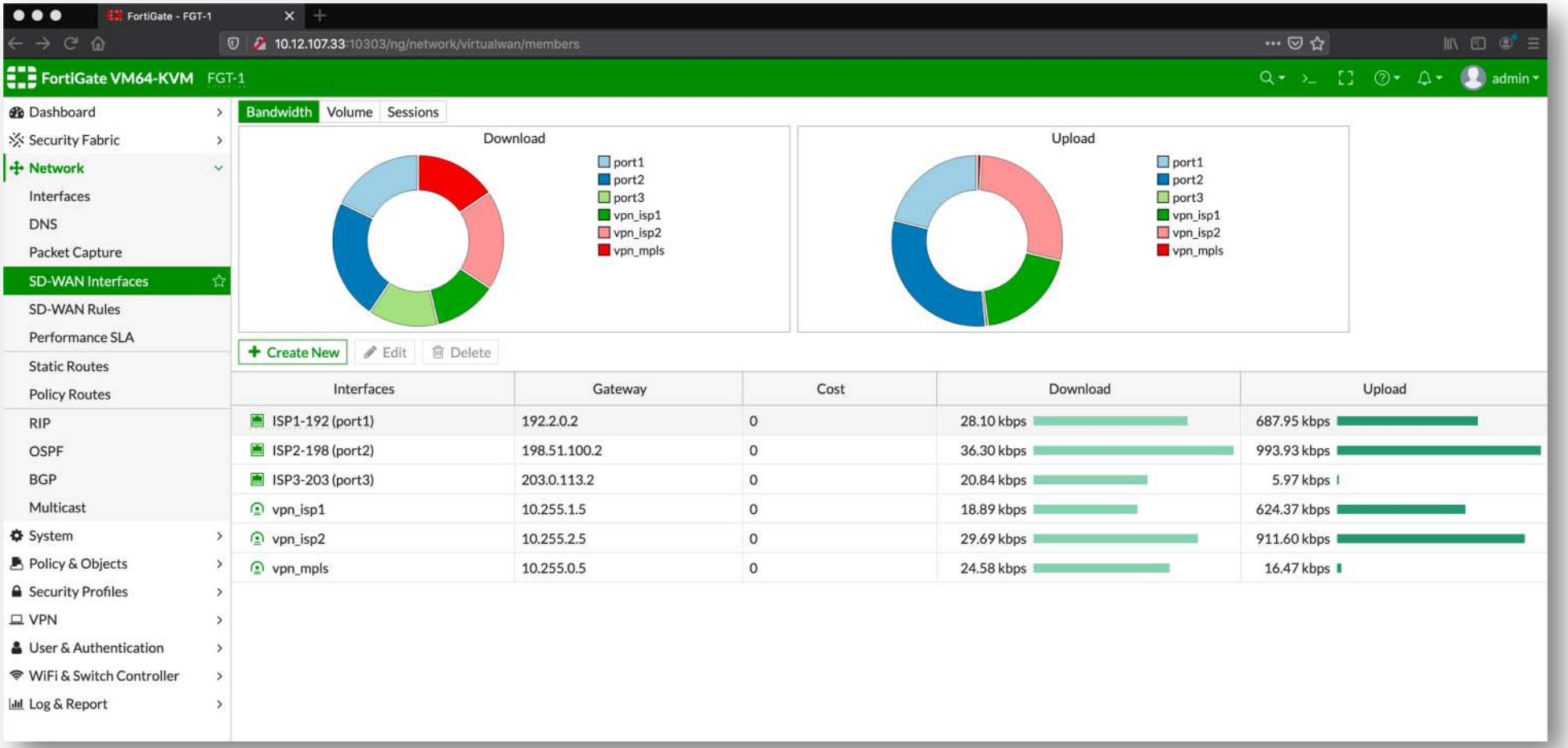
SD-WAN interface

- Fyzický port
- VLAN
- LAG/redundant
- VPN (IPSEC/GRE/IP-in-IP)
- LTE/3G
- Extender

```
config system virtual-wan-link
    set status enable
    config members
        edit 1
            set interface "port1"
            set gateway 10.200.1.254
        next
        edit 2
            set interface "port2"
            set gateway 10.200.2.254
        next
    end
```

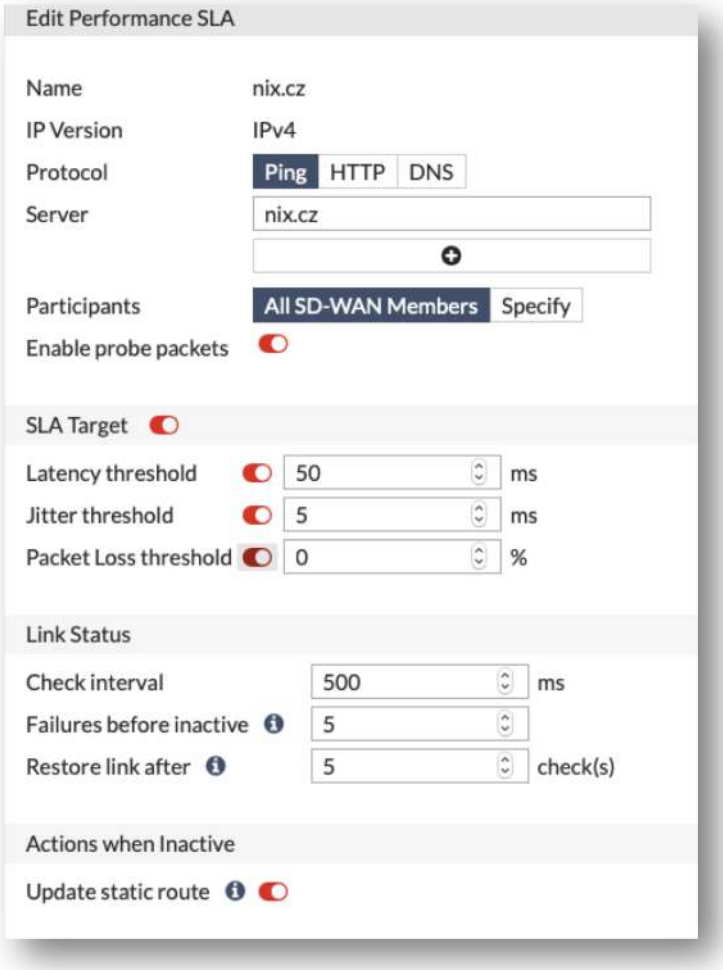


SD-WAN interface



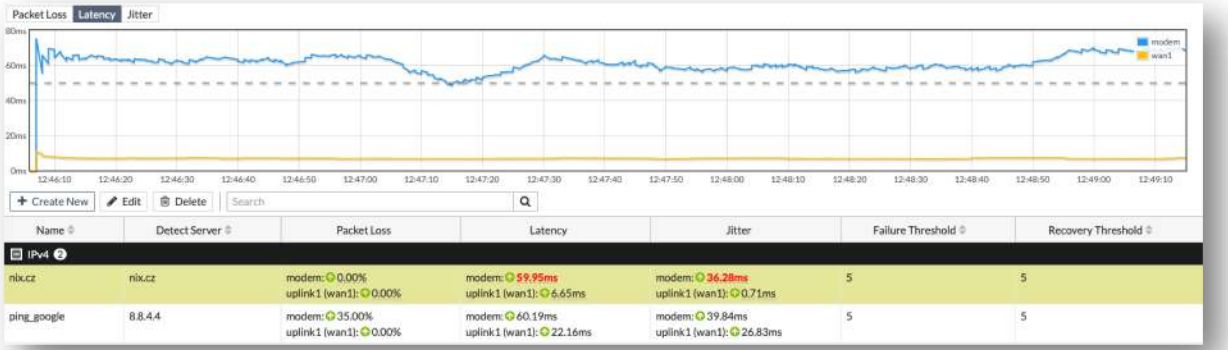
SD-WAN SLA Performance

- **Sleduje stav linek**
  - **Všech**
  - **Vybraných**
- Možnost definice SLA Target
  - Latence
  - Jitter
  - Packet loss

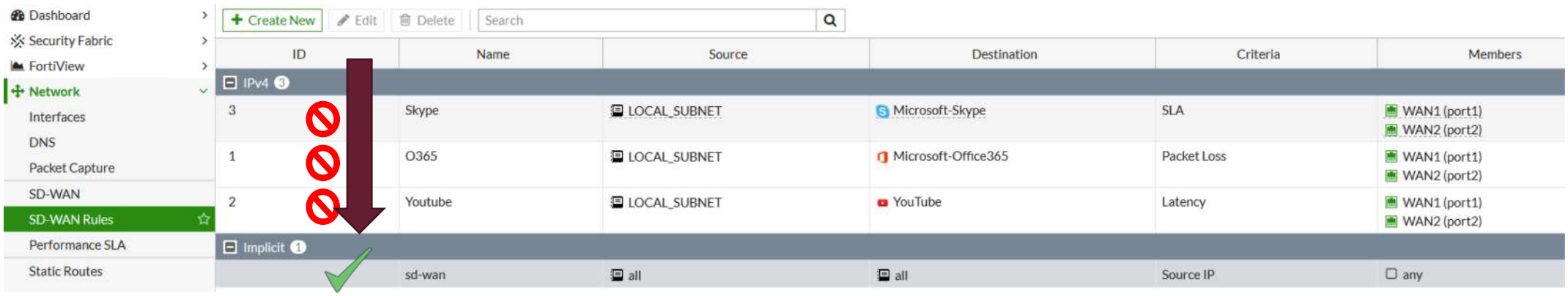


SD-WAN SLA Performance

- Performace SLA odesílá pakety na nastavené servery pro zjištění kvality linky
- V SD WAN Rules je pak možné nastavit, kterou linku FortiGate použije na základě výsledku z Performance SLA
- Performance SLA zároveň funguje jako health check



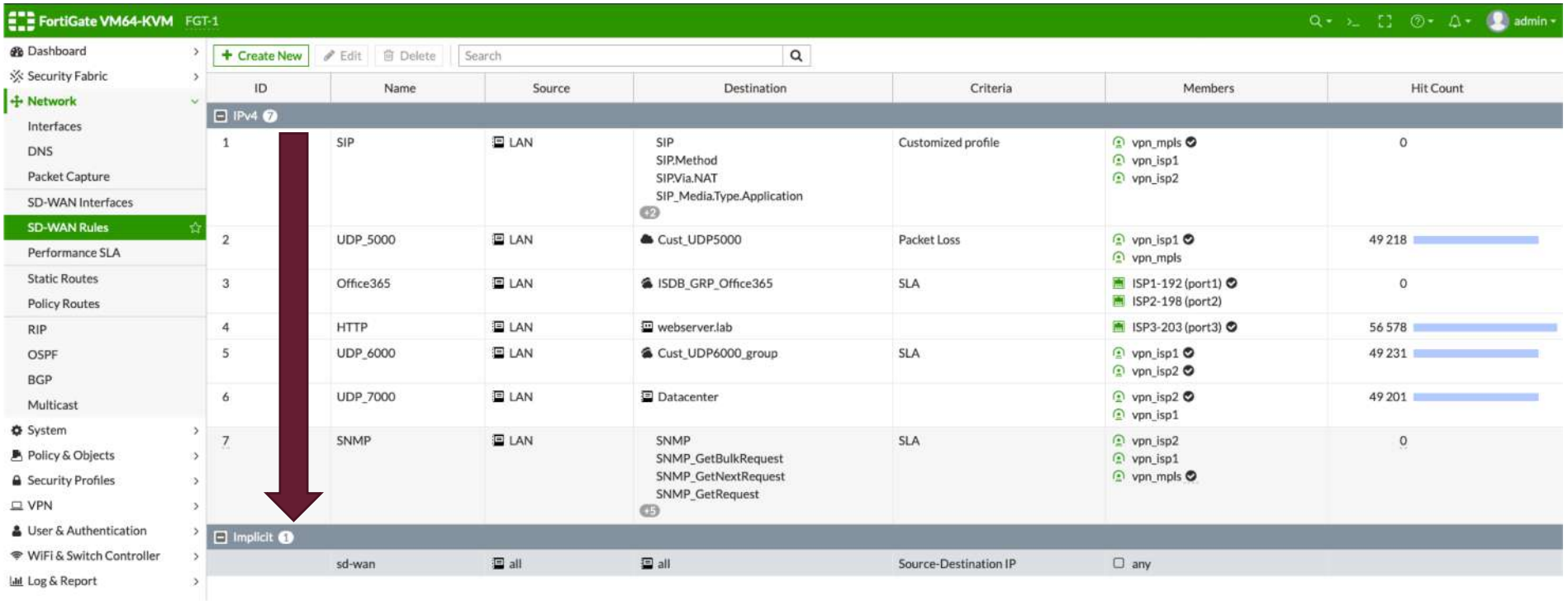
SD-WAN Rules



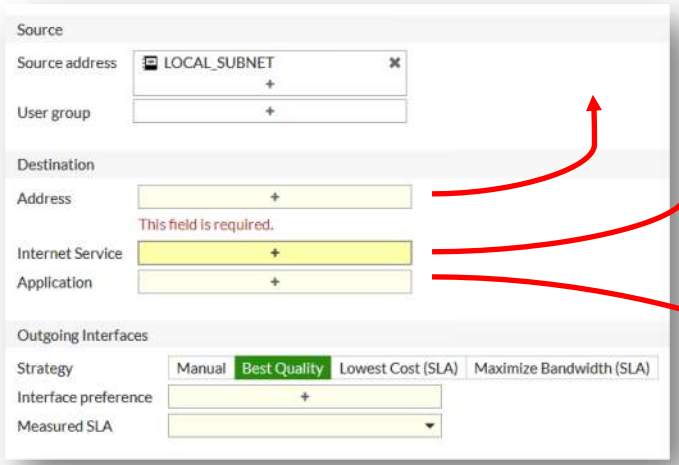
Pokud žádné pravidlo neodpovídá provozu, tak se použije záznam z FIB (forwarding information base)

```
Local # get router info kernel
…
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0->0.0.0.0/0 pref=0.0.0.0
        gwy=10.200.1.254 flag=04 hops=0 oif=3(port1)
        gwy=10.200.2.254 flag=04 hops=0 oif=4(port2)
…
```

SD-WAN Rules - příklad

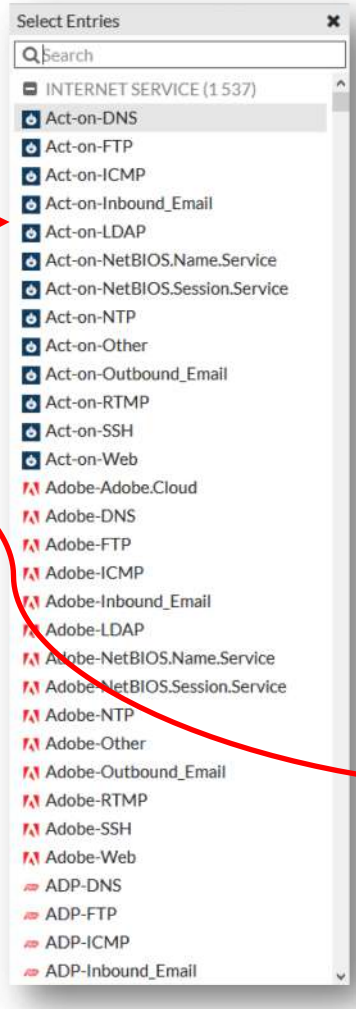


SD-WAN Rules

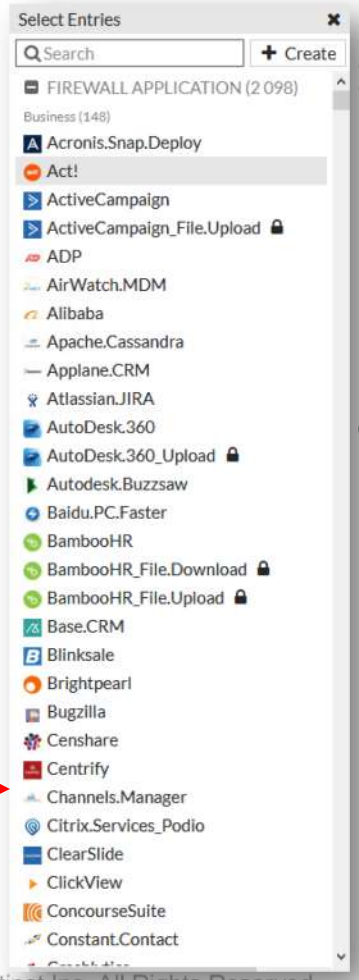


DSCP match (cli only):

```
config system virtual-wan-link
config service
        edit 1
            set tos 0x<tos>
            set tos-mask 0xff
         next
    end
```



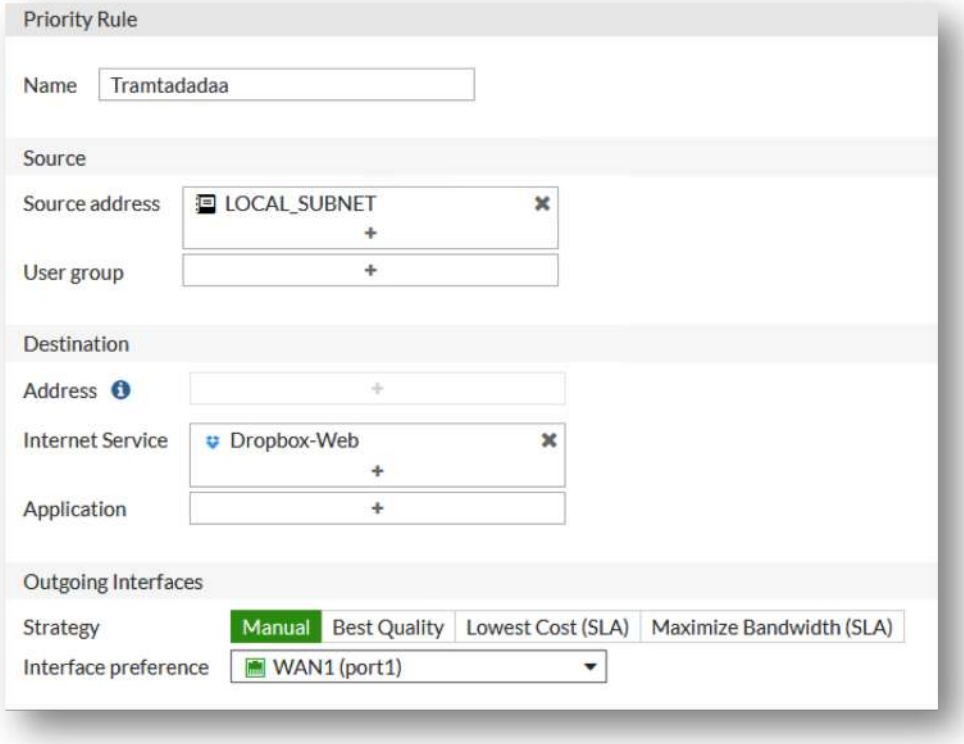
Internet Service Database + custom



Application Control signatures + custom

SD-WAN Strategy - Manual

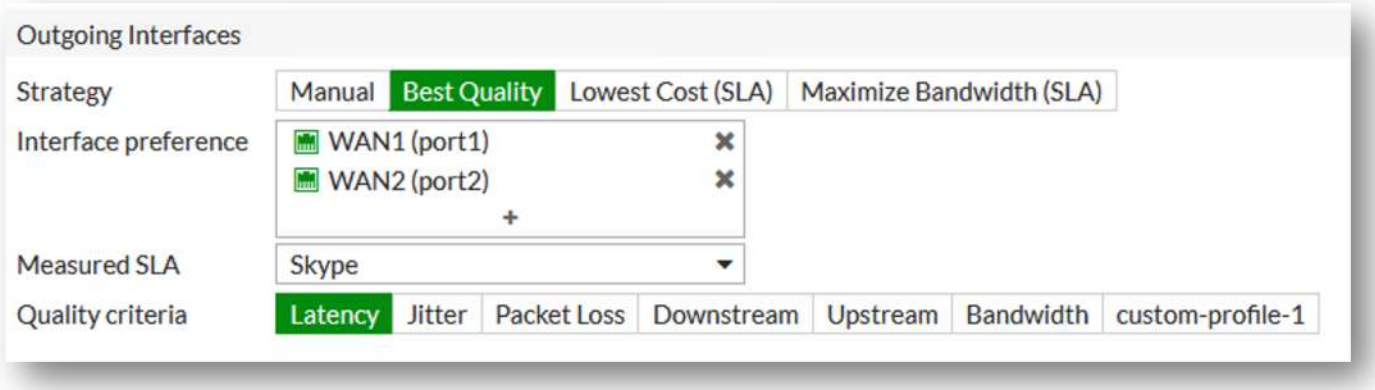
- V podstatě klasický Policy based routing
- Jeden odchozí interface (od FortiOS 6.4 více odchozích interfaces)
- Žádný performance monitoring



SD-WAN Strategy – Best Quality

- Vybere linku z SD WAN members, které nejlépe plní kritéria kvality
- Může dojít k využití více linek najednou např. při častých změnách kvality

- **Latency** - Doporučeno pro aplikace, které vyžadují nízkou odezvu – VoIP/Video
- **Jitter** - Doporučeno pro aplikace s požadavkem na vysokou kvalitu linky - VoIP
- **Packet Loss** - Doporučeno pro klient-server aplikace – Oracle DB, SSH
- **Downstream** - Doporučeno pro aplikace s požadavkem na download dat – Dropbox, OneDrive
- **Upstream** - Doporučeno pro aplikace s požadavkem na upload dat – zálohování
- **Bandwidth** – součet upstream a downstream - Vhodné pro aplikace, kde je požadavek na upload/download – file sharing, cloud storage
- **Custom-profile-1** – možnost nastavit si požadavek na kvalitu linky dle kombinace parametrů



SD-WAN Strategy – Lower Cost SLA

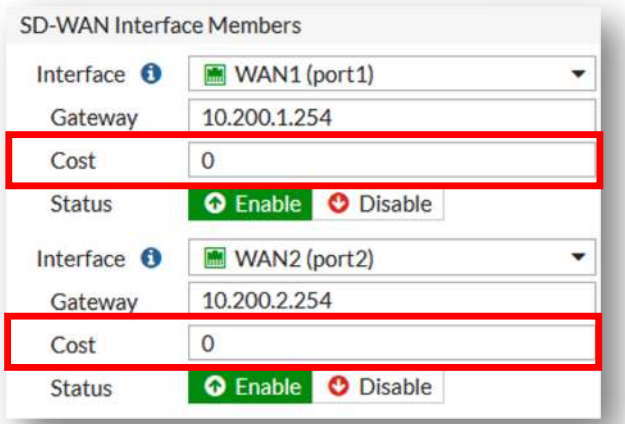
Vybere odchozí interface (link) na základě splnění SLA parametrů, Cost na linku a nastavené Priority interfaců

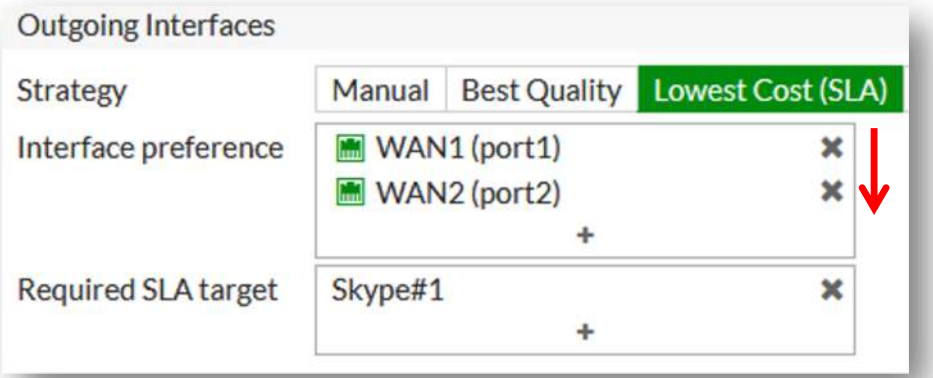
Musí být splněno SLA

Nižší Cost ma vyšší prioritu (0 default)

Seřazení interface dle Priority

Interface	SLA Requirements	Cost	Priority
Interface1	Satisfy	5	4
Interface2	Satisfy	5	3
Interface3	Satisfy	10	2
Interface4	Does not satisfy	2	1



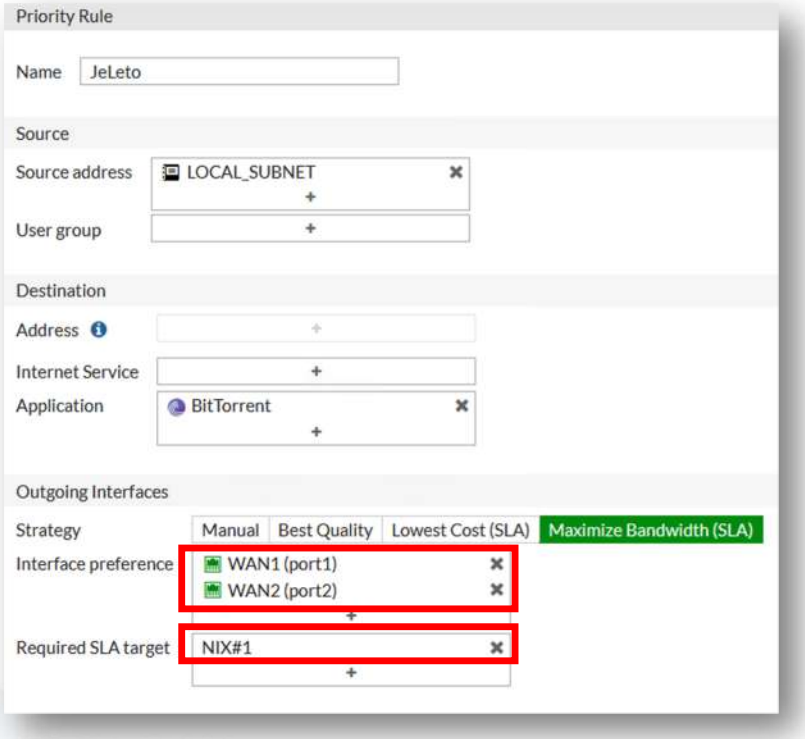



```
set priority-members 1 2
```

SD-WAN Strategy – Maximize Bandwidth

FortiGate balancuje sessions přes všechny interfacy, které splňují SLA.

FortiGate **neřeší** Cost ani prioritu interface.



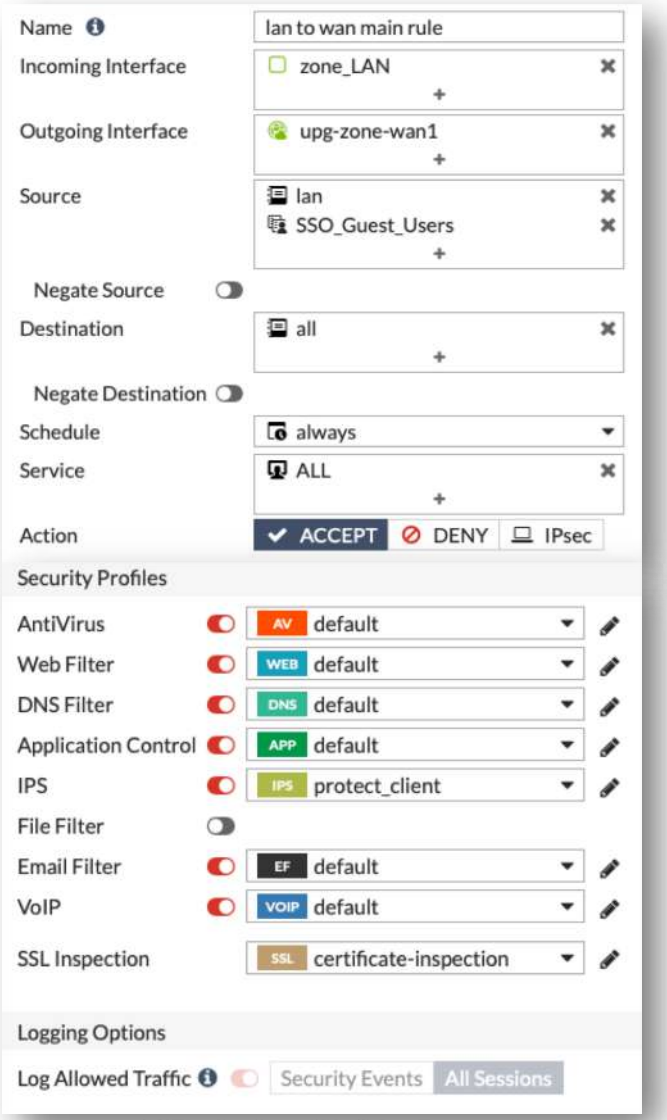
Session-based load balancing – round robin

Když interface přestane splňovat parametry SLA, tak se do něj přestane odesílat provoz

Secure SD-WAN

- Možnost definovat řadu bezpečnostních kontrol:
  - **Antivirus** (řada podporovaných protokolů+sandboxing)
  - **Kategorizace webových stránek** (~80 kategorií)
  - **DNS Filtering** (+DNS sinkhole/portal IP)
  - **Applikační kontrola** (L7 footprint)
  - **Detekce útoků** (IPS signatura, anomálie, DoS)
  - **File Filter** (řada podporovaných protokolů)
  - **Email Filter** (jednoduchý antispam)
  - **VoIP** (zabezpečení VoIP komunikace)
  - **SSL Inspekce** (HTTPS, POP3S, IMAPS, FTPS,SSH,…)
  - **WAF** (web aplikační firewall)
  - **ICS, IoT**

…



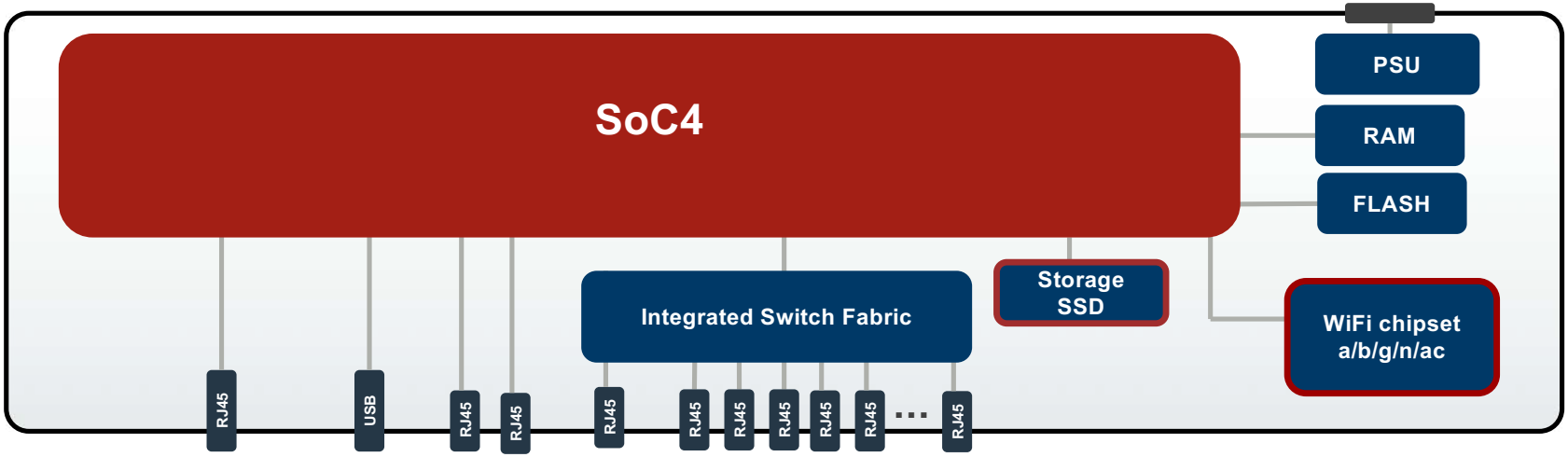
Důkladná inspekce = nízká propustnost?

- CPU architektura vs. HW akcelerovaná platforma

- Akcelerace L2 – L7 inspekce, IPv4 i IPv6
- Akcelerace symetrické a asymetrické kryptografie
- Akcelerace mitigace DoS útoků
- Akcelerace multicast provozu, CAPWAP, VXLAN, GTP
- Velmi nízká latence (jednotky µs)
- Velmi nízká spotřeba elektrické energie
- Paralelní zpracování dat (čipy s propustností až 200 Gbps) → škálování výkonu
- Podpora form-factor pomocí SoC platformy

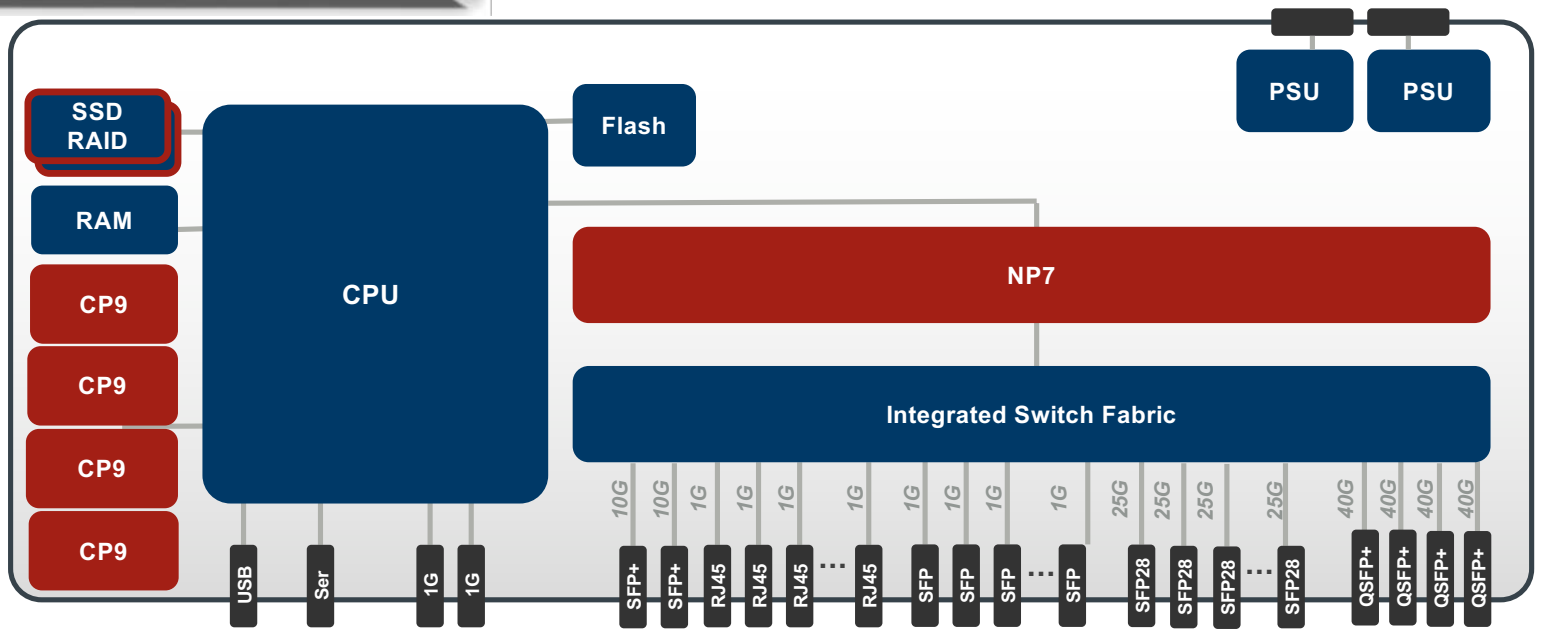
Důkladná inspekce = nízká propustnost?

Firewall	IPS	NGFW	Threat Protection
10 Gbps	1.4 Gbps	1 Gbps	700 Mbps



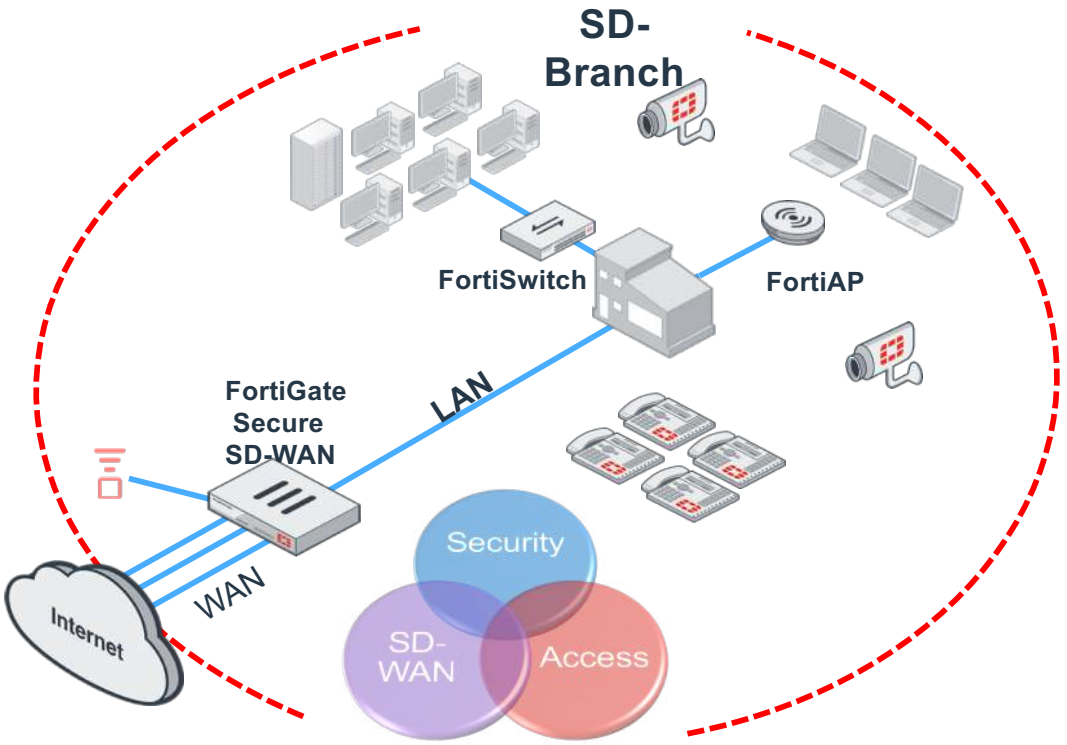
Důkladná inspekce = nízká propustnost?

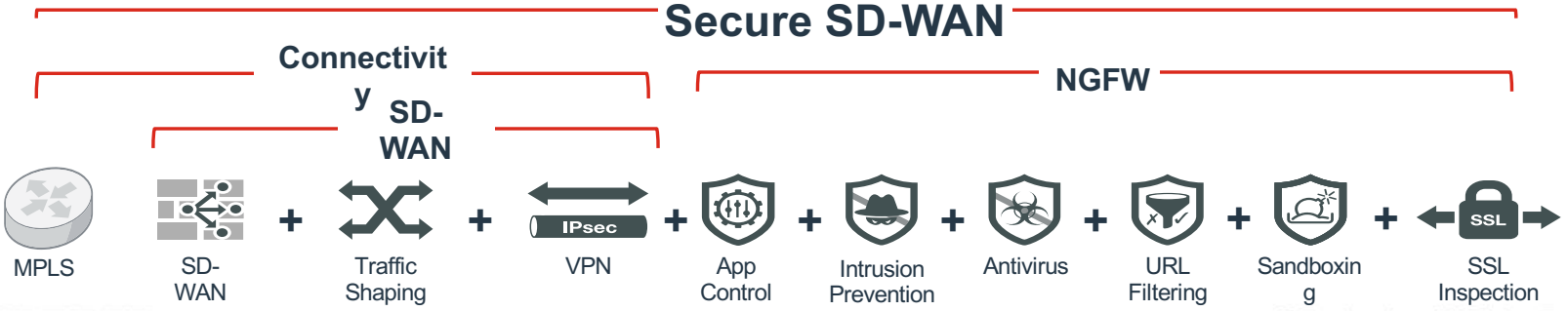
Firewall	IPS	NGFW	Threat Protection
198 Gbps	13 Gbps	11 Gbps	9.1 Gbps



Secure SD - Branch

- Segmentace vnitřní sítě
- Správa hostů (guest management)
- Network Access Control
- User & Entity Behavior Analytics
- Presence Analytics
- Kamery, VoIP

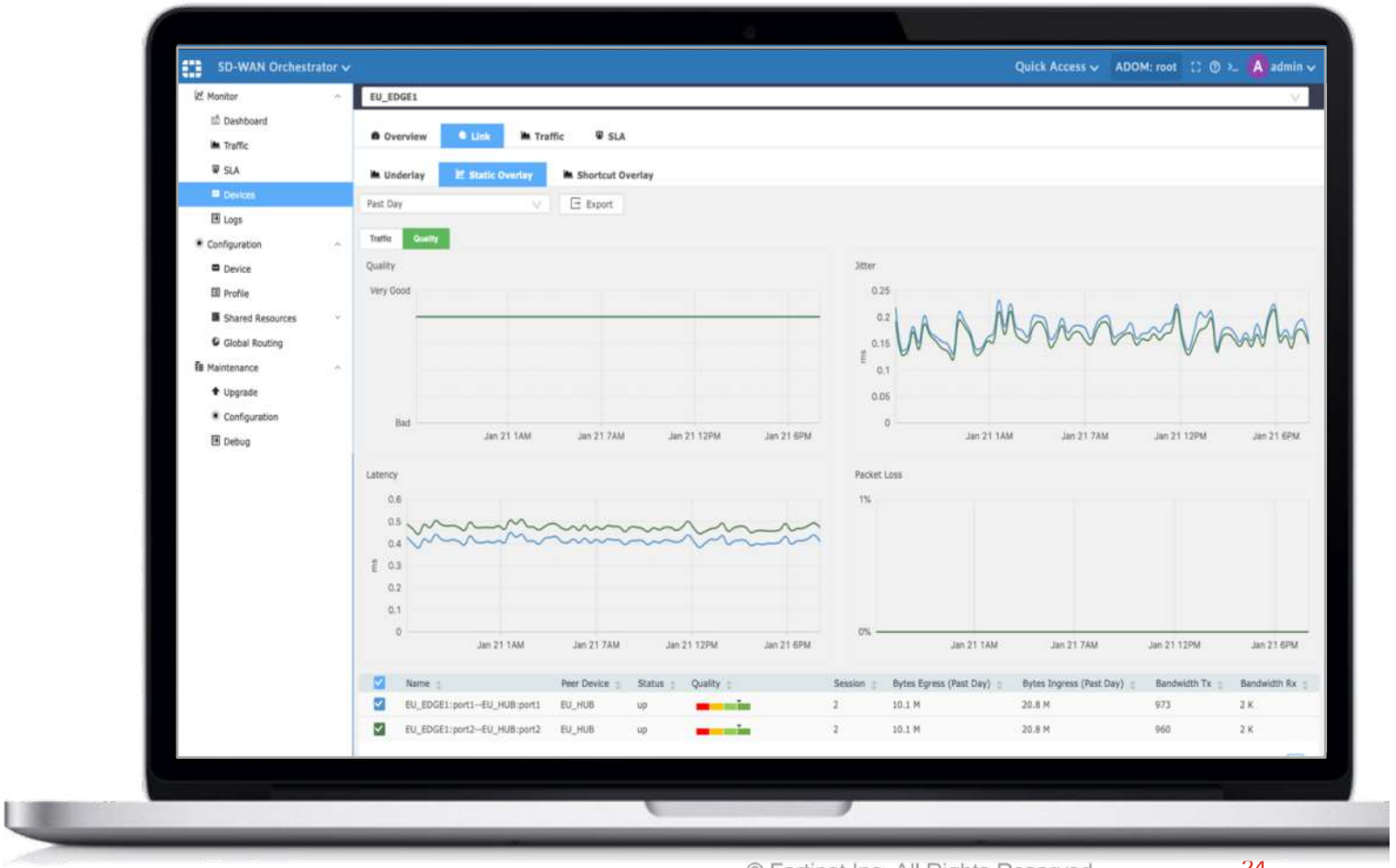




SD-WAN Orchestrace a centrální správa

SD-WAN Orchestrator

- Overlay
- Underlay
- Automatizace úkonů
  - Dyn. Routing
  - VPN
  - Pravidla
- Sdílení objektů
- Workflou
- Vizualizace
- Zero Touch Provizioning



Děkuji za pozornost.

Jan Václavík
Systems Engineer CEE
Fortinet

jvaclavik@fortinet.com

BMW i Motorsport
Official Partner