



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

BMW i Motorsport
Official Partner



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 vytvořit 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

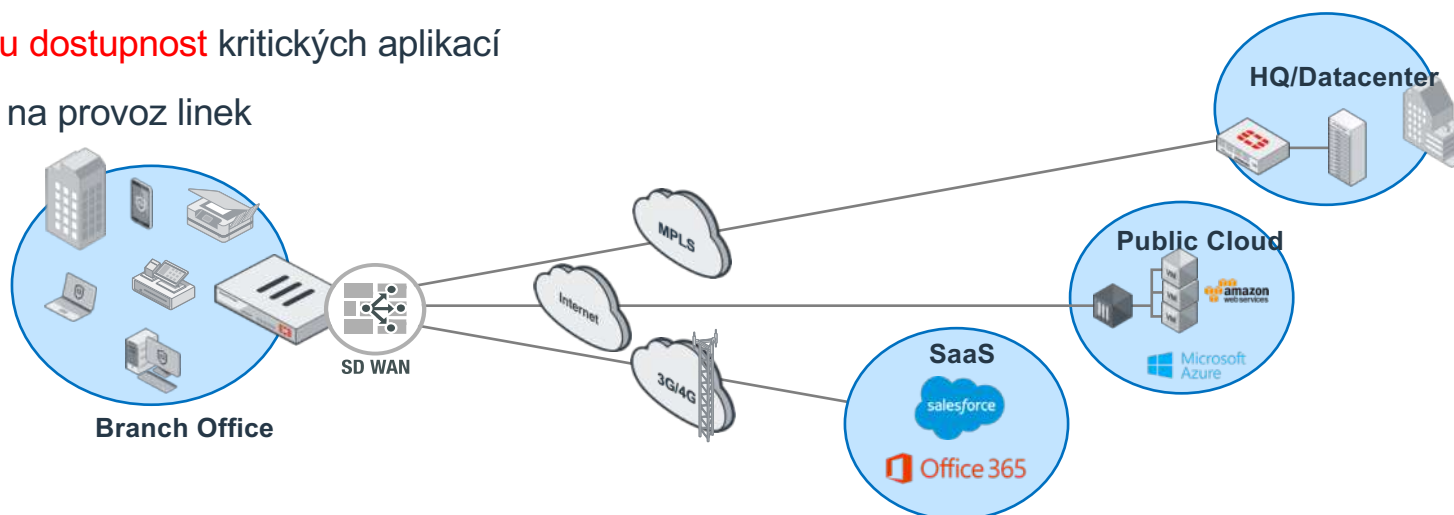
Možnosti inspekce síťového provozu

Secure SD-Branch

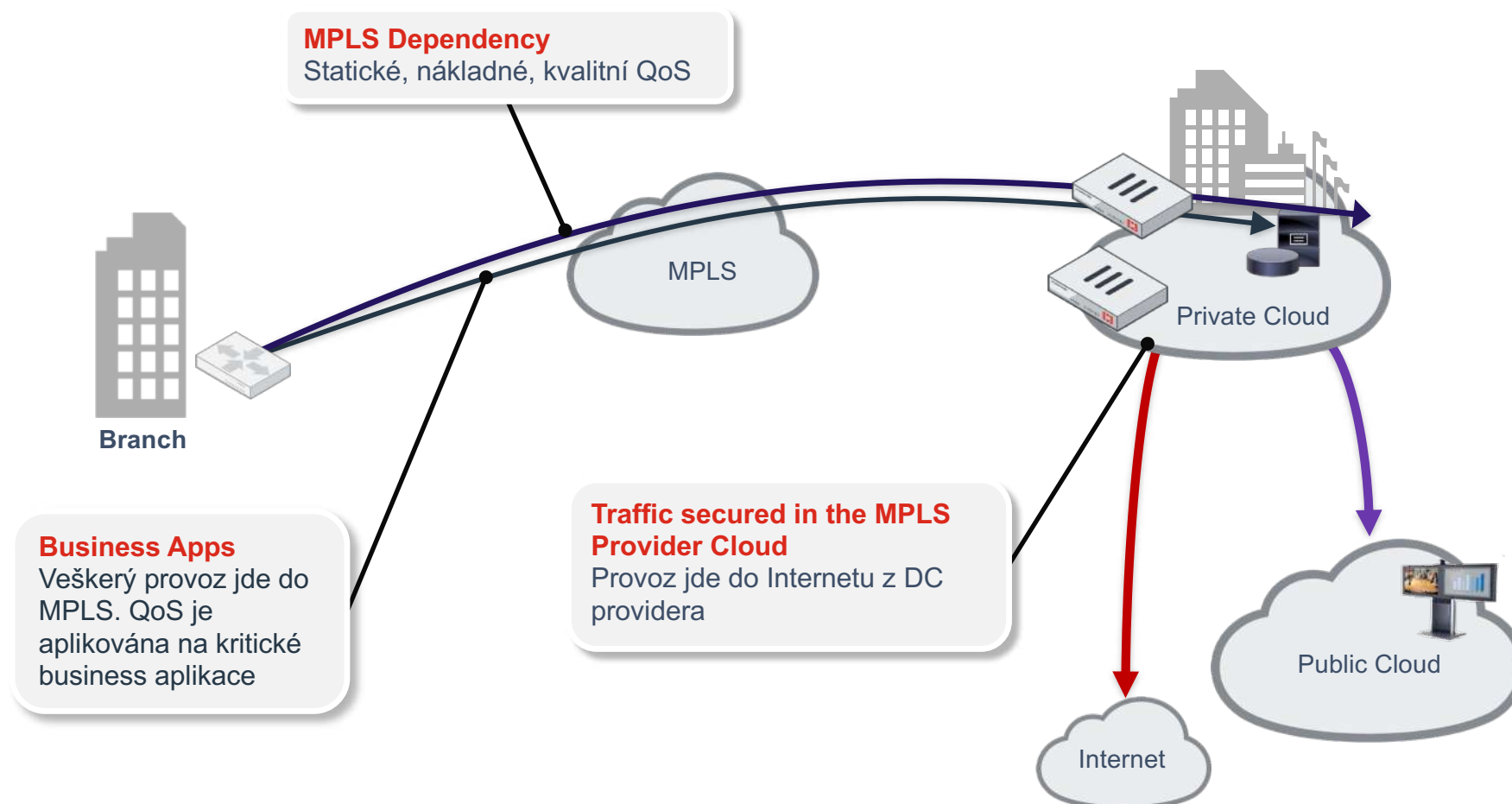
Orchestrace a centrální správa

Co je to SD-WAN?

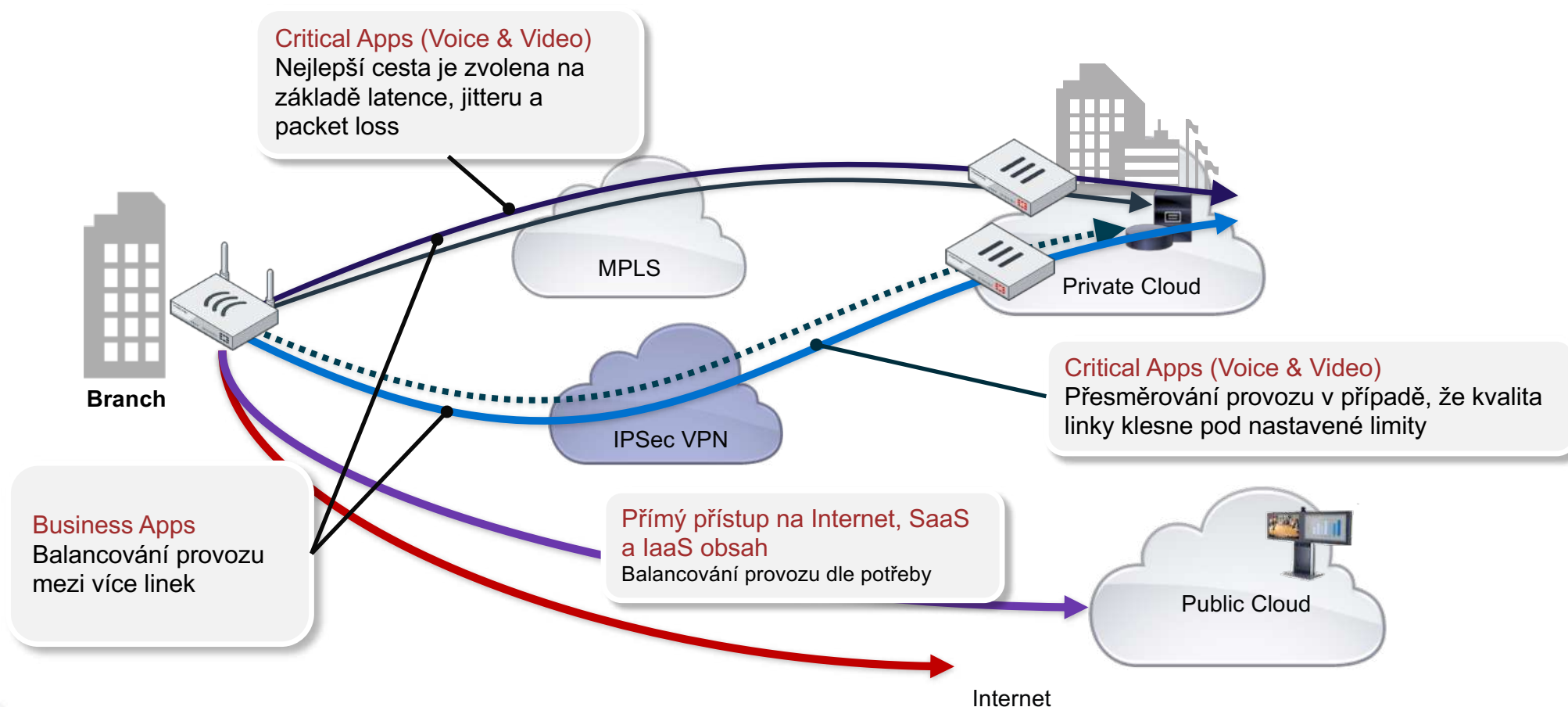
- Virtuální interface, do kterého lze vložit různé druhy interfaců, které směřují do různých cílů
- Poskytuje efektivní **rozkládání zátěže** za použití různých balancovacích algoritmů
- Umožňuje směrování do různých linek na základě **statických nebo dynamických objektů**, aplikací a nebo ISDB*
- Podporuje 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



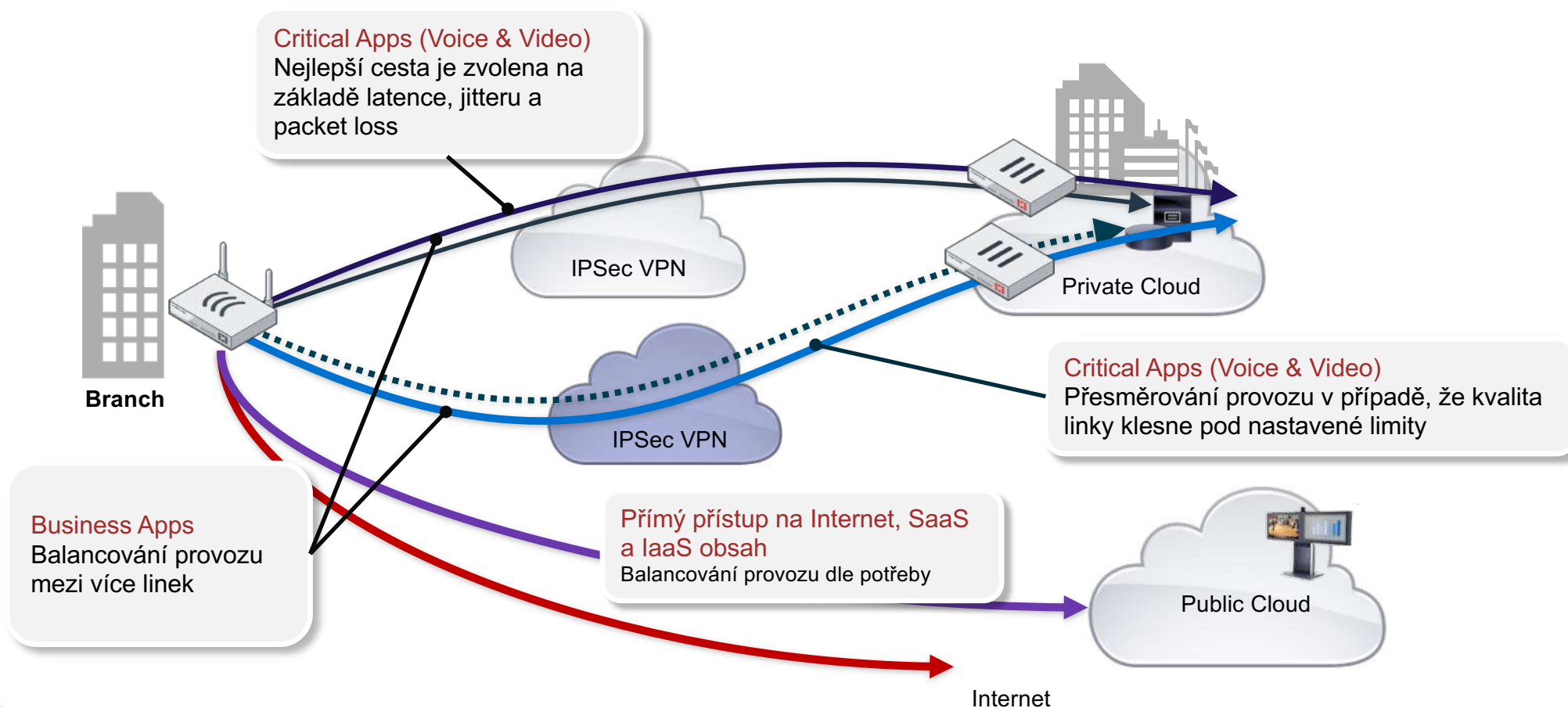
„Enterprise“ SD-WAN use case



„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
```

The screenshot shows the FortiGate VM64 Local configuration page for the SD-WAN interface. The left sidebar contains a navigation menu with options: Dashboard, Security Fabric, FortiView, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN (selected), SD-WAN Rules, Performance SLA, Static Routes, Policy Routes, RIP, OSPF, BGP, and Multicast. The main content area is titled 'SD-WAN' and displays the following configuration:

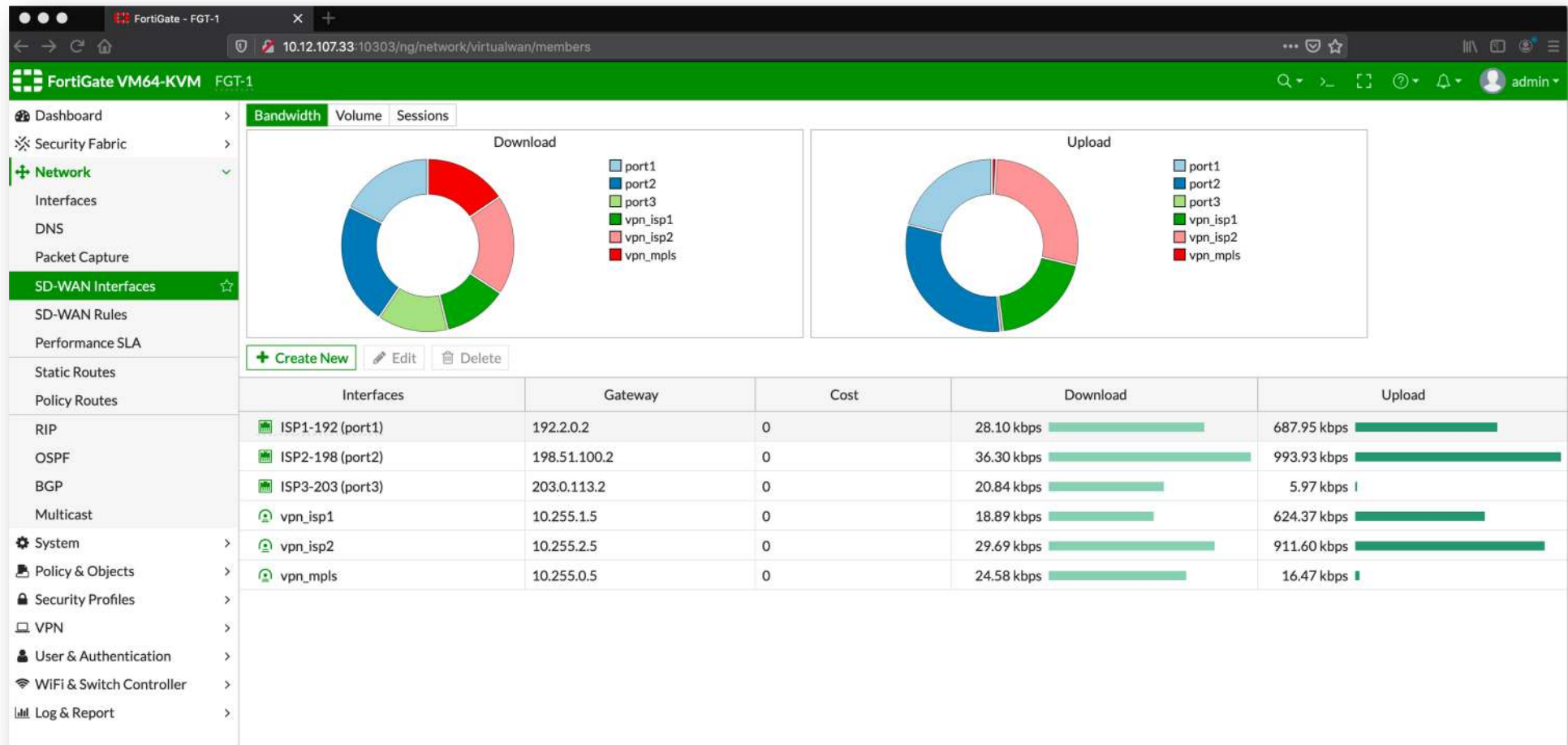
- Name: SD-WAN
- Type: SD-WAN Interface
- Status: ☒ Enable ☐ Disable

Below this, the 'SD-WAN Interface Members' section lists two interfaces:

- Interface 1:** WAN1 (port1)
 - Gateway: 10.200.1.254
 - Cost: 0
 - Status: ☒ Enable ☐ Disable
- Interface 2:** WAN2 (port2)
 - Gateway: 10.200.2.254
 - Cost: 0
 - Status: ☒ Enable ☐ Disable

A plus sign (+) button is visible at the bottom of the interface members list, indicating the option to add more members.

SD-WAN interface



SD-WAN SLA Performance

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

Edit Performance SLA

Name	nix.cz
IP Version	IPv4
Protocol	Ping HTTP DNS
Server	nix.cz
Participants	All SD-WAN Members Specify
Enable probe packets	<input checked="" type="checkbox"/>

SLA Target ☒

Latency threshold	<input checked="" type="checkbox"/>	50	ms
Jitter threshold	<input checked="" type="checkbox"/>	5	ms
Packet Loss threshold	<input checked="" type="checkbox"/>	0	%

Link Status

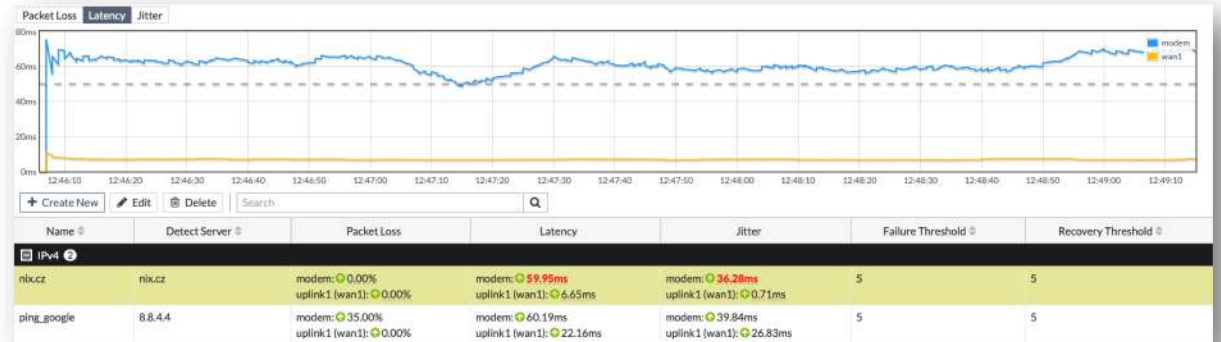
Check interval	500	ms
Failures before inactive ⓘ	5	
Restore link after ⓘ	5	check(s)

Actions when Inactive

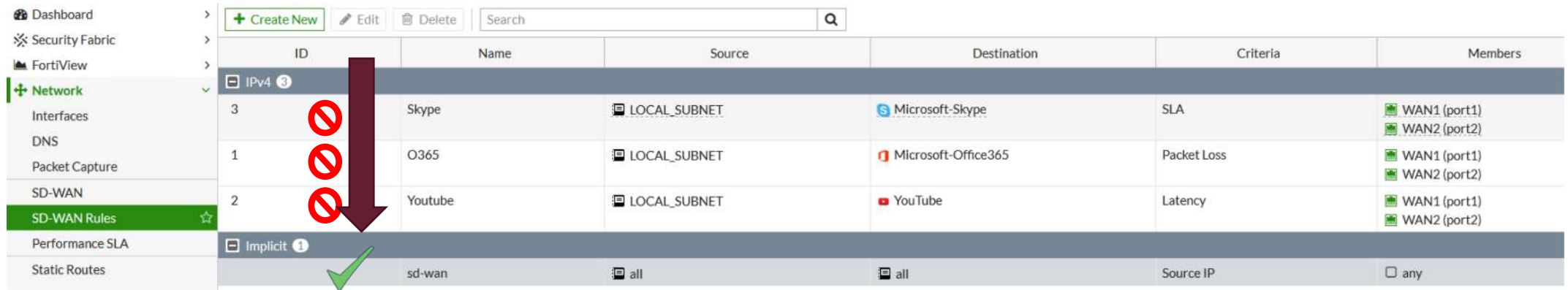
Update static route ⓘ	<input checked="" type="checkbox"/>
-----------------------	-------------------------------------

SD-WAN SLA Performance

- Performance 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



ID	Name	Source	Destination	Criteria	Members
3	Skype	LOCAL_SUBNET	Microsoft-Skype	SLA	WAN1 (port1) WAN2 (port2)
1	O365	LOCAL_SUBNET	Microsoft-Office365	Packet Loss	WAN1 (port1) WAN2 (port2)
2	Youtube	LOCAL_SUBNET	YouTube	Latency	WAN1 (port1) WAN2 (port2)
Implicit	sd-wan	all	all	Source IP	any

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

FortiGate VM64-KVM FGT-1							
<div>Dashboard</div> <div>Security Fabric</div> <div>Network</div> <div>Interfaces</div> <div>DNS</div> <div>Packet Capture</div> <div>SD-WAN Interfaces</div> <div>SD-WAN Rules</div> <div>Performance SLA</div> <div>Static Routes</div> <div>Policy Routes</div> <div>RIP</div> <div>OSPF</div> <div>BGP</div> <div>Multicast</div> <div>System</div> <div>Policy & Objects</div> <div>Security Profiles</div> <div>VPN</div> <div>User & Authentication</div> <div>WiFi & Switch Controller</div> <div>Log & Report</div>	<div>+ Create New</div> <div>Edit</div> <div>Delete</div> <div>Search</div>						
	ID	Name	Source	Destination	Criteria	Members	Hit Count
	IPv4 7						
	1	SIP	LAN	SIP SIP.Method SIP.Via.NAT SIP_Media.Type.Application	Customized profile	vpn_mpls vpn_isp1 vpn_isp2	0
	2	UDP_5000	LAN	Cust_UDP5000	Packet Loss	vpn_isp1 vpn_mpls	49 218
	3	Office365	LAN	ISDB_GRP_Office365	SLA	ISP1-192 (port1) ISP2-198 (port2)	0
	4	HTTP	LAN	webserver.lab		ISP3-203 (port3)	56 578
	5	UDP_6000	LAN	Cust_UDP6000_group	SLA	vpn_isp1 vpn_isp2	49 231
	6	UDP_7000	LAN	Datacenter		vpn_isp2 vpn_isp1	49 201
	7	SNMP	LAN	SNMP SNMP_GetBulkRequest SNMP_GetNextRequest SNMP_GetRequest	SLA	vpn_isp2 vpn_isp1 vpn_mpls	0
Implicit 1							
sd-wan			all	all	Source-Destination IP	any	

SD-WAN Rules

Source

Source address: LOCAL_SUBNET

User group:

Destination

Address:

Internet Service:

Application:

Outgoing Interfaces

Strategy: Manual **Best Quality** Lowest Cost (SLA) Maximize Bandwidth (SLA)

Interface preference:

Measured SLA:

DSCP match (cli only):

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

Select Entries

Search

INTERNET SERVICE (1 537)

- Act-on-DNS
- Act-on-FTP
- Act-on-ICMP
- Act-on-Inbound_Email
- Act-on-LDAP
- Act-on-NetBIOS.Name.Service
- Act-on-NetBIOS.Session.Service
- Act-on-NTP
- Act-on-Other
- Act-on-Outbound_Email
- Act-on-RTMP
- Act-on-SSH
- Act-on-Web
- Adobe-Adobe.Cloud
- Adobe-DNS
- Adobe-FTP
- Adobe-ICMP
- Adobe-Inbound_Email
- Adobe-LDAP
- Adobe-NetBIOS.Name.Service
- Adobe-NetBIOS.Session.Service
- Adobe-NTP
- Adobe-Other
- Adobe-Outbound_Email
- Adobe-RTMP
- Adobe-SSH
- Adobe-Web
- ADP-DNS
- ADP-FTP
- ADP-ICMP
- ADP-Inbound_Email

Internet Service Database + custom

Select Entries

Search

+ Create

FIREWALL APPLICATION (2 098)

Business (148)

- Acronis.Snap.Deploy
- Act!
- ActiveCampaign
- ActiveCampaign_File.Upload
- ADP
- AirWatch.MDM
- Alibaba
- Apache.Cassandra
- Applane.CRM
- Atlassian.JIRA
- AutoDesk.360
- AutoDesk.360_Upload
- Autodesk.Buzzsaw
- Baidu.PC.Faster
- BambooHR
- BambooHR_File.Download
- BambooHR_File.Upload
- Base.CRM
- Blinksale
- Brightpearl
- Bugzilla
- Censhare
- Centrify
- Channels.Manager
- Citrix.Services_Podio
- ClearSlide
- ClickView
- ConcourseSuite
- Constant.Contact

Application Control signatures + custom

© Fortinet Inc. All Rights Reserved.

SD-WAN Strategy - **Manual**

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

The screenshot shows the 'Priority Rule' configuration page in Fortinet's SD-WAN interface. The rule is named 'Tramtadadaa'. Under the 'Source' section, 'LOCAL_SUBNET' is selected for the source address. Under the 'Destination' section, 'Dropbox-Web' is selected for the internet service. The 'Outgoing Interfaces' section shows the 'Manual' strategy selected, with 'WAN1 (port1)' as the interface preference.

Priority Rule	
Name	Tramtadadaa
Source	
Source address	LOCAL_SUBNET
User group	
Destination	
Address	
Internet Service	Dropbox-Web
Application	
Outgoing Interfaces	
Strategy	Manual
Interface preference	WAN1 (port1)

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

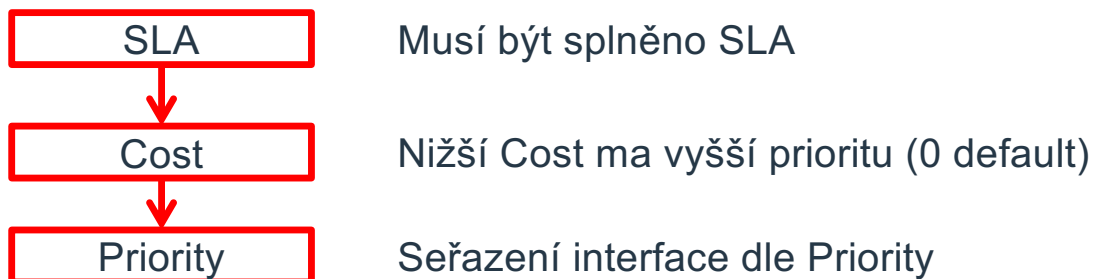
- **Latency** - Doporučeno pro aplikace, které vyžadují nízkou odezvu – VoIP/Video
- **Jitter** - Doporučeno pro aplikace s požadavkem na vysokou kvalitu linky - VoIP
- **Packet Loss** - Doporučeno pro klient-server aplikace – Oracle DB, SSH
- **Downstream** - Doporučeno pro aplikace s požadavkem na 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

Outgoing Interfaces

Strategy	Manual Best Quality Lowest Cost (SLA) Maximize Bandwidth (SLA)
Interface preference	<div><div> WAN1 (port1) </div><div> WAN2 (port2) </div><div>+</div></div>
Measured SLA	Skype
Quality criteria	Latency Jitter Packet Loss Downstream Upstream Bandwidth custom-profile-1

SD-WAN Strategy – Lower Cost SLA

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



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

SD-WAN Interface Members

Interface	WAN1 (port1)
Gateway	10.200.1.254
Cost	0
Status	Enable Disable
Interface	WAN2 (port2)
Gateway	10.200.2.254
Cost	0
Status	Enable Disable

Outgoing Interfaces

Strategy	Manual Best Quality Lowest Cost (SLA)
Interface preference	<div>WAN1 (port1) ×</div> <div>WAN2 (port2) ×</div> <div>+</div>
Required SLA target	<div>Skype#1 ×</div> <div>+</div>

set priority-members 1 2

SD-WAN Strategy – Maximize Bandwidth

FortiGate balancuje sessions přes všechny interfacery, které splňují SLA.

FortiGate neřeší Cost ani prioritu interface.

Priority Rule

Name: JeLeto

Source

Source address: LOCAL_SUBNET

User group:

Destination

Address:

Internet Service:

Application: BitTorrent

Outgoing Interfaces

Strategy: Manual, Best Quality, Lowest Cost (SLA), **Maximize Bandwidth (SLA)**

Interface preference: WAN1 (port1), WAN2 (port2)

Required SLA target: NIX#1

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**

...



FORTINET

Name	lan to wan main rule
Incoming Interface	zone_LAN
Outgoing Interface	upg-zone-wan1
Source	lan SSO_Guest_Users
Negate Source	<input type="checkbox"/>
Destination	all
Negate Destination	<input type="checkbox"/>
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec
Security Profiles	
AntiVirus	<input checked="" type="checkbox"/> AV default
Web Filter	<input checked="" type="checkbox"/> WEB default
DNS Filter	<input checked="" type="checkbox"/> DNS default
Application Control	<input checked="" type="checkbox"/> APP default
IPS	<input checked="" type="checkbox"/> IPS protect_client
File Filter	<input type="checkbox"/>
Email Filter	<input checked="" type="checkbox"/> EF default
VoIP	<input checked="" type="checkbox"/> VOIP default
SSL Inspection	<input type="checkbox"/> SSL certificate-inspection
Logging Options	
Log Allowed Traffic	<input type="checkbox"/> Security Events <input checked="" type="checkbox"/> All Sessions

© Fortinet Inc. All Rights Reserved.

Důkladná inspekce = nízká propustnost?

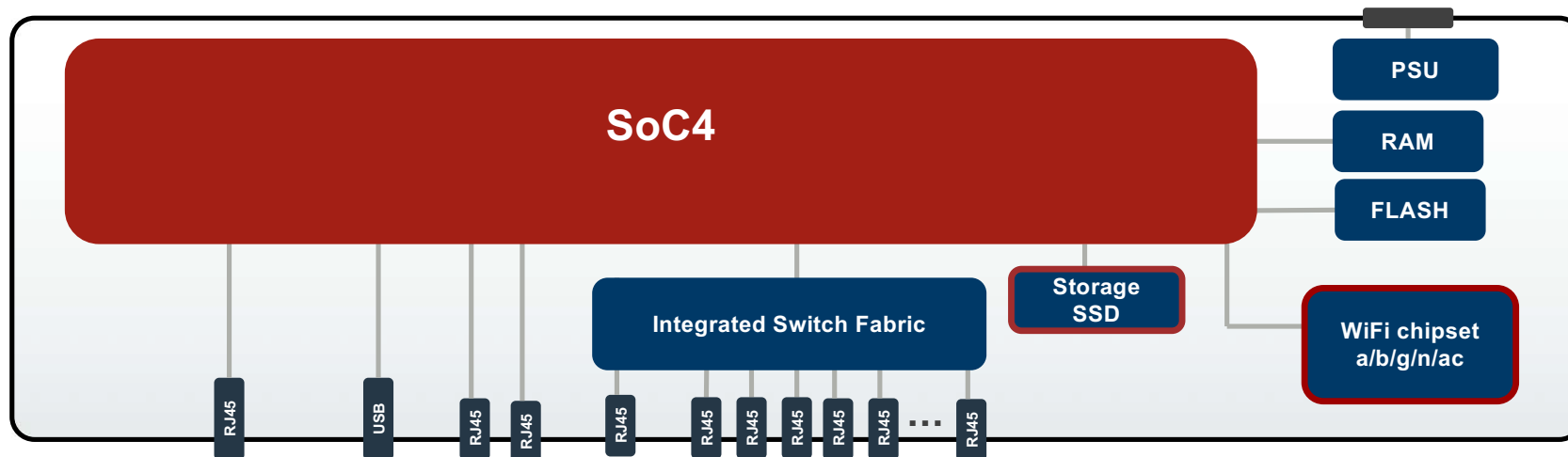
- CPU architektura vs. HW akcelerovaná platforma
- Akcelerace L2 – L7 inspekce, IPv4 i IPv6
- Akcelerace symetrické a asymetrické kryptografie
- Akcelerace mitigace DoS útoků
- Akcelerace multicast provozu, CAPWAP, VXLAN, GTP
- Velmi nízká latence (jednotky μ s)
- Velmi nízká spotřeba elektrické energie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



Důkladná inspekce = nízká propustnost?



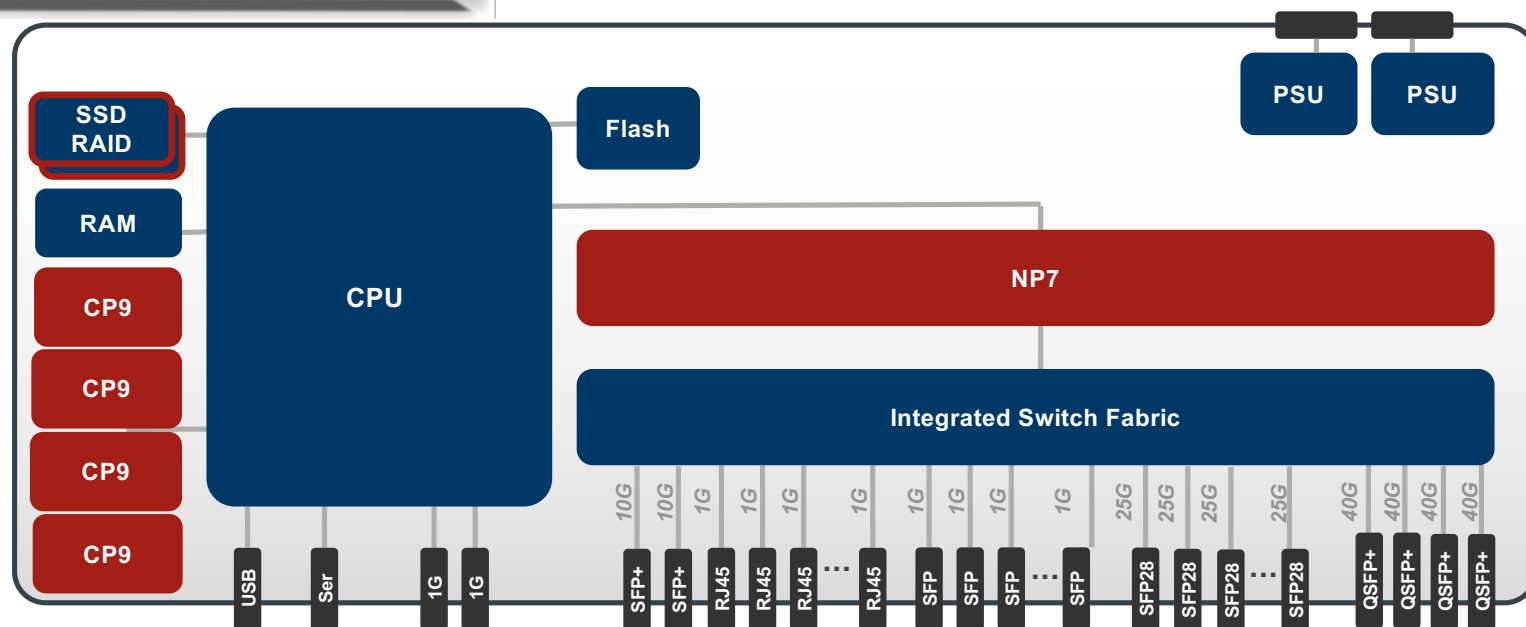
Firewall	IPS	NGFW	Threat Protection
10 Gbps	1.4 Gbps	1 Gbps	700 Mbps



Důkladná inspekce = nízká propustnost?

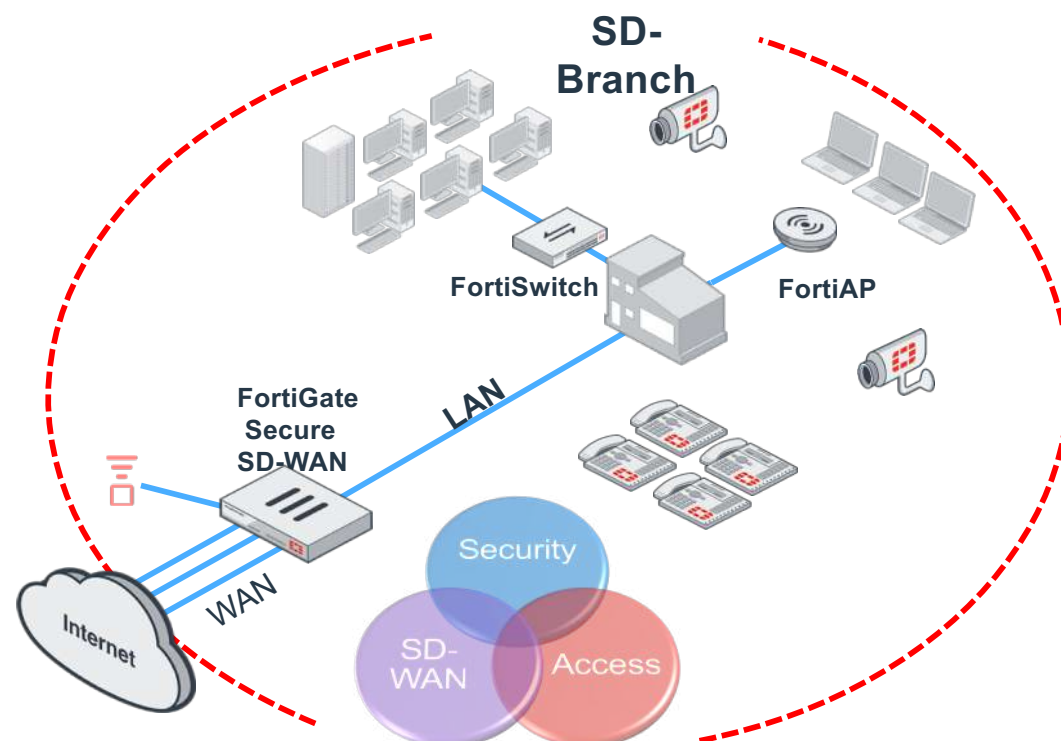


Firewall	IPS	NGFW	Threat Protection
198 Gbps	13 Gbps	11 Gbps	9.1 Gbps

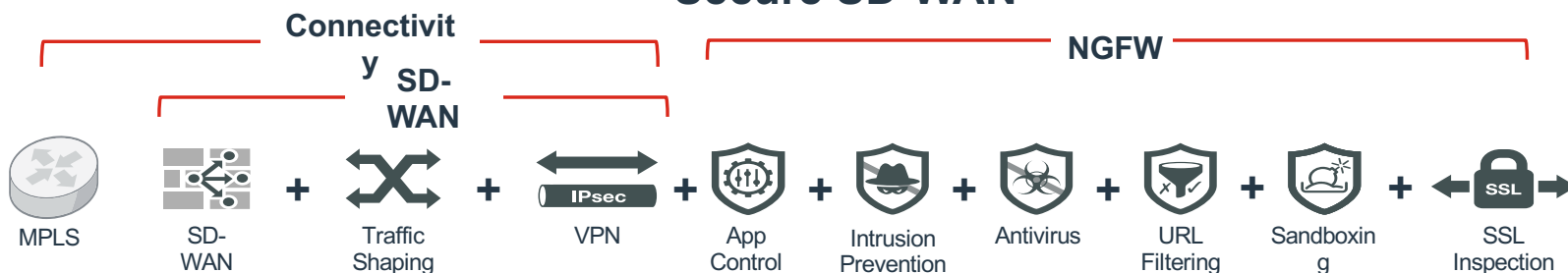


Secure SD - Branch

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



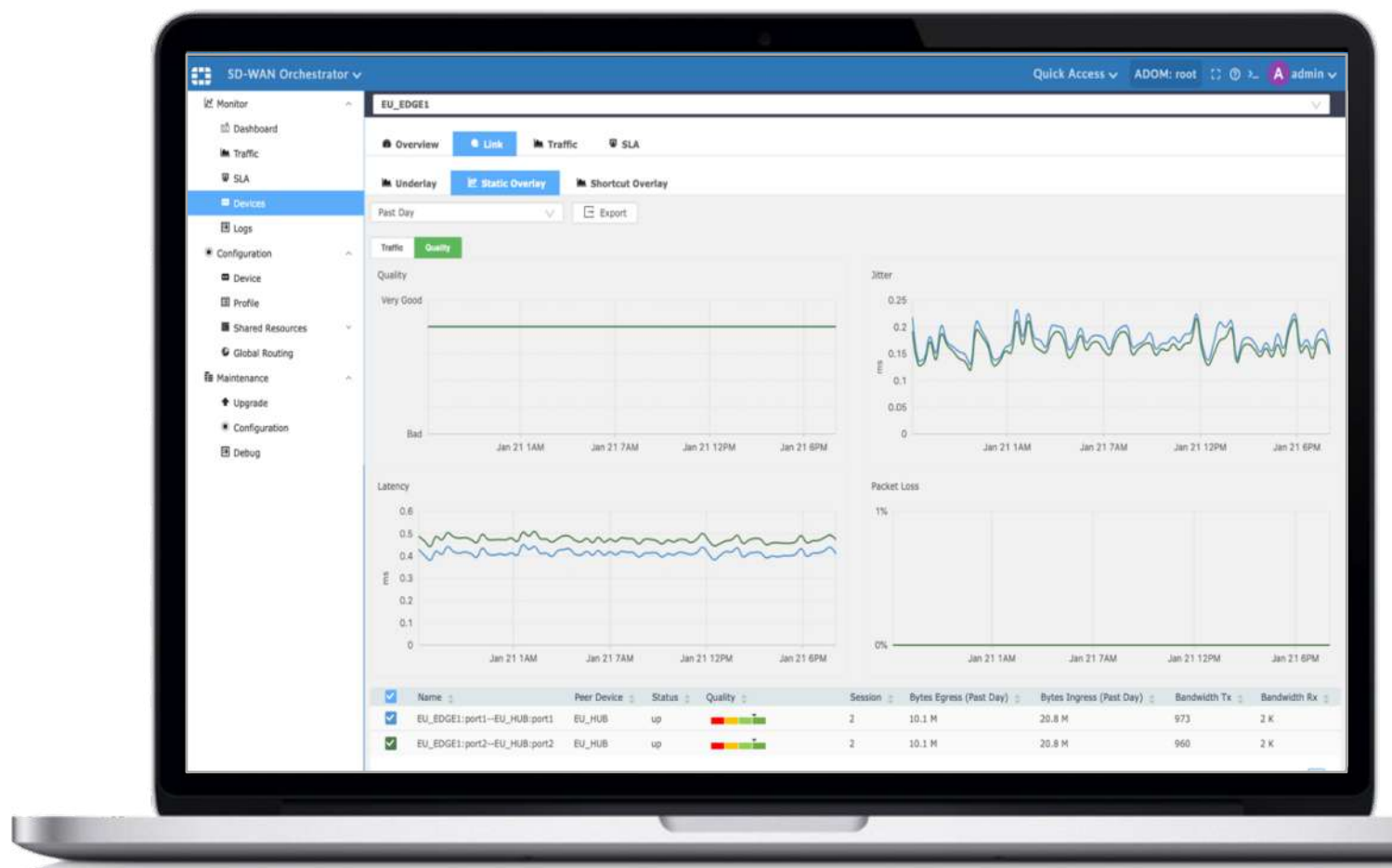
Secure SD-WAN



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

