Network project

Maciej Piotrowski

Junior Network Engineer

https://github.com/trojan8131

Contact: maciek8131@protonmail.com

1 Project assumptions

Klient

- Trade company would like to start a business in Poland, you signed a contract with this client for comprehensive IT infrastructure service, the network infrastructure will be built "from scratch"

4 Locations

- Poznań
- Wrocław
- Warszawa
- Data Center

Office

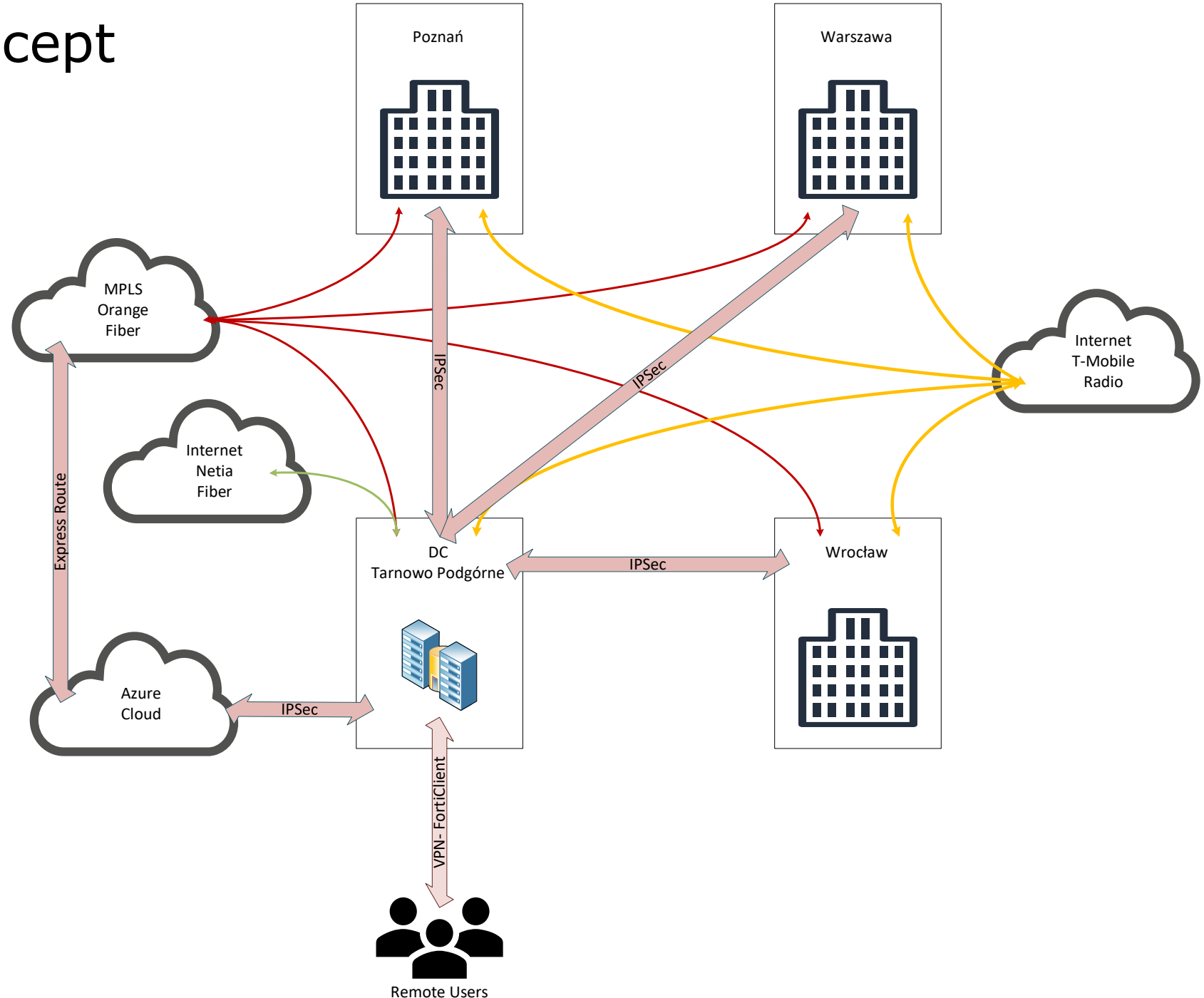
- 200 Users
- 20 Printers
- 15 Access Points

Data Center

- System SAP HANA for 450 users
- DMZ for web systems
- Active Directory for 600 users
- Cloud Azure
- Remote access for 600 users

2 General concept

General concept

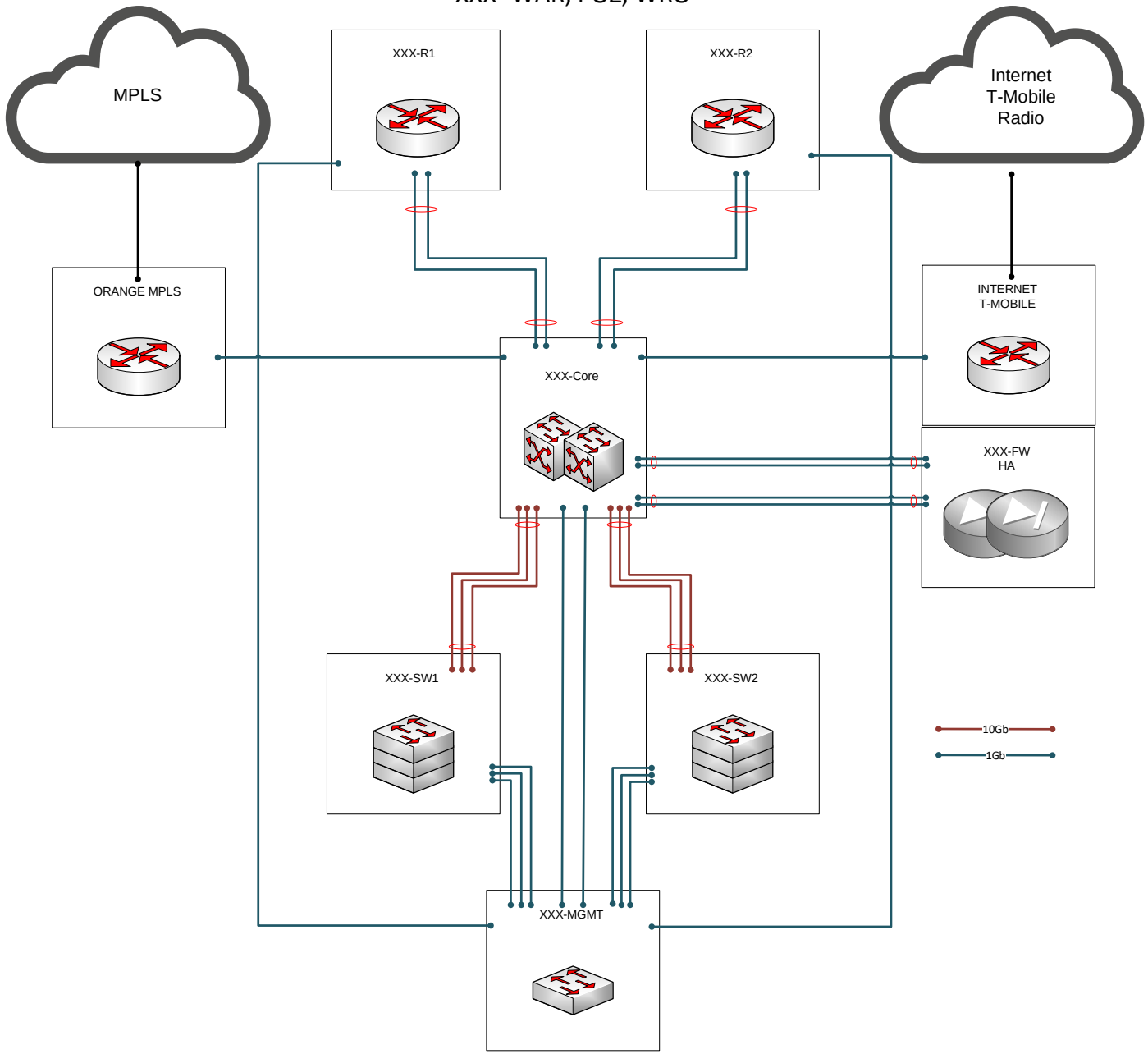


3 Offices

Layer 2 for offices
XXX- POZ,WRO,WAR

Device name	Device model	Ports
XXX-CORE	2x C9300X-12Y-A	12xSFP28
XXX-R1	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
XXX-R2	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
XXX-SW1	3x C9200L-48P-4X	48x1GE RJ45 + 4xSFP+
XXX-SW2	3x C9200L-48P-4X	48x1GE RJ45 + 4xSFP+
XXX-MGMT	C9200L-24P	24x1GE RJ45
XXX-FW	2xFG-40F	10xSFP+ + 18xGE RJ45
XXX-APXX	15x9105 AP	5x GE RJ45

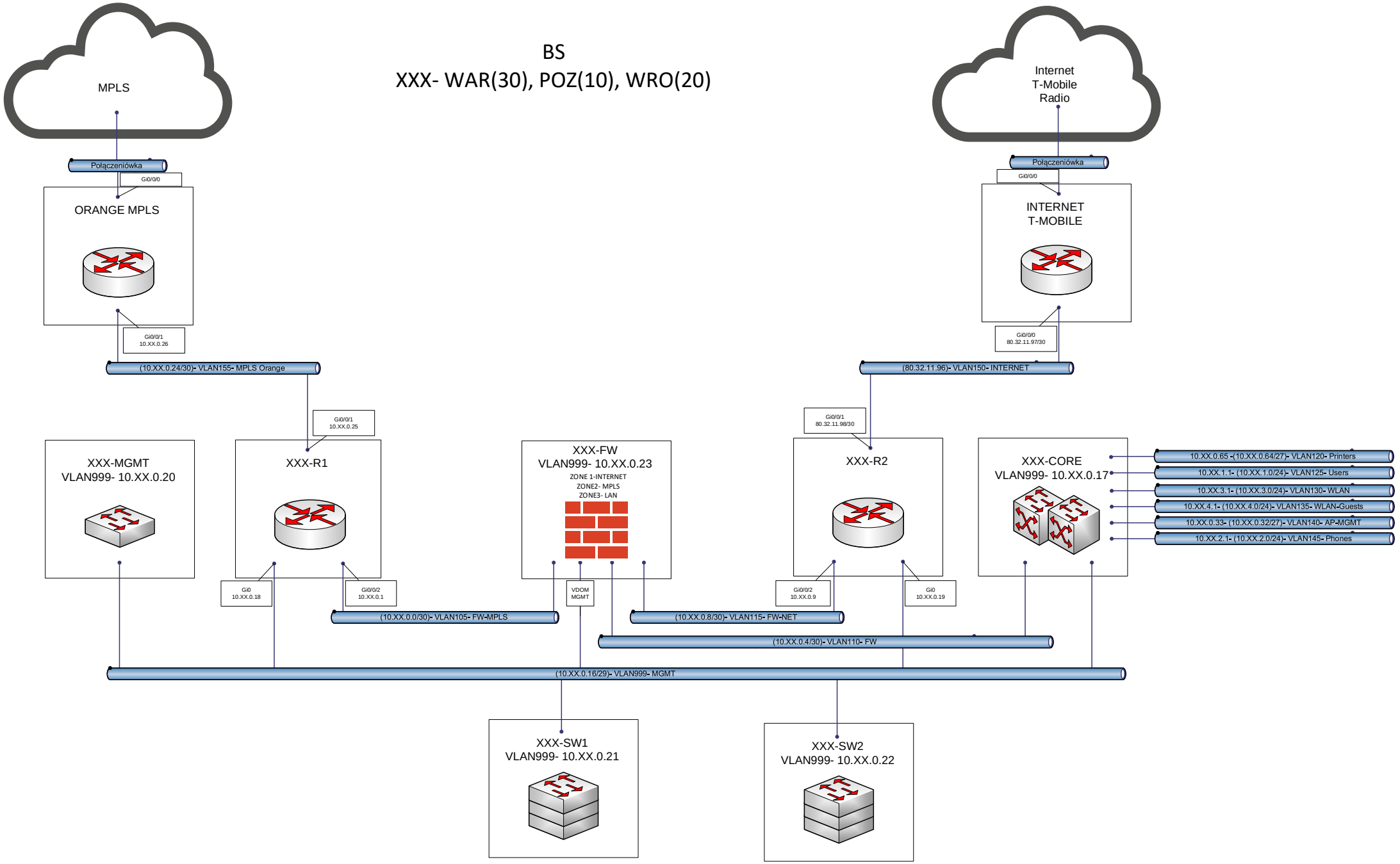
BS
XXX- WAR, POZ, WRO



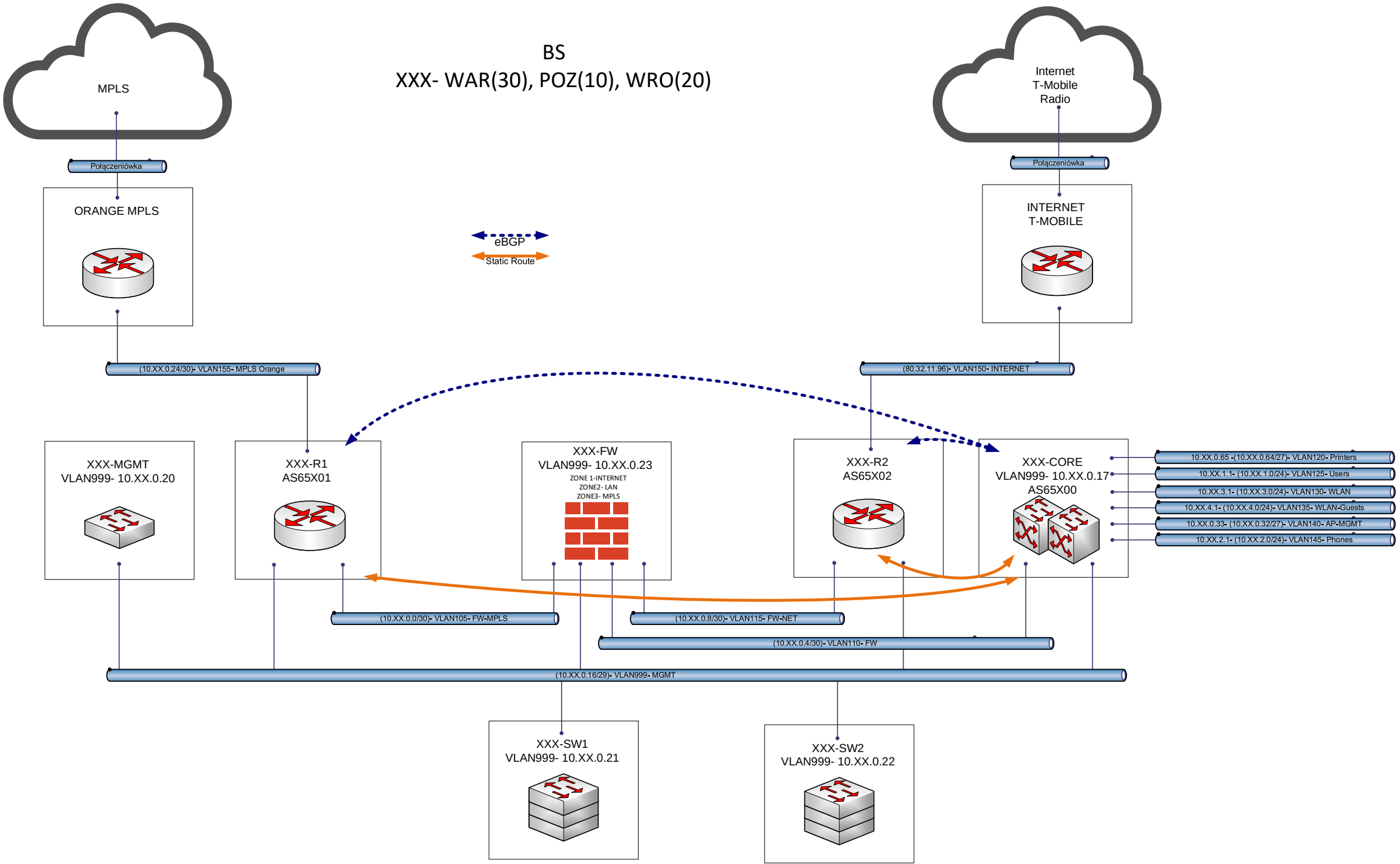
Layer 3 for single office

Name	Network address	Prefix	Hosts	First host	Last host	Broadcast
VLAN105- FW-MPLS	10.10.0.0	30	2	10.10.0.1	10.10.0.2	10.10.0.3
VLAN110- FW	10.10.0.4	30	2	10.10.0.5	10.10.0.6	10.10.0.7
VLAN115- FW-NET	10.10.0.8	30	2	10.10.0.9	10.10.0.10	10.10.0.11
VLAN120- PRINTERS	10.10.0.64	27	30	10.10.0.65	10.10.0.94	10.10.0.95
VLAN125- USERS	10.10.1.0	24	254	10.10.1.1	10.10.1.254	10.10.1.255
VLAN130- WLAN	10.10.3.0	24	254	10.10.3.1	10.10.3.254	10.10.3.255
VLAN135- WLAN_GUESTS	10.10.4.0	24	254	10.10.4.1	10.10.4.254	10.10.4.255
VLAN140- AP-MGMT	10.10.0.32	27	30	10.10.0.33	10.10.0.62	10.10.0.63
VLAN145- PHONES	10.10.2.0	24	254	10.10.2.1	10.10.2.254	10.10.2.255
VLAN150- INTERNET	80.32.11.96	30	2	80.32.11.97	80.32.11.98	80.32.11.99
VLAN155- MPLS	10.10.0.24	30	2	10.10.0.24	10.10.2.25	10.10.2.26
VLAN999- MGMT	10.10.0.16	29	6	10.10.0.17	10.10.0.22	10.10.0.23

BS
XXX- WAR(30), POZ(10), WRO(20)



BS
XXX- WAR(30), POZ(10), WRO(20)



External links

Orange VPN

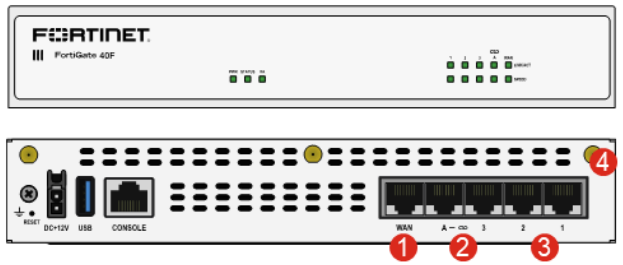
- It is an MPLS provided by Orange, it is used to connect the location with the WAN. The available bandwidth is 100Mbps.

Internet

T-Mobile

- Internet connection provided by radio link. 100Mbps bandwidth available. The link used for IPSec tunnels, which are the backup link. Internet access is not available locally, the Internet connection is in the Data Center.

FortiGate/FortiWiFi 40F



1. 1 x GE RJ45 WAN Port
2. 1 x GE RJ45 FortiLink Port
3. 3 x GE RJ45 Ports
4. WiFi Variant: 802.11a/b/g/n/ac W2

5 Gbps
Firewall throughput

35,000
New Sessions/Sec

700,000
Concurrent Sessions

310 Mbps
SSL Inspection Throughput

1 Gbps
IPS Throughput

800 Mbps
NGFW Throughput

600 Mbps
Threat Protection Throughput

Small Business / Remote Office
NGFW / Secure SD-WAN

FORTINET

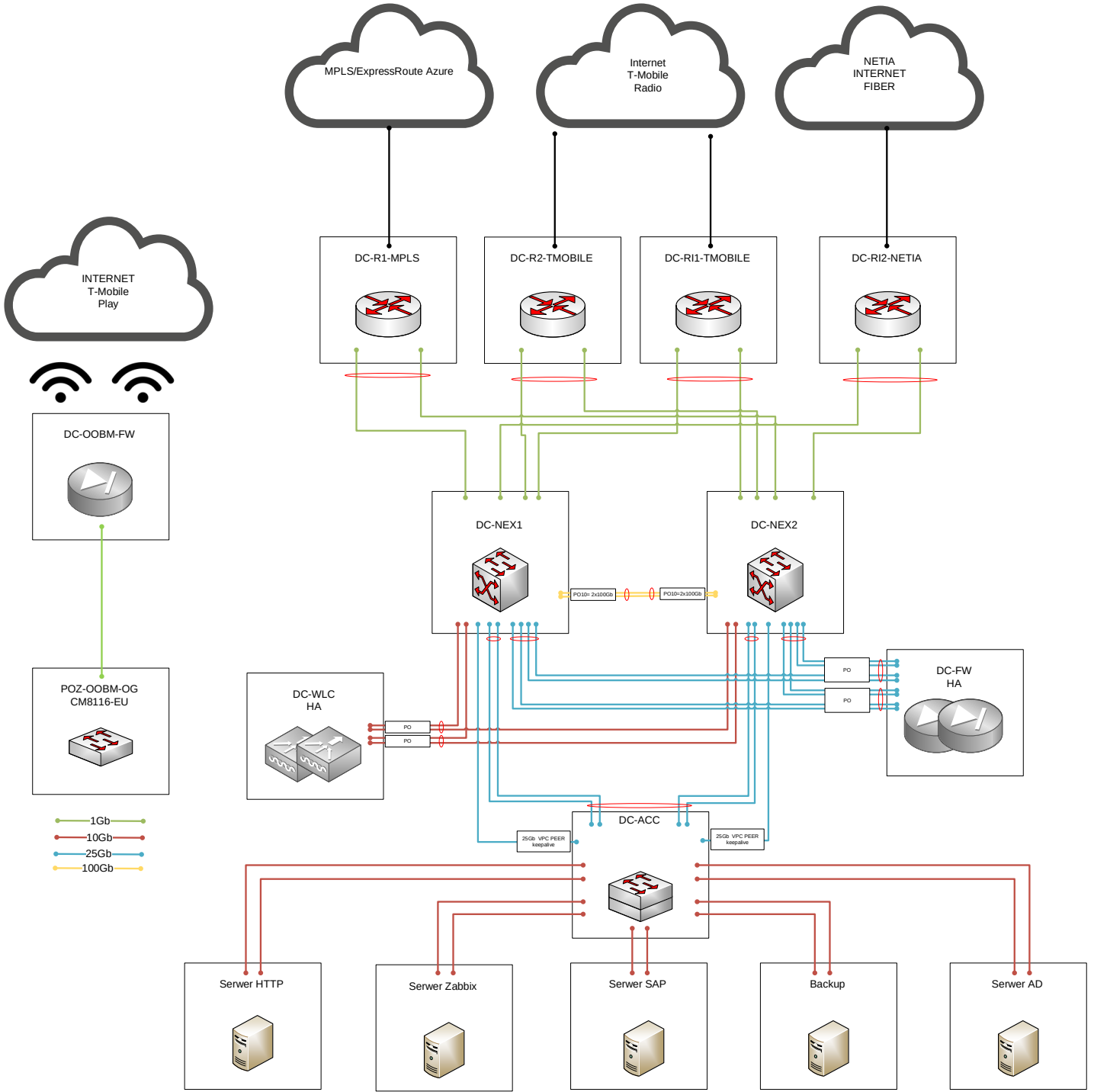
© Fortinet Inc. All Rights Reserved.

	FG/FWF-40F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps
IPS Throughput (Enterprise Mix) [2]	1 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	800 Mbps
Threat Protection Throughput (Ent. Mix) [2, 5]	600 Mbps
Firewall Latency	2.97 µs
Concurrent Sessions	700,000
New Sessions/Sec	35,000
Firewall Policies	5,000
Max G/W to G/W IPSEC Tunnels	200
Max Client to G/W IPSEC Tunnels	250
SSL VPN Throughput	490 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps
Application Control Throughput (HTTP 64K) [2]	990 Mbps
Max FortiAPs (Total / Tunnel)	16 / 8
Max FortiSwitches	8
Max FortiTokens	500
Virtual Domains (Default/Max)	10 / 10
Interfaces	5x GE RJ45
Local Storage	—
Power Supplies	Single AC PS
Form Factor	Desktop
Variants	WiFi, 3G4G

4 Data Center

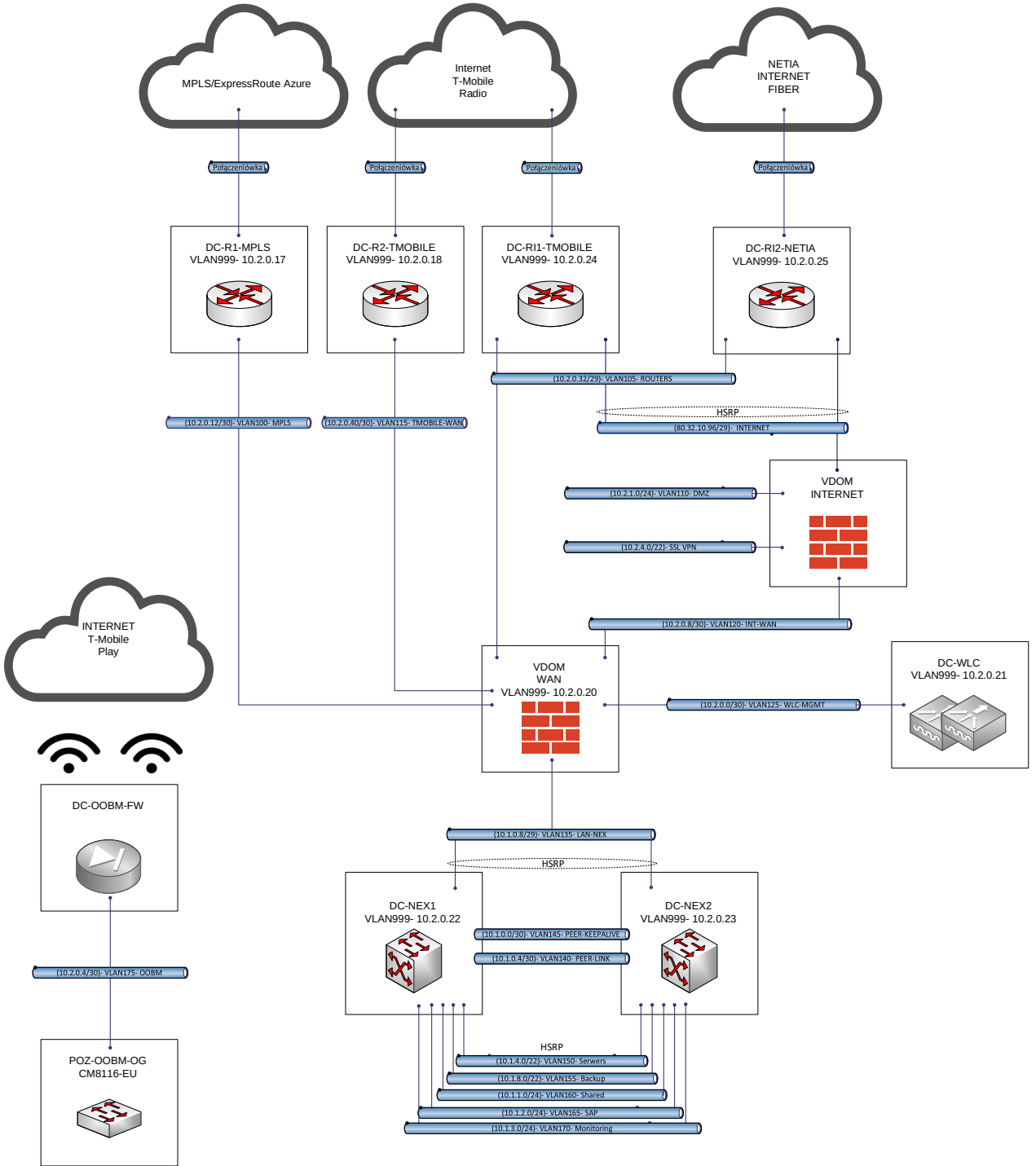
Layer 2

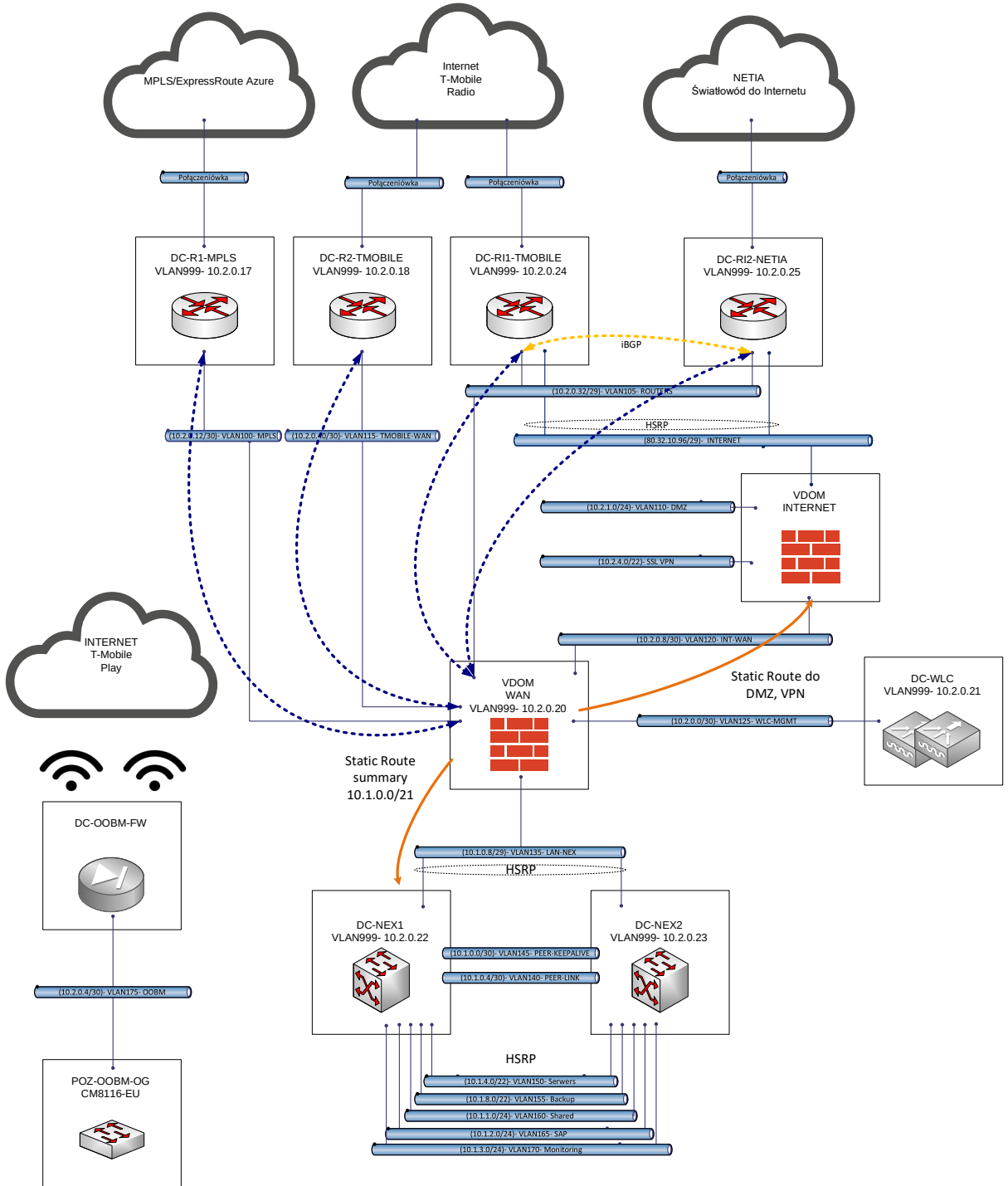
Location	Device name	Device model	Ports
DC	DC-R1-MPLS	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
DC	DC-R2-TMOBILE	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
DC	DC-RI1-TMOBILE	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
DC	DC-RI2-NETIA	CISCO ISR4331/K9	2x1GE RJ45 + 1xSFP + Combo Console/Aux port
DC	DC-NEX1	N9K-C93180YC-EX	48xSFP+ + 6xQSFP28
DC	DC-NEX2	N9K-C93180YC-EX	48xSFP+ + 6xQSFP28
DC	DC-WLC	2xC9800-L-C-K9	4xGE RJ45 + 2x10G RJ45, Maks 250 AP
DC	DC-FW	2xFortinet Firewall 1100E	2xQSFP+ (40G) + 4xSFP28 + 4xSFP+ + 8xSFP + 16xGE RJ45
DC	DC-ACC	2xC9300X-12Y-A	12xSFP28
DC	DC-OOBM-OG	CM8116-EU	16X1GE RJ45
DC	DC-OOBM-FW	FG-40F-3G4G	5xGE RJ45 + 2xSIM Slot


MPLS/ExpressRoute Azure
Internet
T-Mobile
Radio
NETIA
INTERNET
FIBER
INTERNET
T-Mobile
Play
DC-R1-MPLS
DC-R2-TMOBILE
DC-RI1-TMOBILE
DC-RI2-NETIA
DC-OOBM-FW
DC-NEX1
DC-NEX2
PO10= 2x100Gb
PO10=2x100Gb
DC-FW
HA
DC-WLC
HA
PO
PO
POZ-OOBM-OG
CM8116-EU
DC-ACC
25Gb VPC PEER
keepalive
1Gb
10Gb
25Gb
100Gb
Serwer HTTP
Serwer Zabbix
Serwer SAP
Backup
Serwer AD

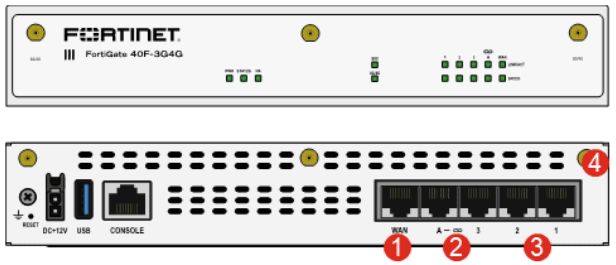
Layer 3

Name	Network Address	Prefix	Number of hosts	First host	Last host	Broadcast
VLAN145- PEER-KEEPALIVE	10.1.0.0	30	2	10.1.0.1	10.1.0.2	10.1.0.3
VLAN140- PEER-LINK	10.1.0.4	30	2	10.1.0.5	10.1.0.6	10.1.0.7
VLAN135- LAN-NEX	10.1.0.8	29	6	10.1.0.9	10.1.0.14	10.1.0.15
VLAN160- Shared	10.1.1.0	24	254	10.1.1.1	10.1.1.254	10.1.1.255
VLAN165- SAP	10.1.2.0	24	254	10.1.2.1	10.1.2.254	10.1.2.255
VLAN170- Monitoring	10.1.3.0	24	254	10.1.3.1	10.1.3.254	10.1.3.255
VLAN150- Serwers	10.1.4.0	24	254	10.1.4.1	10.1.4.254	10.1.4.255
VLAN155- Backup	10.1.5.0	24	254	10.1.5.1	10.1.5.254	10.1.5.255
		SUMMARY	10.1.0.0/20			
Name	**Network Address**	**Prefix**	**Number of hosts**	**First host**	**Last host**	**Broadcast**
VLAN125- WLC-MGMT	10.2.0.0	30	2	10.2.0.1	10.2.0.2	10.2.0.3
VLAN175- OOBM	10.2.0.4	30	2	10.2.0.5	10.2.0.6	10.2.0.7
VLAN120- INT-WAN	10.2.0.8	30	2	10.2.0.9	10.2.0.10	10.2.0.11
VLAN100- MPLS	10.2.0.12	30	2	10.2.0.13	10.2.0.14	10.2.0.15
VLAN999- MGMT	10.2.0.16	28	14	10.2.0.17	10.2.0.30	10.2.0.31
VLAN110- DMZ	10.2.1.0	24	254	10.2.1.1	10.2.1.254	10.2.1.255
VLAN105- ROUTERS	10.2.0.32	29	6	10.2.0.33	10.2.0.38	10.2.0.39
VLAN115- TMOBILE-WAN	10.2.0.40	30	2	10.2.0.41	10.2.0.42	10.2.0.43
VPN	10.2.4.0	22	1022	10.2.4.1	10.2.7.254	10.2.7.255
INTERNET	80.32.10.96	29	6	80.32.10.97	80.32.10.102	80.32.10.103

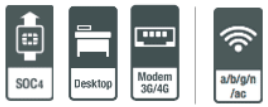

MPLS/ExpressRoute Azure
Internet
T-Mobile
Radio
NETIA
INTERNET
FIBER
Połączeniówka
Połączeniówka
Połączeniówka
Połączeniówka
DC-R1-MPLS
VLAN999- 10.2.0.17
DC-R2-TMOBILE
VLAN999- 10.2.0.18
DC-RI1-TMOBILE
VLAN999- 10.2.0.24
DC-RI2-NETIA
VLAN999- 10.2.0.25
(10.2.0.32/29)- VLAN105- ROUTERS
HSRP
(80.32.10.96/29)- INTERNET
(10.2.0.12/30)- VLAN100- MPLS
(10.2.0.40/30)- VLAN115- TMOBILE-WAN
VDOM
INTERNET
(10.2.1.0/24)- VLAN110- DMZ
(10.2.4.0/22)- SSL VPN
INTERNET
T-Mobile
Play
(10.2.0.8/30)- VLAN120- INT-WAN
VDOM
WAN
VLAN999- 10.2.0.20
DC-WLC
VLAN999- 10.2.0.21
(10.2.0.0/30)- VLAN125- WLC-MGMT
DC-OOBM-FW
(10.1.0.8/29)- VLAN135- LAN-NEX
HSRP
DC-NEX1
VLAN999- 10.2.0.22
DC-NEX2
VLAN999- 10.2.0.23
(10.1.0.0/30)- VLAN145- PEER-KEEPALIVE
(10.1.0.4/30)- VLAN140- PEER-LINK
(10.2.0.4/30)- VLAN175- OOBM
HSRP
(10.1.4.0/22)- VLAN150- Serwers
(10.1.8.0/22)- VLAN155- Backup
(10.1.1.0/24)- VLAN160- Shared
(10.1.2.0/24)- VLAN165- SAP
(10.1.3.0/24)- VLAN170- Monitoring
POZ-OOBM-OG
CM8116-EU


MPLS/ExpressRoute Azure
Internet
T-Mobile
Radio
NETIA
Światłowód do Internetu
Połączeniówka
Połączeniówka
Połączeniówka
Połączeniówka
DC-R1-MPLS
VLAN999- 10.2.0.17
DC-R2-TMOBILE
VLAN999- 10.2.0.18
DC-RI1-TMOBILE
VLAN999- 10.2.0.24
DC-RI2-NETIA
VLAN999- 10.2.0.25
iBGP
(10.2.0.32/29)- VLAN105- ROUTERS
HSRP
(80.32.10.96/29)- INTERNET
(10.2.0.12/30)- VLAN100- MPLS
(10.2.0.40/30)- VLAN115- TMOBILE-WAN
VDOM
INTERNET
(10.2.1.0/24)- VLAN110- DMZ
(10.2.4.0/22)- SSL VPN
INTERNET
T-Mobile
Play
(10.2.0.8/30)- VLAN120- INT-WAN
VDOM
WAN
VLAN999- 10.2.0.20
Static Route do
DMZ, VPN
DC-WLC
VLAN999- 10.2.0.21
(10.2.0.0/30)- VLAN125- WLC-MGMT
Static Route
summary
10.1.0.0/21
DC-OOBM-FW
(10.1.0.8/29)- VLAN135- LAN-NEX
HSRP
DC-NEX1
VLAN999- 10.2.0.22
DC-NEX2
VLAN999- 10.2.0.23
(10.1.0.0/30)- VLAN145- PEER-KEEPALIVE
(10.1.0.4/30)- VLAN140- PEER-LINK
(10.2.0.4/30)- VLAN175- OOBM
HSRP
(10.1.4.0/22)- VLAN150- Serwers
(10.1.8.0/22)- VLAN155- Backup
(10.1.1.0/24)- VLAN160- Shared
(10.1.2.0/24)- VLAN165- SAP
(10.1.3.0/24)- VLAN170- Monitoring
POZ-OOBM-OG
CM8116-EU

FortiGate/FortiWiFi 40F-3G4G



① 1 x GE RJ45 WAN Port
② 1 x GE RJ45 FortiLink Port
③ 3 x GE RJ45 Ports
④ WiFi Variant: 802.11a/b/g/n/ac W2



5 Gbps
Firewall throughput

1 Gbps
IPS Throughput

35,000
New Sessions/Sec

700,000
Concurrent Sessions

800 Mbps
NGFW Throughput

310 Mbps
SSL Inspection Throughput

600 Mbps
Threat Protection Throughput

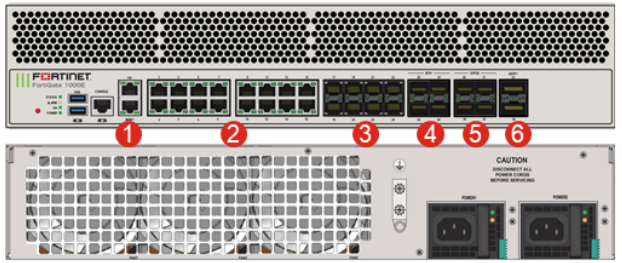
Small Business / Remote Office
NGFW / Secure SD-WAN

FORTINET

© Fortinet Inc. All Rights Reserved.

	FG/FWF-40F
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps
IPS Throughput (Enterprise Mix) [2]	1 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	800 Mbps
Threat Protection Throughput (Ent. Mix) [2, 5]	600 Mbps
Firewall Latency	2.97 µs
Concurrent Sessions	700,000
New Sessions/Sec	35,000
Firewall Policies	5,000
Max G/W to G/W IPSEC Tunnels	200
Max Client to G/W IPSEC Tunnels	250
SSL VPN Throughput	490 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps
Application Control Throughput (HTTP 64K) [2]	990 Mbps
Max FortiAPs (Total / Tunnel)	16 / 8
Max FortiSwitches	8
Max FortiTokens	500
Virtual Domains (Default/Max)	10 / 10
Interfaces	5x GE RJ45
Local Storage	—
Power Supplies	Single AC PS
Form Factor	Desktop
Variants	WiFi, 3G4G

FortiGate 1100E/-DC and 1101E



1. 2 x GE RJ45 MGMT/HA Ports
2. 16 x GE RJ45 Ports
3. 8 x GE SFP Slots
4. 4 x 10GE SFP+ Slots
5. 4 x 25GE SFP28/10GE SFP+ Slots
6. 2 x 40GE QSFP+ Slots

80 Gbps
Firewall throughput

500,000
New Sessions/Sec

8 Million
Concurrent Sessions

10 Gbps
SSL Inspection Throughput

12.5 Gbps
IPS Throughput

9.8 Gbps
NGFW Throughput

7.1 Gbps
Threat Protection Throughput

Large Enterprise / Data Center / SP
NGFW / ISFW / IPS / SWG / Mobile Security

FORTINET

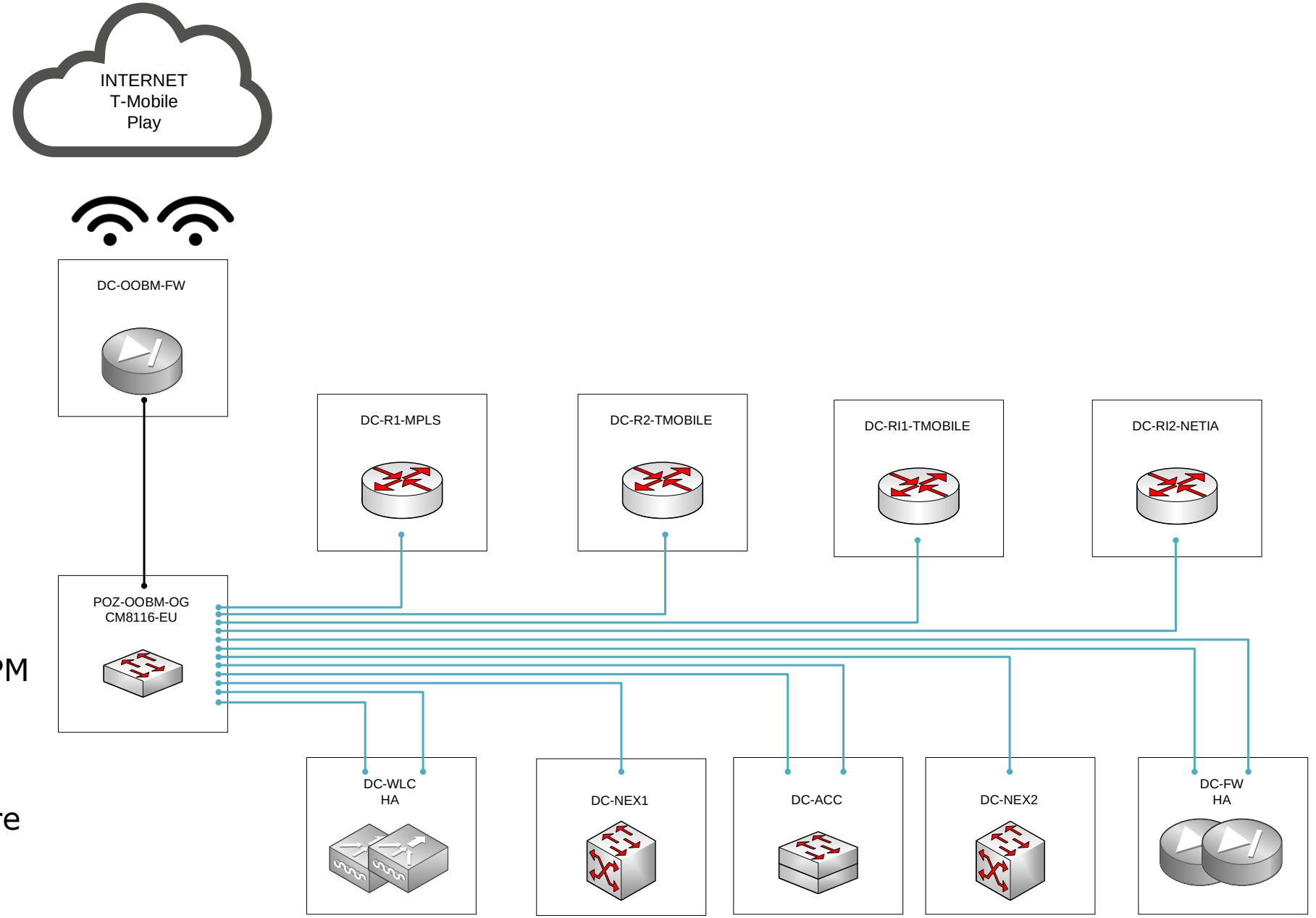
© Fortinet Inc. All Rights Reserved.

	FG-1100E
Firewall Throughput (1518/512/64 byte UDP)	80 / 80 / 45 Gbps
IPsec VPN Throughput (512 byte) [1]	48 Gbps
IPS Throughput (Enterprise Mix) [2]	12.5 Gbps
NGFW Throughput (Enterprise Mix) [2, 4]	9.8 Gbps
Threat Protection Throughput (Ent. Mix) [2, 5]	7.1 Gbps
Firewall Latency	2.76 µs
Concurrent Sessions	8 Million
New Sessions/Sec	500,000
Firewall Policies	100,000
Max G/W to G/W IPSEC Tunnels	20,000
Max Client to G/W IPSEC Tunnels	100,000
SSL VPN Throughput	8.4 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	10 Gbps
Application Control Throughput (HTTP 64K) [2]	26 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048
Max FortiSwitches	196
Max FortiTokens	20,000
Virtual Domains (Default/Max)	10 / 250
Interfaces	2× 40GE QSFP+, 4× 25GE SFP28, 4× 10GE SFP+, 8x GE SFP, 18x GE RJ45
Local Storage	960 GB (1101E)
Power Supplies	Dual PS
Form Factor	2 RU
Variants	DC

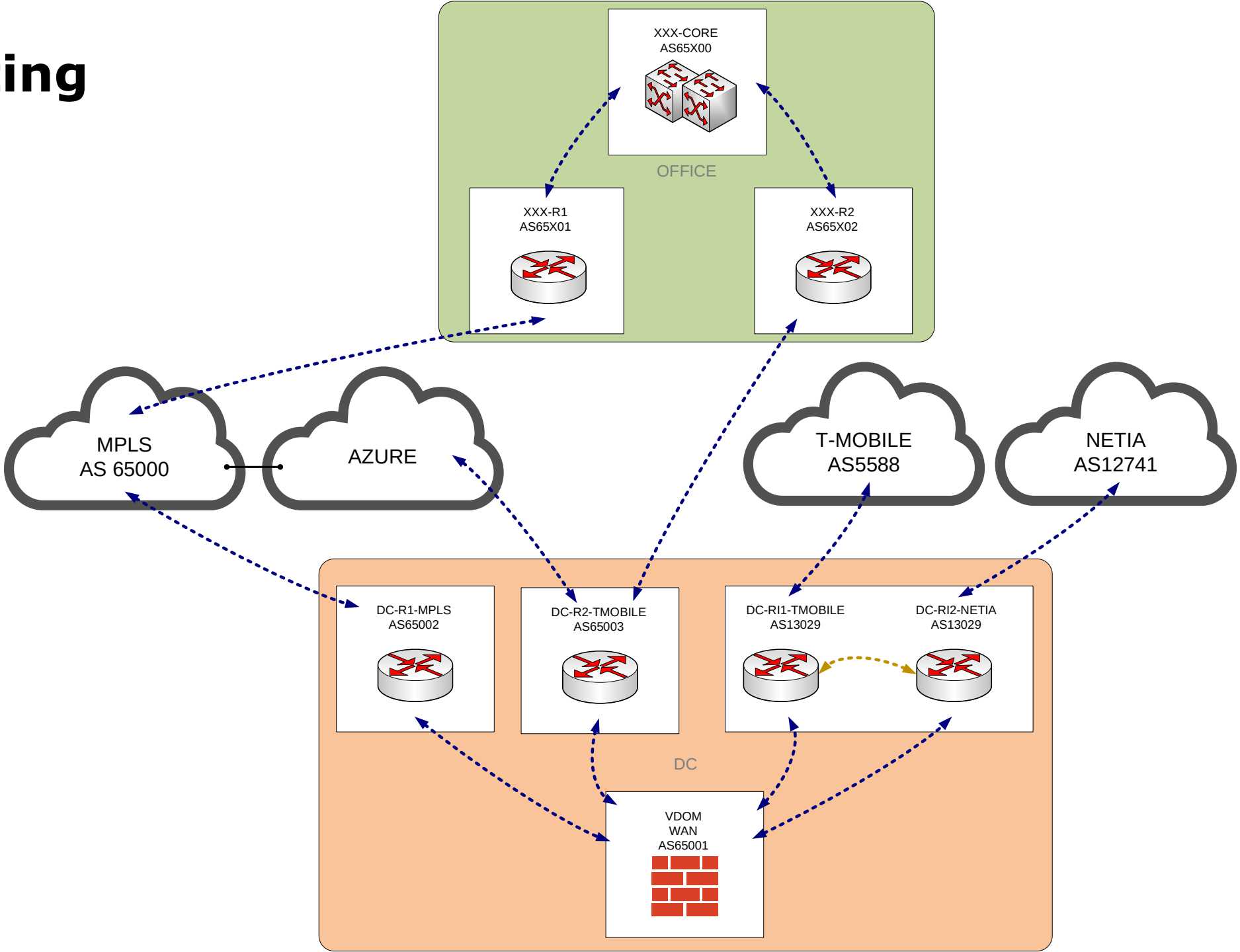
OOBM

OpenGear CM8116-EU

-Server with 16 ports of serial console with Smart OOB ™ function
-Built-in physical security via TPM 2.0 module
-Dual power supply with independent monitoring
-Integrated ambient temperature monitoring

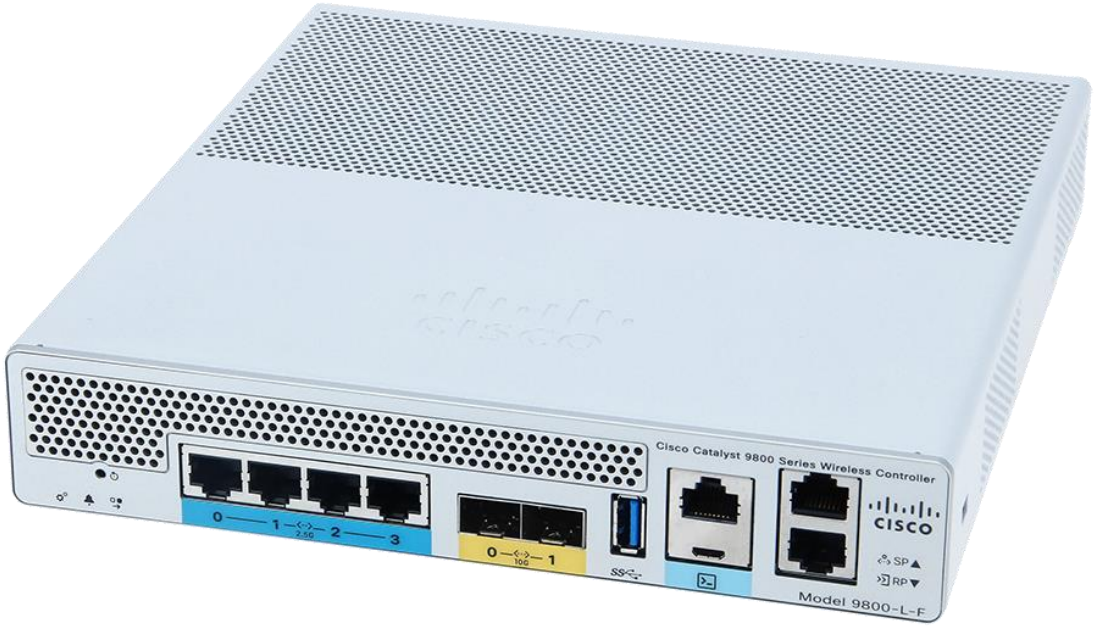


Routing


XXX-CORE
AS65X00
OFFICE
XXX-R1
AS65X01
XXX-R2
AS65X02
MPLS
AS 65000
AZURE
T-MOBILE
AS5588
NETIA
AS12741
DC-R1-MPLS
AS65002
DC-R2-TMOBILE
AS65003
DC-RI1-TMOBILE
AS13029
DC-RI2-NETIA
AS13029
DC
VDOM
WAN
AS65001

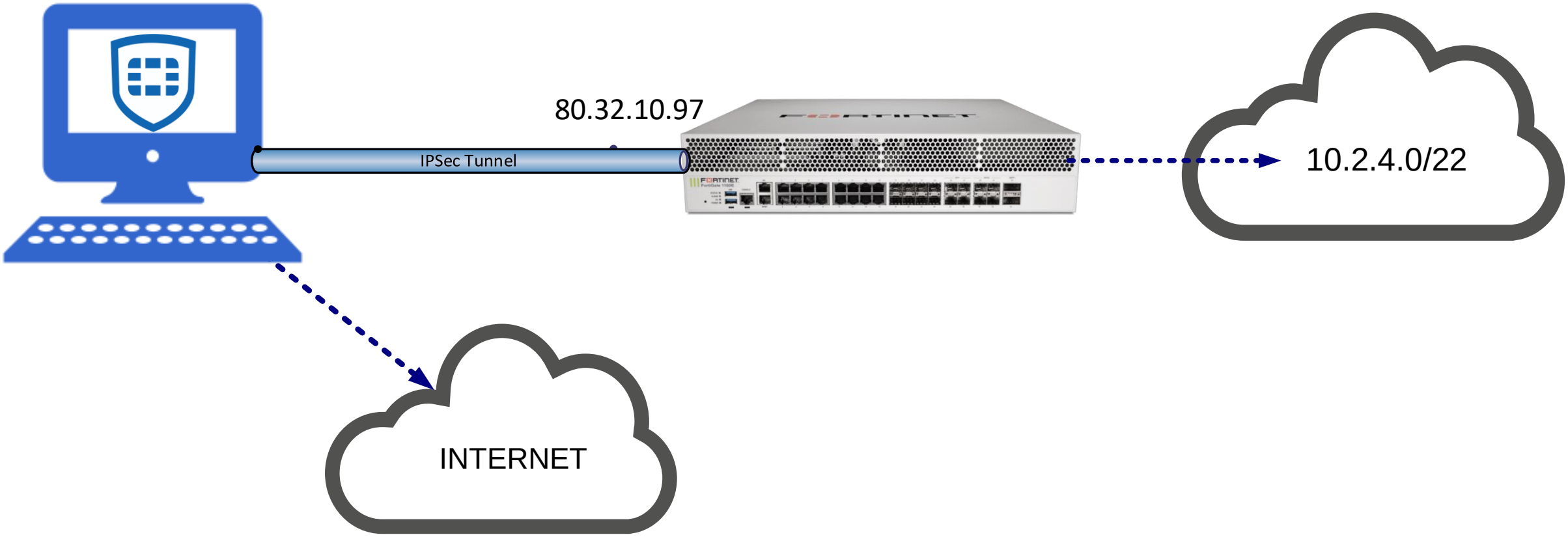
WLAN

Cisco C9105



Cisco C9800-L-F-K9

Remote Access- IPSec



Access to Cloud Azure
10.50.0.0/16

ExpressRoute

Orange- Primary link to Cloud Azure

VPN Tunnel as backup