

Lumen SASE with Fortinet

Technical Overview



Lumen SASE Overview

How the Lumen Platform enables SD-WAN & SASE

A platform modeled on SASE is only as good as its underlying infrastructure

The Lumen network is one of the largest, most connected and most deeply peered networks in the world:

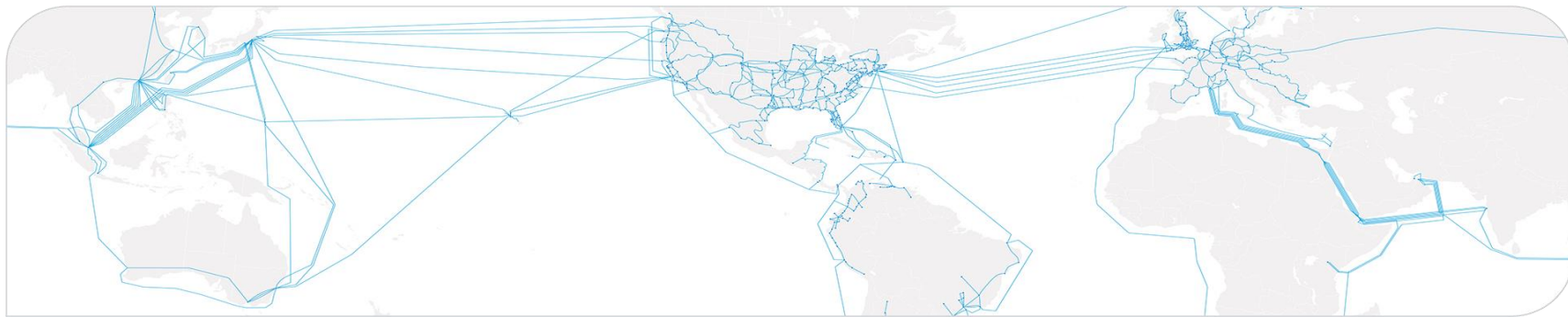
- ~450,000 route miles of fiber
- ~190,000 on-net fiber locations
- Services to customers in 60+ countries

The Lumen network is the #1 peered global network*:

- Dynamic connectivity to more than 2,200 public and private data centers
- Seamless access to all of the top cloud providers

Lumen excels at the edge to supercharge compute-intensive application experiences:

- More than 60 edge node deployments
- A dense metro IP network of PoPs
- Designed to deliver 5ms or less of latency to 95% of businesses in the U.S.



*CAIDA AS Ranking, May 2022

The Lumen Platform


Secure any-to-any connectivity

Combines expansive threat intelligence, connected cloud data centers, and leading security partner capabilities.

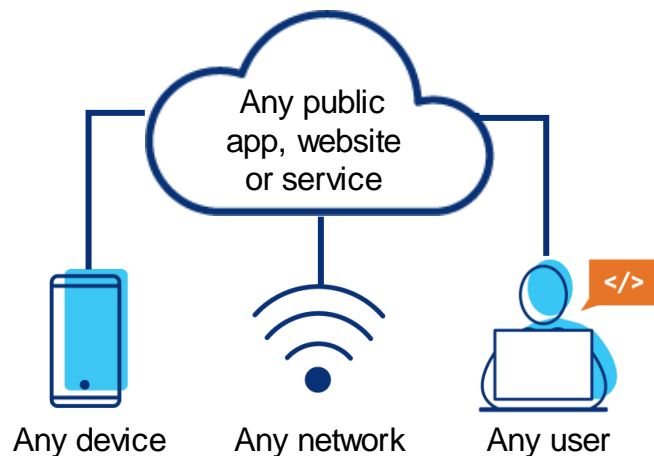
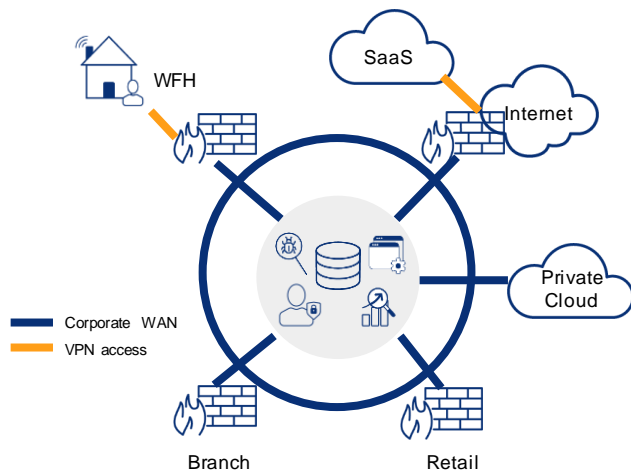
Provides secure access to work resources from virtually anywhere, on any device, at any time.

Through Black Lotus Labs[®], the Lumen Platform benefits from more than 200 billion NetFlow sessions, 1 billion DNS queries, and 2.3 million unique threats monitored every day.



**BLACK
LOTUS**  **LABS[®]**

Business has moved from walled garden to wild west



Yesterday's dedicated WAN

- Centralized control of data, apps, traffic, devices, and users
- Secure perimeter with appliance and software
- VPN access to corporate network assets
- Hairpin access through data center to public cloud SaaS and web services

Today's distributed reality

- Remote workers using unapproved devices and network access that avoids underperforming VPN
- Haphazard security protocols
- Shadow IT using unsupported cloud applications
- Workforce highly susceptible to malware, phishing, and botnet attack vectors

Lumen® SD-WAN & SASE evolution

- As more applications move to **Internet delivered SaaS**, traditional central internet egress suffers performance and capacity challenges

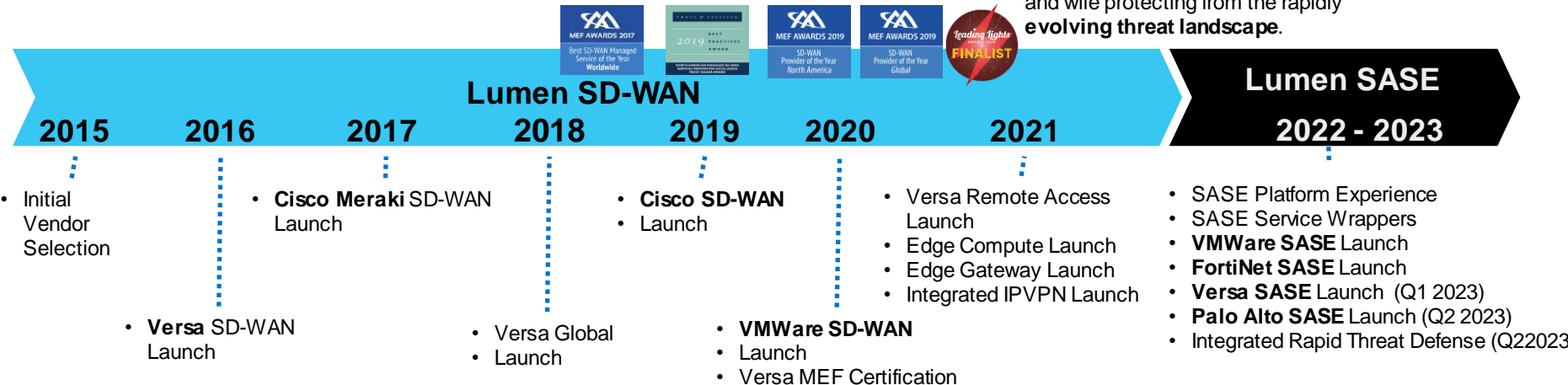
- Pandemic** makes **work from home** mainstream and organizations rush to handle remote worker traffic loads and address new security concerns quantity of devices outside the firewall

- How do you transform to a new technology while keep the lights on?
- How do network and security play in the same sandbox
- Increasing rate of change drives need for agility

- SD-WAN promises to lower network **costs** by enabling use of commodity internet circuits

- Organizations look to **distribute some/all internet egress** to the sites but struggle to keep their security posture

- Customers need an **integrated platform** that solves for both **premise and remote workers** accessing of **internal and external applications** and while protecting from the rapidly **evolving threat landscape**.



The Secure Access Service Edge (SASE) Pillars

Work from Anywhere and Multicloud are driving the next evolution in network security



SD-WAN

Most enterprises have already deployed or are planning to deploy SD-WAN

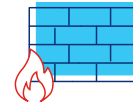
- Initially focused on cost optimization, improved management capabilities, application centric networking and the ability to better support multi-cloud architectures and SaaS
- Now an integral part of the go forward SASE architecture



Remote Access / ZTNA

Pandemic driven hybrid worker requirements have created a need to rethink and optimize how end users connect

- Currently deployed remote access solutions are data center centric and require redesign to support multi-cloud
- Capacity increase and scalability decisions were tactical, not strategic
- Enterprises want a common access platform that supports users no matter their location

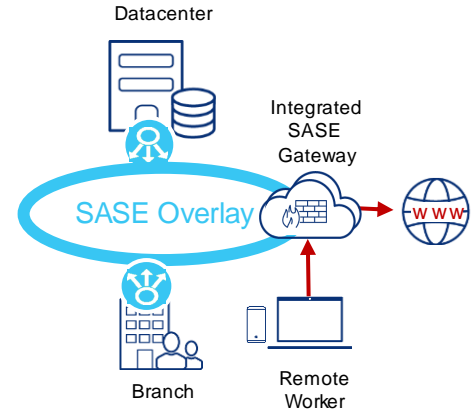
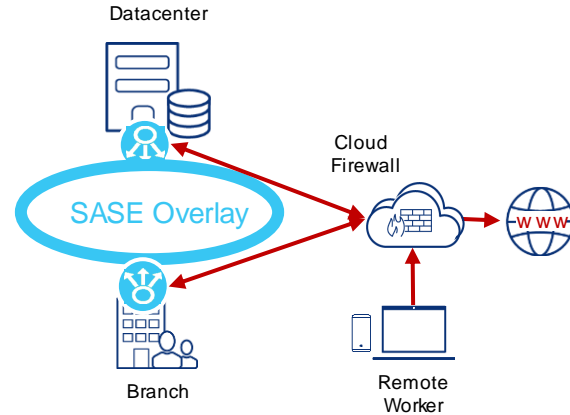
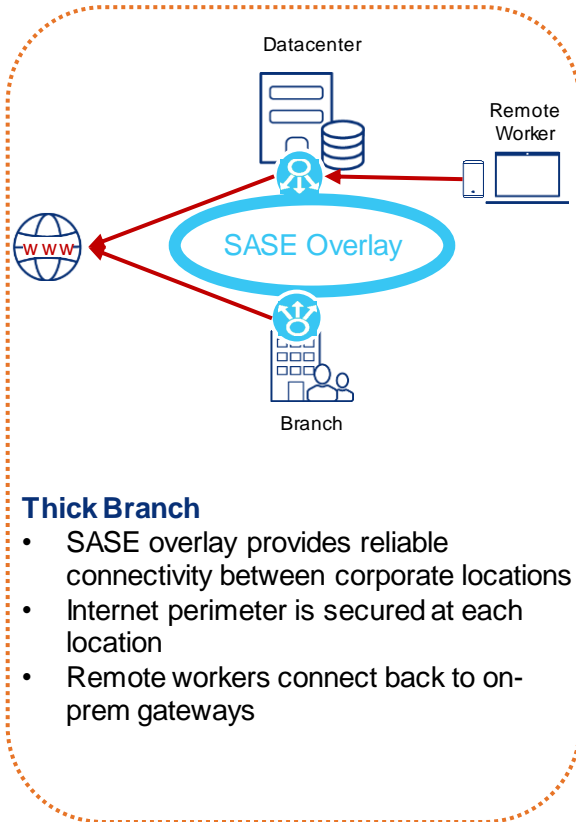


NGFW / SWG / CASB

Multi-cloud and Work-from-Anywhere introduces a need for full protection, no matter the source or destination

- Flexibility to deploy common security policy in the cloud or at the branch is seen as a requirement by many enterprises
- Operational complexity and risk are top concerns as IT executives reevaluate network security solutions

Sample SASE architectures



Thick Branch

- SASE overlay provides reliable connectivity between corporate locations
- Internet perimeter is secured at each location
- Remote workers connect back to on-prem gateways

Thin Branch w/ multi-vendor cloud security

- SASE overlay provides reliable connectivity between corporate locations
- Standard IPSec/GRE tunnels connect SASE Gateway to corporate locations
- Internet egress is secured by the SASE gateways
- Remote workers connect to cloud gateways and only backhaul to the corporate sites for internal resources

Thin Branch w/ Integrated cloud security

- SASE Overlay provides reliable connectivity between corporate locations **AND SASE Gateways**
- Internet egress is secured by SASE Gateways
- Remote workers connect to cloud gateways and only backhaul to corporate sites for internal resources



Fortinet Overview

WHO IS FORTINET?

Fortinet is a global leader in cybersecurity, delivering a broad, integrated and automated security fabric to enable customers to accelerate their digital journey.

\$3.09B
FY2020 Billing

Financially Stable

28B+ Market Cap (as of 2.21.21)
Nasdaq: FTNT

S&P 500

BBB+ Baa1
Security Investment Grade Rating

Leading the Cybersecurity Industry

50
Integrated Fabric Products

Broadest Attack Surface Coverage

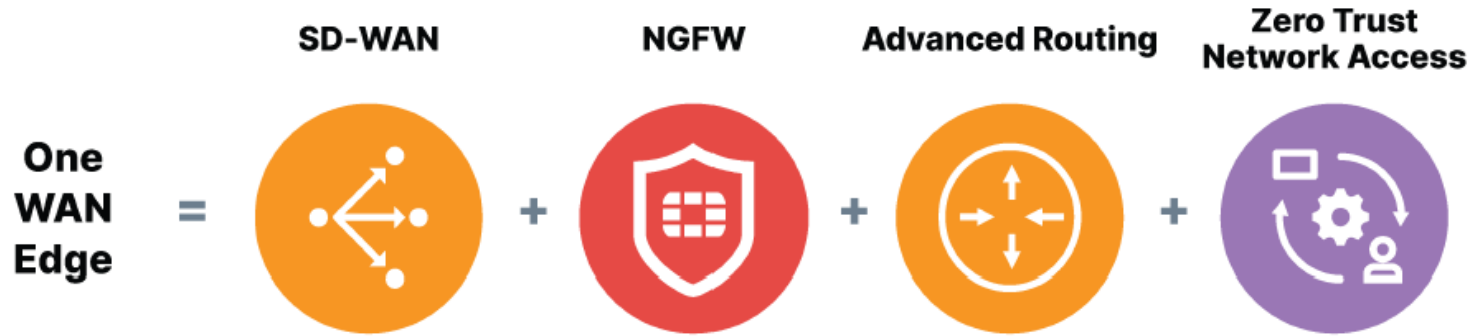
500,000+
Customers Worldwide

Massive Customer Input

600,000+
NSE Certifications

WEF Cybersecurity Founders

Fortinet Secure Access Service Edge (SASE)



One WAN Edge Powered by **One** OS, **One** Management

Fortinet is recognized as a Leader in 2 Gartner 2021 Magic Quadrant Reports:



Network Firewalls



WAN Edge Infrastructure

Fortinet is also recognized in 4 additional Gartner 2021 Magic Quadrant Reports, including a wide range of technologies:



Web Application and API Protection



SIEM



Wired and WLAN



Endpoint Protection Platforms*

And Fortinet is mentioned as a 'Vendor To Consider' in 2 additional Gartner 2021 Magic Quadrant Reports:



Secure Web Gateway



Indoor Location Services

And Fortinet is listed in 6 Gartner Market Guides



IDPS



Email



NAC



ZTNA



OT



SOAR

Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. *This report last publishes in 2019 and is provided here for historical purposes.

Materials: Lumen SASE with Fortinet

- **Co-branded Content Assets**

- Joint value prop
- Infographic
- Video
- Solution Brief
- Data Sheets
 - SD-WAN
 - FortiManager
 - FortiClient
 - FortiAnalyzer
- FAQs

Secure access for...

The digital revolution is here. Do you have secure, high performance access for your users?

- Remote Users**
Users need a seamless, secure experience as they move through hybrid workspaces.
- Expanding Attack Surface**
The perimeter is now your branch edges, endpoints, and cloud—increasing security risks.

Lumen SASE with Fortinet
Fully managed, fully integrated network and security converged experience.

- Next generation firewall as a service
- Secure SD-WAN
- Zero-trust network access (ZTNA)
- Threat intelligence and response

Fortinet Security Fabric
Unified management for strategic operations and mixed environments.

Fortinet Security Processing Units
Exceptional speed, throughput, and efficiency.

Lumen Platform
Global IP with local gateways + automation for high performance from edge-to-cloud.

Fortinet and Lumen are better together.

Fortinet
Secure networking for a hyperconnected world. Driving convergence to enable security at any network edge.

Lumen Technologies
Automated threat detection. Built-in protection. The platform with integrated security from the core to the edge.

Gartner
Fortinet is recognized as a LEADER in Gartner® 2021 Magic Quadrant™ Reports
Network Firewalls
WAN Edge Infrastructure

IDC
Fortinet is positioned as a leader in the 2021 IDC MarketScape for Worldwide SD-WAN Infrastructure

FORRESTER
Fortinet is positioned as a Strong Performer in The Forrester Wave™ Industrial Control Systems (ICS) Security Solutions, Q4 2021

FROST & SULLIVAN
Fortinet is one of the top vendors recognized in Frost & Sullivan's Frost Radar™ for email security, NAC, DNS, and SD-WAN.

LUMEN **FORTINET**

Lumen® SASE with Fortinet
A fully integrated network and security converged solution deployed at the edge, enabling a single, seamless, secure access experience.

A Wakeup Call to Distributed Businesses

Enterprise networks increasingly rely on cloud-based applications to run their businesses and support remote and mobile users. The enterprise network has grown beyond the conventional network edge, challenging IT to secure and manage an ever-expanding attack surface. VPN solutions alone are not enough to...

Failure to modernize infrastructure and invest in operations automation and intelligent security practices will severely impact business performance.

LUMEN **FORTINET**

Lumen® SASE Solutions with Fortinet Secure SD-WAN
A Unified WAN Edge, powered by a single OS, to transform and secure the WAN

Key Features

- World's only ASIC-accelerated SD-WAN
- 5000+ applications identified with real-time SSL inspection
- Self-healing capabilities for enhanced user experience
- Cloud on ramp for efficient SaaS adoption
- Simplified operations with NCC/PCC management and analytics
- Enhanced granular analytics for end-to-end visibility and control

Fortinet NSE (Network Security Expert) Program

Mission: Committed to training 1 million people worldwide by 2026



Authorized Training Centers

Supporting language and culture in training
in 136 countries and territories

[Cybersecurity Training information](#)

[Partner Portal Home](#)

Recommended for Lumen:

Sales & Sales Engineers

- [NSE 1-3: Security Awareness \(free online, self-paced\)](#)

Solution Engineers

- NSE 1-3: Security Awareness
 - Online immediate certification (free online, self-paced)
- NSE 4: FortiGate NGFW, Security and Infrastructure
 - \$400 to take certification test at PearsonVUE Testing Center (NSE4)
 - Lumen is EXPERT PARTNER: contact Jody for test voucher
- NSE 5 – 7 Modular, self-selection

2022 Xperts Summit, Nashville, TN – Oct 31 – Nov 4 | [Summit](#)

Jody Holmes, MSSP Systems Engineer

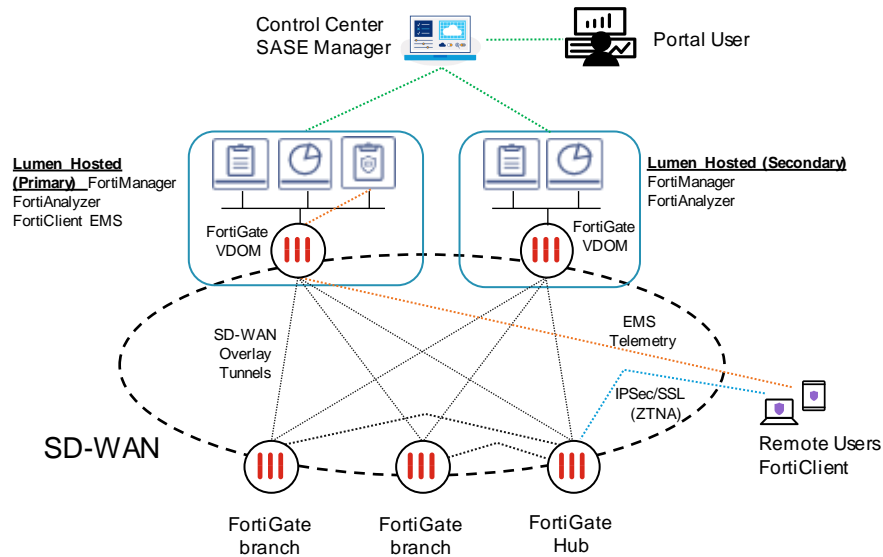
Enterprise, Commercial, SLED
501.428.3909
jholmes@fortinet.com

Sales & Solution Engineering support



Lumen SASE with Fortinet Service Overview

Lumen SASE with Fortinet Architecture



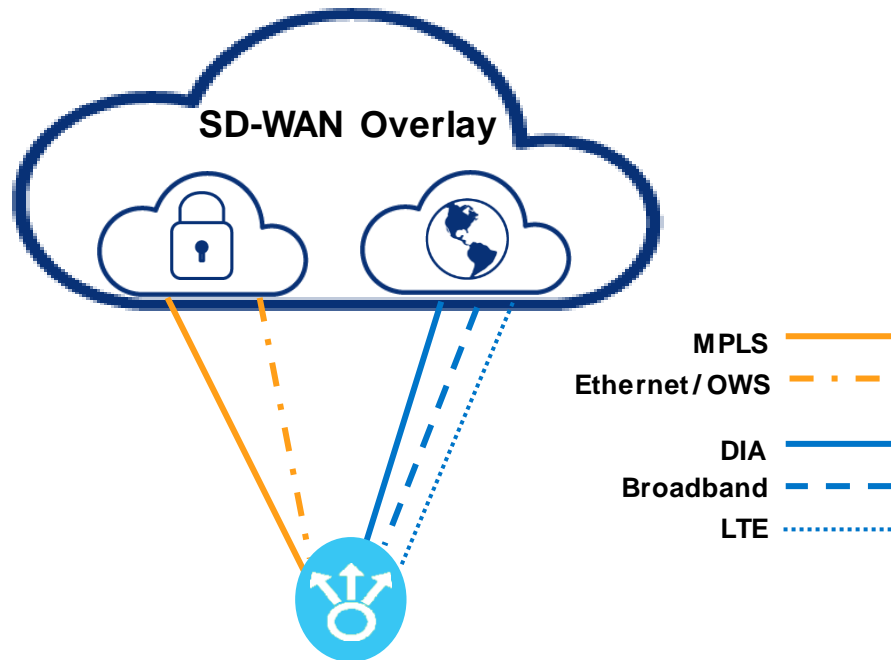
- **Secure, Redundant Centralized Orchestration**
 - **Control Center** – Manage inventory, billing, and ticketing of all your Lumen services
 - **SASE Manager** – Manage your SASE network and access Fortinet management Virtual Machines (VM)
 - **FortiManager** – Centralized FortiGate Orchestrator
 - Manage SASE policies
 - Monitor application performance
 - Identify and respond to security alerts
 - **FortiAnalyzer** – Centralized log collector / Analytics
 - **FortiClient Enterprise Management Server** – Centralized FortiClient / ZTNA management
 - **FortiGate** – Edge SASE appliance
 - **FortiClient** – Endpoint client software enabling secure, remote access to enterprise network.

Transport Options

Flexibility in Transport Providers

- Lumen provider
- Lumen aggregated
 - Cable / DSL / wireless
- Customer provided

Seamlessly mix and match transports based on site requirements

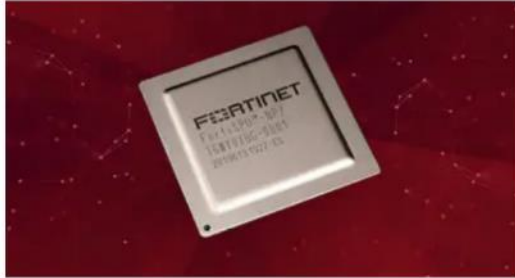


FortiGate Device Options

Size	Model	Description	Performance
Extra Small	40F	<ul style="list-style-type: none"> • Desktop model • 5 – GigE RJ45 ports • Optional Wi-Fi and 3G/4G LTE modem • Rack or wall mount option 	Up to 100Mbps bandwidth
Small	60F	<ul style="list-style-type: none"> • Desktop model • 10 – GigE RJ45 ports • Rack or wall mount options 	Up to 500Mbps bandwidth
Medium	100F	<ul style="list-style-type: none"> • Rack mount • 22 – GigE RJ45 ports • 4 – SFP ports • 2x – 10Gig SFP slots • Dual power supply 	Up to 1 Gbps bandwidth
Large	200F	<ul style="list-style-type: none"> • Rack mount • 18 – GigE RJ45 ports • 8 – GigE SFP slots • 4 – 10Gig SFP slots 	Up to 2 Gbps bandwidth
Extra Large	1800F	<ul style="list-style-type: none"> • Rack mount • 4 – 40Gig QSFP+ slots • 12 – 25GigE SFP28/10GigE SFP+ HA slots • 8 – GigE SFP slots, • 18 – GigE RJ45 ports • SPU NP7 and CP9 accelerated • Dual AC power supplies 	Up to 10 Gbps bandwidth



Innovative High Throughput Processors



NP7 runs at the network layer to speed functions that typically slow CPUs, such as IPv4, IPv6, unicast, and multicast. In addition, NP7 accelerates IPsec decryption, VXLAN termination, and address translation, while providing hardware logging and policy enforcement.

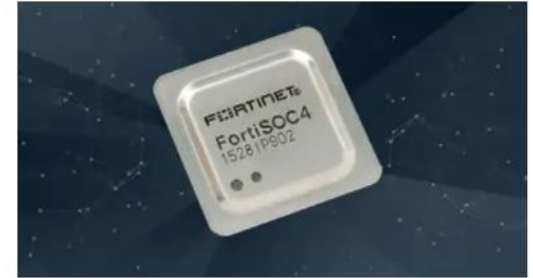
Single-session flow with 100 Gbps throughput needed for high-bandwidth sites.

Fortigate 1800F + Series



CP9 works as a CPU co-processor, taking on resource-intensive security functions such as Application Identification, IPS (pre-scan, signature correlation, etc.), and antivirus, so the CPU can perform other important tasks.

Fortigate 200F Series



SoC4 is a fully integrated set of security functions, including a Layer 7 firewall, on a fast and cost-effective chip. It meets the high-performance requirements for optimal end-user experience and secures branches deployed in SD-WAN environments.

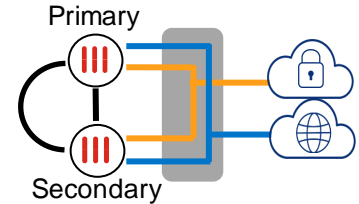
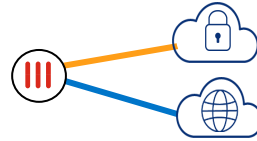
Fortigate 40F – 100F Series

FortiGate Deployment options

- Fortinet Appliances
 - ASIC accelerated SD-WAN
- Single Device or in HA Mode
 - Dual connected circuits
 - Requires Layer 2 WAN Edge
- Virtualized Instances (**Planned**)
 - Public Cloud
- Premise based virtual network function on Lumen Edge Gateway (uCPE) (**Planned**)

Appliances for any bandwidth requirement

150 Mbps
↕
10 Gbps



Google Cloud Platform



LUMEN®

Fortinet Application Steering

First Packet Classification

- First Packet Classification to efficiently assign Apps to specific WAN link
- Special database which dynamically updates cloud application IP address and port numbers

Session Classification

- Once identified via application control, subsequent matching sessions are identified when seen next time on first packet.

Application Control

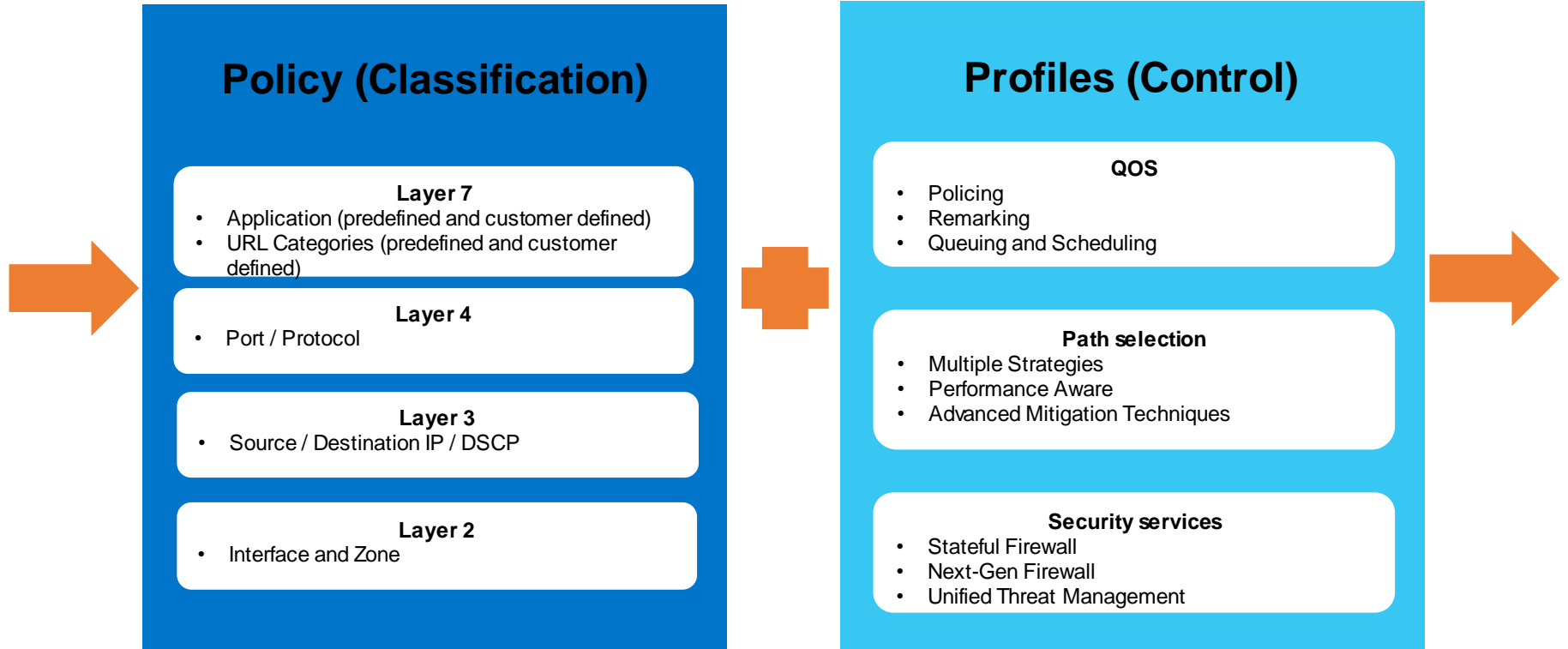
- Industries widest application visibility
5000+ applications supported
- Automatically updated application database

Dynamic Application Learning

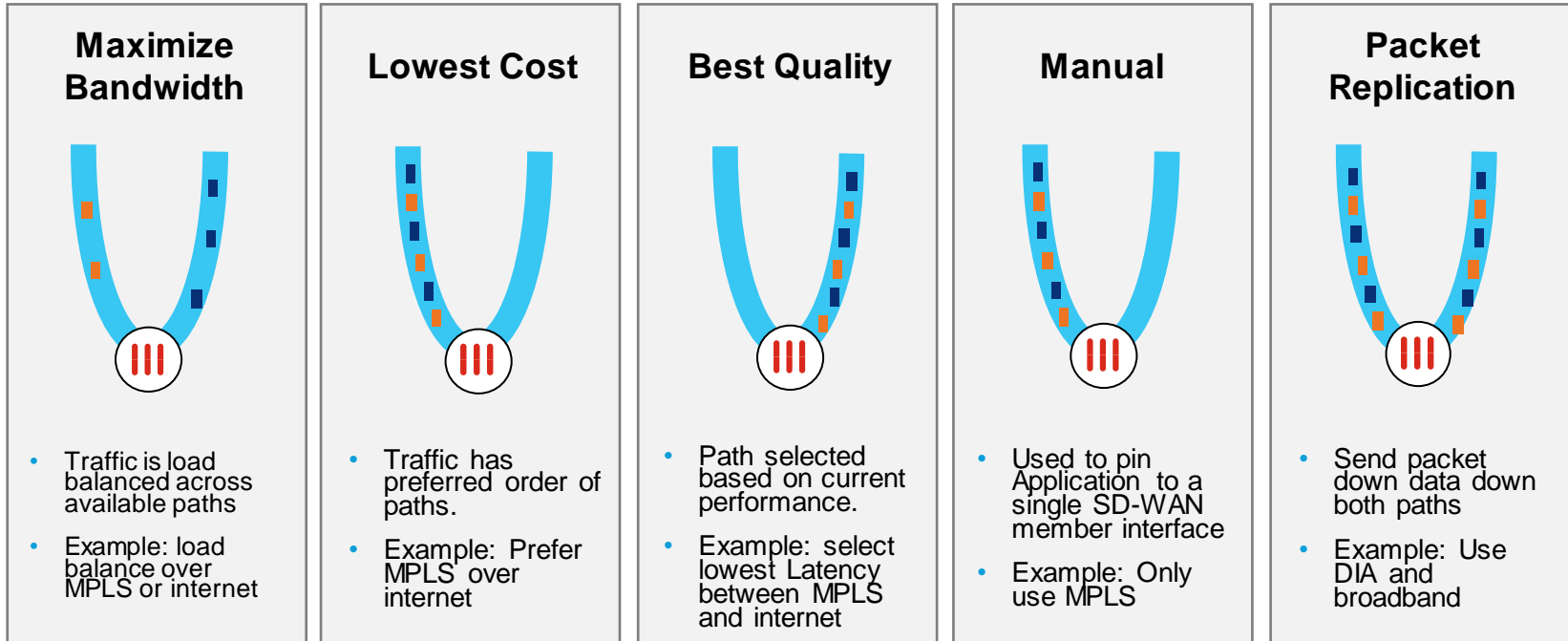
Fortinet Deep Application Visibility



Flexible classification and control



Fortinet Application Steering Strategies



Application SLAs allow for definition of thresholds (latency, packet loss, jitter) to determine if a path is available for traffic.

Fortinet SD-WAN Configuration

SD-WAN Interface Members

- This is your “SD-WAN bundle”
- Nearly any Fortigate interface can be a member
 - Physical ports, VLANs, LAGs, IPSEC/GRE/IPIP, FEX...
- Grouped into SD-WAN Zones

Interface Members

<input type="checkbox"/>	ID	Interface Member
<input type="checkbox"/>	virtual-w	
<input type="checkbox"/>	underlay	
<input type="checkbox"/>	1	port1
<input type="checkbox"/>	overlay	
<input type="checkbox"/>	5	H1_MPLS
<input type="checkbox"/>	3	H1_ISP1
<input type="checkbox"/>	SASE	

Performance SLA

- Health probes to measure latency, jitter and packet-loss over different Members
 - Ping, DNS, HTTP, TWAMP, TCP/UDP Echo
- Different probe protocols
 - Ping, DNS, HTTP, TWAMP, TCP/UDP Echo
- Zero or more SLA Targets
 - For different applications

Performance SLA

<input type="checkbox"/>	Name	Health-Check Server	Detect Protocol
<input type="checkbox"/>	HUB	10.200.99.1	Ping
<input type="checkbox"/>	Internet	8.8.8.8	DNS

SD-WAN Rules (Application Steering)

- Match different types of traffic and apply desired steering strategy to it
 - Selecting the right Member for each session, considering its current health and SLA status
- Different match criteria
 - L3-L7, Application, ISDB, User Group...
- Different steering strategies
 - Pick the cheapest Member that meets SLA target
 - Load-balance across Members that meet SLA target
 - Pick the Member with the best quality
 - Pick a particular Member

SD-WAN Rules

<input type="checkbox"/>	ID	Name	Source	Destination	Criteria	Members
<input type="checkbox"/>	1	Corporate-H1	CORP_LAN	CORP_LAN	HUB#1	H1_ISP1 H1_ISP2 H1_MPLS
<input type="checkbox"/>	2	Corporate-H2	CORP_LAN	CORP_LAN	HUB#1	H2_ISP1 H2_ISP2 H2_MPLS
<input type="checkbox"/>	3	Business-Critical-SaaS	ALL	Salesforce GoToMeeting	Internet#1	part1 part2
<input type="checkbox"/>	sd-wan		ALL	ALL	Sessions	ALL

Fortinet SD-WAN Performance SLA

- Robust active probes using multiple protocols.
 - Extensive configurability
 - Performance SLA applied within SD-WAN Rule
- Optional Probe-free network monitoring using live sessions to calculate latency, jitter, packet loss and bandwidth.

Edit Performance SLA

Name: Direct

IP Version: IPv4 IPv6

Protocol: Ping TCP ECHO UDP ECHO HTTP TWAMP DNS TCP CONNECT FTP

Server: 8.8.8.8 + 🗑

Participants: All SD-WAN Members Specify

🔍

wan ✕

lan3 ✕

2 Entries Selected

Enable Probe Packets:

SLA Targets ⓘ

Target 1 🗑

Latency Threshold: 150 Milliseconds

Jitter Threshold: 25 Milliseconds

Packet Loss Threshold: 2 %

+ Add Target

Link Status

Interval: 500 Milliseconds

Failure Before Inactive: 5 (max 3600)

Restore Link After: 5 (max 3600)

Action When Inactive

Update Static Route:

Cascade Interfaces:

Fortinet QoS

- Traffic Shaping
 - » Pre-configured Traffic Shapers
 - » L7 Analysis for QoS rules based on Users, Apps, URLs...
 - » Use App Classification to control, bandwidth reservation, limitation, Diffserv marking and prioritization

Edit Shared Traffic Shapers

Name	<input type="text" value="guarantee-100kbps"/>
Apply Shaping	<input checked="" type="radio"/> Per Policy <input type="radio"/> For all policies using this shaper
Bandwidth Unit	<input checked="" type="radio"/> Kbps <input type="radio"/> Mbps <input type="radio"/> Gbps
Guaranteed Bandwidth (0 - 16776000)	<input type="text" value="100"/>
Maximum Bandwidth (0 - 16776000)	<input type="text" value="1048576"/>
Traffic Priority	<input checked="" type="radio"/> High <input type="radio"/> Medium <input type="radio"/> Low
<input type="checkbox"/> DSCP (000000 - 111111)	<input type="text" value="000000"/>
Advanced Options	
dscp-marking-method	<input type="text" value="static"/>
exceed-bandwidth	<input type="text" value="0"/>
exceed-class-id	<input type="text" value="Click to select"/>
exceed-dscp	<input type="text" value="000000"/>
maximum-dscp	<input type="text" value="000000"/>
overhead	<input type="text" value="0"/>

Edit Traffic Shaping Policy

IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Name	<input type="text" value="Voicq"/>
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Comments	<div style="background-color: #d4edda; padding: 5px; border: 1px solid #c3e6cb;">0/255</div>
If Traffic Matches:	
Source Internet Service	<input type="checkbox"/>
Source Address	<input type="text" value="all"/>
Source User	<input type="text" value="+"/>
Source User Group	<input type="text" value="+"/>
Destination Internet Service	<input type="checkbox"/>
Destination Address	<input type="text" value="all"/>
Schedule	<input type="text" value="+"/>
Service	<input checked="" type="checkbox"/> ALL
Application	<input type="text" value="+"/>
Application Category	<input type="text" value="VoIP"/>
Application Group	<input type="text" value="+"/>
URL Category	<input type="text" value="+"/>
Type Of Service	<input type="text" value="0x00"/>
Type Of Service Mask	<input type="text" value="0x00"/>
Then:	
Action	<input checked="" type="radio"/> Apply Shaper <input type="radio"/> Assign Group
Outgoing Interface	<input type="text" value="any"/>
Shared Shaper	<input checked="" type="checkbox"/> guarantee-100kbps
Reverse Shaper	<input type="text" value="+"/>
Per-IP Shaper	<input type="text" value="+"/>
Differentiated Services	<input type="checkbox"/>

Traffic management – best practices

Traffic type	Rule	Match criteria	QOS profile	Path selection profile	
				Option 1	Option 2
Voice	Voice-DSCP	DSCP: EF or CS5	Ef1_profile_rw enable	Packetreplication-lte	
	VoiceApps	Application: RTP or RTCP			
	Voice-ZONE	Source zone: VOICE			
Video conferencing	VideoConference-DSCP	DSCP: AF41 or CS4	Ef2_profile_rw enable	Prefer-mpls-dia-bb	
High priority apps	HighPriorityApps	Application: ICA, RDP or SIP	Af1_profile_rw enable	Prefer-mpls-dia-bb-lte	Loadbalanced-lte
Business apps	BusinessApps-SaaS	Application: office365-apps, salesforce-apps and more...	Af2_profile_rw enable	Prefer-mpls-dia-bb-lte	Loadbalanced-lte
	BusinessApps-Internal	Source and destination IP: RFC1918			
Low priority apps	Low PriorityApps	Application: SCCM	Be1_profile_rw enable	Prefer-bb-dia-mpls	Loadbalanced
General internet	Internet-All	Default rule (everything else)	Be2_profile_rw enable	Prefer-bb-dia-mpls	Loadbalanced
	Internet-Proxy	Destination IP: customer defined			
Guest internet	GuestInternet-ZONE	Source zone: GUEST	Be3_profile_rw enable	Local egress only	

Security Policies / Profiles

- Profiles can be created for:
 - AntiVirus
 - Web Filtering
 - Application Control
 - Intrusion Detection / Prevention
 - SSL / SSH Inspection
 - User Authentication

Firewall/Network Options

NAT

NAT NAT46 NAT64

IP Pool Configuration

Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port

Protocol Options default

Disclaimer Options

Display Disclaimer

Security Profiles

Profile Type

Use Standard Security Profiles Use Security Profile Group

AntiVirus Profile wifi-default

Web Filter Profile SATLAB-GUEST-FILTER

Application Control wifi-default

IPS Profile wifi-default

DNS Filter default

SSL/SSH Inspection certificate-inspection

Introducing FortiClient



Comprehensive end-point protection & security enforcement



Broad endpoint visibility



Endpoint compliance and vulnerability management



Proactive endpoint defense (Planned)



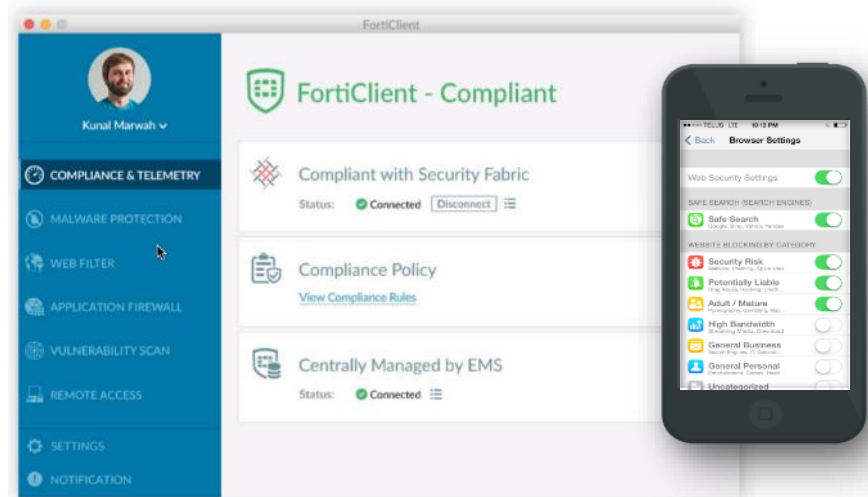
Automated threat containment
(Planned)




Secure remote access



Easy to deploy and manage



Fortinet Licensing / Package Options

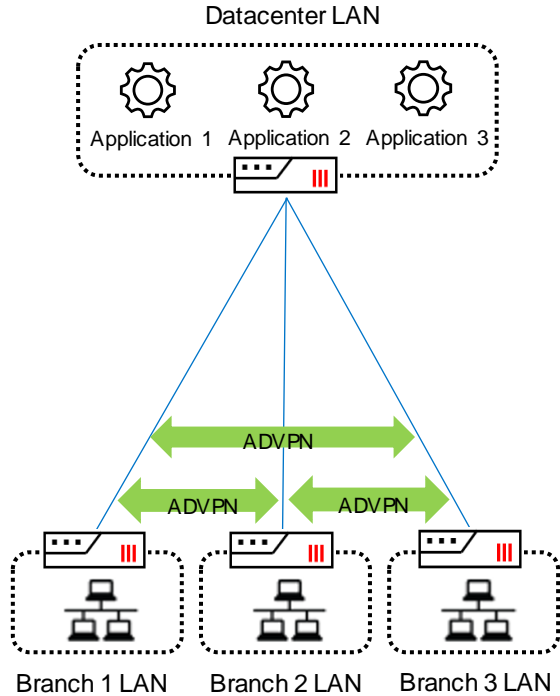
- SD-WAN Only
 - CPE
 - SD-WAN
 - Stateful Firewall
 - FortiCare
- Next Generation Firewall 
 - Adds FortiGuard Unified Threat Protection (UTP) License
 - SD-WAN not supported with NGFW only
- SASE w/ ZTNA
 - Adds EMS and FortiClient

SASE Function	SD-WAN Only	NGFW Only	SD-WAN w/ NGFW	SASE w/ ZTNA
SD-WAN	Yes	No	Yes	Yes
Firewall as a Service	Stateful	NGFW	NGFW	NGFW
Intrusion Detection/Prevention	No	Yes	Yes	Yes
SSL/TLS Inspection	No	Yes	Yes	Yes
Anti-Virus / Anti-Malware	No	Yes	Yes	Yes
Data Loss Prevention	No	Yes	Yes	Yes
Secure Web Gateway	No	Yes	Yes	Yes
Cloud Access Service Broker	No	Roadmap	Roadmap	Roadmap
Zero Trust Network Access	No	No	No	Yes

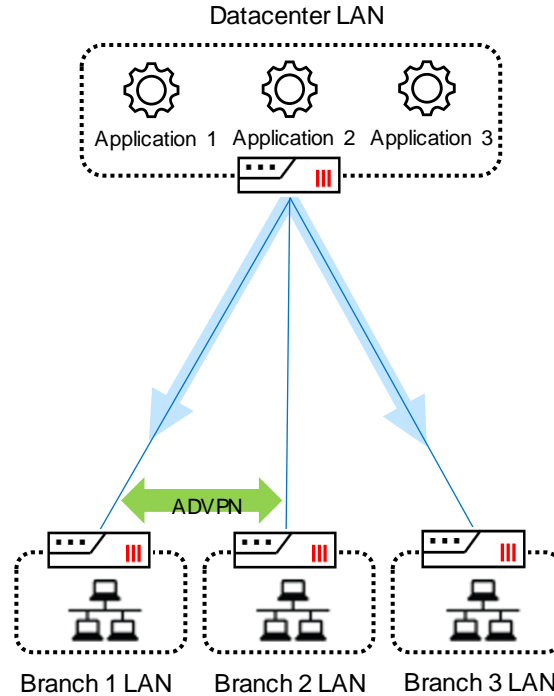


Fortinet SD-WAN Overlay and Topologies

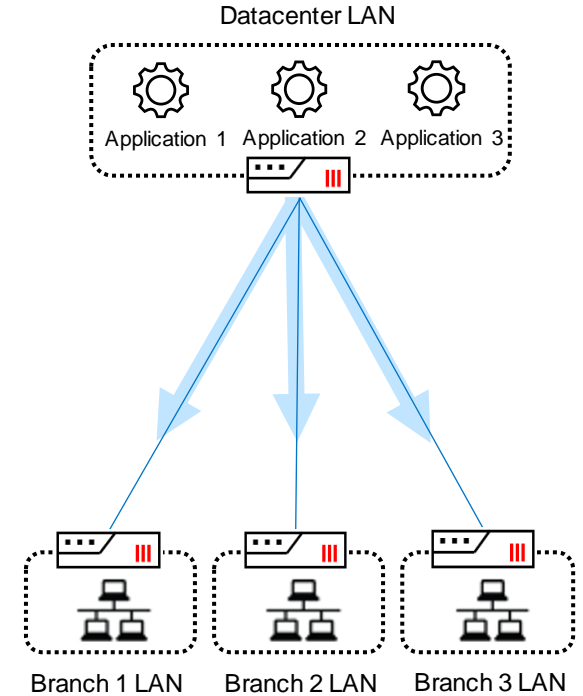
SD-WAN Overlay Topology Options



Full Mesh

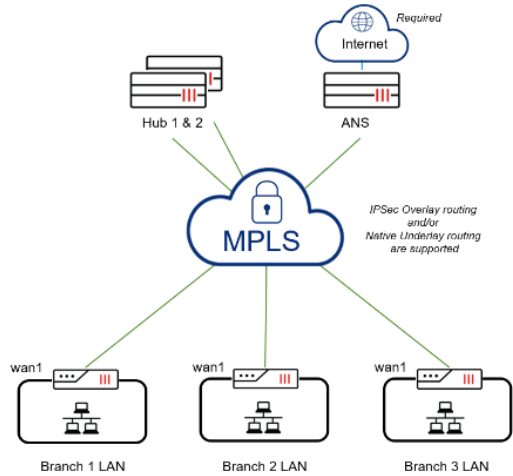


Partial Mesh

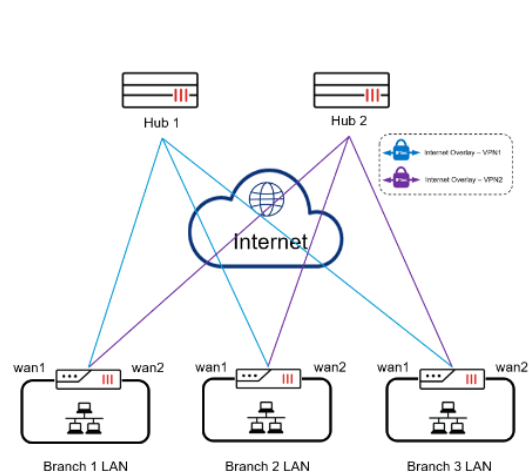


Hub-n-Spoke

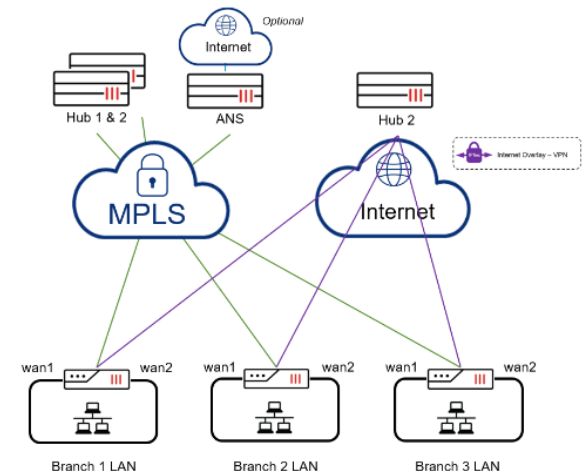
SD-WAN Underlay Network Options



MPLS-Only



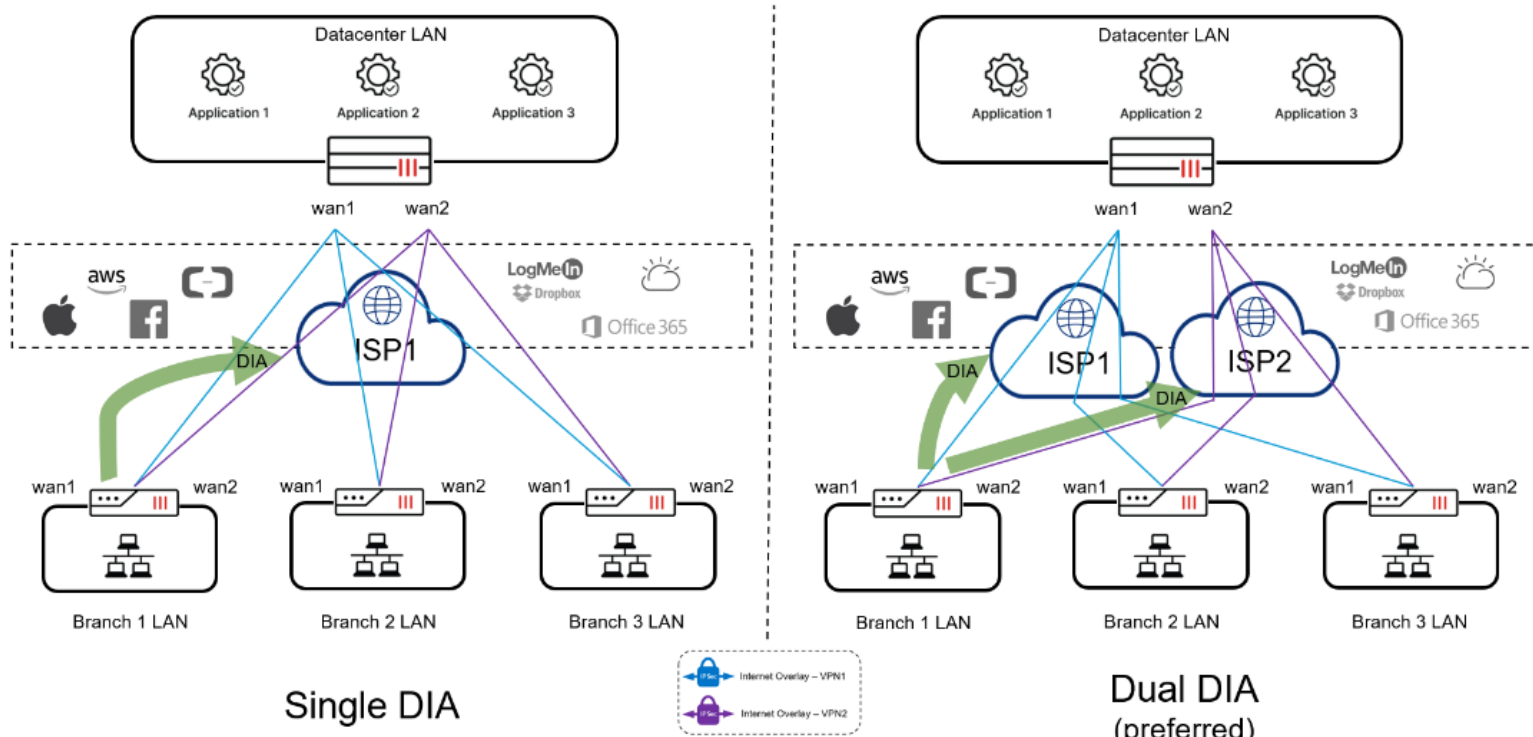
Internet-Only



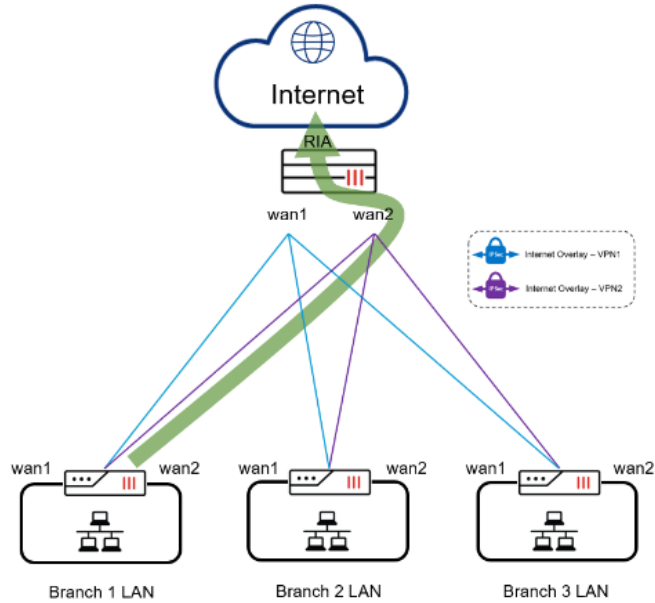
Hybrid
MPLS & Internet

NOTE: Lumen provided LTE/5G WILL NOT be supported for a Phase 1 release

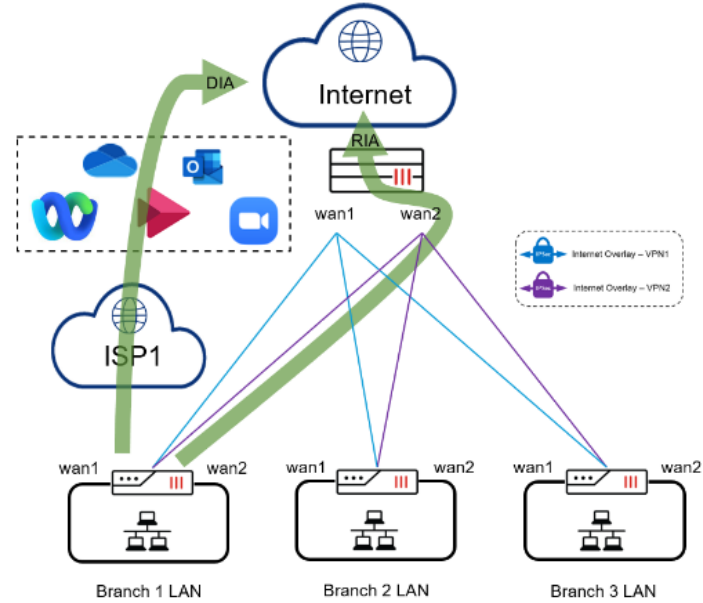
Direct Internet Access



Remote Internet Access



RIA



Hybrid DIA + RIA

FortiGate High Availability

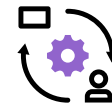
- HA design requiring **active/active** use of multiple WAN links require WAN facing edge switch or router to split WAN service to both FortiGates (dual connected WAN).
 - WAN edge can be any Layer 2 or Layer 3 edge device.
- HA design with **active/standby** use of multiple WAN links can be supported with each WAN connection directly terminated to each FortiGate (directly connected WAN).
- Several HA options are supported by FortiGate:
 - Virtual Router Redundancy Protocol (VRRP)
 - Route-Based Failover
 - FortiGate Session Life Support Protocol (FGSP)
 - FortiGate Clustering Protocol (FGCP)



Fortinet Zero Trust Network Access

Evolution of VPN tunnels

Bringing Zero Trust principles to remote access

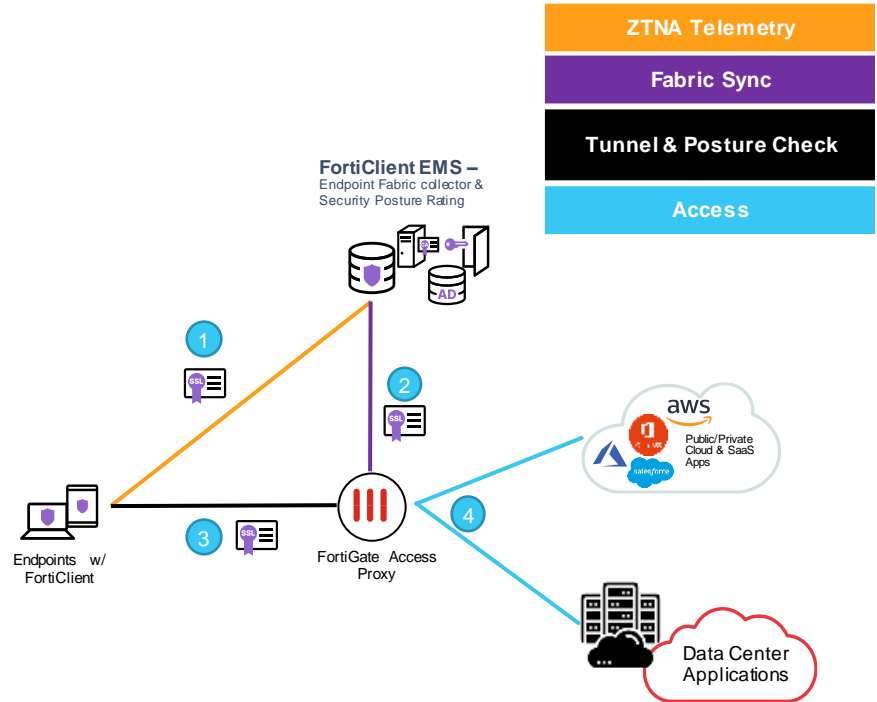


- Ongoing verification
 - Per session user identity checks
 - Per session device posture checks (OS version, A/V status, vulnerability assessment)
- More granular control
 - Access granted only to specific application
 - No more broad VPN access to the network
- Easier user experience
 - Auto-initiates secure tunnel when user accesses applications
 - Same experience on and off-net



Fortinet Zero Trust Network Access – How it Works

1. FortiClient Endpoint builds Telemetry Connection with EMS
 - a) FortiClient requests Certificate and shares device information, user logon, and security posture information.
 - b) EMS validates user against Active Directory and returns signed Certificate and tags FortiClient with Zero Trust rules
2. EMS synchronizes endpoint certificate info and ZTNA tags with the FortiGate
3. FortiClient requests access via FortiGate
4. FortiGate verifies client identity using certificate and grants access based on the ZTNA tags applied in the ZTNA rules



Secure Network Access with Zero Trust Framework

- Zero Trust Network Access (ZTNA) with Fortinet Secure Network Stack
 - Access Control method to provide role-based application access using
 - Client Device Identification
 - Authentication
 - Zero Trust Tags
- Administrators get flexibility to manage network access for
 - On-net (Local users) and Off-net (remote users)
- Access to applications is granted only after
 - Device Verification
 - Authenticating the user's identity
 - Authorizing the user
 - Performing context-based posture checks using Zero Trust Tags
- Full ZTNA & IP/MAC Filtering
 - Full ZTNA
 - Allows Users to securely access resources through an SSL encrypted access proxy, simplifying remote access by eliminating the user of VPNS
 - IP/MAC Filtering
 - ZTNA tags to provide an additional factor for identification to implement role-based zero trust access.

Fortinet Zero Trust Network Access Licensing

- Monthly charge per device
- Client can be used for remote and local users
- Includes FortiClient Agent and FortiClient EMS
- License/charge applied whether device is active/inactive
- Best practice is to apply to all users that have mobile devices and need access to resources while out of the office.
- FortiClient Supported on:
 - Windows, Mac, Linux, IOS, and Chromebook

Feature	EPP ₁	ZTNA
Zero Trust Security		
Zero Trust Agent	✓	✓
Central management via EMS	✓	✓
Dynamic Security Fabric Connector	✓	✓
Vulnerability agent and remediation	✓	✓
SSL VPN with MFA	✓	✓
IPsec VPN with MFA	✓	✓
Sandbox appliance	✓	
Next Generation Endpoint Security		
AI-powered next generation AV	✓	
FortiClient Cloud Sandbox	✓	
Automated endpoint quarantine	✓	
Application inventory	✓	
Application Firewall	✓	
Software Inventory	✓	

1. Not in scope for Release 1.



Fortinet Orchestration and Reporting

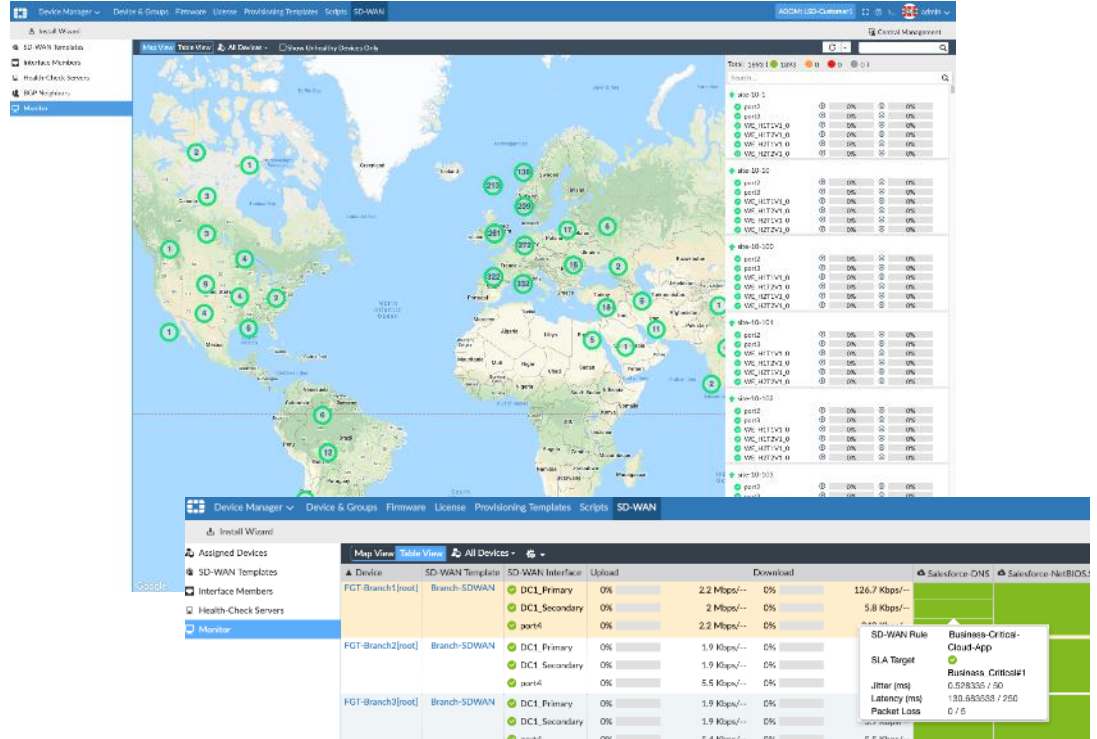
Fortinet Orchestration and Reporting

WAN Centralized Management

- Automated visibility

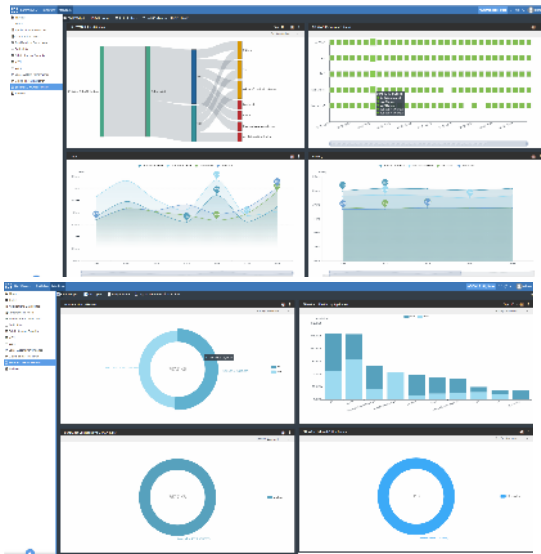
Leverage FortiManager SD-WAN Dashboard:

- Assign Devices to Groups
- Import and Export SD-WAN Templates
- Monitor for Real-time Health of SD-WAN Deployment

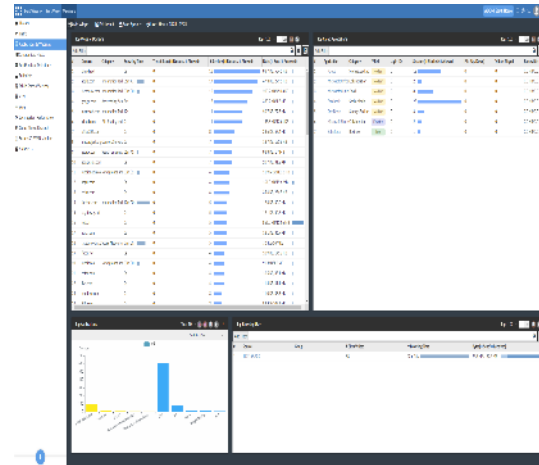


Fortinet Monitor Dashboards

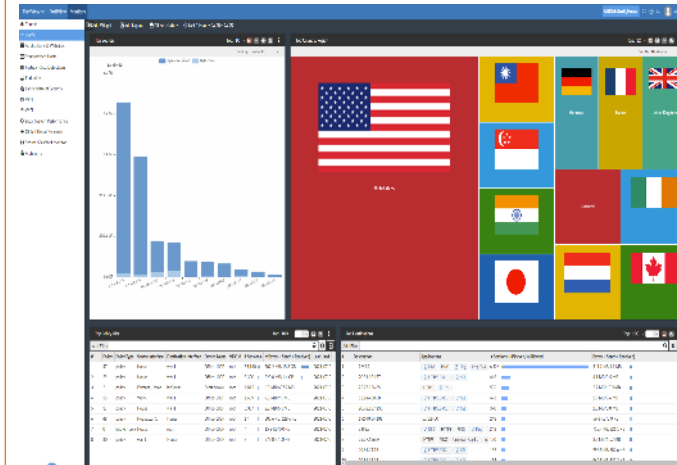
SD-WAN monitor provides Network and Security insight by presenting information on utilization, performance, jitter, latency, packetloss and applications:



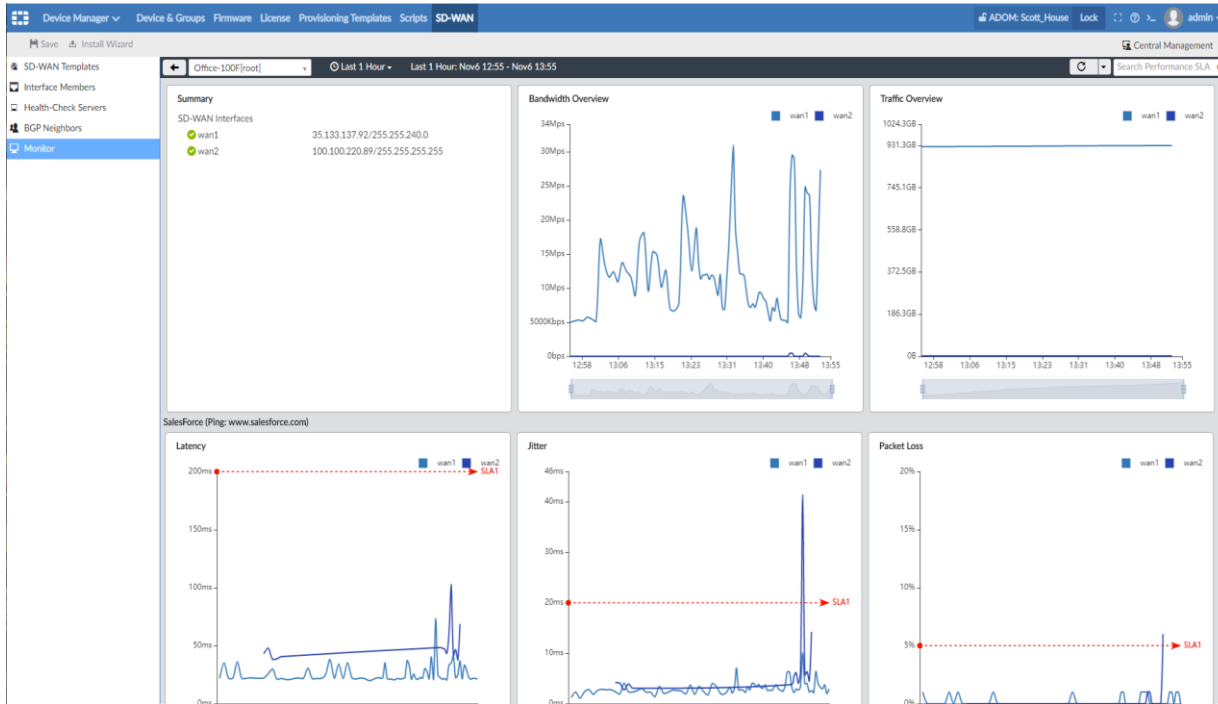
Application & Websites monitor provides insight by presenting information the following Top Websites, Top Cloud Applications, Top Applications and Top Browsing User.



Traffic monitor provides insight by presenting information the following Top Sources, Top Country/Region, Top Policy, Top Destinations, Top Sources and User Flow Data.



Fortinet SD-WAN Real-Time SLA Visibility



FortiManager

Leverage FortiManager SD-WAN Monitor for Real-time Visibility:

- Understand RT Bandwidth Usage
- Real-time SLA Insights
- Bandwidth Overview
- Traffic Overview

Fortinet Reports

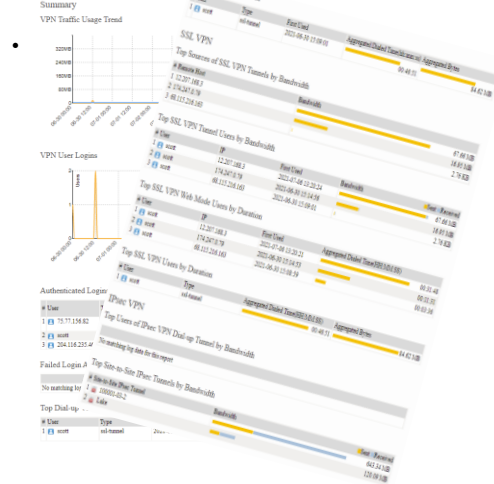
SD-WAN report provides Network and Security insight by presenting information in two major categories:

- **SD-WAN Performance Monitor**
- **SD-WAN Utilization**

Teleworker report provides user insight by presenting information the following categories:

- **User Traffic Trends**
- **User login**

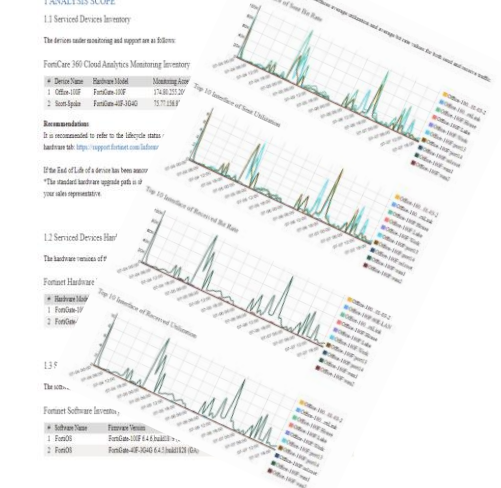
• **User by Duration**



360 report provides insight by presenting information the following categories:

- **Device Utilization**
- **Interface Performance**
- **Operational Faults**

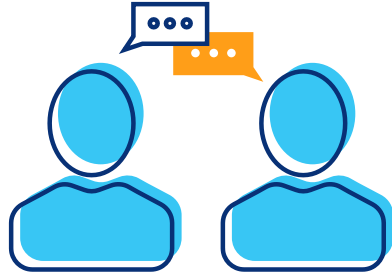
• **Device Details**





SASE Ordering Experience

Lumen SASE Solutions **purchasing paths**



Lumen Direct Sales

- Traditional consultative sales experience using DQP for Quote/Orders
- Opportunities to cross-sell Lumen platform elements (network, cloud, edge)



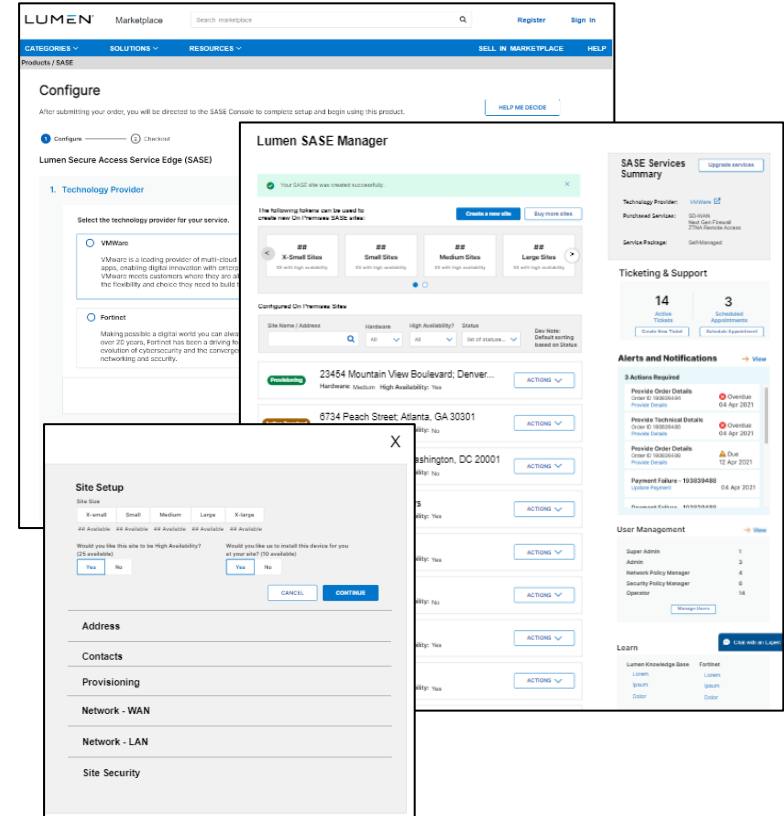
Lumen® Marketplace

- Online design and purchase
- Multiple partner options

Lumen SASE Solutions: How to order in Marketplace



- Customer orders directly through Lumen Marketplace
- Centralized SASE Manager experience to
 - configure location and user services,
 - Upgrade
 - access policies, add new services, access partner portals, receive performance alerts, and more.
 - Ability to instantly upgrade, change, and delete network and security services using a common online experience
- Contact sales options available



Lumen SASE Manager

Configure, update, and manage your entire Lumen SASE Solution from one place

Lumen SASE Manager

The screenshot displays the Lumen SASE Manager interface, divided into several sections:

- SASE Sites:** A navigation bar with "SASE Sites" and "SASE Services" tabs. Below it, a message states: "The following tokens can be used to create new On Premises SASE sites:" followed by buttons for "Create a new site" and "Buy more sites". A carousel shows site size options: "X-Small Sites", "Small Sites", "Medium Sites", and "Large Sites", each with "XX sites high availability".
- Configured On Premises Sites:** A table listing sites with columns for "Site Name / Address", "Hardware", "High Availability?", "Status", and "Dev Note: Default sorting based on Status". Sites include: "23454 Mountain View Boulevard, Denver...", "6734 Peach Street; Atlanta, GA 30301", "7635 7th Street NW; Washington, DC 20001", "Southwest Headquarters", "St. Louis Office", "Dallas Site", "Site 1", "Site 2", and "Site 3". Each row has an "ACTIONS" dropdown menu.
- SASE Services Summary:** A panel with an "Upgrade services" button. It lists: "Technology Provider: VMware", "Purchased Services: SD WAN, Next Gen Firewall, ZTNA Remote Access", and "Service Package: SelfManaged".
- Ticketing & Support:** A panel showing "14 Active Tickets" and "3 Scheduled Appointments", with buttons for "Create New Ticket" and "Schedule Appointment".
- Alerts and Notifications:** A panel titled "3 Actions Required" with a "View" link. It lists overdue tasks: "Provide Order Details" (Order ID 193839484, Overdue 04 Apr 2021), "Provide Technical Details" (Order ID 193839488, Overdue 04 Apr 2021), "Provide Order Details" (Order ID 193839488, Due 12 Apr 2021), and "Payment Failure - 193839488" (Update Payment 04 Apr 2021).
- User Management:** A panel with a "View" link showing a list of users: "Super Admin" (1), "Admin" (3), "Network Policy Manager" (4), "Security Policy Manager" (6), and "Operator" (14). A "Manage Users" button is at the bottom.
- Learn:** A panel with a "Chat with an Expert" button and a table for "Lumen Knowledge Base" and "Fortinet":

Lumen Knowledge Base	Fortinet
Lumen	Lumen
Ipsum	Ipsum
Dolor	Dolor

1. Existing service upgrades and additions
2. Add new sites and users
3. Lumen SASE Solutions site configuration
4. Ticket and support generation and current status
5. Lumen alerts and notifications
6. New and existing service status
7. SASE Manager users
8. Chat with an expert
9. Knowledge base content



Pro-Managed Experience

Deployment and operations responsibilities

	Lumen	Customer
Deployment design	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service configuration	<input checked="" type="checkbox"/>	
Site activation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Configuration change management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Appliance/circuit monitoring and event management	<input checked="" type="checkbox"/>	
Release certification and operationalization	<input checked="" type="checkbox"/>	
Appliance upgrades	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SD-WAN transformation team

Project Manager

- Single point of contact coordinating all Lumen resources
- Develops project plan
- Define deployment waves (wave 0 is the initial sites where we burn in the configs)
- Identify dependences (i.e. new transports)
- Manage the project
- Weekly status update calls
- SharePoint site



Design Engineer

- WAN Topology and Routing
- QOS, SD-WAN and Security Policies
- Site Classification and Standardization
- Collection of site-specific configuration data
- Configures SASE Service



Activation Engineer

- Onboards Devices
- Activates new Lumen WAN Transport
- Runs site cutover call



Service Assurance

- Performs monitoring and event management
- Performs Change Requests
- Provides Portal Training



Control of What Matters Most

Path selection policies

QoS policies

Routing policies

Security policies

Analytics

Monitoring

Implementation

- SD-WAN design engineer
- Implementation design
- Template creation
- Device onboarding
- Design guides
- Lab environment

Global infrastructure

- HA director instances
- Controllers in 5 regions
- Lumen public & private backbone
- Infrastructure security

CPE

- Bare metal CPE
- Global distribution
- Sparing & replacement
- Virtual appliance

Transport

- Lumen
- Third-party
- Customer-provided

Operation

- 24/7 resources
- Event correlation
- Ticketing integration
- CPE event mgmt.
- Circuit outage mgmt.

Infrastructure operations

- Certification lab
- Release mgmt.
- Infrastructure event management



Optional Design and Deployment Services

Optional: SASE Technology Adoption Assessment

Activities:

- Meet with technical and business leaders to understand the requirements and desired target architecture
- Review existing LAN/WAN Architecture of Enterprise
- Identify critical applications architecture and inter-dependencies, as well as internet and cloud breakout locations

Deliverable: Business case presentation to Leadership Team outlining “SASE” readiness

Optional: SASE Design & Engineering

Provide overall architectural design of SD-WAN solution based on your business and technical requirements.

- Assess existing WAN infrastructure, traffic pattern, and existing spending.

Activities:

- Define and Develop Use cases
- High Level Design, Prepare Bill of Materials and Capex Estimates
- Present High-Level Design, Stake Holder Review and Sign-off
- Prepare Low Level Design, Configuration Documents and Configuration Templates for Branch Sites
- Prepare High Level Migration Plan
- Stake Holder Review and Sign-off

Deliverables: High Level Design, Low Level Design, Configuration Documents and Migration Plan

Optional on-site technician

On-site installation:

- Devices shipped to the customer site where the technician will:
 - Technician Install device(s) and connects WAN transport(s)
 - Support activation engineer in validation and any troubleshooting of WAN connectivity

On-site maintenance:

- On a device failure, Lumen will ship a replacement device to the site
- Upon delivery of the device, Lumen will dispatch a tech to install the device

