

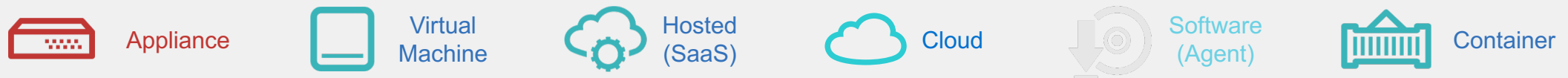
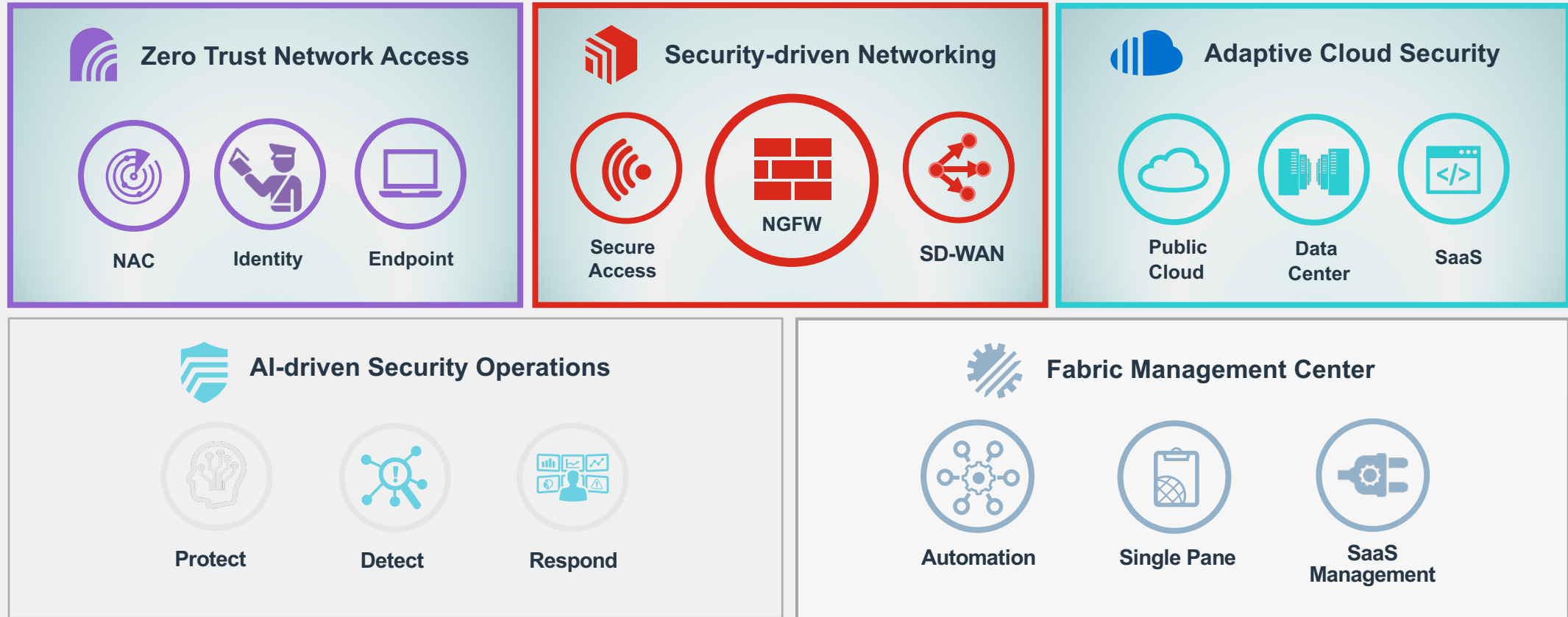


FortiOS 7.0

What's New

Massimo Montalto, Channel Systems Engineer
Ludovic Peny, Channel Systems Engineer

Cybersecurity Platform for the Digital Attack Surface





Overview



Platform Support

FortiOS 7.0

Grey = EoO Products

	6.2.6	6.4.4	7.0.0
FG/FWF-30E/50E Series	•		
FG/FWF-60E	•	•	•
FG/FWF-40F Series	•	•	•
FG/FWF-60F Series	•	•	•
FG-80D	•		
FG-80E Series	•	•	•
FG-80F Series	•	•	•
FG-90E Series	•	•	•
FG/FWF-92D Series	•		
FG-100D/140D Series	•		
FG-100/101E Series	•	•	•
FG-100F Series	•	•	•
FG-200/201E	•	•	•
FG-300E/500E Series	•	•	•

	6.2.6	6.4.4	7.0.0
FG-400E/600E Series	•	•	•
FG-800D/900D/1x00D Series	•	•	•
FG-1100E Series	•	•	•
FG-1800F Series	•	•	•
FG-2200E, 3300E Series	•	•	•
FG-2000E, 2500E	•	•	•
FG-2600F Series	•	•	•
FG-3X00D Series	•	•	•
FG-3400E/3600E	•	•	•
FG-3960E/3980E	•	•	•
FG-4200/4400F Series	•	•	•
FG-5001D/5001E	•	•	•
FG-6000/7000 Series	•	•	•





Security-driven Networking



Security-driven Networking

FortiGuard Video Filtering Service

Add FortiGuard service that provides category rating for videos under new video filter profile panel

- For YouTube, Vimeo and Daily Motion
- static filter option for YouTube channels

The screenshot shows the FortiGuard Video Filtering Service configuration interface. On the left is a sidebar menu with the following items: Favorite, Video Filter (selected), Firewall Policy, Dashboard, Security Fabric, Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report. The main panel is titled 'Edit Video Filter Profile'. It contains a 'Name' field with the value 'category_filter' and a 'Comments' field with the placeholder 'Write a comment...'. Below these fields is a toggle for 'FortiGuard Category Based Filter', which is currently turned on. Under this toggle is a table with two columns: 'Category' and 'Action'. The table contains the following rows: 'Not Rated' (Block), 'Business' (Block), 'Entertainment' (Allow), 'Games' (Allow), 'Knowledge' (Monitor), 'Lifestyle' (Allow), 'Music' (Allow), 'News' (Allow), and 'People' (Allow). At the bottom of the table is a progress bar showing '0%' and a count of '11'. Below the table is a section for 'YouTube' with a toggle for 'Restrict YouTube access' and a 'Channel override list'. The 'Channel override list' has a '+ Create New' button, an 'Edit' button, a 'Delete' button, and a search bar. Below the search bar is a table with three columns: 'Channel ID', 'Comments', and 'Action'. The table is currently empty and shows 'No results'. At the bottom right of the main panel is an 'OK' button.

Category	Action
Not Rated	Block
Business	Block
Entertainment	Allow
Games	Allow
Knowledge	Monitor
Lifestyle	Allow
Music	Allow
News	Allow
People	Allow

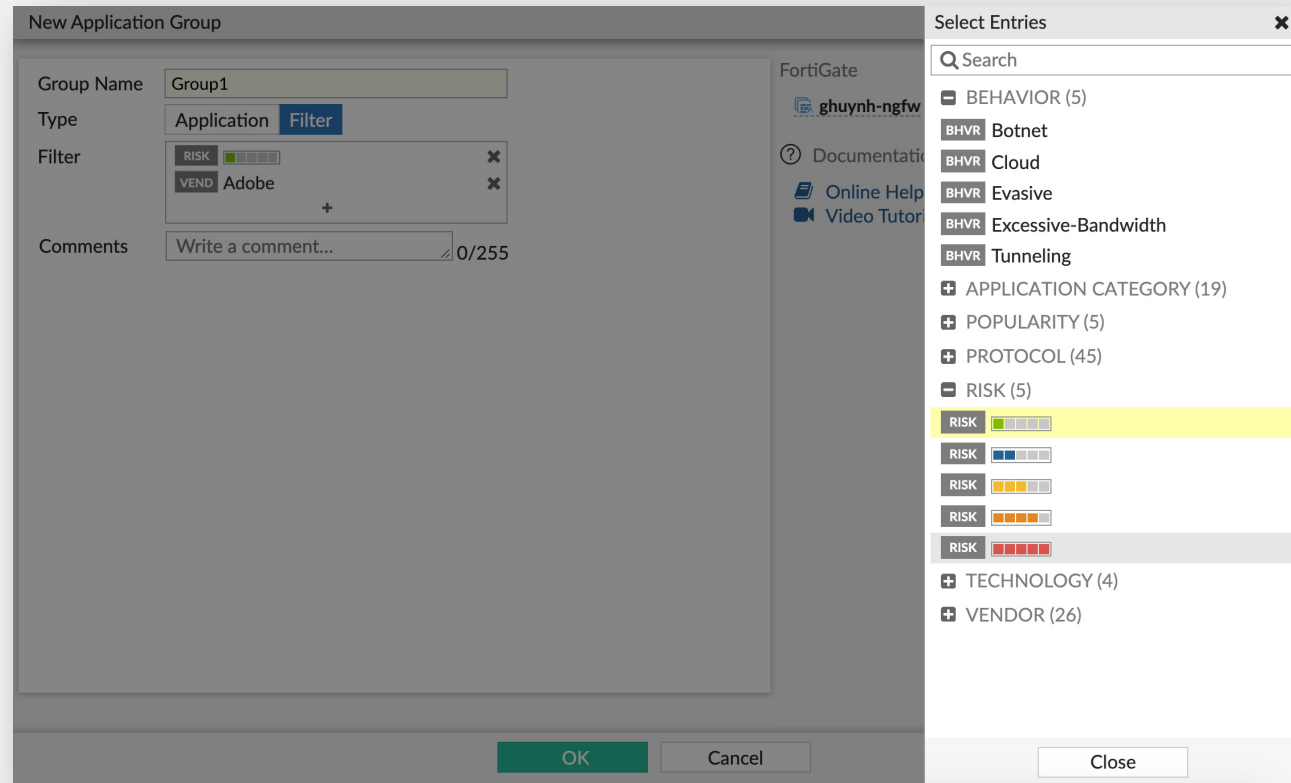
Channel ID	Comments	Action
No results		

Security-driven Networking

Application Grouping

Expand application group definition

- In NGFW policy mode, grouping can also be defined by risk, technology, vendor, popularity, name

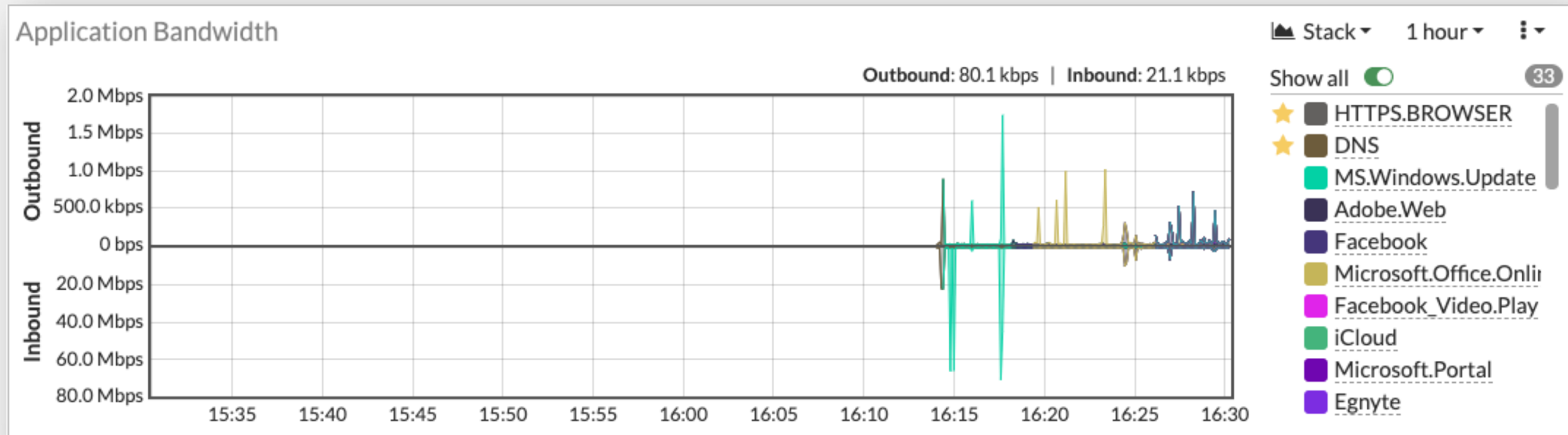


Security-driven Networking

Application Bandwidth Utilization Graph

New widget to illustrate real-time app traffic utilization

- Customers will be able to be filtered to show only interested applications
- Default filter showing the top X bandwidth-consuming applications



Security-driven Networking

DNS Inspection Enhancements

Expand DNS protocols supported on FortiOS

- Add proxy support so DNS over HTTPS and TLS can be inspected using DNS inspection profile
- GUI to provide DNS protocol options – DNS (UDP), DNS over TLS, and DNS over HTTPS

DNS Settings

DNS servers

Use FortiGuard Servers

Specify

Primary DNS server

208.91.112.53

Secondary DNS server

208.91.112.52

Local domain name

+

DNS Protocols

DNS (UDP/53)

TLS (TCP/853)

HTTPS (TCP/443)

SSL certificate

Fortinet_Factory

Server hostname

+

FortiGuard DDNS

DNS Servers

208.91.112.53

60 ms

208.91.112.52

60 ms

DNS Filter Rating Servers

173.243.140.53

330 ms

Additional Information

API Preview

Edit in CLI

Local Out Setting

Setup guides

DNS Local Domain List


Using FortiGate as a DNS Server

FortiGuard DDNS

Documentation

Online Help

Video Tutorials



© Fortinet Inc. All Rights Reserved.

9

Security-driven Networking

Interface Migration Wizard

GUI wizard to migrate interfaces from one area of the configuration to another.

- Provide ability to move existing objects around even when they have references
- Examples:
 - Change VLAN ID after assigned
 - Move interface into SD-WAN when it already has policies associated with it
 - Add interface to a Zone when it has policies or other configuration associated with it

Move port2 into an interface

1 Select Migration Option > 2 Select/Create Interface > 3 Review Settings > 4 Summary

Select where you wish to move the interface.

- ☒ **Migrate to Interface**
Move selection to a new or existing interface. Aggregate interfaces, redundant interfaces, and software switches are supported.
- ☐ **Migrate to Zone**
Move selection to a new or existing zone.
- ☐ **Migrate to SD-WAN**
Move selection to a existing SD-WAN zone

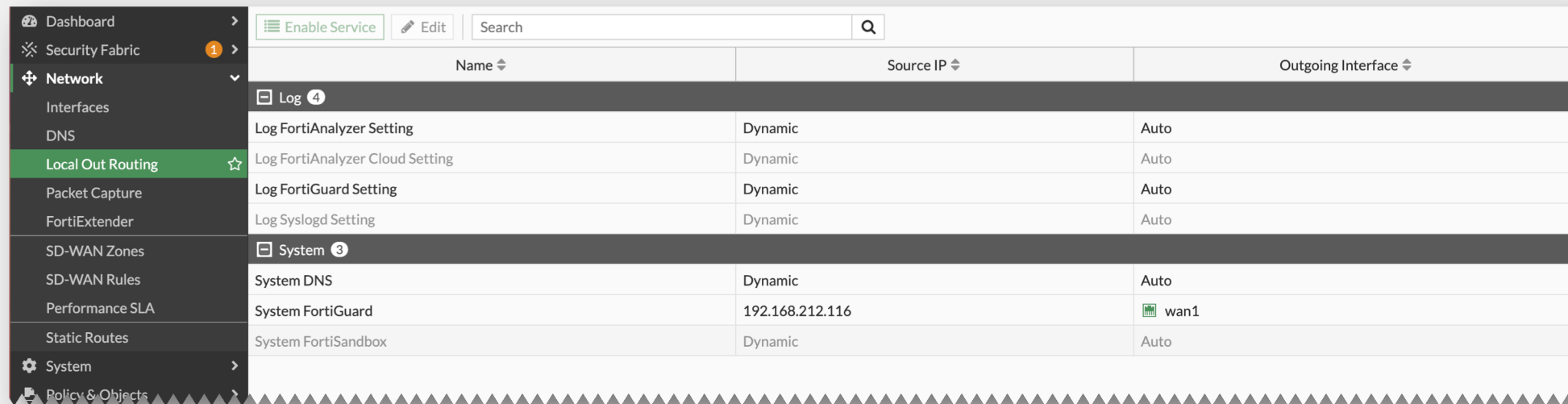
< Back Next >

Security-driven Networking

Local Out Page

Consolidate various Local Out settings to a single page under “Network” for ease-of-use

- displays all the possible local out setting - those relating to system, logging and external authentication service
- The settings available may be either global or at VDOM level



Name	Source IP	Outgoing Interface
Log 4		
Log FortiAnalyzer Setting	Dynamic	Auto
Log FortiAnalyzer Cloud Setting	Dynamic	Auto
Log FortiGuard Setting	Dynamic	Auto
Log Syslogd Setting	Dynamic	Auto
System 3		
System DNS	Dynamic	Auto
System FortiGuard	192.168.212.116	wan1
System FortiSandbox	Dynamic	Auto

Security-driven Networking

ACME Support

Automatically generate a certificate for a device, using ACME (Automated Certificate Management Environment)

- For HTTPS / SSL-VPN GUI access
- Provide a simplified way for administrators to assign a certificate to the device, without complexities of manually managing certificates

The image shows a screenshot of the FortiGate web interface. On the left, the 'System Settings' page is visible, showing various configuration options like System Time, Administration Settings, and WiFi Settings. On the right, an 'Import Certificate' dialog box is open. The 'Type' tab is selected, and the 'Automated' option is chosen. A blue information box states: 'This certificate will be automatically provisioned using the ACME protocol with the Let's Encrypt service. It's the easiest way to install a trusted certificate on your FortiGate. For more information, please visit: [Let's Encrypt](#).' Below this, there are input fields for 'Certificate name', 'Domain', and 'Email'. The 'ACME service' is set to 'Let's Encrypt'. A yellow warning box says: 'By continuing, you agree to the CA [Terms of Service](#).' The 'RSA key size' is set to 2048, and the 'Renew window' is set to 30. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Security-driven Networking

NGFW



HA Failover based on memory utilization

- Allow user to define a base line and threshold of RAM usage for failover
- Threshold may be referencing conserve mode
- A flip timeout may be implemented



FGSP 4-member cluster support

- Resolving challenges supporting 4 FGs in a FGSP cluster
- By supporting FGSP sync when session TTL is set to 300 seconds



Link Monitoring and Failover Improvements

- If certain network is not accessible and failure detected with link monitor, only the route to this network will be removed from routing table.
- New option for 10ms heartbeat interval, compared to default 100ms

Security-driven Networking

NGFW



Extended Netflow Visibility of Logical Interfaces

ela2

-
- Add NetFlow visibility for 2 types of logical interfaces - FortiExtender and VPN tunnel interfaces

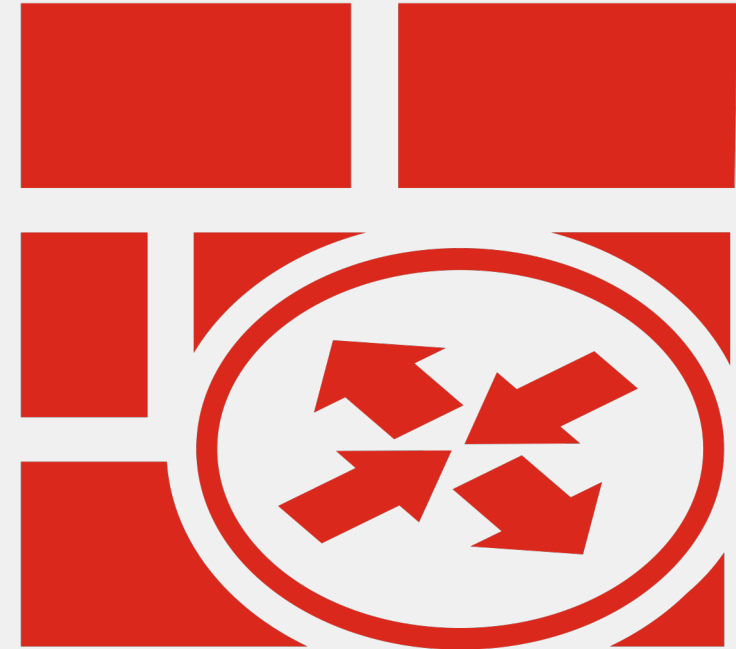
Security-driven Networking

SD-WAN - Advanced Routing

BGP & OSPF Improvements

Expansion to BGP & OSPF support to better handle various use cases

- Add new option for ECMP for recursive BGP NH resolution to support more complex SD-WAN deployments
- Support Recursive BGP resolution via another BGP route for new use cases such as Multi-Regional SD-WAN with cross-region ADVPN support
- GUI improvements for BGP and OSPF configurations



Security-driven Networking

SD-WAN



Passive Application Performance Measurement

- Uses probe-free network monitoring specific to the application by various methodologies
- Reduced load on the network and simplified configurations



Packet duplication Improvement

- New IPsec Interface to handle packet duplication, supports static and dialup VPNs



SSL VPN Client on FortiGate

- Allow site-to-site connection using SSL VPN
- Similar to IPsec dial-up client on FGT behaviour

Security-driven Networking

Secure Access - Wireless



Radio transmit power in dBm levels

-
- For auto Tx power levels, the measurement criteria is changed to dBm levels

Security-driven Networking

Secure Access - Switching



Dynamic Port Profiles and NAC Policy Table for FortiSwitch Ports

- New mode that simplifies NAC policy deployment so that admins do not have to assign NAC policy to each FortiSwitch port



Topology GUI Improvements for FortiLink and FortiSwitch

- Show FortiLink over L3 Switches in Topology and Allow customized display of Switch GUI



FortiLink multi-tenancy basic GUI support

- Adjust implementation of FortiLink multi-tenancy, so that it can be presented and configured on GUI
- Need to be configured via the CLI (port exports) first

Security-driven Networking

Secure Access - Switching



FortiSwitch Recommendations – Part 2

-
- Additional recommendations for port specific settings such as PoE configurations via Security Rating
 - Available on Beta 1 as CLI only



Adaptive Cloud Security




Dynamic Cloud Security

Nutanix Connector

API connector to Nutanix Prism Central

- similar to that of OpenStack Connector

Private SDN


Nutanix

Connector Settings

Name

Status

✓ Enabled

✗ Disabled

Update interval

☐

 Use Default

Specify

Nutanix Connector

IP

Port

Use Default

Specify

Username

Password





Zero-Trust Network Access

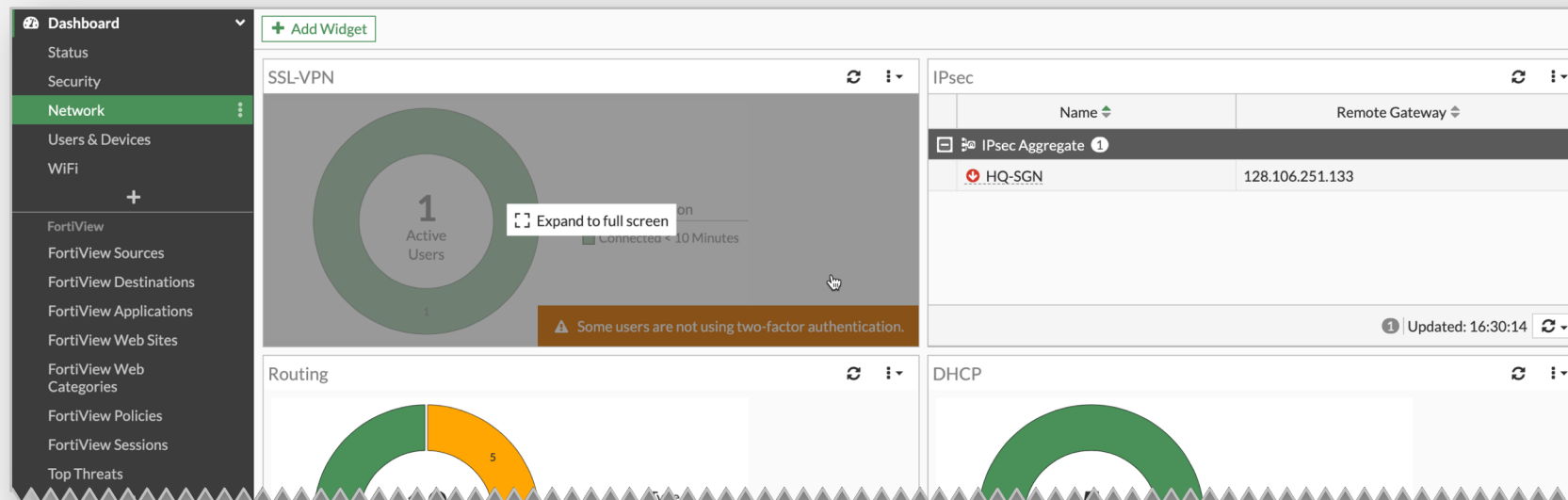


Zero-Trust Network Access

SSL-VPN & IPSEC Monitor Improvements

Provide more information on both dashboard summary and drill-down widgets, plus FortiView Top Source panel

- Top Source panel will be able to rely on EMS to provide detailed endpoint information
- Add summary charts, right click options and many columns on VPN user lists

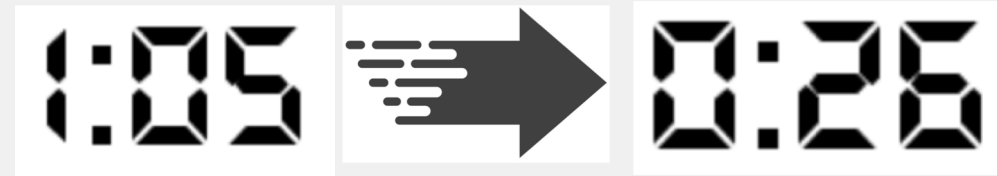


Zero-Trust Network Access

Improve reaction time for NAC

Optimizations made to the process shortens the time it takes for a new device to be recognized and assigned to the VLAN

- By using new event-based approach instead of periodic polling (every minute)
- There is also new cli command to configure how often NAC engine is run if any event is missed



With minimum nac-periodic-interval (5 seconds), it now takes 40 sec shorter for a PC from link up to match to NAC policy

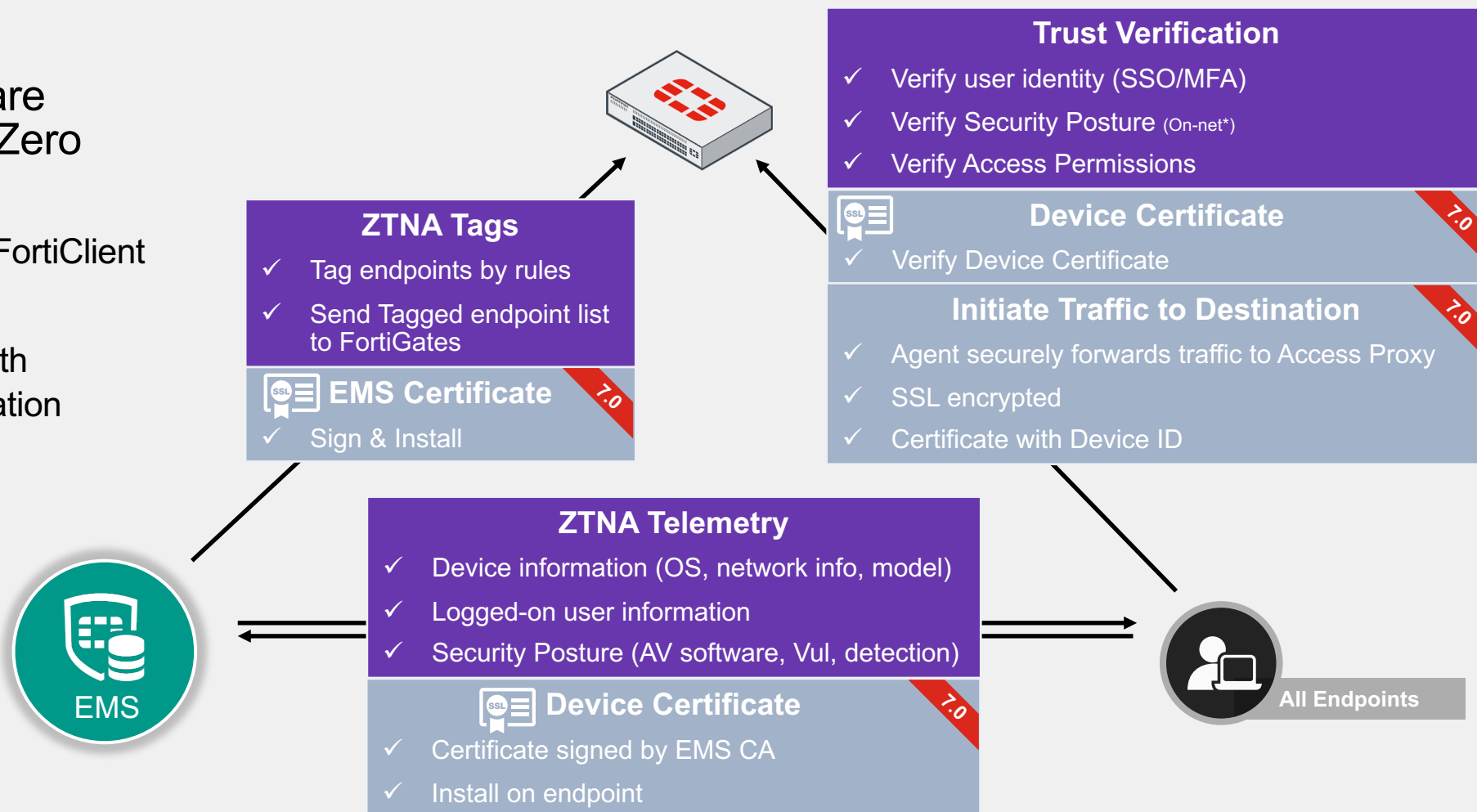
```
config switch-controller
    set nac-periodic-interval <5-60 sec>
end
```

Zero-Trust Network Access

New Zero Trust Solution

Several new features are added to support new Zero Trust solution

- HTTPS access proxy with FortiClient as ZTBA agent
- Support trust verification with certificate-based authentication



Zero-Trust Network Access

Endpoint



Dual IPv4/IPv6 SSL-VPN

- Support dual stack where both IPv4 and IPv6 traffic can be sent over the tunnel and terminate on FortiGate
- To be supported for Web and Tunnel mode



Simplify EMS Pairing

- Allow EMS side to approve connector request for the entire fabric (of FG) with a single click, when the request comes from the root of the fabric.



AI-driven Security Operations



AI-driven Security Operations

AI based Malware Detection

Replacing the old heuristics detection with the new AI based one

- Developed by AV/Sandbox engine teams in the last 4 years.
- Same engine used by FortiClient 6.4

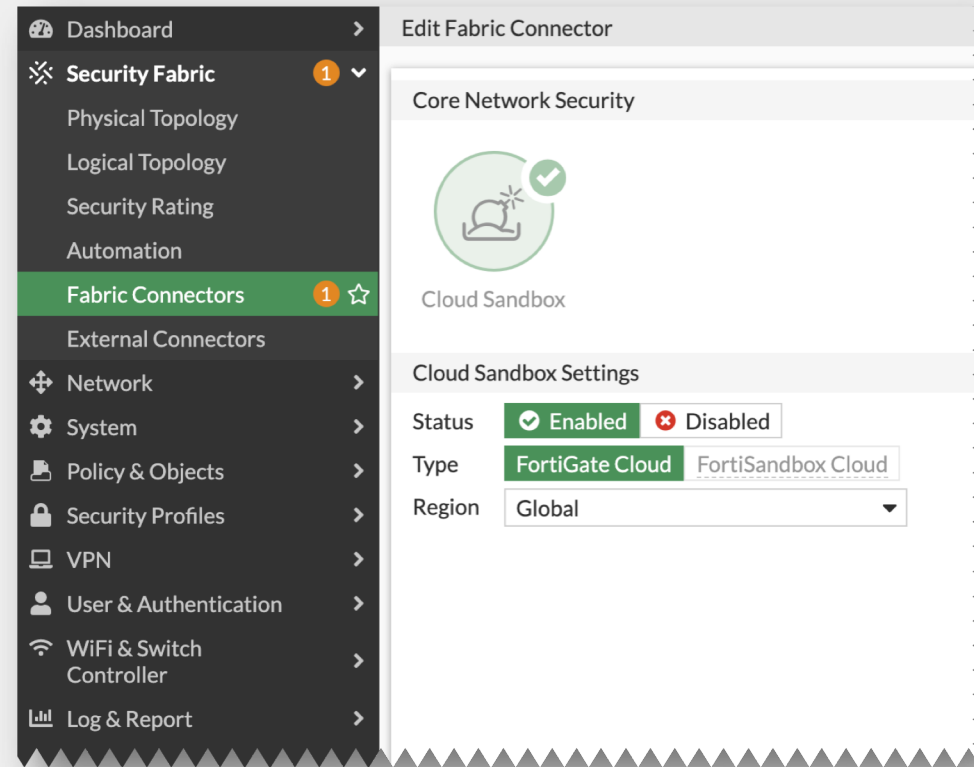


AI-driven Security Operations

Fabric Configuration for FSA Cloud Enhancement

2nd phase enhancement to the configuration of the FSA Cloud Integration

- Includes Support for FSAC entitlement retrieval, guided configuration
- FortiGate Cloud variant is now hidden and has to be enabled via CLI instead





Fabric Management Center



Fabric Management Center

Provision FSW firmware automatically upon authorization

Add option to upgrade of firmware when new access devices is added to FortiGate after authorization automatically

- Requires predefined switch OS to be uploaded onto FGTs
- 4 images of the same switch model for FGTs with disk(s), 1 image for those without disks.

```
config switch-controller managed-switch
  edit "FSW"
    set firmware-provision [ enable |
                           disable ] firmware-provision-version <
                           major.minor.build >
  next
end
```



Fabric Management Center

Link EMS with Exchange Connector

By combining EMS and Exchange connector information, FOS will be able to give user details without the need to do firewall authentication.

- Produce more complete user info for the User Store

FortiClient EMS
Connector



MS Exchange
Connector



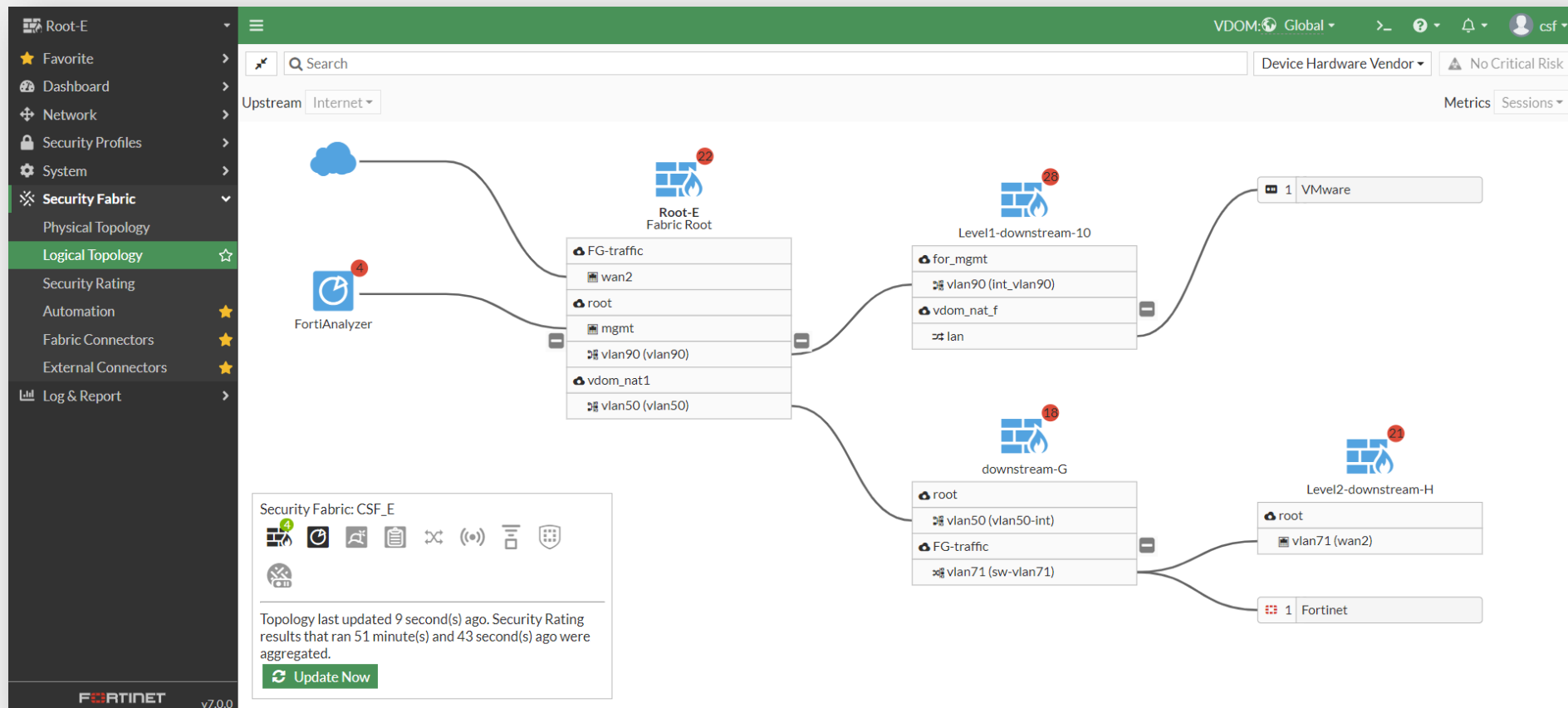
Device Inventory					
Hardware Vendor		Software OS		Status	
Device ID	User ID	Address ID	Software OS ID	Device Family ID	Hardware Vendor ID
Apple					
MACE-MAC-PRO		172.18.58.130 90:54:00:00:00:01	macOS		
iPhone		28:40:30:8F:5:5F	iOS	iPhone	
QA-MAC		172.18.58.245 40:00:00:00:00:00	macOS		
Dell					
FOGA-PC		172.18.58.199 90:54:00:00:00:01	Windows		
WIN-200719		172.18.58.8	Windows		
WIN-200719		172.18.58.130	Windows		
WIN-200719-PC1		172.18.58.130	Windows		
WIN-200719-PC2		172.18.58.130	Windows		

Fabric Management Center

Support for Security Fabric in Multi-VDOM mode

Allow a FortiGate with VDOMs to connect to another FortiGate in a Security Fabric

- Features (as Global scope) include Fabric Topology, Security Rating and Automation



Fabric Management Center

FortiAI, FortiDeceptor, FortiTester, and FortiWeb Extensions



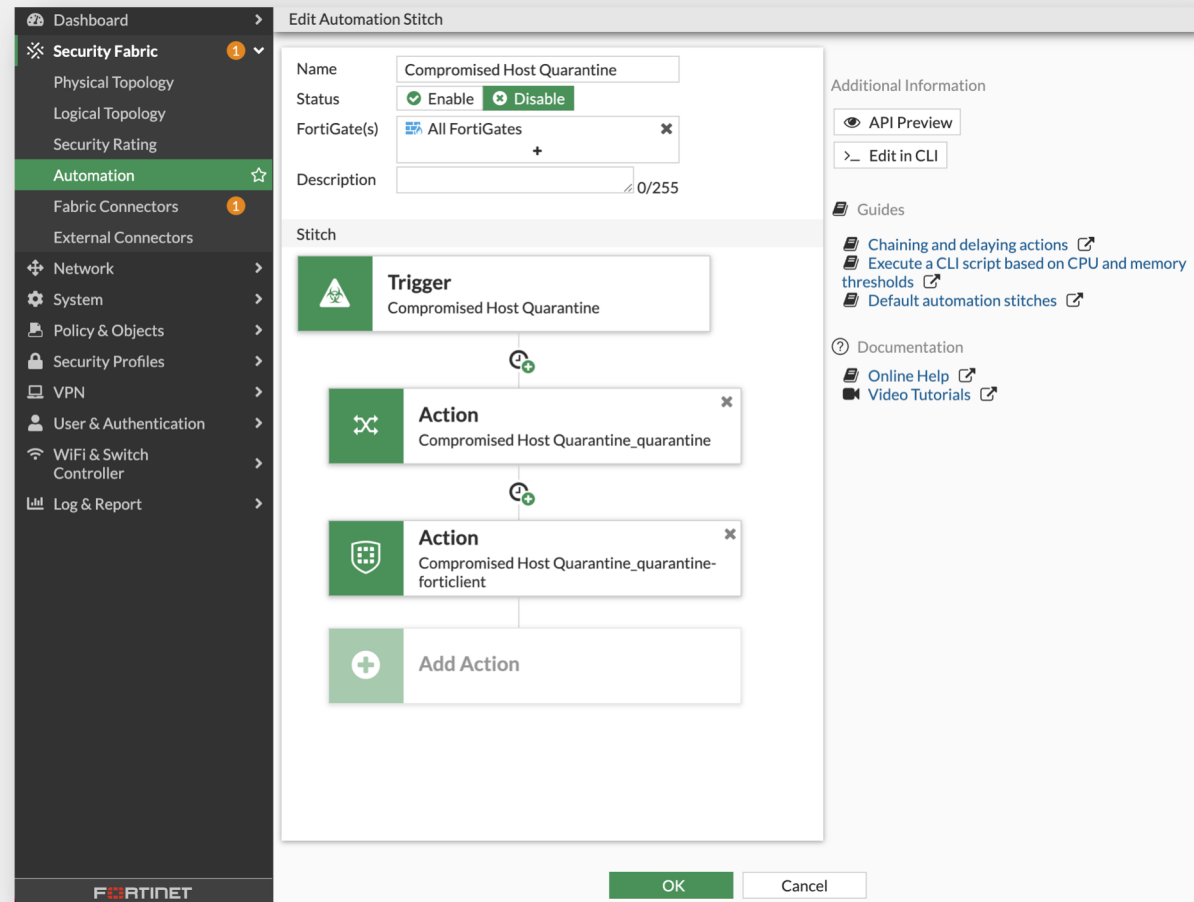
Fabric integration with more Fortinet products to yield unique solutions

Fabric Management Center

Automation Workflow Improvements

Simplify the workflow for managing multiple chained actions, and make it clearer to the user which order the actions will be processed in.

- Also support
 - triggering on multiple event log IDs in the same trigger
 - custom HTTP body code with Slack native notification
 - configuring filters on event logs to narrow down the trigger

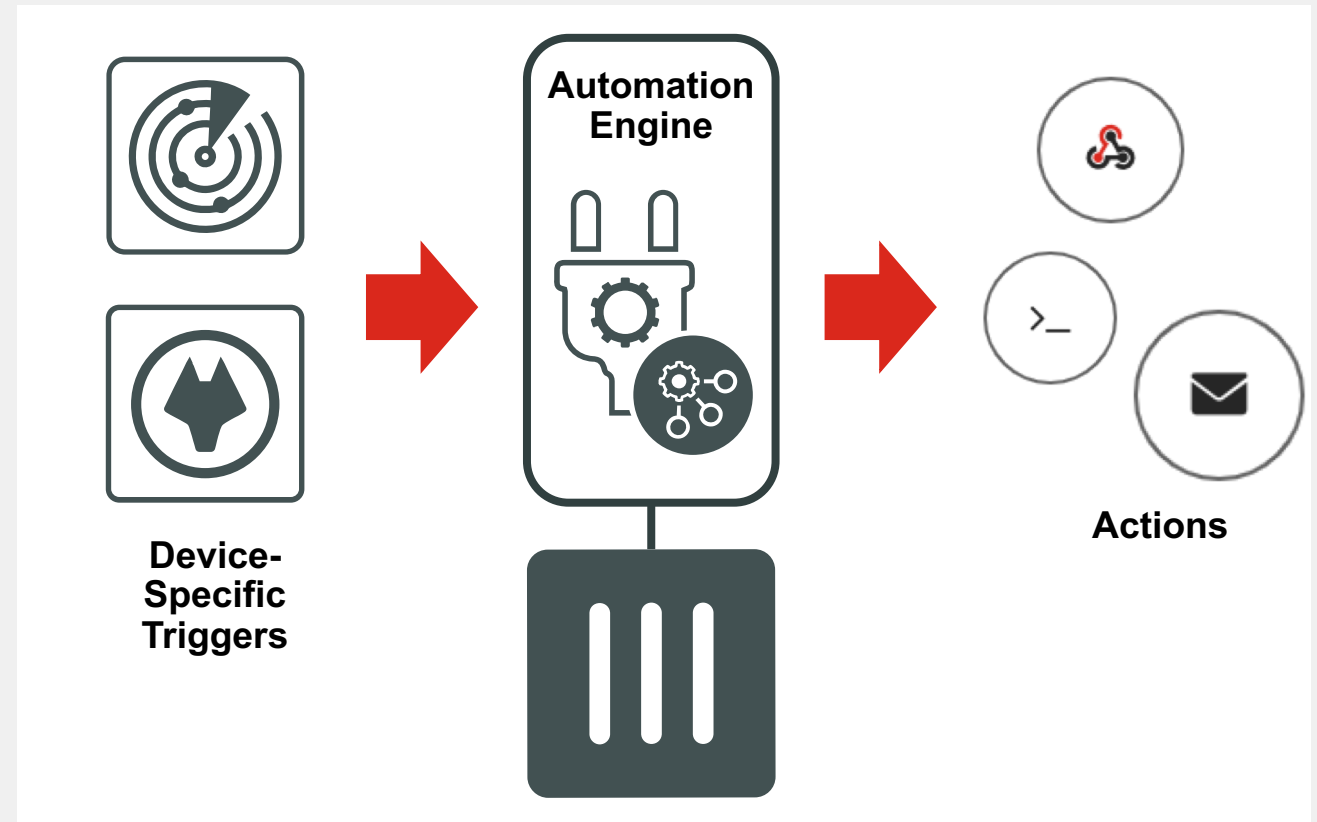


Fabric Management Center

Fabric Devices to trigger Automation Rules

Extend Security Fabric capability by allowing Security Fabric devices to trigger automation rules

- Extend CSF protocol to allow for downstream devices to send queries to an upstream device (eg root FG)
- Similar to FAZ event handling on FGT for front end



Fabric Management Center

Show equivalent REST API commands for GUI actions

Add support to show the REST API commands behind a particular GUI action

- API Preview is added to the right-hand side (gutter) allowing the user to see what API calls will be made when clicking "OK" or "Apply".
- If multiple requests are required, this would be broken into multiple tabs

The screenshot shows the 'System Settings' page in the Fortinet Fabric Management Center. The 'Host name' is 'SG-FTNT'. Under 'System Time', the 'Current system time' is '2021/01/28 17:13:18', the 'Time zone' is '(GMT+8:00) Kuala Lumpur, Singapore', and 'Set Time' is set to 'NTP'. The 'Select server' is 'FortiGuard'. The 'Sync interval' is '60'. The 'Setup device as local NTP server' is checked. The 'Listen on Interfaces' is 'fortilink'. On the right, under 'Additional Information', the 'API Preview' button is highlighted with a red box. Below it, the 'Edit in CLI' button is also visible. The 'API Preview' window is open, showing a message: 'The following REST API requests will be sent when you save your changes. Full API documentation is available [here](#).' Below this, it shows the 'FortiGate' 'SG-FTNT' and a message: 'No changes have been made.' The window also displays a REST API request for PUT /api/v2/cmdb/system/ntp with the following JSON body:

```
{  "method": "PUT",  "url": "/api/v2/cmdb/system/ntp",  "params": {    "datasource": 1,    "vdom": "root"  },  "data": {}}
```

 A 'Copy to clipboard' button is next to the JSON. At the bottom, another REST API request for PUT /api/v2/cmdb/system/global (#1) is partially visible.

Fabric Management Center

MS Teams Connector

New Automation action that provides Microsoft Teams notification

- To configure the Action, an Incoming Webhook connector must first be created on Microsoft Teams.

The screenshot displays the configuration interface for the 'Microsoft Teams Notification' action. It is divided into two sections: '1st Action' and '2nd Action'.

1st Action:

- Name:** teams_1
- Delay:** 0 seconds after previous action
- URL:** https://outlook.office.com/webhook/21828a96-9be3-4b63-b22d-da8c1dbeedd8@2c36c478-3d00-452f-8535-48396f5f01f0/IncomingWebhook/40257cf7e532460b84a10360d252716c/028f9d33-8ba1-4cb0-8b91-62b25a8c3911
- Message:** %%log%%

2nd Action:

- Name:** teams_2
- Delay:** 10 seconds after previous action
- URL:** https://outlook.office.com/webhook/21828a96-9be3-4b63-b22d-da8c1dbeedd8@2c36c478-3d00-452f-8535-48396f5f01f0/IncomingWebhook/40257cf7e532460b84a10360d252716c/028f9d33-8ba1-4cb0-8b91-62b25a8c3911
- Message:** This is for test.

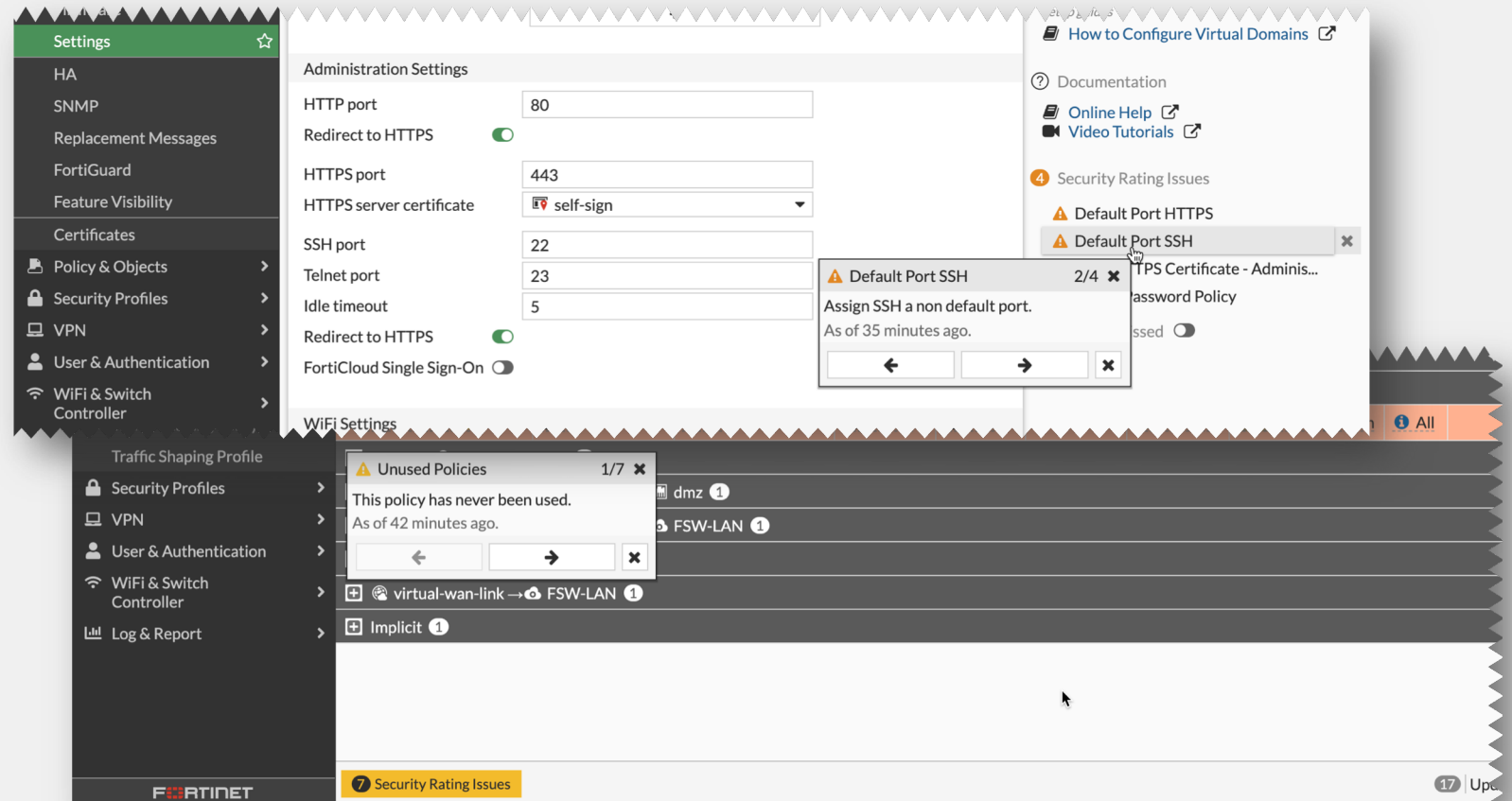
On the right side of the interface, there are two circular icons: a green one with a Teams logo and a checkmark, labeled 'Microsoft Teams Notification', and a red one with a webhook icon, labeled 'Webhook'.

Fabric Management Center

Security Rating Overlays

Security Rating notifications are shown on the settings page which has configuration issues as determined by Security Rating

- Click to open the recommendation to see which configuration item needs to be fixed
- Notifications appear either in the gutter, the footer or as a mutable
- Security Rating License is required for some of the checks and associated pages

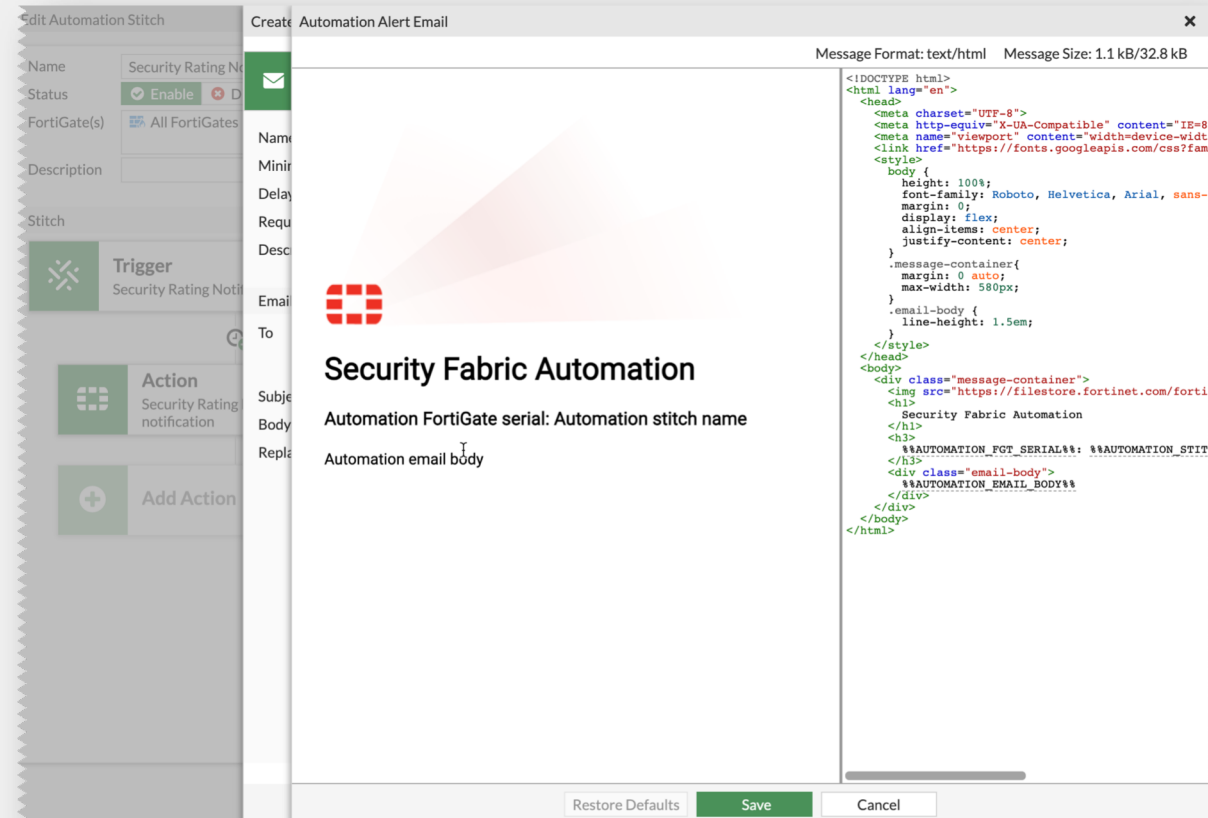


Fabric Management Center

Use replacement message for email alert automation

Automation Email Action can now leverage formatting to create branded email alerts.

- Replace plain text in “Email body” used by “Email” action
- All replacement message templates will be updated to use a new modern style at the same time
- Limited to share single replacement message for all triggers. Subsequent release will allow for different replacement messages for each trigger.

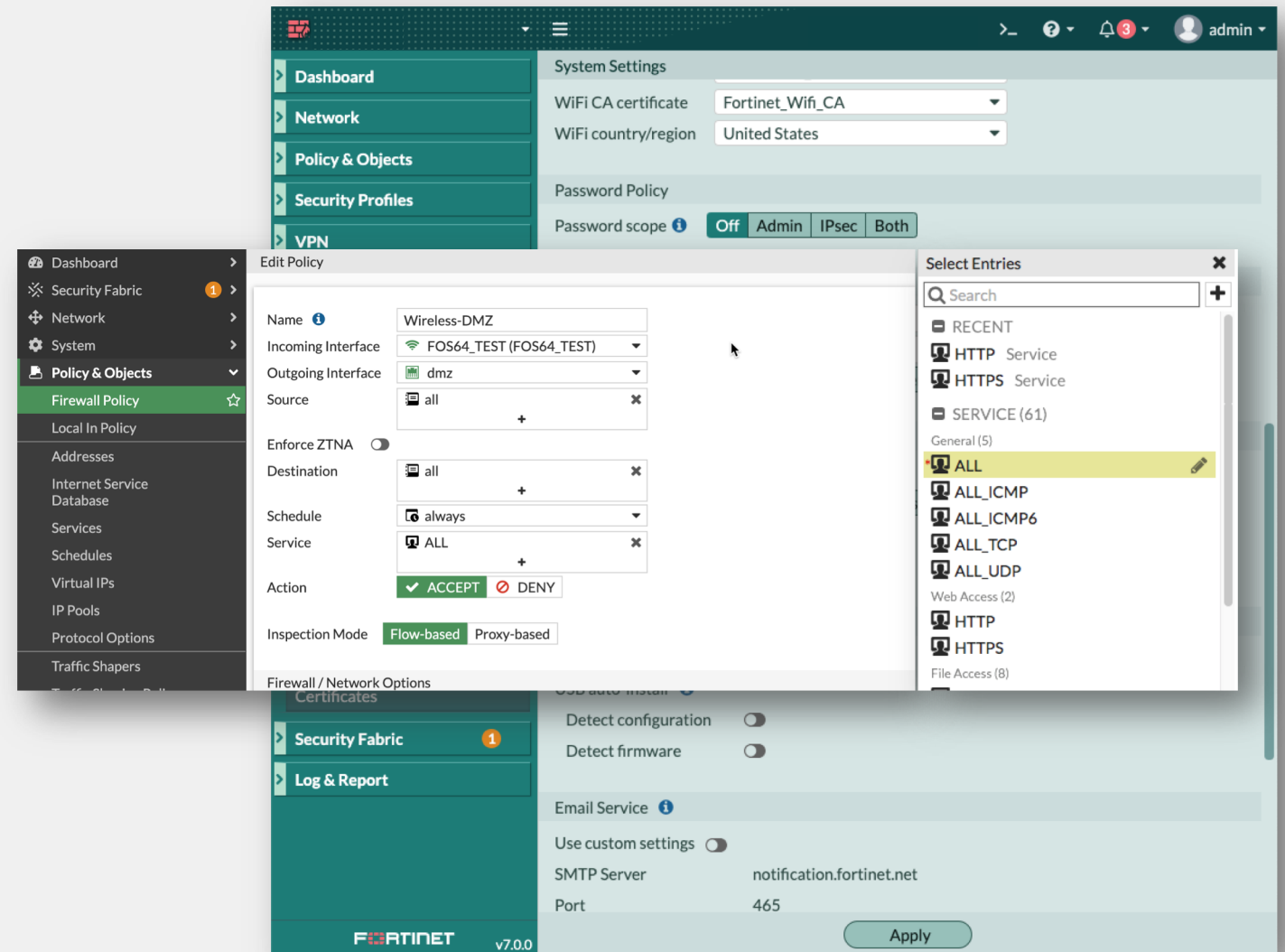


Fabric Management Center

Fabric UX Improvements

Adopting new unified UX design system for consistency and improvements across Fabric products

- Initial components to include navigation, eventually rolled out to other components and products
- Improvement to “Global Search” feature
- Other examples
 - Recently and frequently used objects can be listed near the top
 - sort search/filter results alphabetically or by relevance
 - Add support for nested tooltips
- More themes are added, including the retro v3.0



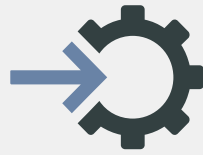
Fabric Management Center

Fabric / Automation



**Simplified pairing
between
FOS/FMG/FAZ**

-
- Use OAuth-like dialog to log into remote FMG/FAZ to authenticate FG request for pairing



**FortiCloud Admin
login**

-
- Allow SAML SSO using FortiCloud credentials
 - Disabled by default



**Threat Feed
Connector per-
VDOM**

-
- Extends Threat Feed connectors to each VDOMs



**FortiGuard
Services**



FortiManager Cloud				•
FortiAnalyzer Cloud				•
FortiCloud SOCaaS NEW				•
SD-WAN Overlay Controller VPN Service				•
SD-WAN Cloud Assisted Monitoring				•
SD-WAN Orchestrator Entitlement				•
FortiConverter Service			•	•
FortiGuard IoT Detection Service			•	•
FortiGuard Industrial Service			•	•
FortiGuard Security Rating Service			•	•
FortiGuard Anti-Spam Service		•	•	•
FortiGuard Web & Video ² Filtering Service		•	•	•
FortiGuard Advanced Malware Protection (AMP) - Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard App Control Service	•	•	•	•
FortiCare (incl. Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB)	24x7	24x7	24x7	ASE ¹
Bundles	Advanced Threat Protection	Unified Threat Protection	Enterprise Protection	360



FortiOS 7.0 Services

Subscription Service	Type	Usage	Remark
IoT MAC Database (7.0 NEW)	MAC Address List	Device Detection (visibility) WiFi Access	Available as part of FortiCare bundled service
DDNS	Cloud-based Hosted Service	DNS Setting (IPv6 support – 7.0 NEW)	Available as part of FortiCare bundled service
Video Filtering NEW	Cloud-based Query	Video Filter Profile	Available as part of Web Filtering subscription
FortiIPAM	Cloud-based Hosted Service	Interface Setting	EoL 2021 NEW
FortiAnalyzer Cloud	Cloud-based Hosted Service	Cloud-based FortiAnalyzer (some features may not be available, now includes NEW Traffic Logs)	Requires additional FortiCloud Premium, optional storage top-up SKUs available
FortiCloud SOCaaS NEW	Cloud-based Hosted Service	Cloud-based SOC service	customer minimum baseline of capability is required



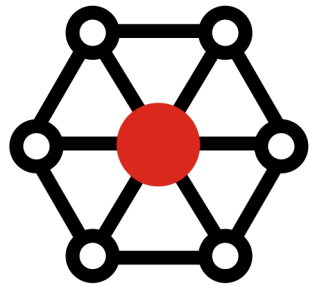
FortiCloud SOCaaS

Managed SOC Monitoring

Fortinet SOC analysts monitor customer's network for security events, and to triage and escalate threats

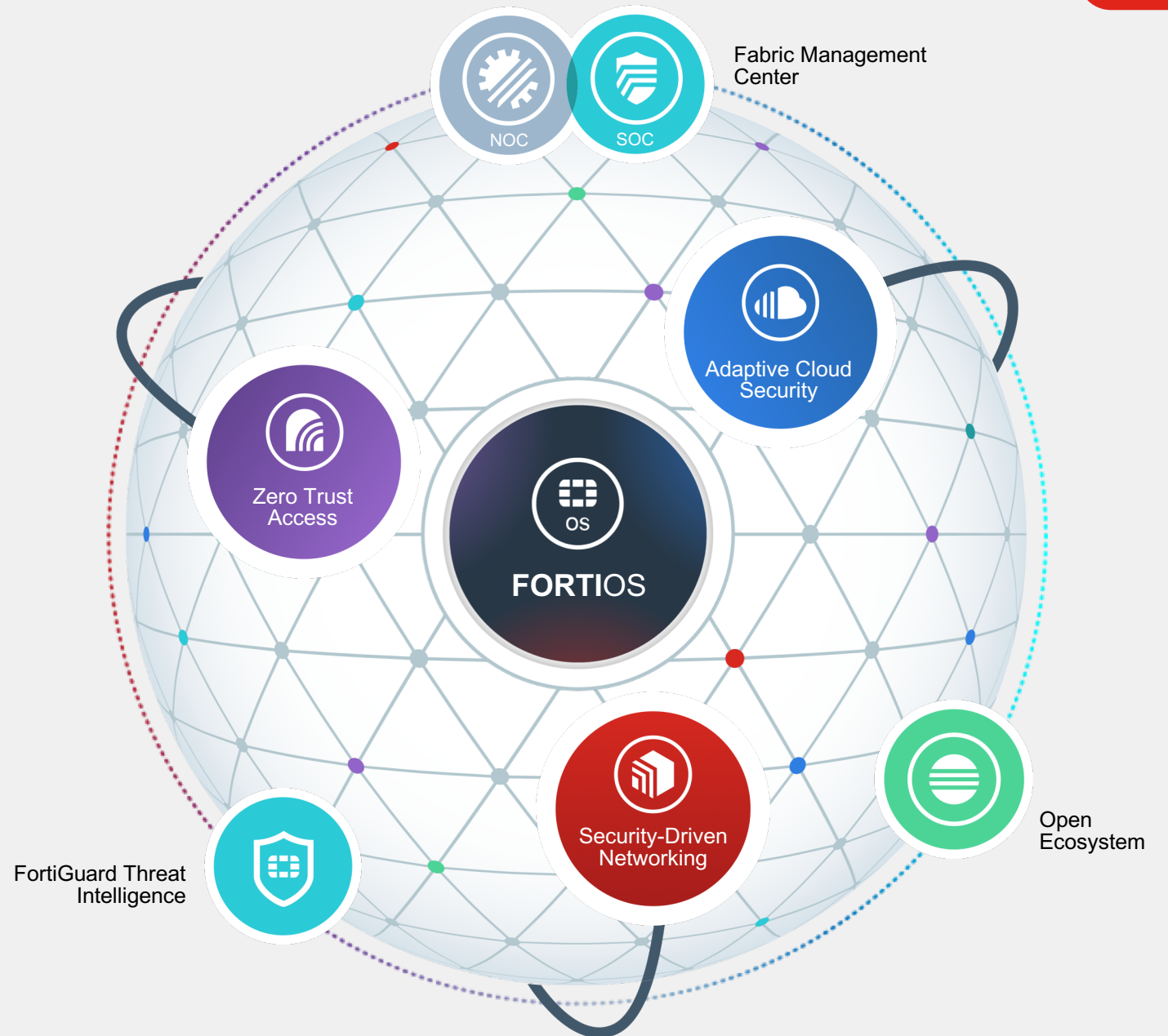
- 7x24x365 with Global SoC locations
- Security focused skill staff with technical expertise on Fabric Devices and Incident Response (IR) best practices





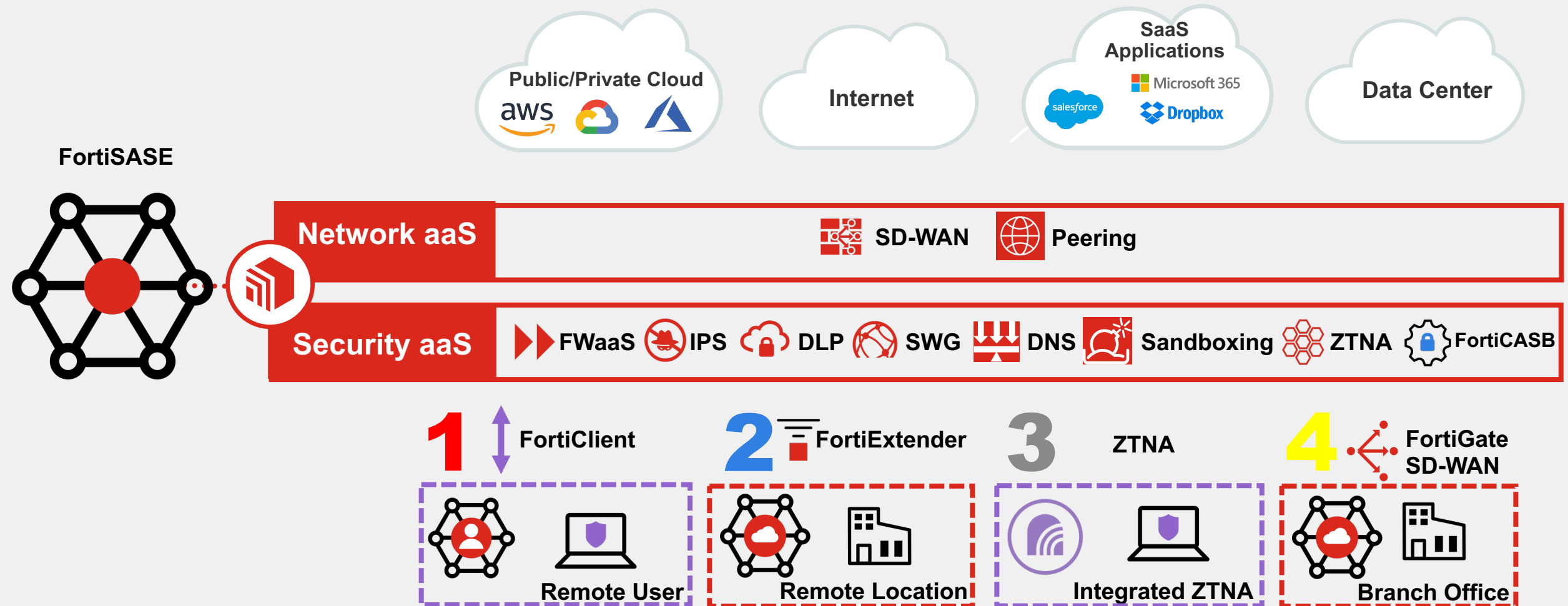
FortiSASE

**Secure Access Service
Edge**

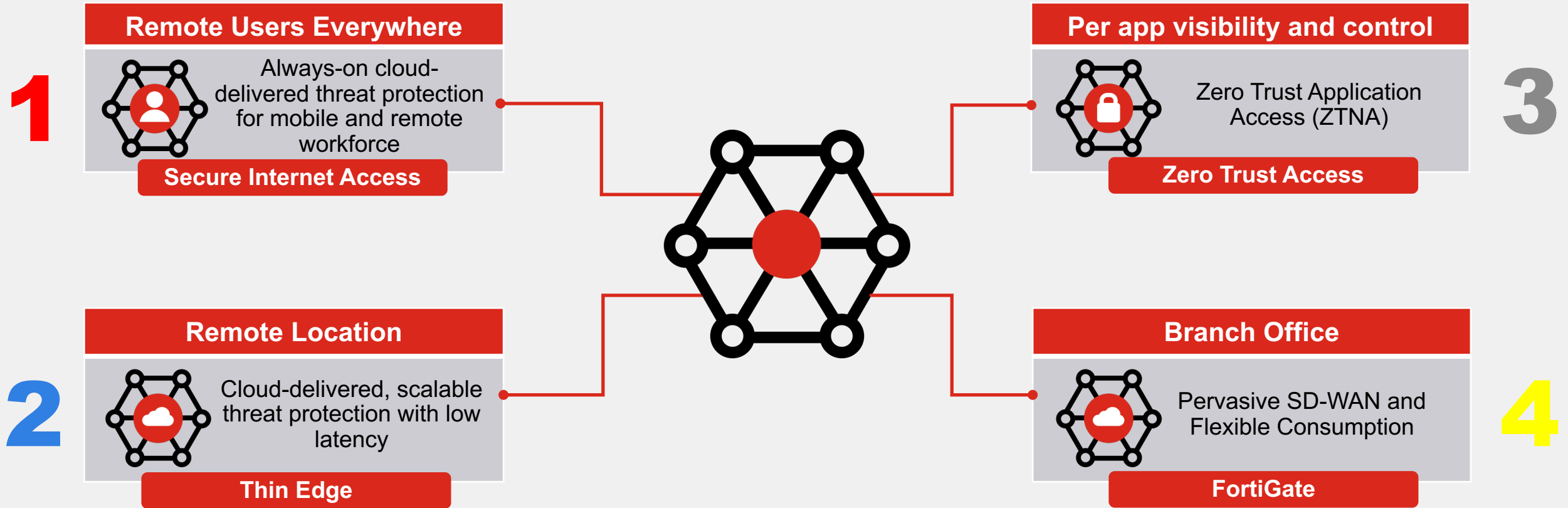


FortiSASE Vision

Cloud-native security for all Access Edges



FortiSASE - Use Cases



FortiSASE SIA - Out of Box-Ready Functionality 1



	SASE Edition Windows, MAC, Linux
Zero Trust Security	
Zero Trust Agent	✓
Dynamic Security Fabric Connector	✓
Vulnerability Agent & Remediation	✓
SSL / IPSEC VPN with MFA	✓
USB Device Control	✓
Automated Endpoint Quarantine	✓
Application Inventory	✓
Cloud Based Endpoint Security (SASE)	
SSL Inspection	✓
Inline AV & Anti-Malware	✓
Intrusion Prevention (IPS)	✓
FortiGuard Web Filtering	✓
Application Firewall	✓
Data Leak Prevention	✓
Additional Services	
24 x 7 Support	Included
SASE Cloud Management	Included
SASE Cloud Logging	Included
Best Practice Onboarding Service	Included in 1st Year

Available in Packs of 25, 500, 2000 and 10,000



FORTINET®