



Lucky Number

引領資安防禦全面升級

Paul Li

Technical Consultant Taiwan



NP7

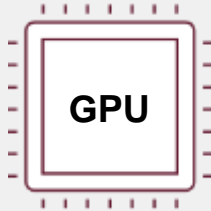
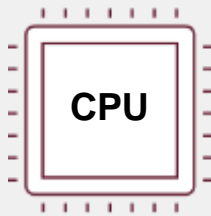
Security
Processing
Unit



Fortinet Designed Security Processing Unit (SPU)

Industry Leading Hyperscale Security with NP7

Gaming and AI Systems



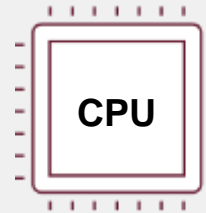
Graphical Processing Unit
(GPU)

Security Processing Unit (SPU)



**Network Processor
(NP)**

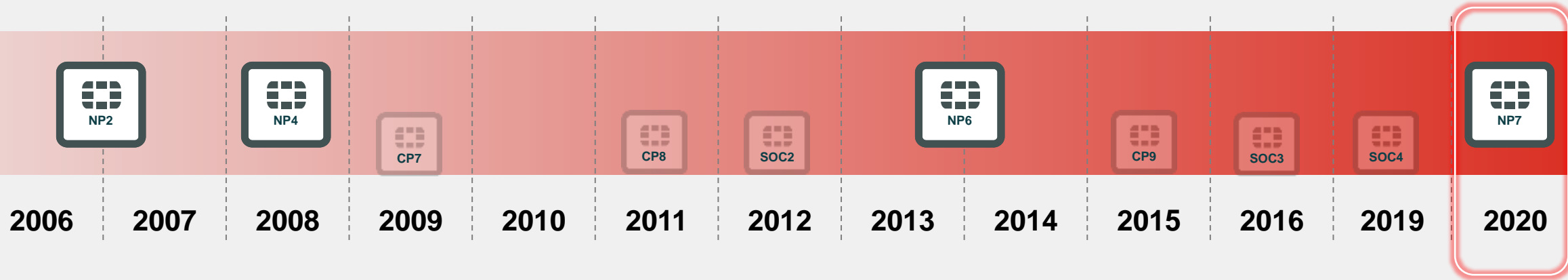
Off-Loads Networking
Functions











**Content Processor
(CP)**

Off-Loads Security
Functions

Redefining Security for Hyper Scale Data Centers



NP7 Leapfrogs competitors and offers security at a scale that is magnitudes higher

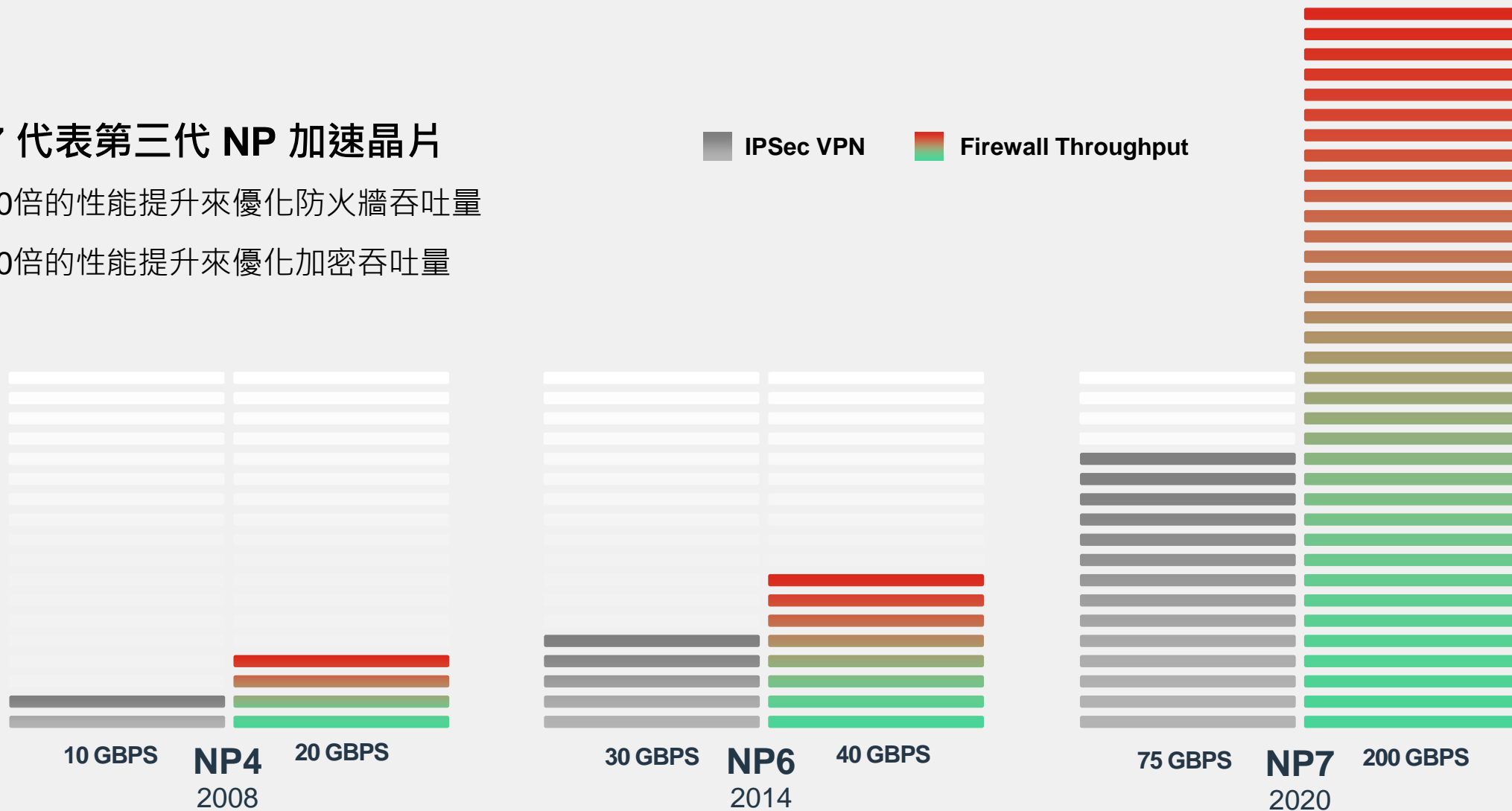
							
2 X 100 G	100 M		2 M/SEC	200GBPS	75 GBPS	VXLAN	20 W
NETWORK PORTS	CONCURRENT SESSIONS	HARDWARE LOGGING	SESSION SETUP RATE	FORWARDING THROUGHPUT	IPSEC THROUGHPUT	NVGRE	POWER ESTIMATION



High Performance DNA

NP7 代表第三代 NP 加速晶片

- 以10倍的性能提升來優化防火牆吞吐量
- 以10倍的性能提升來優化加密吞吐量



Optimizing Performance: How it compares?

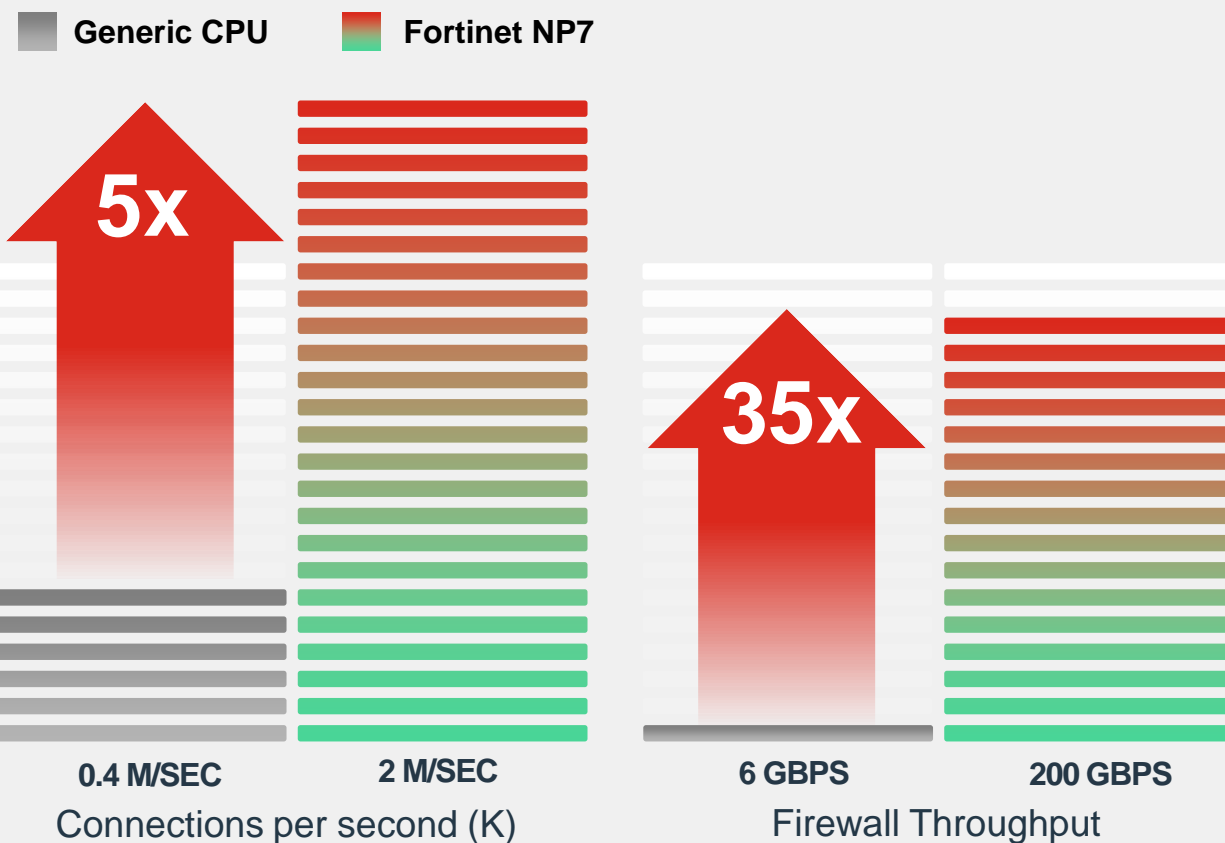
General Purpose CPU vs Security Compute: Forwarding/ Dataplane

Ultra High Performance

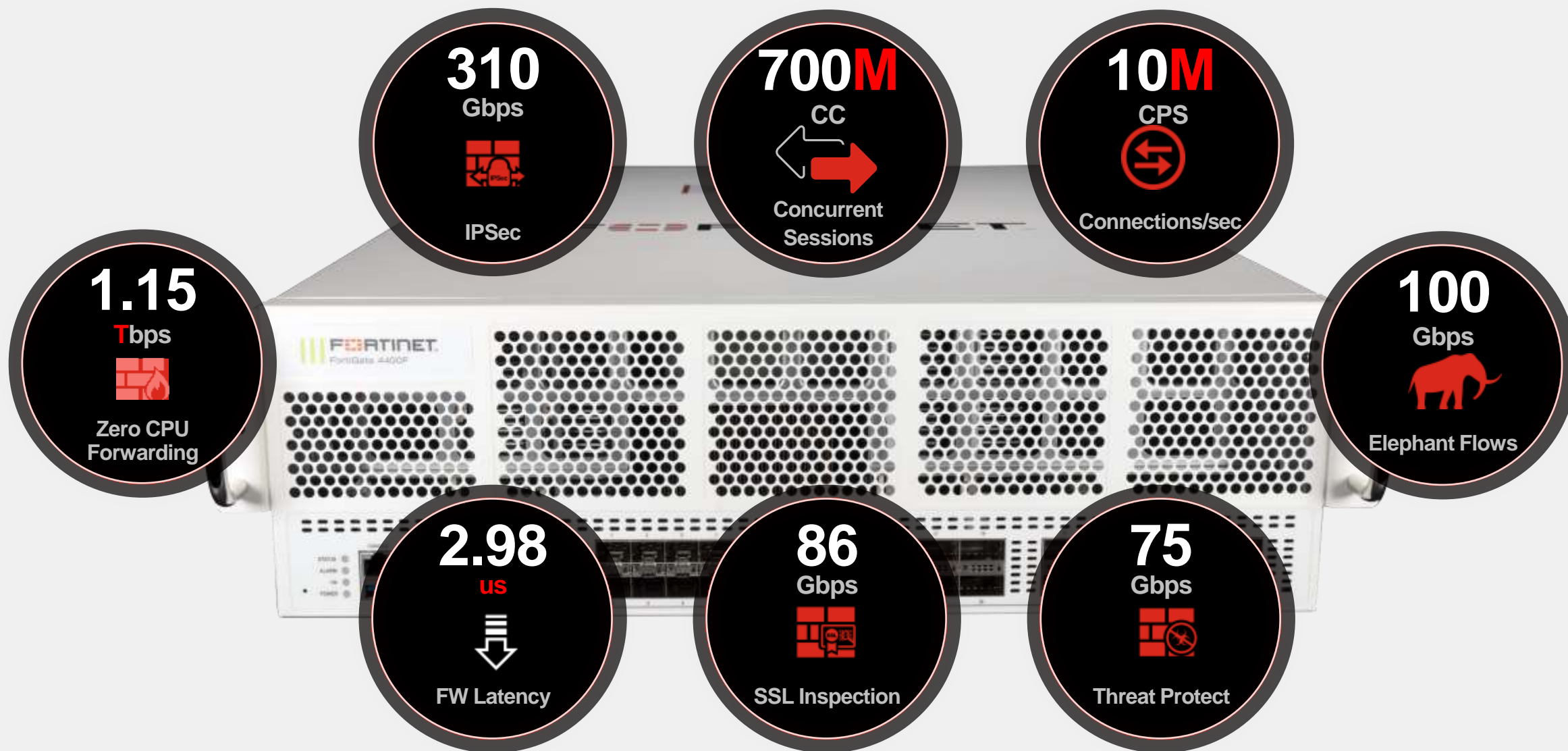
- 硬體架構的創新拉大了性能上的巨大落差
- Why SPUs? 規模經濟
- CPU 將繁重的維護 session table 以及連線初始建立的工作 offloaded 至 NP7
- CPU 可以將完整的資源投入至更複雜的應用程式處理

專門設計的 ASIC 加速晶片具有無與倫比的性價比，這是通用平台無法滿足的

Firewall Acceleration and Connections/sec



FortiGate 4400F Key Specifications





The industry's highest-performing cybersecurity platform

What's New in FortiOS 7.0



Fortinet Security Fabric

Broad

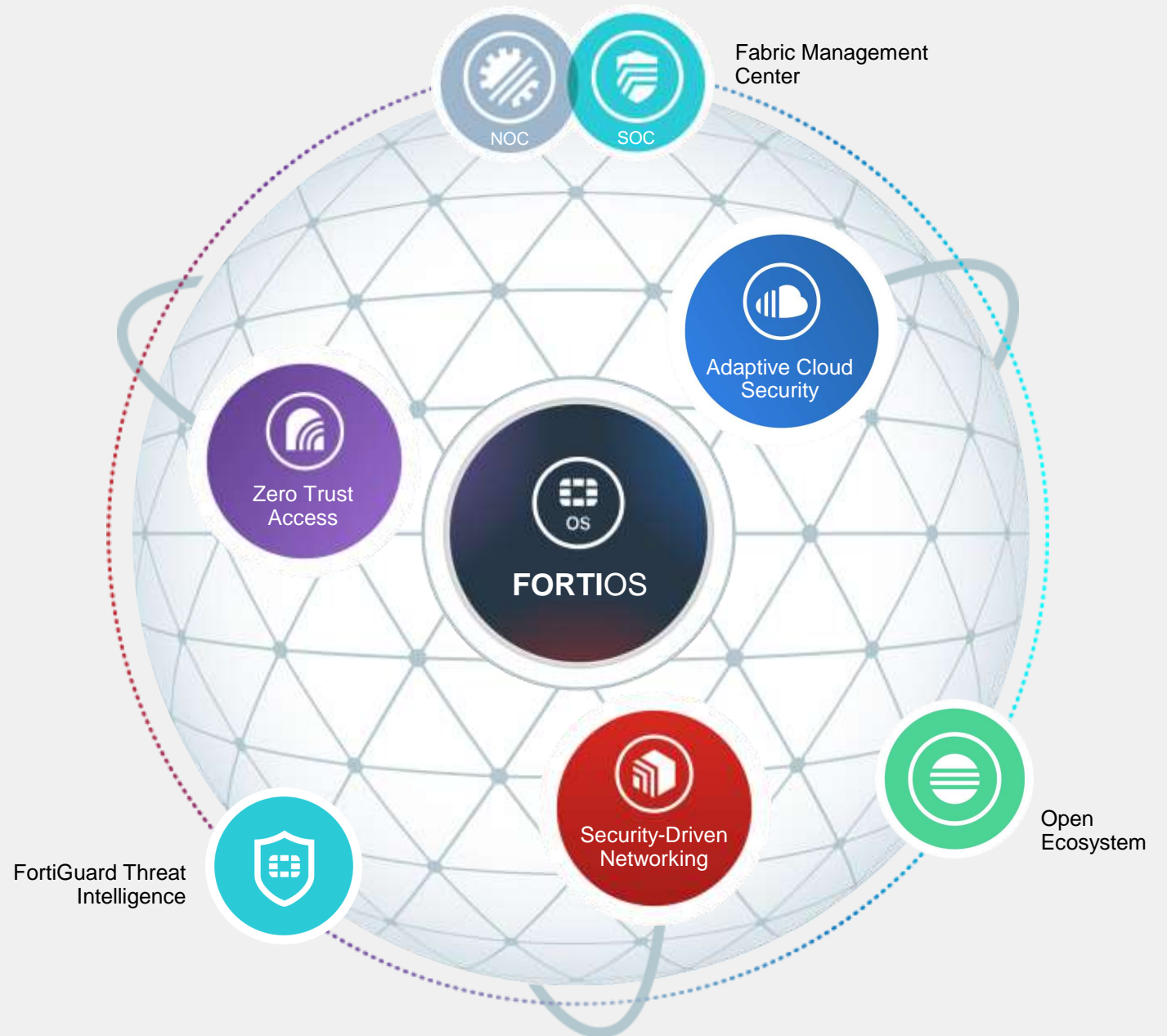
- 資訊安全不只是單點防護，而是要落實在每個服務層面。

Integrated

- 多面向資安防護整合
- 分享與通報即時資安威脅
- 提升防護成效並降低維運複雜

Automated

- 具備AI智能驅動的安全網路
- 打造自動高效的資安生態系統



FOS 7 – 300+ New Features Across the Fabric

Security Driven Networking (SASE Edge - SASE)

- Securing remote workforce with orchestration portal for SASE capabilities
- Securing thin branch with FEX 200F + 25Mbps subscription
- New Thin Edge line us (LTE/5G)
- Journey to Zero Trust with extended risk posture checking

Security Driven Networking (WAN Edge: SD-WAN)

- Increased Resiliency (FEC/DUP)
- Enhanced packet duplication
- Accelerated Convergence (FWF 80F)
- Efficient Operations (scalable ZTP, Analytics, Passive WAN Measurement)
- Accelerated convergence for Thin & WAN edge

Security Driven Networking (DC Edge: NGFW)

- Ultra-Scalability with pay as you grow model (FGT 7121F, 400G)
- Attack surface Reduction (Video filtering , DNS)
- Efficient Operations with network automation (Policy Learn mode, automated upgrades)

Security Driven Networking (LAN Edge: WiFi/Switch)

- Unified code base (L3 FortiLink, NAC Visibility and Zero trust response)
- Convergence (WLM and AIOps on FMG, FortiLAN cloud)
- Simplified Operation AI/ML driven wireless easy classification and remediation)

Security Driven Networking (LTE Edge: 5G)

- 5G backup (+SD-WAN for WWAN with new dual modem)
- LTE portfolio expansion (+WWAN application release, 101F/201F)
- SASE bundle for Thin edge and remote workers

Zero Trust Access (ZTNA)

- single policy for on-net / off-net behavior
- Better & easier VPN with automated setup for HW/VM/SASE & cloud
- Granular access with role based application access
- Leverage existing products

Adaptive Cloud Security (VM, CWP, CASB)

- Centrally managed hybrid cloud (expended support & multi tenant policies)
- Effective usage of resources with autoscaling
- Extended application support for CASB
- Container guardian

Adaptive Cloud Security (WAF & Email)

- Email continuity switch to FortiMail cloud when service go down
- FortiWeb enhanced with ML-based API discovery, deeplearning and more.
- FortiADC/FortiGSLB user experience visibility and Auto-Scaling capabilities

FortiGuard Threat Intelligence (Security Services)

- Increased Attack Surface Coverage – Video Filtering enhancement to our web filtering offering
- Security Rating expended to **Fabric Rating**
- **IoT real-time query service**

Fabric Management Center (SOC)

- MITRE attack analysis with expansion in cover and automated protection across the fabric and ecosystem
- SOAR enhanced AI/ML & out-of-the-box content packs. Integrations. FSR cloud. mobile app.
- IR unified console, FORTISOAR container, FortiCASB connector

Fabric Management Center (NOC)

- Insider threat analysis with EUBA support
- Enhanced visibility with extended product support across the Fabric & SD-Branch
- Efficient and scalable operation with SIEM
- SaaS management with Unified GUI, easy on boarding with ZTP templet and more & efficient full branch operations

Advance Services

- SOC as a Service to augment organization and MSSP's SOC
- Best Practice Evaluation
- FortiGuard Consultant



Deliver Enterprise Protection And User Experience At Any Edge

Network Security



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

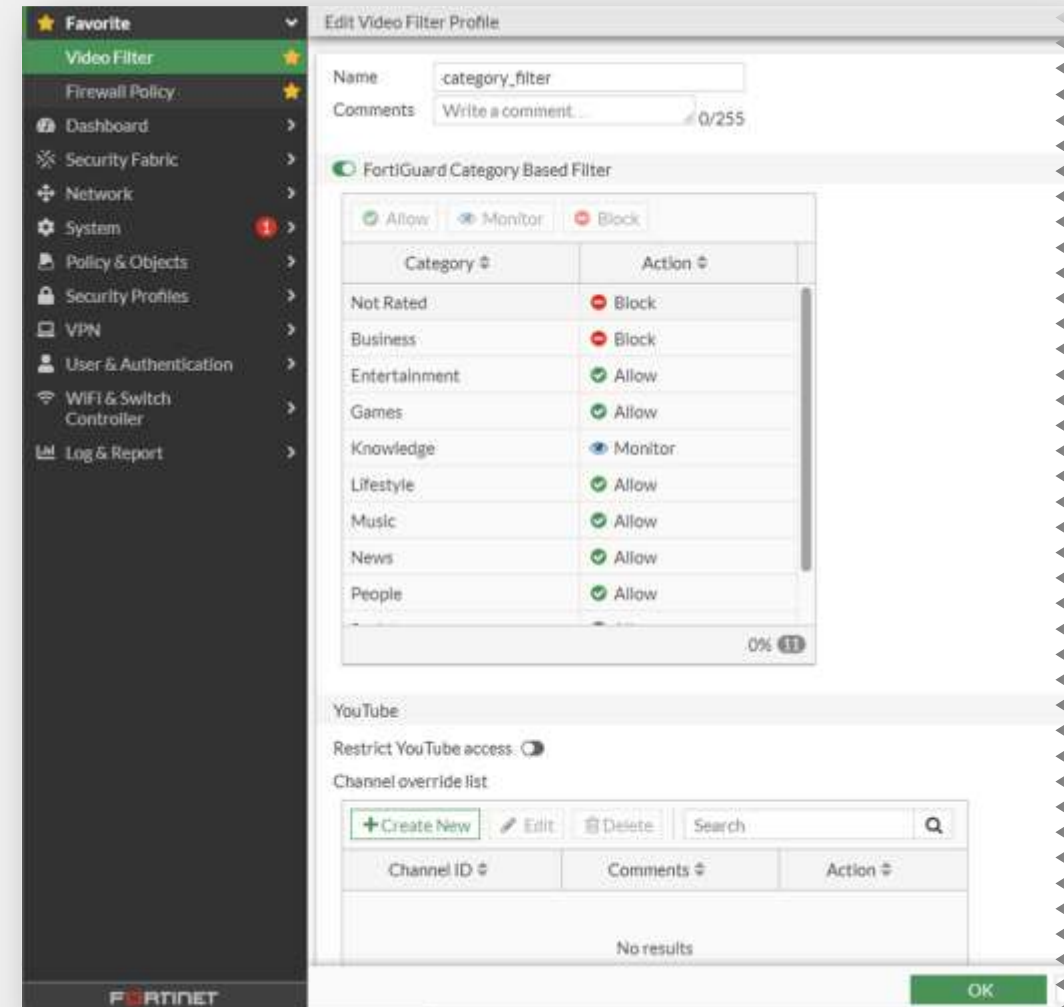
- For YouTube, Vimeo and Daily Motion
- static filter option for YouTube channels
 - With the video filter profile, you can filter YouTube videos by channel ID for a more granular override of a single channel, user, or video.
 - The video filter profile is currently supported in proxy-based policies and requires SSL deep inspection.

The following identifiers are used for YouTube channels:

`www.youtube.com/channel/<channel-id>`

`www.youtube.com/user/<user-id>`

`www.youtube.com/watch?v=<string>`



Security-driven Networking

FortiGuard Video Filtering Service

Edit Video Filter Profile

Name: Only-Allow-FTNT-TWN

Comments: Write a comment... 0/255

☒ FortiGuard Category Based Filter

☒ Allow ☐ Monitor ☐ Block

Category	Action
Not Rated	<input type="radio"/> Block
Business	<input type="radio"/> Block
Entertainment	<input type="radio"/> Block

YouTube

Restrict YouTube access ☒ Moderate ☒ Strict

Channel override list

[+ Create New](#) [Edit](#) [Delete](#) Search

Channel ID	Comments	Action
UCm0oqRiOhTtbrddV9wH2uLg	Fortinet Taiwan	<input checked="" type="radio"/> Allow

Edit Channel Override Entry

Channel ID: Ucm0oqRiOhTtbrddV9wH2uLg

Comments: Fortinet Taiwan 15/255

Action: ☒ Allow ☐ Monitor ☐ Block

[OK](#) [Cancel](#)

Security Profiles

AntiVirus ☐

Web Filter ☐

Video Filter ☒ **VF** Only-Allow-FTNT-TWN [Edit](#)

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

Email Filter ☐

ICAP ☐

Web Application Firewall ☐

SSL Inspection [SSL](#) deep-inspection [Edit](#)

Decrypted Traffic Mirror ☐

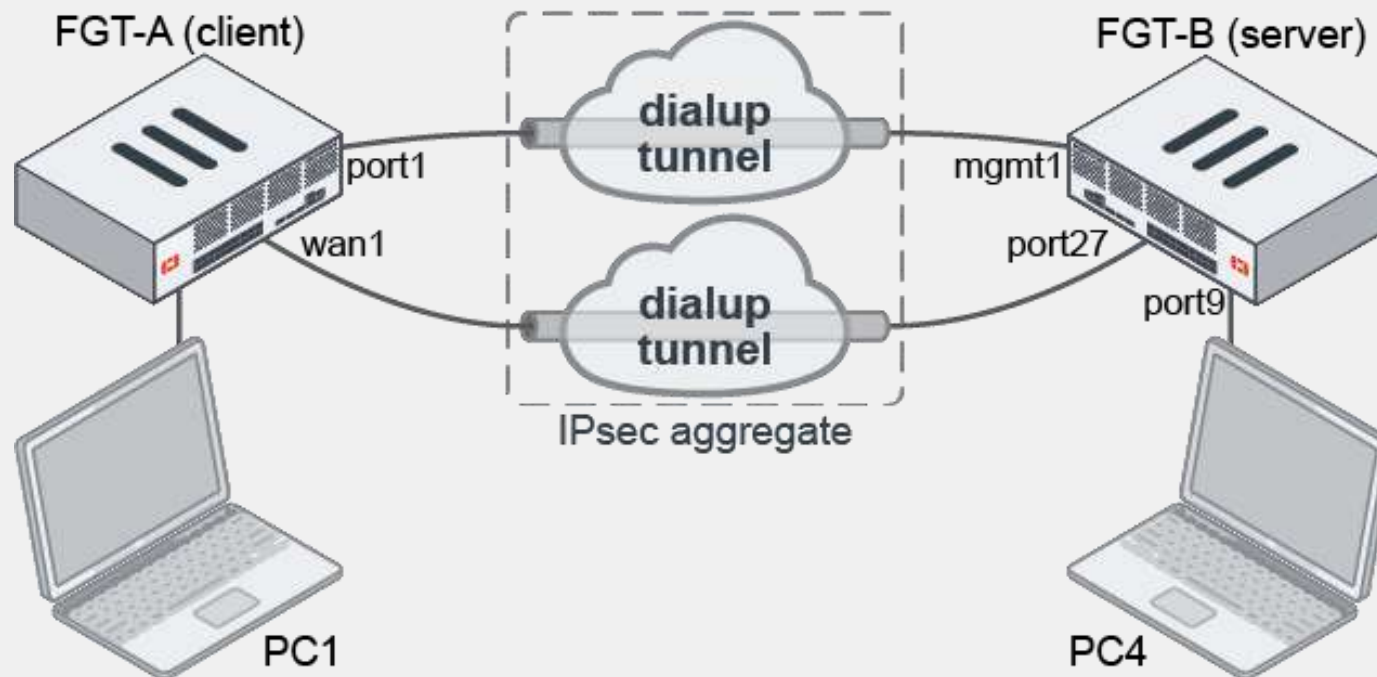


Security-driven Networking

Packet duplication Improvement

Packet duplication for dial-up IPsec tunnels

- To support packet duplication on dial-up IPsec tunnels between sites, each spoke must be configured with a location ID.
 - On the hub, packet duplication is performed on the tunnels in the IPsec aggregate that have the same location ID.
 - Multiple dial-up VPN tunnels from the same location can be aggregated on the VPN hub and load balanced based on the configured load balancing algorithm.
- In this example, packet duplication is performed between two dial-up IPsec tunnels in order to support packet duplication.



Security-driven Networking

SSL VPN Client on FortiGate

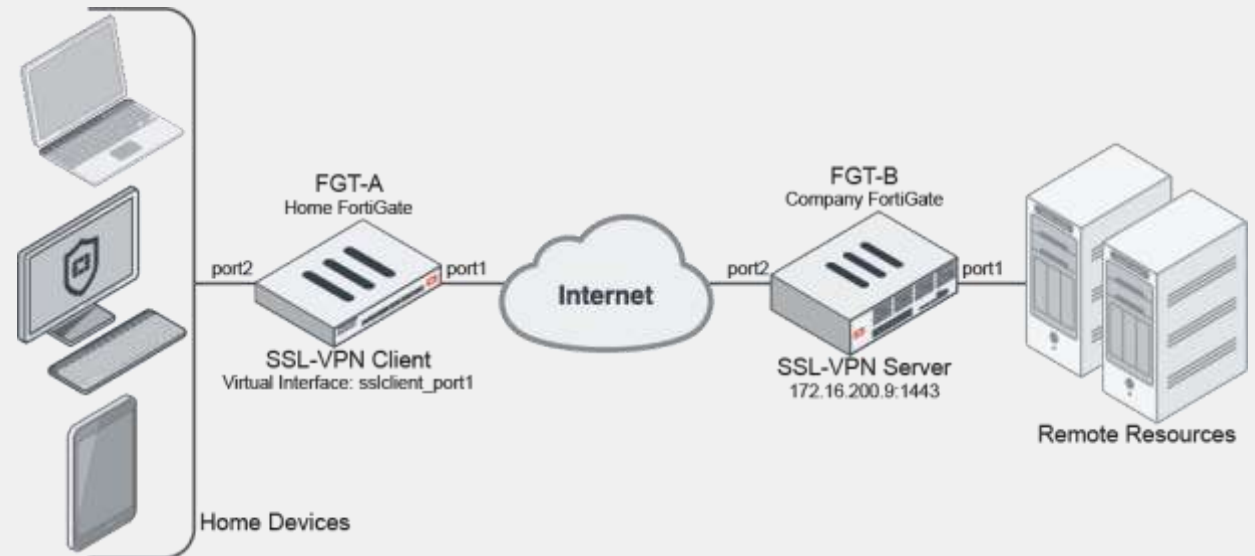


FortiGate as SSL VPN Client

- The FortiGate can be configured as an SSL VPN client, using an *SSL-VPN Tunnel* interface type.
- When an SSL VPN client connection is established, the client dynamically adds a route to the subnets that are returned by the SSL VPN server.
- FortiOS can be configured as an SSL VPN server that allows IP-level connectivity in tunnel mode, and can act as an SSL VPN client that uses the protocol used by the FortiOS SSL VPN server.
- This allows hub-and-spoke topologies to be configured with FortiGates as both the SSL VPN hub and spokes.

For an IP-level VPN between a device and a VPN server, this can be useful to avoid issues caused by intermediate devices, such as:

- ESP packets (IP protocol 50) being blocked.
- UDP ports 500 (IKE) or 4500 (IPSEC NAT-T) blocked.
- Fragments being dropped, causing IKE negotiation that uses large certificates to fail if the peer does not support IKE fragmentation.



Security-driven Networking

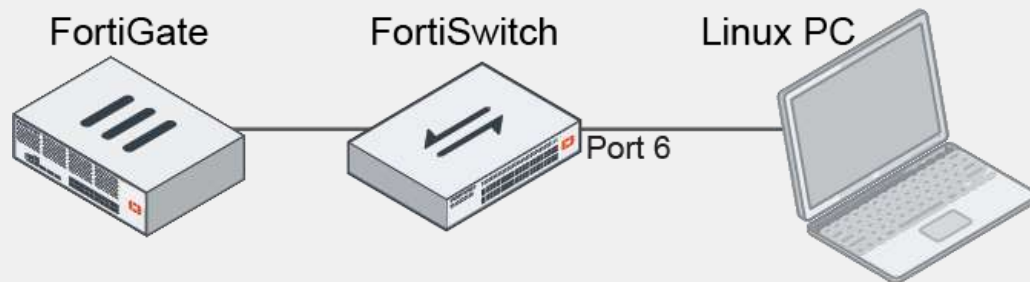
Integrated NAC feature on FortiSwitch



- You can configure a FortiSwitch network access control (NAC) policy within FortiOS that matches devices with the specified criteria, devices belonging to a specified user group, or devices with a specified FortiClient EMS tag.
- Devices that match are assigned to a specific VLAN or have port-specific settings applied to them.

Example

In this example, NAC settings are enabled and configured so that a **Linux** PC is automatically moved into a VLAN dedicated to Linux PCs after it comes online and gets identified.



```
# diagnose user device get 00:11:32:24:91:90
vd root/0 00:11:32:24:91:90
created 6214173s gen 1393
ip 10.1.200.151 src mac
hardware vendor 'Synology' sr
os 'Linux' src tcp id 163 wei
host 'SYNOLOGY_DS213J' sr
```

Device Patterns	
Category	Device User EMS Tag
MAC address	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Hardware vendor	<input type="checkbox"/>
Device family	<input type="checkbox"/>
Type	<input type="checkbox"/>
Operating system	<input checked="" type="checkbox"/> Linux
User	<input type="checkbox"/>

Security-driven Networking

Integrated NAC feature on FortiSwitch



When Enabled, device connected to defined ports will be put into the onboarding VLAN, to be match against NAC policies for next action

- NAC can be applied to specific switch and/or ports
- Access mode on the affected switch ports are changed from “Normal” to “NAC” while the Native VLAN is set to the onboarding VLAN
- Various device match methods with ability to
 - Redirect to desired VLAN
 - Change port settings
- Matched device can be viewed from drill in NAC policy

NAC Settings

Onboarding VLAN: nac.port16

Bounce port: port2

Use NAC policies on FortiSwitch ports: FS108D3W15000170

Edit NAC Policy

Name: Linux_to_Vlan1000

FortiSwitches: All

Description:

If device matches all of the following patterns:

Category: Device User

MAC address: ☐

Hardware vendor: ☐

Device family: ☐

Type: ☐

Operating system: Linux

User: ☐

Then:

☒ **Assign VLAN**
Assign a specific VLAN to a device matching above patterns.

☐ **Apply Port Specific Settings**
Apply LLDP Profile, QoS Policy, 802.1x Policy...

VLAN: vlan_Linux

Traffic action: Allow Block

Port Configuration Table:

Port	Mode	Edge Port	Spanning Tree Protocol	FAP_LINK	qtn.port16
port1	Normal	✔	✔	FAP_LINK	qtn.port16
port2	NAC	✔	✔	nac.port16	qtn.port16

OK **Cancel**



Security-driven Networking

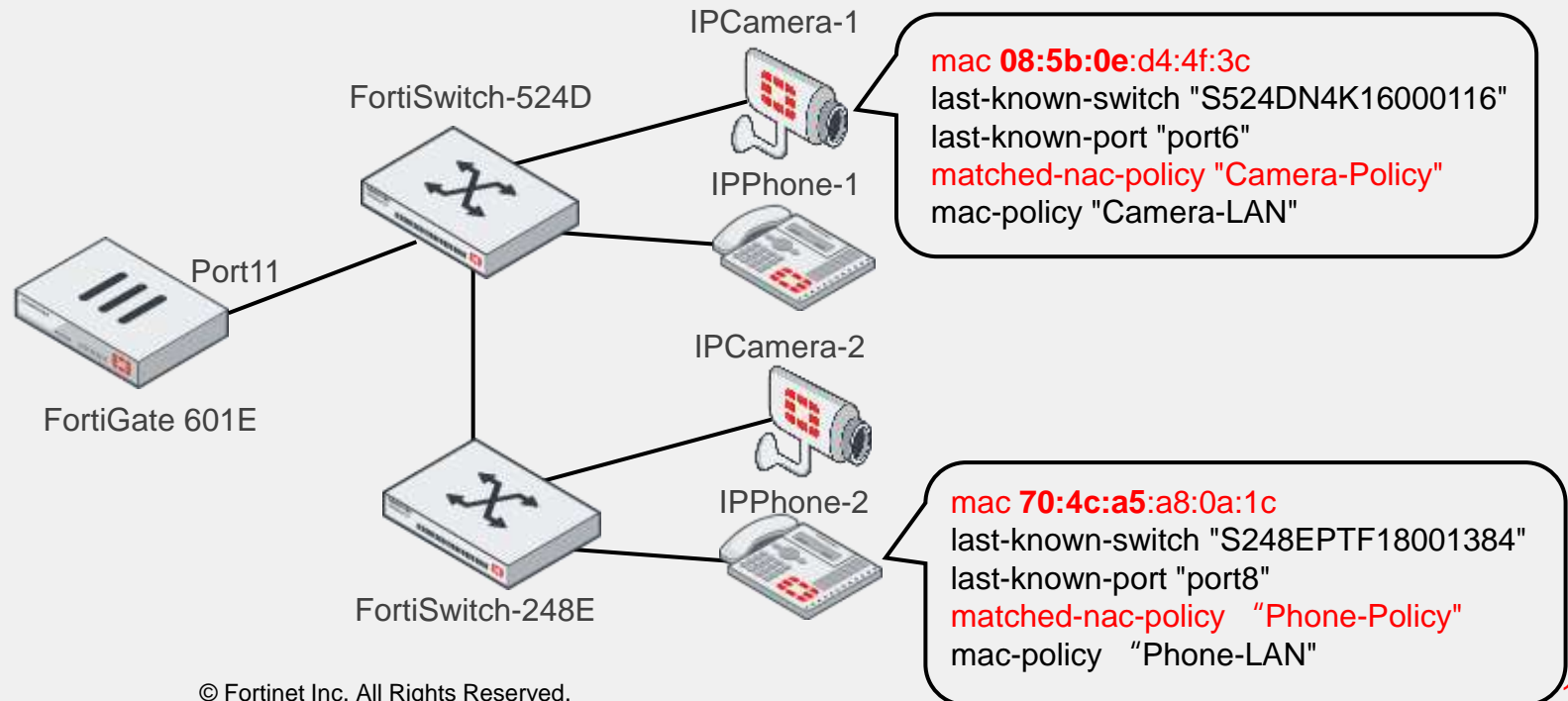
Use wildcards in a MAC address in a NAC policy



When configuring a NAC policy, you can use the wildcard * character when manually specifying a MAC address to match the device.

- In this example, IPCamera-1 and IPCamera-2 both have MAC addresses that start with 08:5b:0e.
- A NAC policy is created on the FortiGate 601E to match both IP-Camera.
- After the IP-Cameras are connected to the FortiSwitch units, they are detected by the NAC policy and assigned to Camera_VLAN.

```
config user nac-policy
edit "Camera-Policy"
  set mac "08:5b:0e:*.*.*)"
  set switch-fortilink "port11"
  set switch-mac-policy "Camera-LAN"
next
!
edit "Phone-Policy"
  set mac "70:4c:a5:*.*.*)"
  set switch-fortilink "port11"
  set switch-mac-policy "Phone-LAN"
next
```

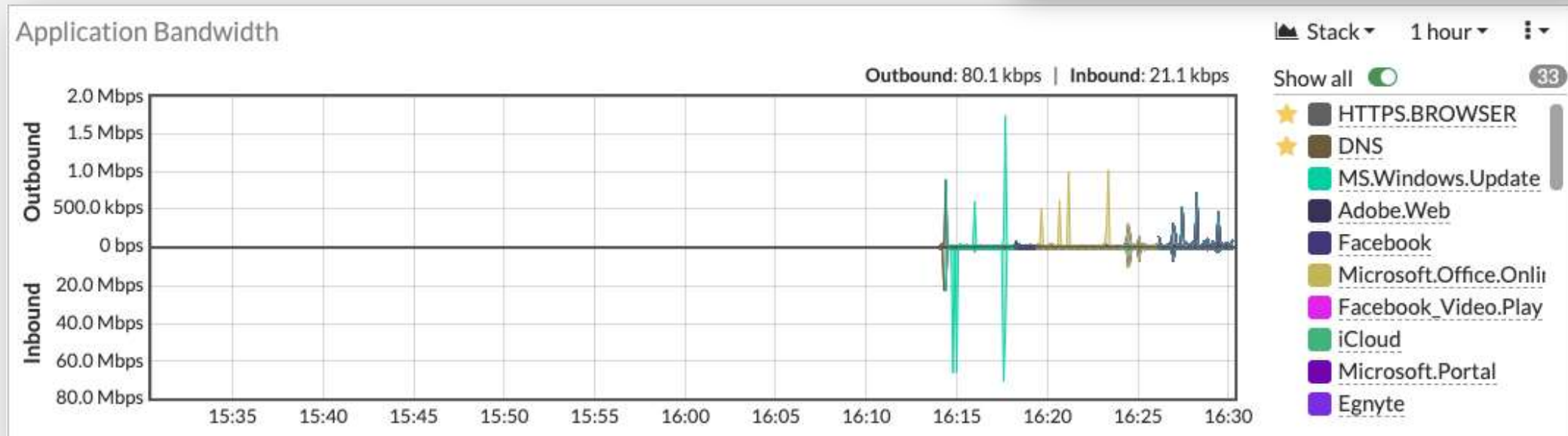
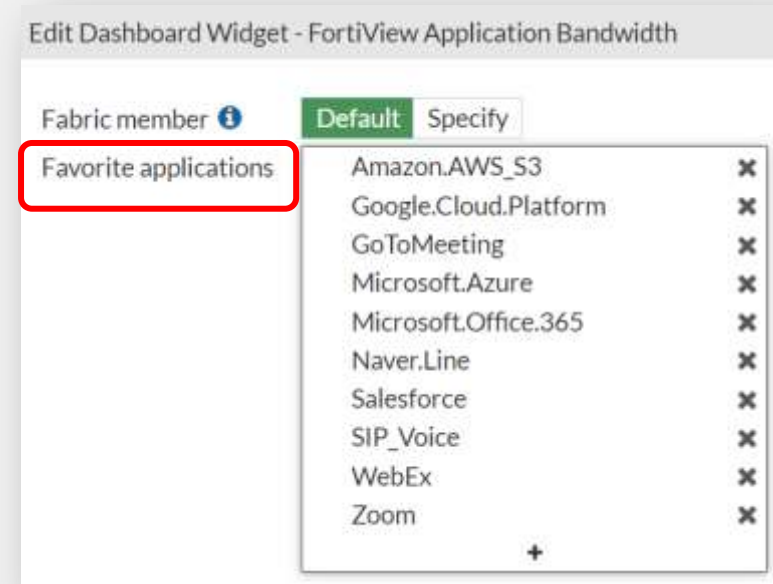


Security-driven Networking

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

Local Out Routing 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
- FortiGuard, System DNS , FortiSandbox, FortiAnalyzer, Syslog, LDAP, RADIUS, TACACS, External Resource

The screenshot displays the FortiGate web interface for the 'Local Out Routing' page. The left sidebar shows the navigation menu with 'Local Out Routing' highlighted. The main content area lists various services and their configurations. A table at the bottom shows the 'System DNS' settings, including the source IP and outgoing interface.

Name	Source IP	Outgoing Interface
External Resource 2		
AWS-IP-Block-List	10.1.215.61	wan1
AWS-Malware-List	Dynamic	SD-WAN
LDAP Servers 1		
LDAP	10.1.215.61	wan1
Log 4		
Log FortiAnalyzer Setting	Dynamic	Auto
Log FortiAnalyzer Cloud Setting	Dynamic	Auto
FortiGate Cloud Log Settings	Dynamic	Auto
Log Syslogd Setting	192.168.101.254	LAN-101 (port2)
RADIUS Servers 1		
FAC-206	10.10.10.1	dmz
System 3		
System DNS	10.1.215.61	wan1
System FortiGuard	10.1.215.61	wan1
System FortiSandbox	Dynamic	Auto
TACACS+ 1		
TACACS1	10.1.215.61	wan1

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 Servers

208.91.112.53 50 ms

208.91.112.52 50 ms

Additional Information

API Preview

Edit in CLI

Local Out Setting

Source IP

Edit Local Out Setting

Name: System.DNS

Outgoing interface: Auto SD-WAN Specify

Use Interface IP: Manually

10.1.215.61

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



ACME Support (Automated Certificate Management Environment)

- The (ACME), as defined in [RFC 8555](#), is used by the public Let's Encrypt certificate authority to provide free SSL server certificates
- The FortiGate can be configured to use certificates that are managed by Let's Encrypt, and other certificate management services, that use the ACME protocol.



Extended Netflow Visibility of Logical Interfaces

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

**Knowing and
controlling
everyone and
everything on
and off the
network**

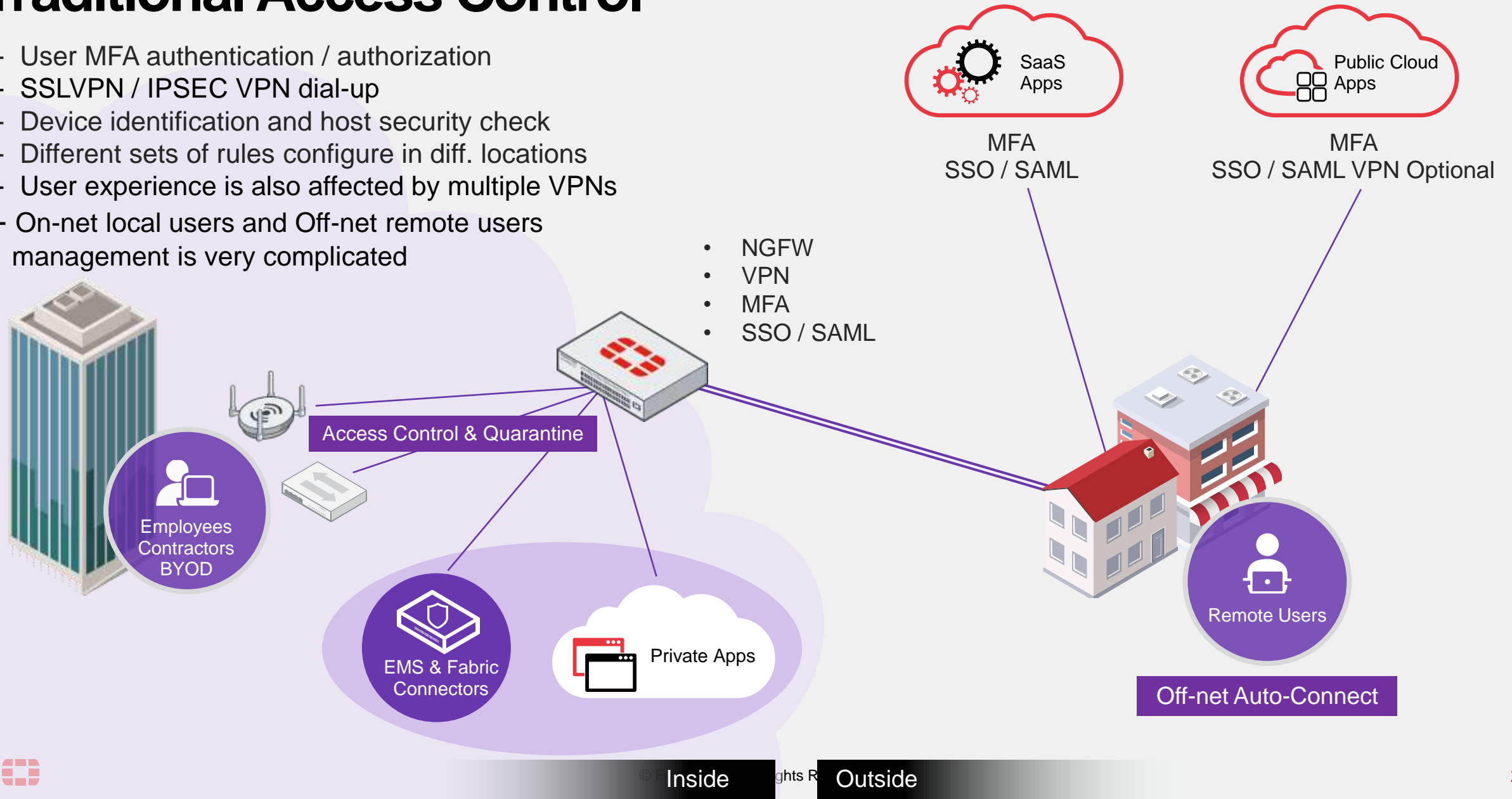
Users and Device Security



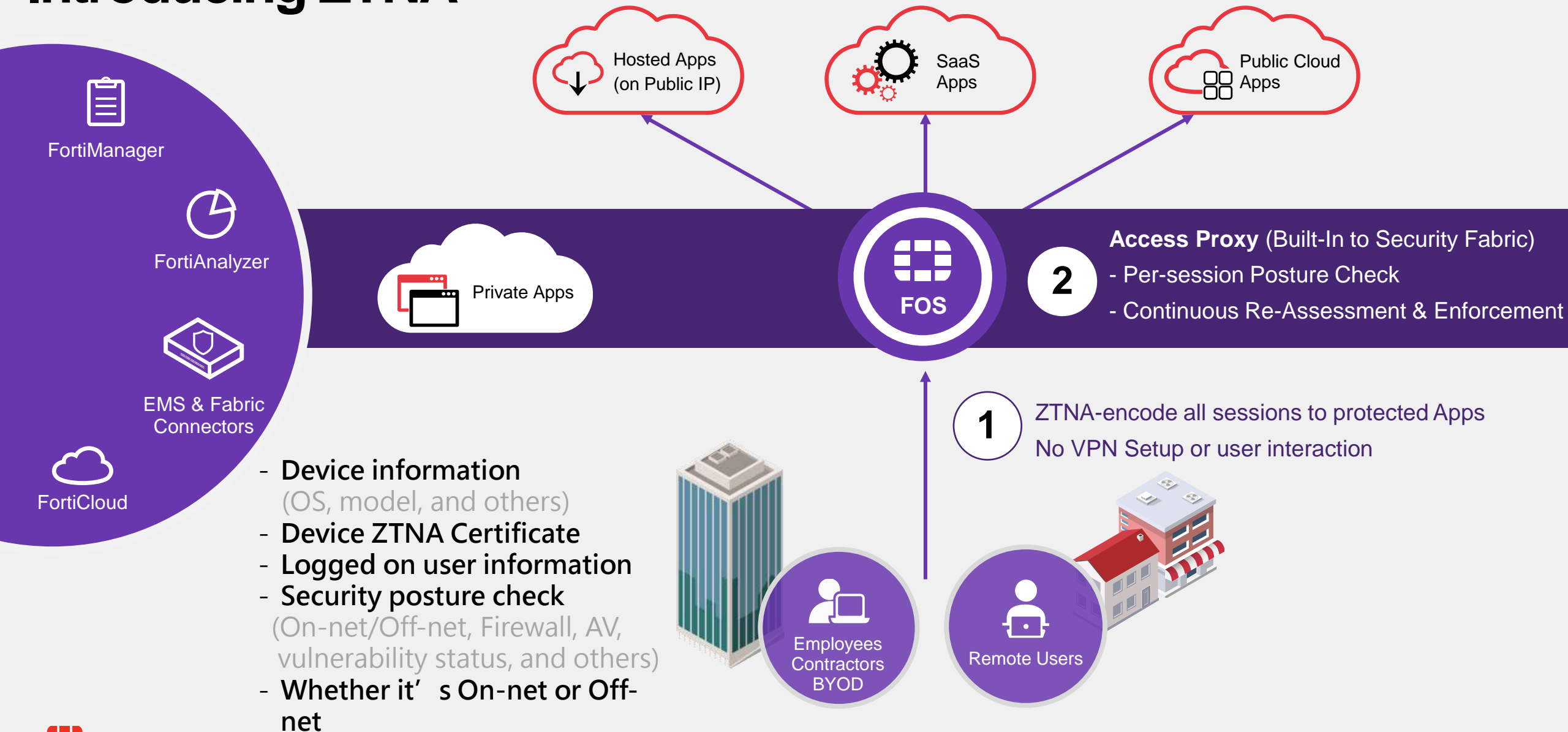
**Zero Trust
Access**

Traditional Access Control

- User MFA authentication / authorization
- SSLVPN / IPSEC VPN dial-up
- Device identification and host security check
- Different sets of rules configure in diff. locations
- User experience is also affected by multiple VPNs
- On-net local users and Off-net remote users management is very complicated



Introducing ZTNA

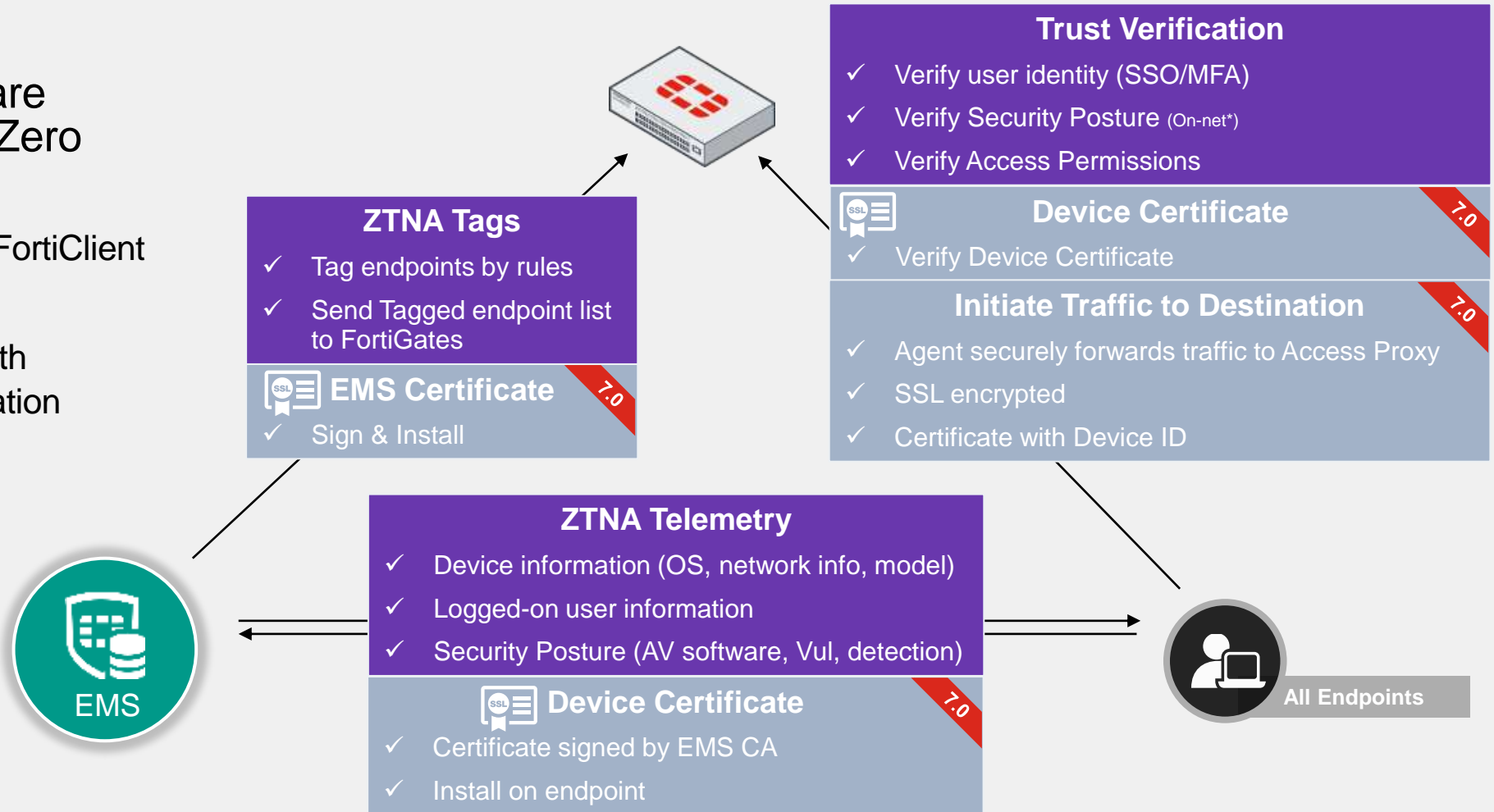


Zero-Trust Network Access

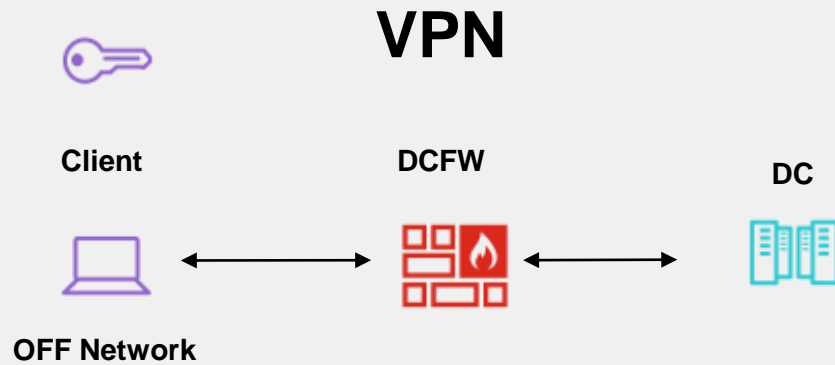
New Zero Trust Solution

Several new features are added to support new Zero Trust solution

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



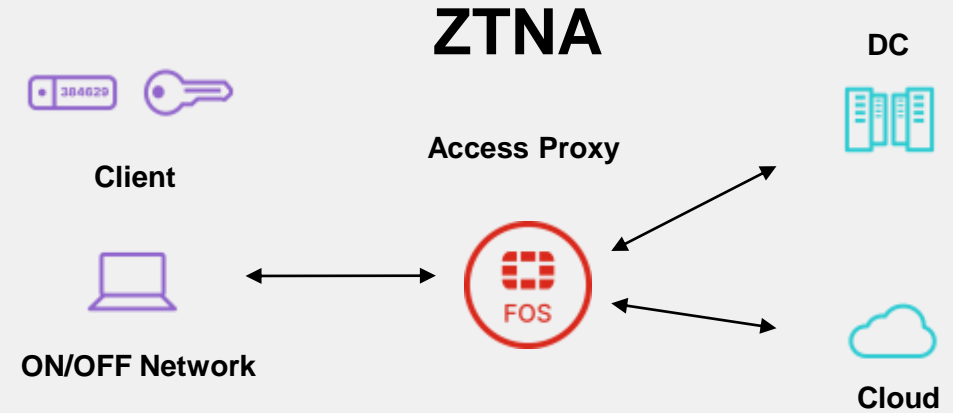
Evolution from Traditional VPN to ZTNA



One Time Trust Check

Access Entire Network

Generic Rule Set



Continuous Trust Check

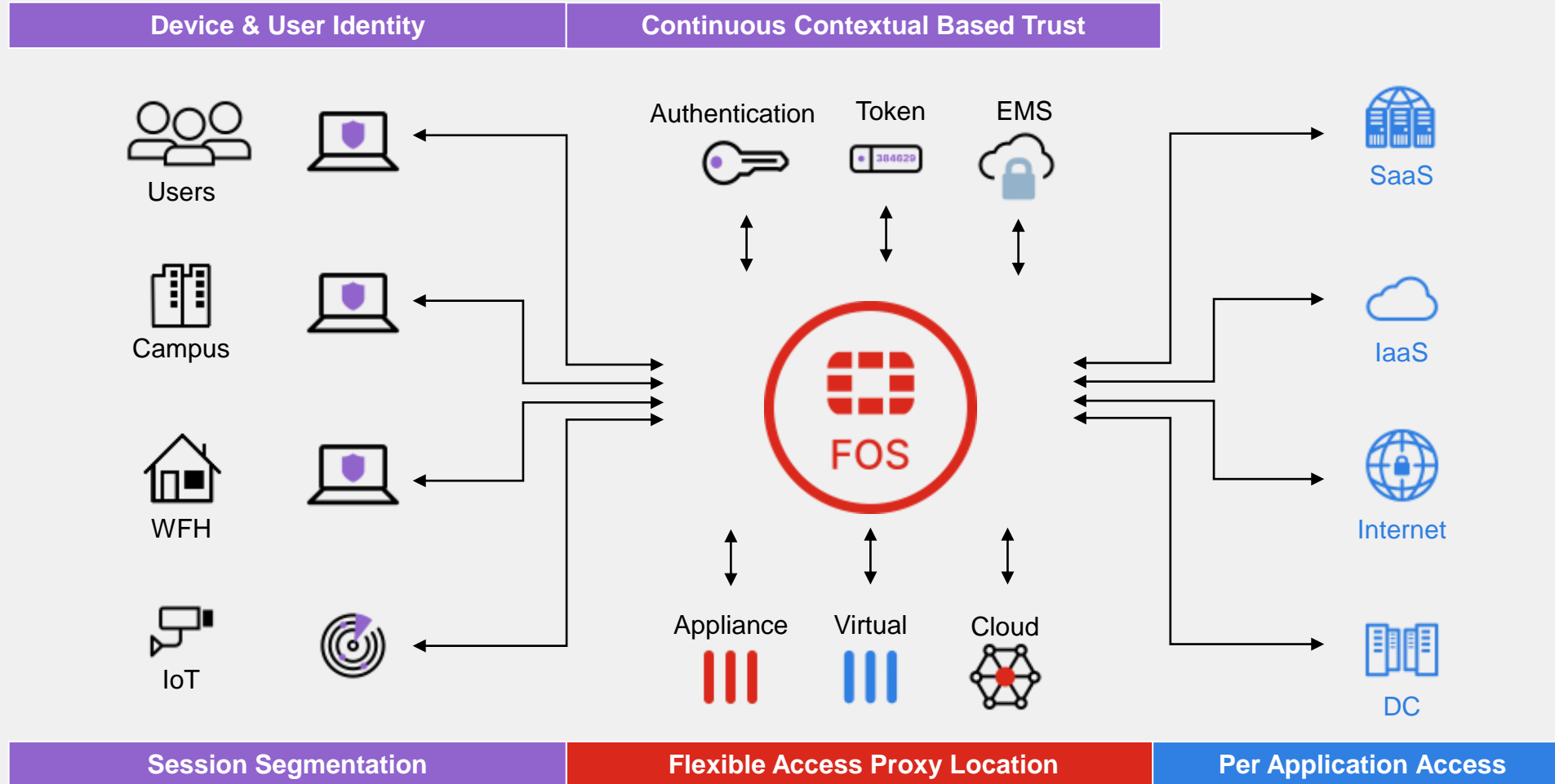
Access Specific Applications

User Contextual Rule Set



Zero Trust Access (ZTA) Vision

Secure Application Access Anytime and Anywhere



AI-driven Security Operations



**FortiGuard
Threat
Intelligence**

AI-driven Security Operations

AI based Malware Detection

Replacing the old heuristics detection with the new AI based one

- The **AV Engine AI malware detection model** integrates into regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks.
- Previously, this type of detection was handled by heuristics that analyzed file behavior. With AV Engine AI, the module is trained by FortiGuard AV against many malware samples to identify file features that make up the malware.
- The AV Engine AI package can be downloaded by FortiOS via FortiGuard on devices with an active AV subscription.

```
# config antivirus settings
```

```
set machine-learning-detection {enable| monitor | disable}
```

```
end
```

```
# get system status
```

```
...
```

```
Firmware Signature: certified
```

```
Virus-DB: 84.00632(2021-03-11 10:16)
```

```
Extended DB: 84.00632(2021-03-11 10:16)
```


```
AV AI/ML Model: 2.00021(2021-03-08 13:56)
```

```
...
```



External Block List (Threat Feed) – Malware Hash

- The external malware block list is a new feature introduced in FortiOS 6.2.0.
- This feature provides another means of supporting the AV Database by allowing users to add their own malware signatures in the form of MD5, SHA1, and SHA256 hashes.
- **Using different types of hashes simultaneously may slow down the performance of malware scanning.**
- **For this reason, users are recommended to only use one type of hash (either MD5, SHA1, or SHA256), not all three simultaneously. Preference is SHA1**
- If the list goes above the maximum size, it will be truncated and a log will be generated.



Malware Hash


The file contains one hash per line in the format `<hex hash> [optional hash description]`. Each line supports MD5, SHA1, and SHA256 hex hashes. It is automatically used for *Virus Outbreak Prevention* on antivirus profiles with *Use External Malware Block List* enabled.

Note: For optimal performance, do not mix different hashes in the list. Only use one of MD5, SHA1, or SHA256.

Example:

```
292b2e6bb027cd4ff4d24e338f5c48de
dda37961870ce079defbf185eeef905 Trojan-Ransom.Win32.Locky.abf1
3fa86717650a17d075d856a41b3874265f8e9eab Trojan-Ransom.Win32.Locky.abf1
c35f705df9e475305c0984b05991d444450809c35dd1d96106bb8e7128b9082f Trojan-Ransom.Win32.Locky.abf1
```

See [External malware blocklist for antivirus](#) for an example.



Antivirus

External Block List (Threat Feed) – Malware Hash

The screenshot displays the Fortinet Security Fabric interface. On the left, the navigation menu includes Dashboard, Security Fabric, Physical Topology, Logical Topology, Security Rating, Automation, Fabric Connectors, External Connectors (highlighted), Network, System, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, and Log & Report.

The main panel shows the 'Threat Feeds' section. A 'Malware Hash Threat Feed' from 'virusshare.com' is configured with the following details:

- Type: Malware Hash Threat Feed
- URI: https://virusshare.com/VirusShare_00389.md5
- Connection Status: ✓ 2021/03/29 18:23:56
- Last Content Update: ✓ 2021/03/29 18:23:56
- Entries: 65536 Valid

A 'View Entries' button is visible. A red box highlights the 'View Entries' button and the 'Malware Hash Threat Feed' card. A red arrow points from the 'View Entries' button to a detailed view of the threat feed entries on the right.

The detailed view shows the 'Malware Hash Threat Feed: virusshare.com' with a search bar and a table of entries. The table has two columns: 'Entry' and a status column. All entries are marked as 'Valid'.

Entry	Status
42508a98d6ea5129ebc3a131041b32a4	✓ Valid
81d272e00423d3f86a6192d3b5d8d736	✓ Valid
1b69e9e73cc98aa4e7f88027db8e03e7	✓ Valid
e9547b806102cd4a125f30b437af906f	✓ Valid
d4fab5366a288475dee5b667816a0571	✓ Valid
2595a00320794ac40b746d569e6524f2	✓ Valid
870fde03d46c0697949a7aa85c01b451	✓ Valid
56d6686e1a27658afbd4dee1a0a9b31e	✓ Valid
7aa8da322b6e6b786ab11710ae849101	✓ Valid
ebc66d0f775578f52f42593d418ac312	✓ Valid
71f170d34251089c00490e390422acce	✓ Valid
e62c54e397c891b2008c50692068031d	✓ Valid
f5509140a78c096bc7ab652b009d797a	✓ Valid
85687910489f1a96e7ec48ca433c6d48	✓ Valid
74fcb87841ea4346616b273d63bbb282	✓ Valid
3caa46a3d7fa496a19c1989d1804413c	✓ Valid
7a715c45af8ae647148452bdda33d262	✓ Valid
dca2b285d42077ac53f430e475e05ddd	✓ Valid
255e970c0210195efc5e5be84821b080	✓ Valid
6bab2ea1dc45997bc25be236315e0125	✓ Valid
715274fb9281ebd145eafc2d7331335a	✓ Valid

New: Outbreak Alert

What is it?

Add on offering to FortiAnalyzer, providing pre define reports based on IoC identified in related to Outbreak Attack

Why is it needed?

Speed to detection, and mitigate for new attacks and vulnerabilities in the wild

Who needs it?

SOC and NOC teams

How to get it ?

Add on to FortiAnalyzer

- A-la-carte
 - 20% of HW
- Inside the Fortianalyzer Enterprise bundle
 - 90% of HW



Pre requirements:

- OS version: 7.0.0 and next 6.4 patch.
- FortiGate: Active services for AV, IPS, Botnet
- FortiClient: Endpoint vulnerability



New: Outbreak Alert

- Current outbreak reports include *DearCry Report*, *Hafnium M.S.Exchange Attack Detection Report*, and *SolarWinds Normalized Report*, available in Fabric ADOMs.
- Right click a report to run the report. Reports can be generated in HTML, PDF, XML, and CSV formats.



HAFNIUM, DearCry, and more

Targeting Exchange Servers with 0-day exploits

Issue	Impact	Targets
Microsoft has detected multiple 0-day exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. (Device Security)	Threat actor use these vulnerabilities steal data and perform additional malicious actions that lead to further compromise. <u>DearCry</u> Ransomware is piggybacking on the original attack (Content Security)	HAFNIUM primarily in the United States Industry sectors: infectious disease law firms, higher education institutions, defense policy think tanks, Set 2 attacks like have a wider range

March 12, 2021

Latest Developments

FortiGuard Labs released the **Threat Signal**
<https://www.fortiguards.com/threat-signal-report/3885/observed-in-the-wild-campaigns-leveraging-recent-microsoft-exchange-server-vulnerabilities-to-install-doejocrypt-dearcry-ransomware>

Summary

This report displays the findings on attack attempts to exploit MS. Exchange vulnerabilities from Fortigate.

This table shows detections by FortiGate IPS:

FortiGate IPS Detection

#	Device	Source	Destination	Attack	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	172.16.68.21	111.206.21.0.75	HTTP.Unknown.Tunnelling	3	2021-04-13 18:12:50	2021-04-13 20:44:44
2	Van_Office_FW1_Master	172.18.34.35	74.125.124.94	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
3	Van_Office_FW1_Master	172.16.197.102	10.50.0.0	TCP.PORT0	3	2021-04-13 18:12:50	2021-04-13 20:44:44
4	Van_Office_FW1_Master	172.16.171.64	172.18.22.4.8	MS.Exchange.Server.UM.Core.Remote.Co de.Execution	3	2021-04-13 18:12:50	2021-04-13 20:44:44
5	FGT91E4Q16000534	172.16.68.21	111.206.21.0.75	HTTP.Unknown.Tunnelling	1	2021-04-13 18:15:19	2021-04-13 18:15:19
6	FGT91E4Q16000534	172.16.171.64	172.18.22.4.8	MS.Exchange.Server.UM.Core.Remote.Co de.Execution	1	2021-04-13 18:15:19	2021-04-13 18:15:19
7	FGT91E4Q16000534	172.18.34.35	74.125.124.94	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19
8	FGT91E4Q16000534	172.16.197.102	10.50.0.0	TCP.PORT0	1	2021-04-13 18:15:19	2021-04-13 18:15:19

This table shows detections by FortiGate AV:

FortiGate AV Detection

#	Device	Source	Destination	Virus	Total Count	First Seen	Last Seen
1	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	HTML/Agent.A121tr	1	2021-04-13 20:44:55	2021-04-13 20:44:55
2	Van_Office_FW1_Master	10.2.60.143	10.2.175.110	ASP/WebShell.cltr	1	2021-04-13 20:44:55	2021-04-13 20:44:55



Automate Security Operations Across The Security Fabric

Security Operations

Security
Operations Center
(SOC)



**Fabric
Management
Center**

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 FortiGate GUI 'System Settings' page. The 'Host name' is 'SG-FTNT'. The 'System Time' section shows the current time as '2021/01/28 17:13:18' and the time zone as '(GMT+8:00) Kuala Lumpur, Singapore'. The 'Set Time' section has buttons for 'NTP', 'PTP', and 'Manual settings'. The 'Select server' section has buttons for 'FortiGuard' and 'Custom'. On the right-hand side, there is an 'Additional Information' section with a red box highlighting the 'API Preview' and 'Edit in CLI' links. Below this, there is a 'Virtual Domain' section with links for 'Setup guides' and 'How to Configure Virtual Domains'. At the bottom, there are two panels: 'CLI Console (1)' and 'API Preview'. The 'CLI Console' panel shows the following commands:

```
FortiGate-101E # config system global
FortiGate-101E (global) # show
config system global
  set admintimeout 60
  set alias "FortiGate-101E"
  set gui-certificates enable
  set gui-fortigate-cloud-sandbox enable
  set gui-ipv6 enable
  set gui-local-out enable
  set gui-replacement-message-groups enable
  set hostname "FortiGate-101E"
  set switch-controller enable
  set timezone 04
  set virtual-switch-vlan enable
end
FortiGate-101E (global) #
```

 The 'API Preview' panel shows a message: 'The following REST API requests will be sent when you save your changes. Full API documentation is available [here](#).' Below this, there is a section for 'FortiGate-101E' with a toggle for 'Show modified changes only'. A yellow banner indicates 'No changes have been made.' Below this, there is a section for the REST API request:

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

 A 'Copy to clipboard' button is next to the API request.

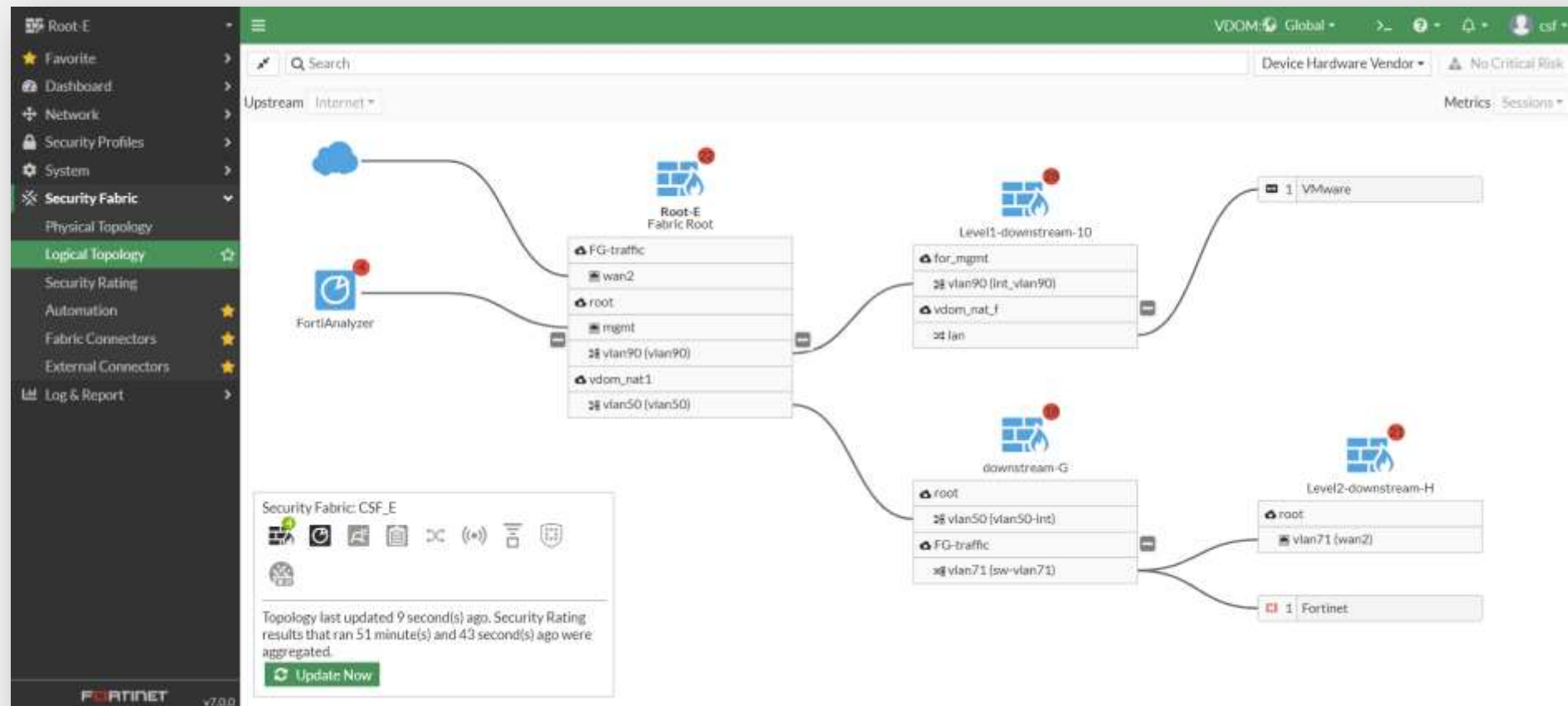


Fabric Management Center

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

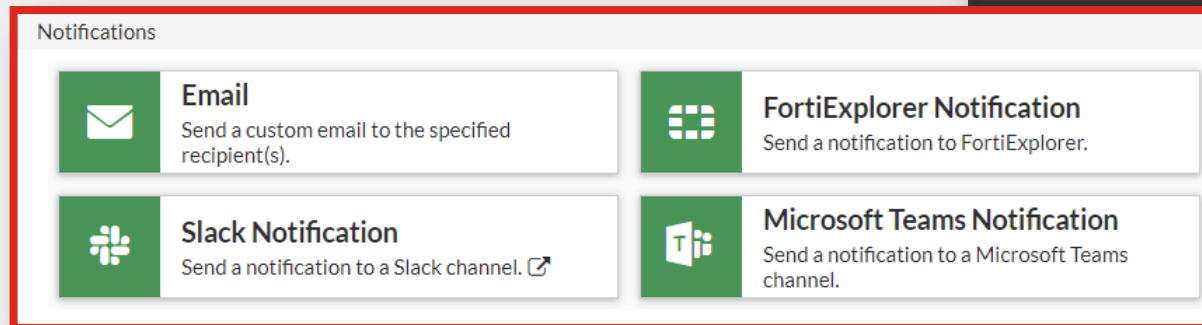
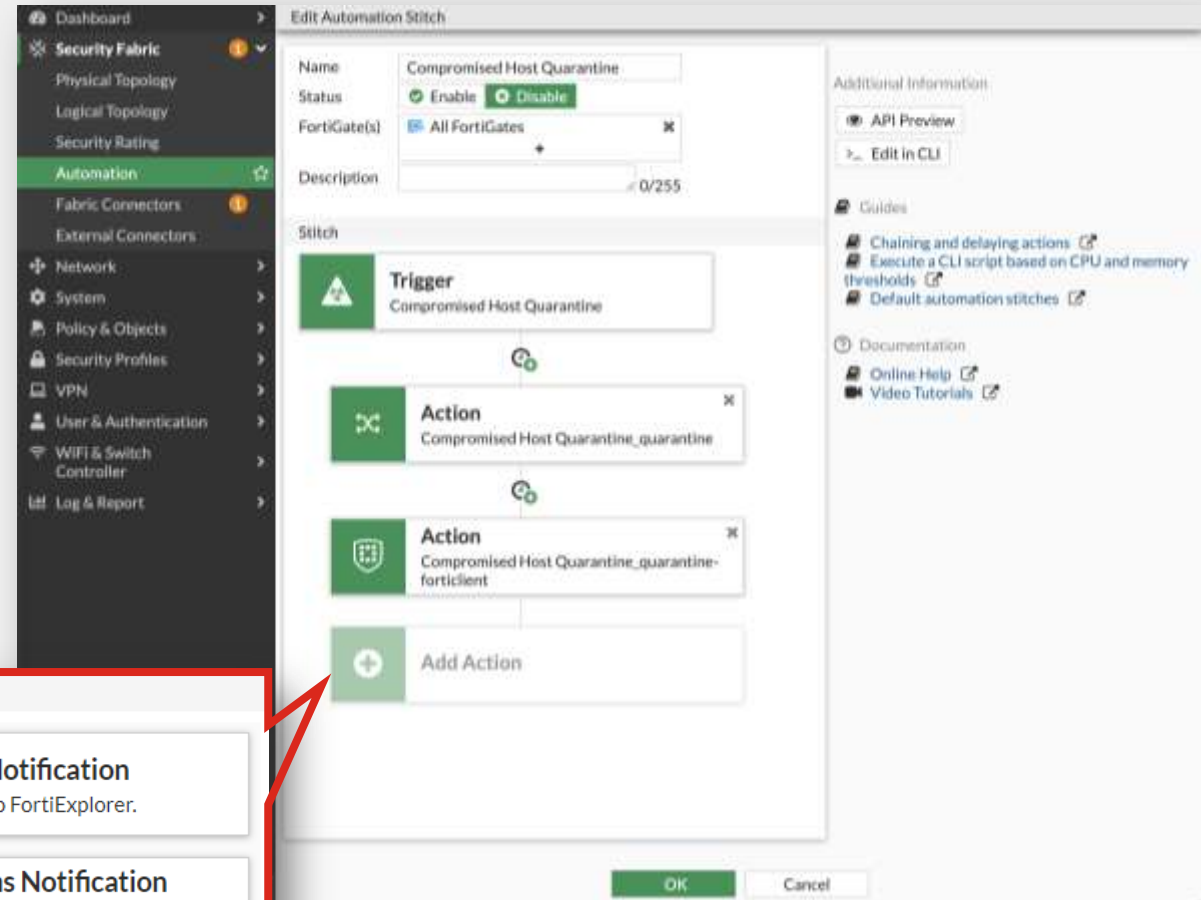


Fabric Management Center

Automation Workflow Improvements

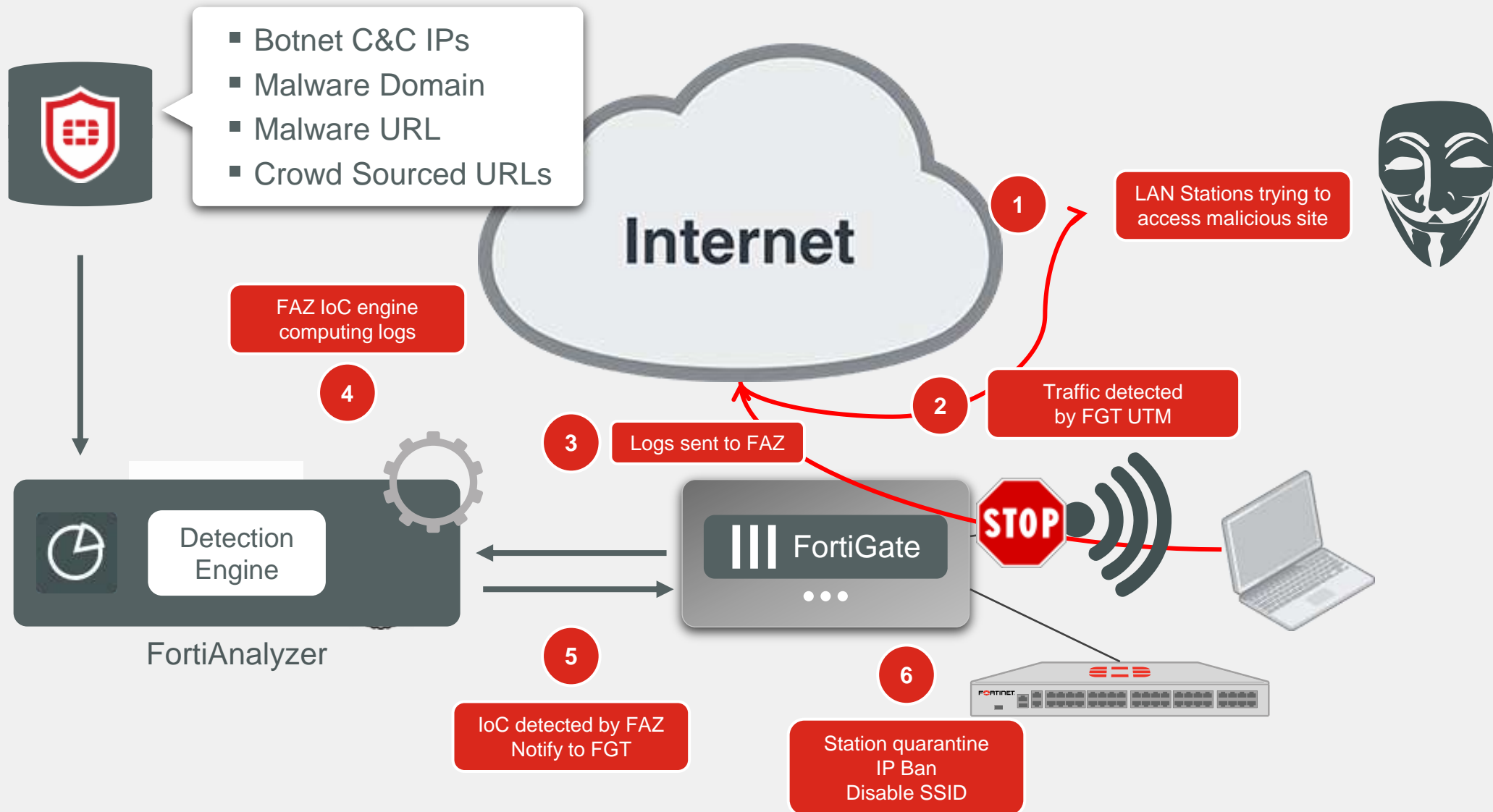
Simplify the workflow for managing multiple chained actions, and make it clearer to the user which order the actions will be processed in.

- 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



New Automation action that provides Microsoft Teams notification

Automation Workflow



FortiOS 7.0 新增 300 項功能，資安防禦全面升級

Fortinet 作業系統全面更新！
FortiOS 7.0 新增
300 項功能
資安防禦全面升級

FORTINET



- Fortinet Secure Access Service Edge (FortiSASE)
- Fortinet Zero Trust Network Access (ZTNA)
- FortiGuard Video Filtering and IoT Real-time Query
- Over 300 New Features and Updates Deliver Even More Reasons to Choose Fortinet





FORTINET®