Service Bundle Example Guide

SD-WAN 7.6

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 05, 2026
SD-WAN 7.6 Service Bundle Example Guide
01-76-1271578-20260605

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-06-05	Initial release.

Introduction

This guide provides a practical, example-driven overview of how to deploy and operate an SD-WAN service bundle using FortiOS 7.6. It brings together key capabilities across SD-WAN underlay provisioning, performance measurement, application-aware steering, and cloud-integrated services to demonstrate how organizations can build a resilient, performance-optimized WAN architecture. Rather than focusing on isolated features, the document shows how these components work together to simplify initial deployment, improve visibility, and enable data-driven traffic steering decisions.

In addition to core SD-WAN configuration, this guide extends into adjacent service domains (SASE onboarding, FortiGate Cloud provisioning, Overlay-as-a-Service (OaaS), Security Rating, and FortiTelemetry) to illustrate a broader operational model that combines networking, security, and analytics. The included procedures, examples, and validation steps are designed to help administrators move from initial setup to ongoing optimization, ensuring consistent application performance and a scalable foundation for modern distributed environments.

SD-WAN Services Bundle vs Add-on

	FortiGate 60F and smaller Bundle (1337)	FortiGate 60F and smaller Add-on (1387)	FortiGate 60G+ Bundle (1329)	FortiGate 60G+ Add-on (1389)
FortiGuard Speed Testing Service	✅	✅	✅	✅
SD-WAN Setup Assistance	✅	✅	✅	✅
FortiGuard SLA Database	✅	✅	✅	✅
Application Performance Monitoring (APM)	✅	✅	✅	✅
FortiTelemetry (SaaS Monitoring)	✅	✅	✅	✅
FortiGate Cloud Standard	✅	✅	✅	✅
FortiSASE User Starter Kit			✅	✅
FortiSASE Secure Private Access (SPA) Connector	✅	✅	✅	✅
FortiCare Premium Support	✅		✅	
IoT Security & Security Ratings	✅		✅	
Recommended Use Case	Standalone SD-WAN deployment	Add-on to UTP or Enterprise bundle	Standalone SD-WAN deployment	Add-on to UTP or Enterprise bundle

SD-WAN Configuration

Software-Defined Wide Area Networking (SD-WAN) in FortiOS simplifies deployment and enhances operational visibility by combining guided provisioning, intelligent path selection, and performance-driven insights. The Underlay Setup Wizard accelerates initial configuration by converting WAN interfaces into SD-WAN members, building zones, and establishing baseline traffic steering with minimal effort. Ongoing link evaluation is strengthened by the FortiGuard SLA Database, which provides curated, continuously updated targets for reliable health-check monitoring.

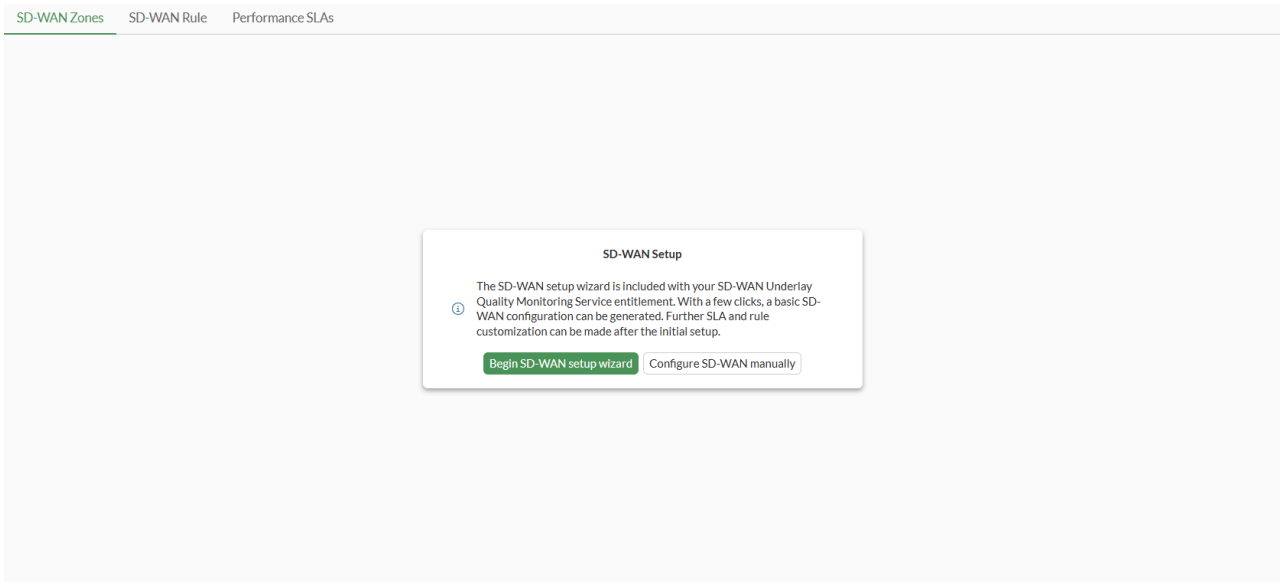
Complementing this, the FortiGuard Speed Test enables both scheduled and on-demand bandwidth validation, allowing administrators to align SD-WAN decisions with real-world link capacity. Finally, Application Performance Monitoring (APM) delivers deep, application-level visibility by measuring metrics such as latency, jitter, and packet loss across live traffic, enabling informed troubleshooting and ensuring that steering policies consistently deliver optimal end-user experience.

Underlay Setup Wizard

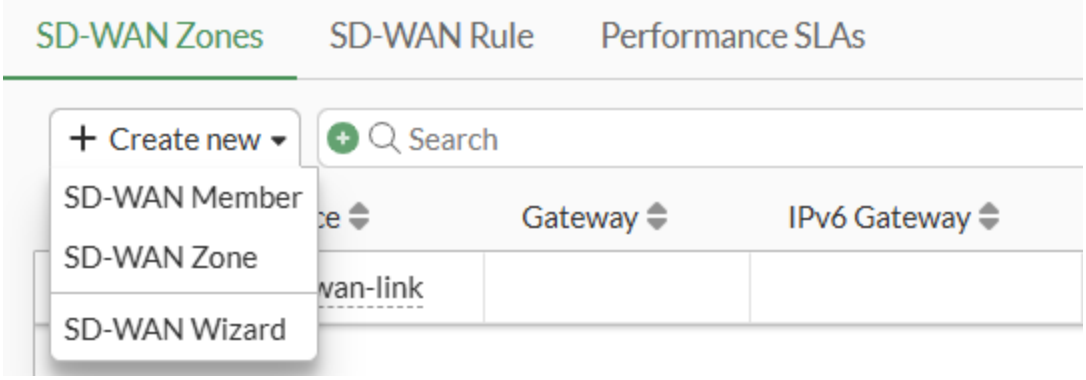
The SD-WAN Setup Wizard is intended to bootstrap an SD-WAN underlay quickly by converting one or more WAN interfaces into SD-WAN members, creating a default SD-WAN zone, and guiding you through initial performance monitoring and traffic steering.

Example: Two-ISP underlay with a default internet rule

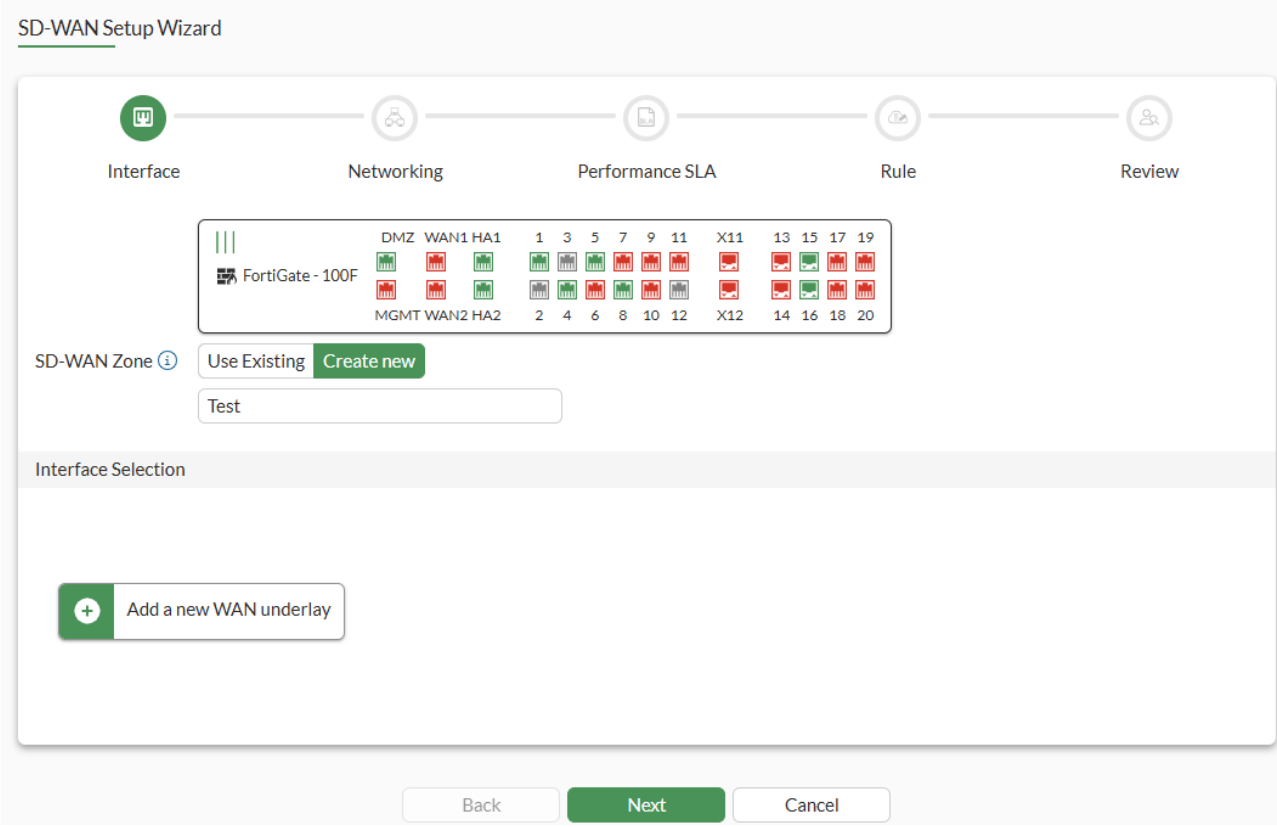
1. In the GUI, go to Network > SD-WAN and launch the SD-WAN Setup Wizard.



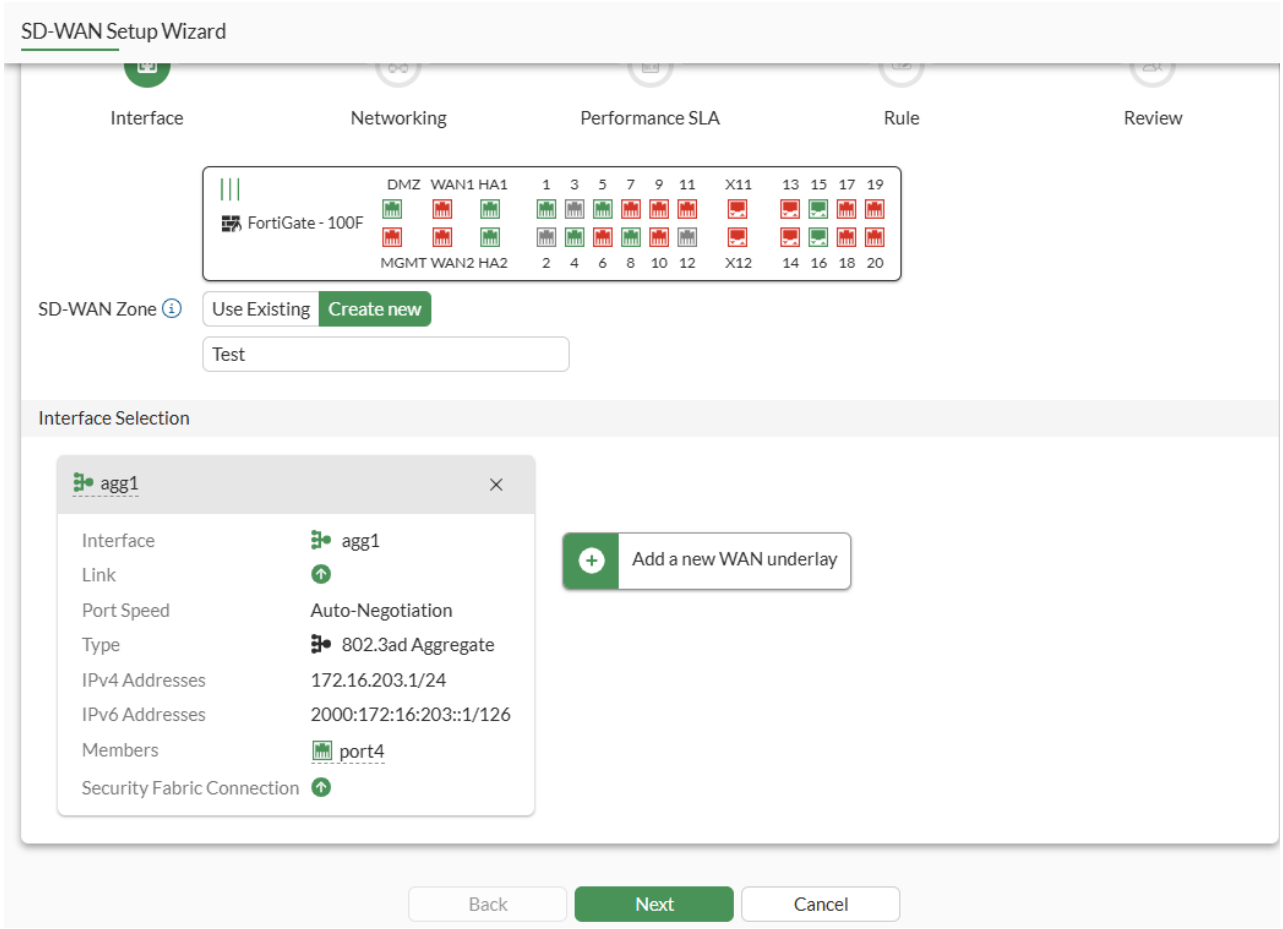
2. Select wan1 and wan2 as members. Provide each interface's gateway (or enable DHCP where appropriate).



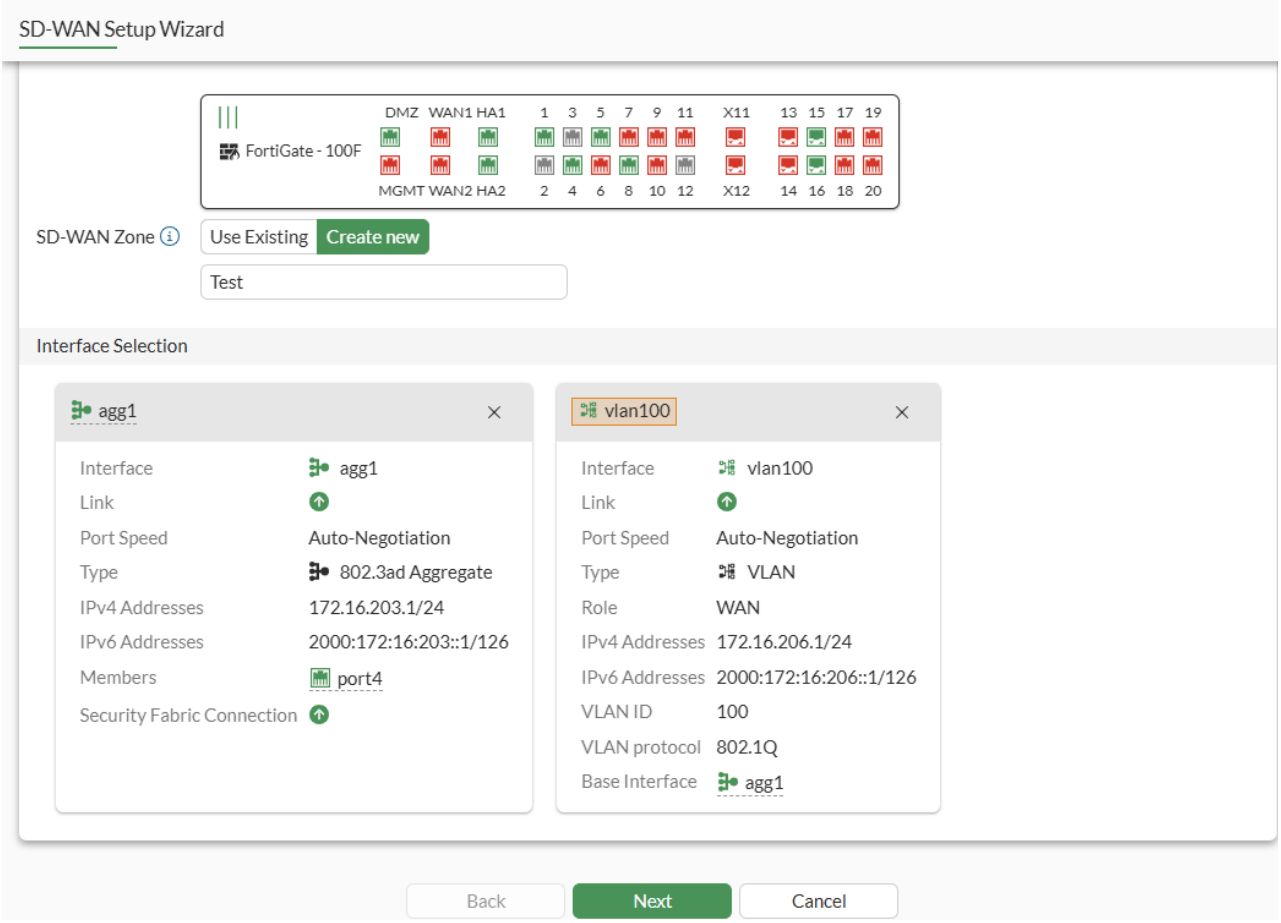
3. Accept the default SD-WAN zone (commonly virtual-wan-link) or create a new SD-WAN zone.



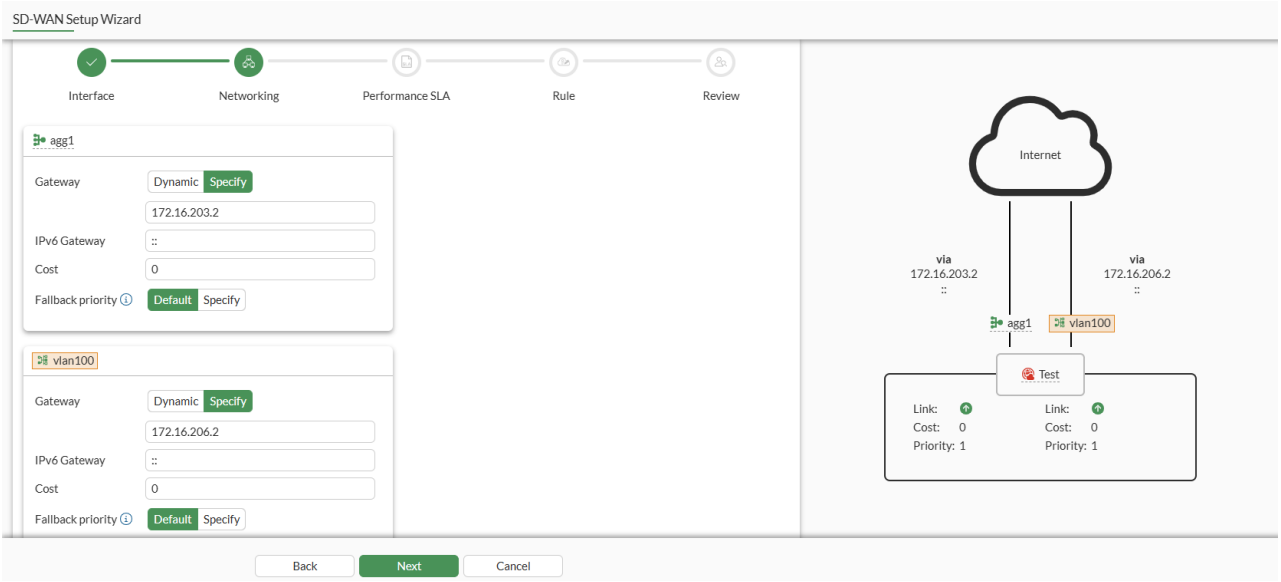
4. Click *Add a new WAN underlay*, select an interface, and click *Apply*.



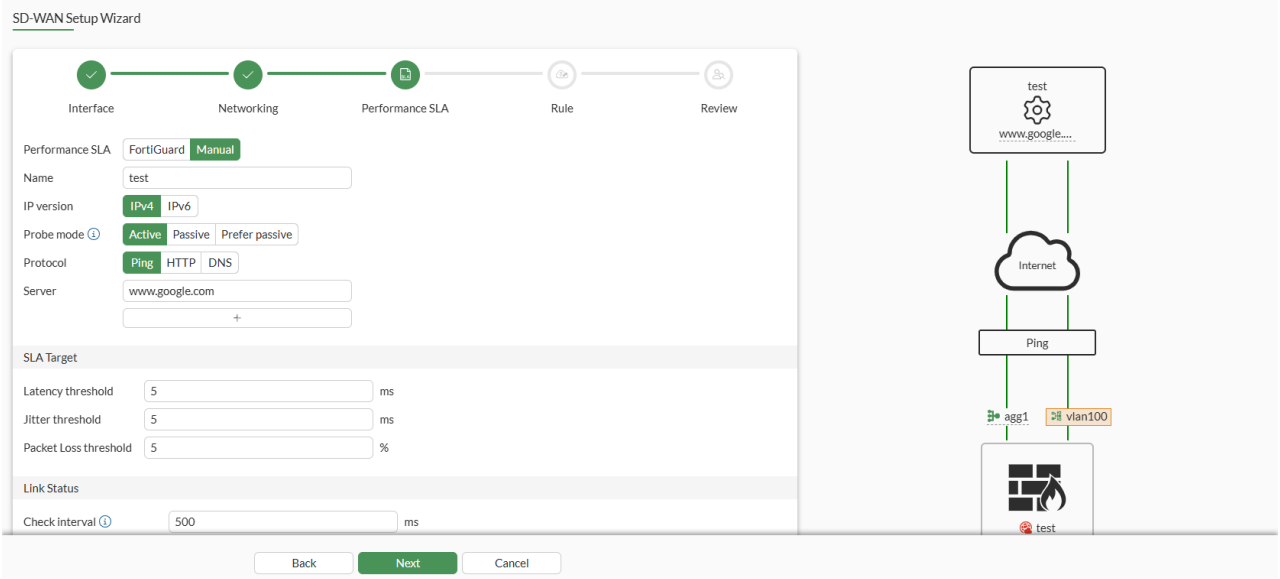
5. Repeat to add the second interface, then select Next when added.



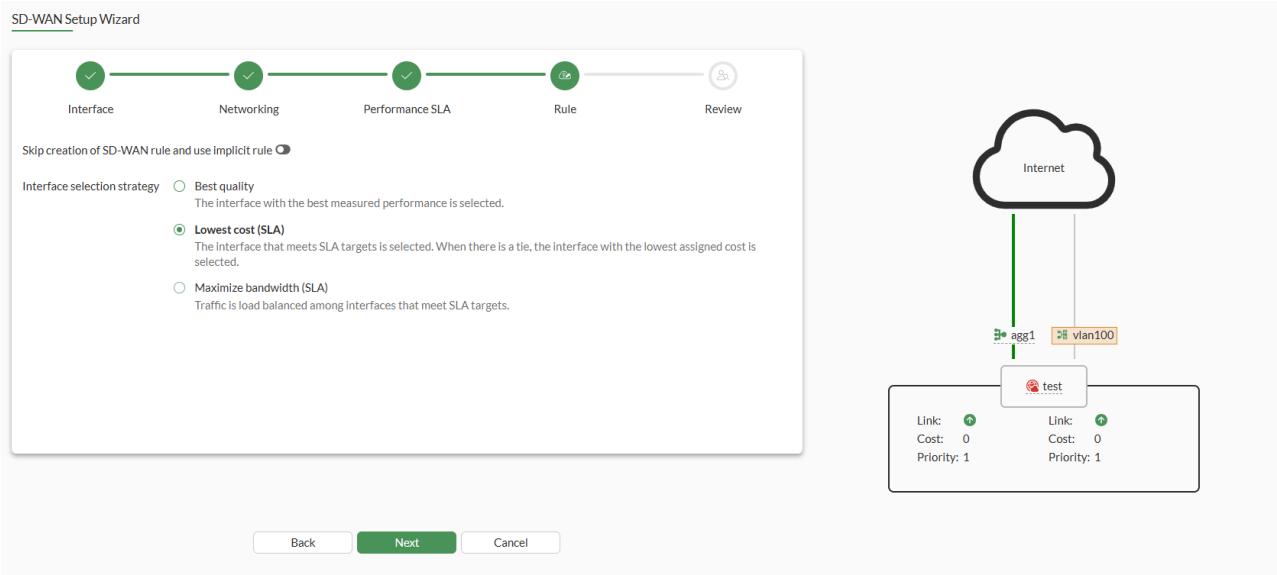
6. For the *Networking* step, set the gateway and priority for each interface, and click *Next*:



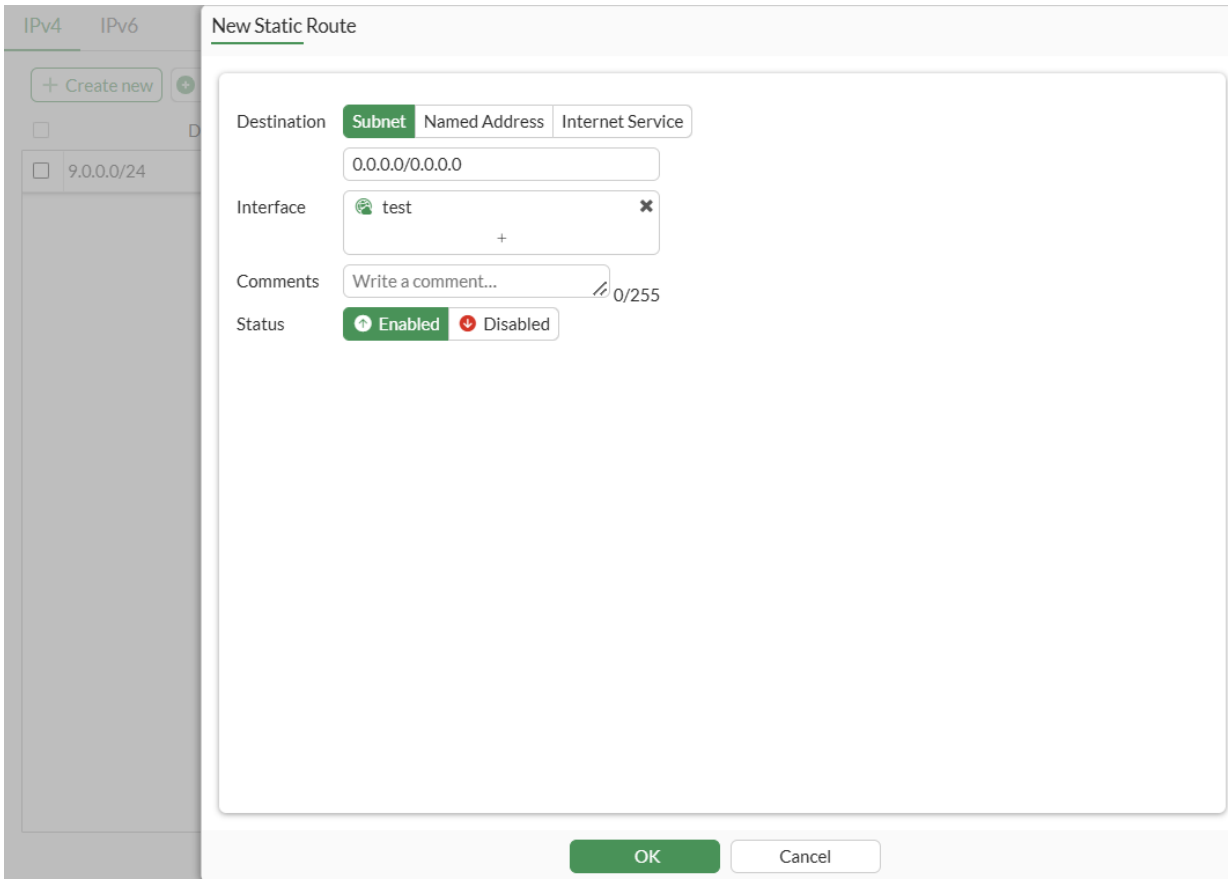
7. Add a basic Performance SLA (health check) such as DNS/HTTPS toward a reliable target and include both WAN members. FortiGuard SLA Database includes a large variety of pre-defined Performance SLAs that are monitored and dynamically updated as necessary.



8. Create a default SD-WAN rule that matches internet-bound traffic (0.0.0.0/0) and uses a strategy such as Best Quality or Lowest Cost with SLA.

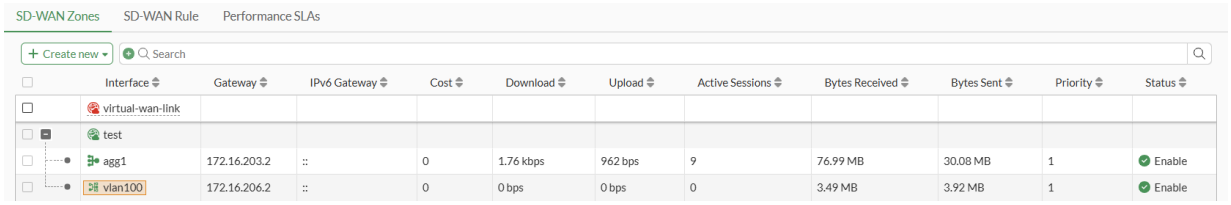


9. Create a static route for the SD-WAN interface (that is the SD-WAN zone):
   a. Go to *Network* > *Static Routes*, and click *Create new*.
   b. Complete the options, and click *OK*.

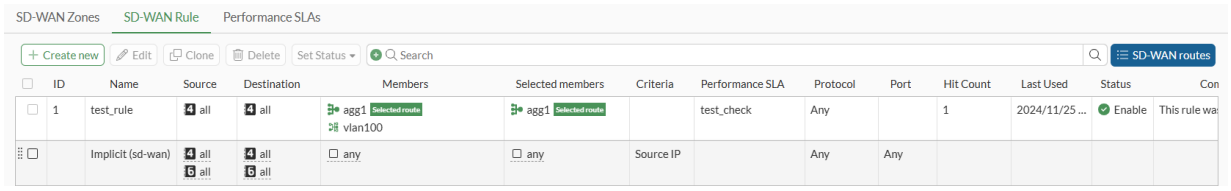


10. Review the SD-WAN configuration:

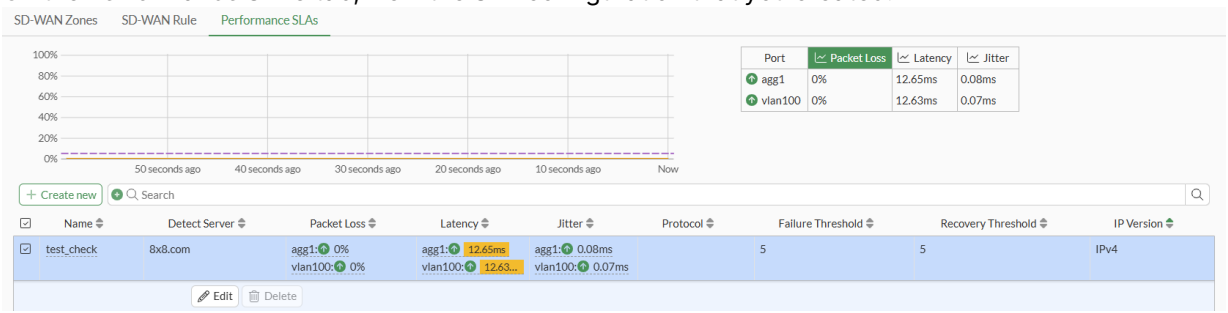
a. Go to *Network* > *SD-WAN* > *SD-WAN Zones*, and view the zone and members that you created.



b. On the *SD-WAN Rule* tab, view the rule that you created.



c. On the *Performance SLAs* tab, view the SLA configuration that you created.



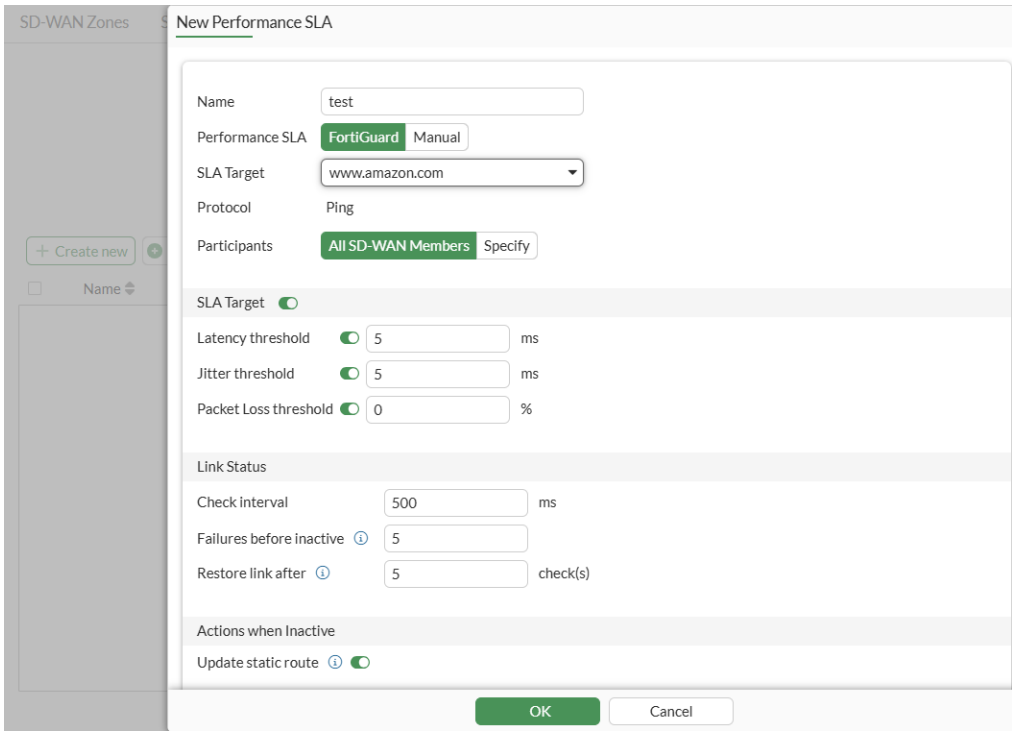
11. Update or create an outbound firewall policy to use the SD-WAN zone as the outgoing interface.

FortiGuard SLA Database

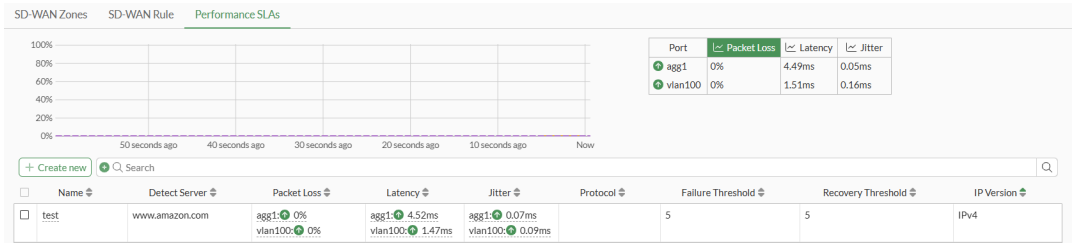
The FortiGuard SLA Database provides a curated list of common SaaS and internet destinations (and recommended probe settings) that can be used as SD-WAN Performance SLA targets.

Example: Use the FortiGuard SLA database target ‘Amazon’ in a health-check

1. Go to *Network* > *SD-WAN* > *Performance SLA*, and click *Create New*. The *New Performance SLA* pane is displayed.
2. Set *Performance SLA* to *FortiGuard* to select the database, and set *SLA Target* to the *www.amazon.com* target from the database.



3. Complete the remaining options, and click *OK*. The configuration is displayed on the *Performance SLAs* pane.
4. On the *Performance SLAs* pane, select the configuration to view the health-check status.



FortiGuard Speed Test

FortiGuard Speed Test provides a mechanism to measure the real-world bandwidth capacity of WAN interfaces. These measurements can be used to inform SD-WAN decision-making, traffic shaping policies, and overall link utilization strategies. This section covers both scheduled and on-demand speed testing, along with best practices for interpreting results.

The FortiGate must be able to reach FortiGuard/FortiCloud speed test servers.

Use a maintenance window if you expect the test to consume significant bandwidth.

Scheduled

In this example, a speed test is configured to occur within a three hour window, with a specific server group selected to prioritize that server (the default is FTNT_Auto). A retry mechanism is configured for failed speed tests, and minimum in and out bandwidths are specified for the speed test results. The results of the speed test are then applied to the in and out bandwidths in memory so that QoS can use them.

Example: Execute the speed test according to a schedule

1. Configure the recurring schedule:

```
config firewall schedule recurring
    edit "speedtest_recurring"
        set start 17:07
        set day sunday monday tuesday wednesday thursday friday saturday
        set label-day midday
    next
end
```

   Midday is configured as the three hour window to run the speed test. The test will be initiated between 10 AM and 1 PM.

2. Configure the speed test schedule:

```
config system speed-test-schedule
    edit "port1"
        set server-name “FTNT_CA_Burnaby”
        set schedules "speedtest_recurring"
        set retries 2
        set retry-pause 60
        set update-interface-shaping enable
        set update-inbandwidth-minimum 80000
        set update-outbandwidth-minimum 400000
    next
end
```

   The speed test server `FTNT_CA_Burnaby` is configured as the first server that the speed test will be performed against.

   The speed test will attempt 2 connections (`retries`), then wait 60 seconds (`retry-pause`). This repeats 3 times for a total of 6 connection attempts. If all 6 connections fail, select the next server from the list and repeat the 6 attempts, then continue to the next server if that server fails all tests.

3. Check the results of the speed test applied to the interface:

```
# show sys interface port1
config system interface
    edit "port1"
       ...
        set measured-upstream-bandwidth 425252
        set measured-downstream-bandwidth 97319
        set bandwidth-measure-time 1689811759
```

```
        ...
    next
end
```

The interface reflects the results of the speed test. The actual test results are applied because they are more than the minimum considered downloading/uploading bandwidth.

4. Verify that the bandwidth is applied in memory so that QoS can utilize the values:

```
# diagnose netlink interface list port1
...
inbandwidth=97319(kbps)         total_bytes=587645K     drop_bytes=522341K
outbandwidth=425252(kbps)

        priority=0      allocated-bandwidth=13(kbps)    total_bytes=517765K     drop_
bytes=235786K
        priority=1      allocated-bandwidth=0(kbps)     total_bytes=0   drop_bytes=0
        priority=2      allocated-bandwidth=0(kbps)     total_bytes=0   drop_bytes=0
        priority=3      allocated-bandwidth=0(kbps)     total_bytes=1330        drop_bytes=0
        priority=4      allocated-bandwidth=425238(kbps)        total_bytes=0   drop_bytes=0
...
```

Recommendations:

- We recommend recurring scheduled tests to validate connectivity meets the needs of your users. Each device is limited to 10 tests per day.
- Consider what time the speed test will run. Different times will provide different insight:

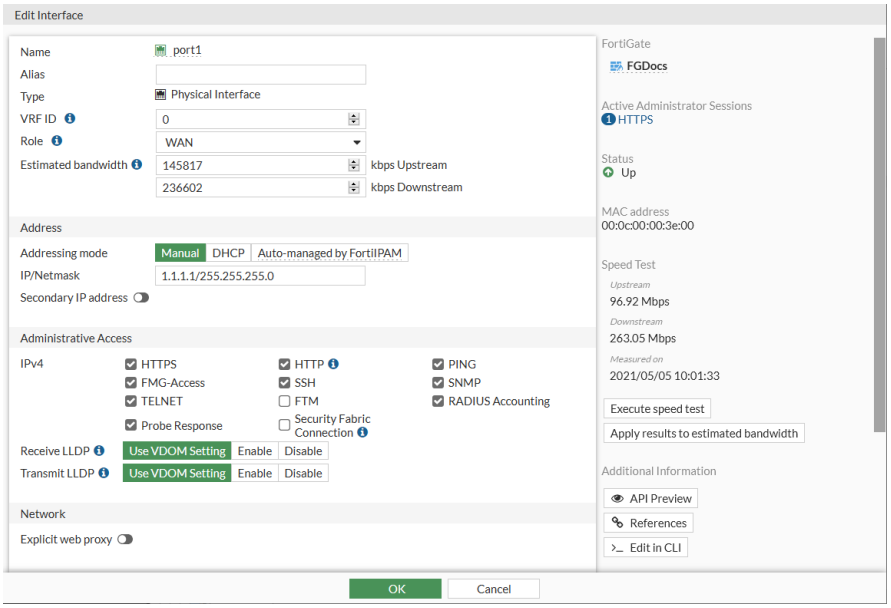
	Pro	Con
Peak hours	• Captures congestion at ISP.	• Can be noisy • Results can vary from day to day • Captured issues can be difficult to reproduce
Off-peak hours	• No contention with business traffic. • Provides an accurate technical capacity of the path.	• Can be overly optimistic which may not reflect user experience.
During times of known issues	• Can be scheduled if the issue has a pattern	• Activity may be unrelated but could provide additional troubleshooting context

GUI Speed Test

A manual interface speed test provides an immediate bandwidth baseline for a WAN link. You can optionally apply the measured bandwidth to the interface's estimated bandwidth values so shaping and SD-WAN logic can reference more accurate numbers.

Example: Run a manual speed test and apply the results

1. Go to *Network* > *Interfaces*.
2. Edit a WAN interface. The interfaces can be grouped by role using the grouping dropdown on the right side of the toolbar.
3. Click *Execute speed test* in the right pane.



4. When the test completes, select *Apply results to estimated bandwidth* (if you want to update the interface values).
5. Click *OK* to save.

CLI Speed Test

The CLI speed test can be used when GUI access is unavailable, or when you want to script repeatable tests. The FortiGate first downloads a server list, then runs a test using Auto/TCP/UDP modes.

Example: Download servers and run an Auto speed test

1. Configure the speed test settings:

```
config system speed-test-setting
  set latency-threshold 60
  set multiple-tcp-stream 4
end
```

2. Download the server list from FortiCloud:

```
execute speed-test-server download
```

3. Verify the list:

```
execute speed-test-server list
```

4. Run the speed test:

> A speed test can be run with or without specifying a server. The system will automatically choose one server from the list and run the speed test. The test results are shown in the command terminal.

```
execute speed-test <interface> <server> {Auto | TCP | UDP}
```

5. Verify the results:

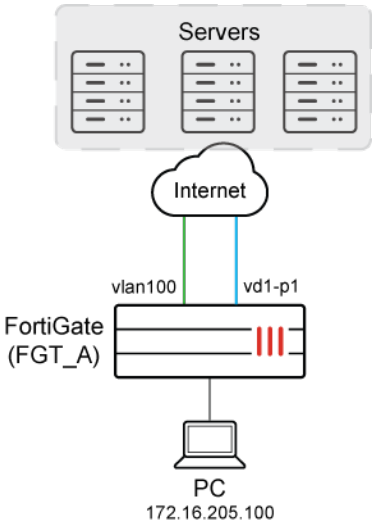
```
show system interface wan1 | grep measured
```

Application Performance Monitoring

Application Performance Monitoring (APM) provides application-level visibility into network performance by passively measuring metrics such as latency, jitter, and packet loss across live traffic. This enables administrators to correlate SD-WAN steering decisions with actual end-user experience. This section demonstrates how to enable APM and interpret its outputs.

Example: Enable APM and review metrics for Telnet

In this example, SD-WAN is configured with a zone named virtual-wan-link, and it contains two members (vlan100 and vd1-p1). A firewall policy is configured for the SD-WAN zone with application performance monitoring from the PC to a server.



1. Configure SD-WAN:

```
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
    end
    config members
        edit 1
            set interface "vd1-p1"
        next
        edit 2
            set interface "vlan100"
            set gateway 172.16.206.2
        next
    end
    config service
        edit 1
            set name "1"
            set dst "all"
            set src "172.16.205.0"
            set priority-members 1 2
        next
    end
end
```

2. Identify the preferred interface:
   In this example `vd1-p1` is the preferred SD-WAN member.

```
# diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(manual)
  Members(2):
    1: Seq_num(1 vd1-p1 virtual-wan-link), alive, selected
    2: Seq_num(2 vlan100 virtual-wan-link), alive, selected
  Src address(1):
        172.16.205.0-172.16.205.255
  Dst address(1):
        0.0.0.0-255.255.255.255
```

3. Configure a firewall policy for the SD-WAN zone to monitor traffic from the PC:
   In this example, the dstintf option is set to the SD-WAN zone (virtual-wan-link), the srcaddr option identifies the PC (172.16.205.0), and application performance monitoring is enabled.

```
config firewall policy
    edit 1
        set name "APM"
        set srcintf "any"
```

```
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "172.16.205.0"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set app-monitor enable
        set passive-wan-health-measurement enable
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set application-list "g-default"
        set logtraffic all
        set auto-asic-offload disable
    next
end
```

4. As traffic passes from the PC through FortiGate to the server, TCP traffic is measured and logged, and you can view a session list:

```
# diagnose sys session list

(...)
hook=pre dir=org act=noop 172.16.205.100:51128->172.16.202.2:22(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.202.2:22->172.16.205.100:51128(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=1 pol_uuid_idx=843 auth_info=0 chk_client_info=0 vd=0
serial=00006eb8 tos=ff/ff app_list=6000 app=16060 url_cat=0
sdwan_mbr_seq=1 sdwan_service_id=1
rpdb_link_id=ff000001 ngfwid=n/a
tcp_srt=240 tcp_nrt=0 tcp_org_rtrs=17 tcp_rpl_rtrs=273 tcp_syn_rtrs=0 tcp_syn_ack_rtrs=0 tcp_
rst=00
npu_state=0x1041001 no_offload
no_ofld_reason:  disabled-by-policy non-npu-intf
total session: 1
```

5. View detailed application performance metrics in SD-WAN logs:

```
# execute log display

1: date=2025-03-06 time=09:40:33 eventtime=1741210833244790449 tz="+1200" logid="0113022941"
type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN application
performance metrics via kernel" eventtype="Application Performance Metrics" appid=16091
interface="vd1-p1" serverresponsetime="162.0" networktransfertime="0.0" latency="162.0"
rttsample=5 originjitter="0" replyjitter="100" jitter="100.0" originpktloss="21.8"
replypktloss="2.6" packetloss="3.7" retransample=6 originretransmission=13
replyretransmission=17 synretransmission=0 synackretransmission=0 originreset=0 replyreset=0
msg="Application Performance Metrics via kernel"
```

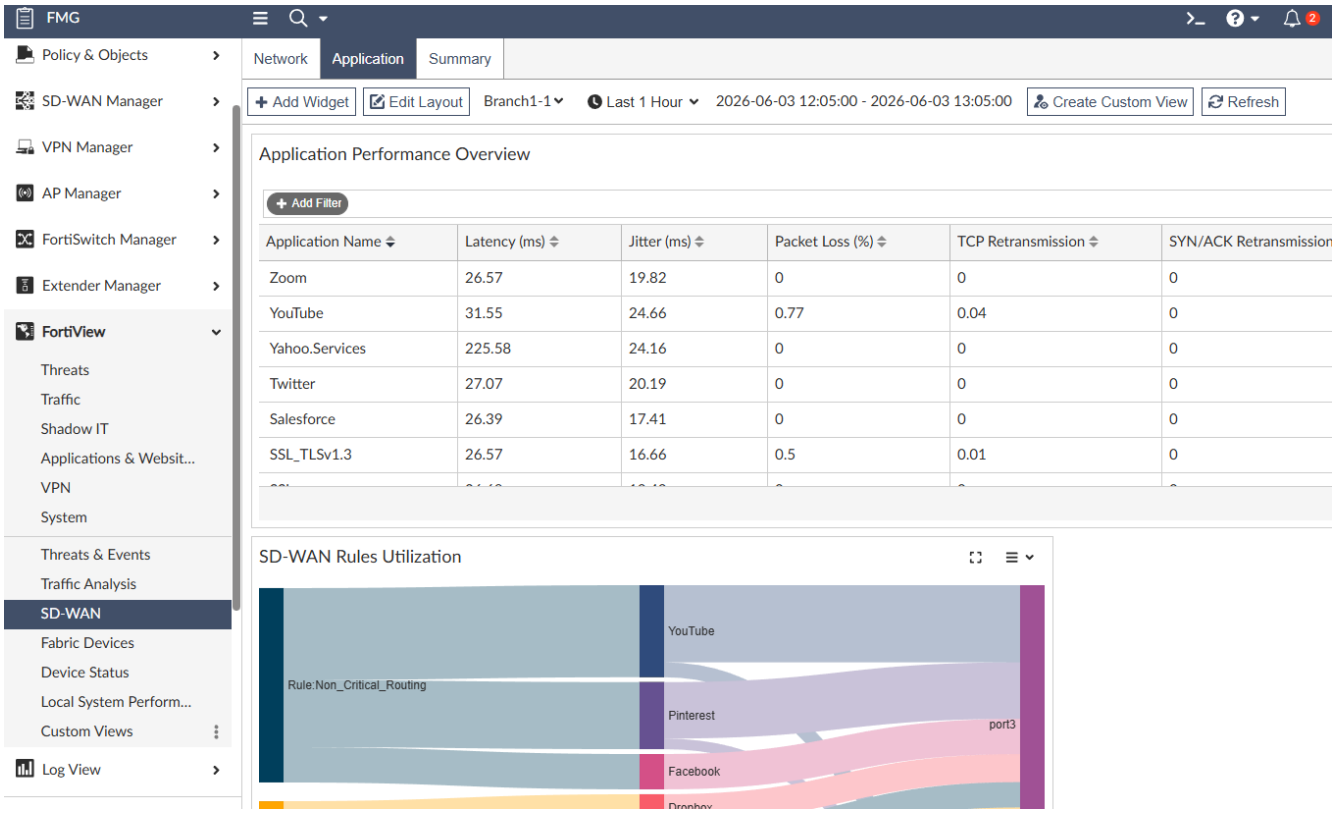
To interpret this log: the application 16091 - Telnet is experiencing a latency of 162 ms on 5 session samples. Some packet losses were experienced in both origin and reply directions, leading to some retransmissions. Details are listed in the table.

Metric	Value
Server Response Time (ms)	162.0
Network Transfer Time (ms)	0.0
Latency (ms)	162.0
RTT Sample	5
Origin Jitter (ms)	0
Reply Jitter (ms)	100
Jitter (ms)	100.0
Origin Packet Loss (%)	21.8
Reply Packet Loss (%)	2.6
Packet Loss (%)	3.7
Retransmission Sample	6
Origin Retransmission	13
Reply Retransmission	17
SYN Retransmission	0
SYN-ACK Retransmission	0
Origin Reset	0
Reply Reset	0

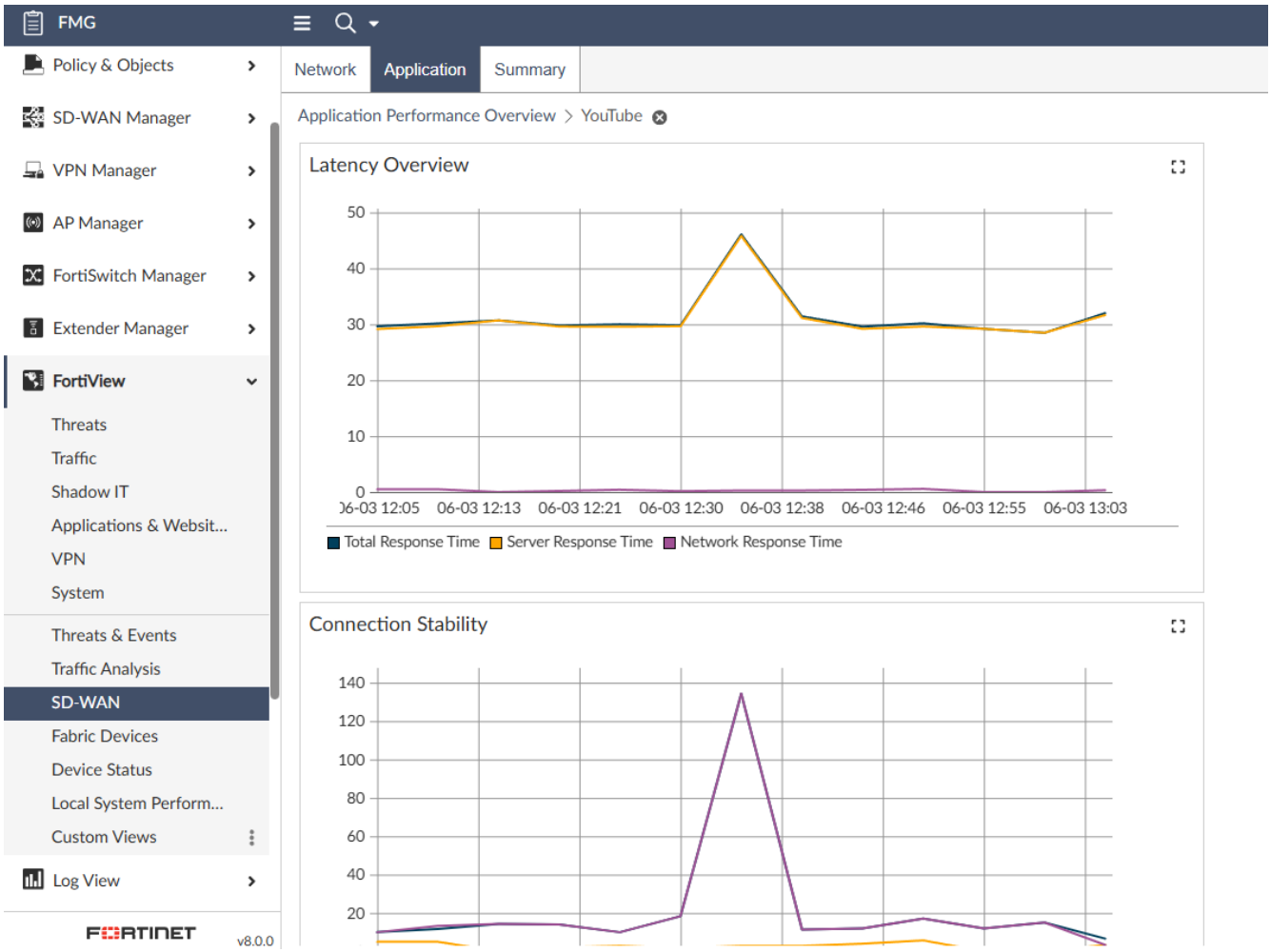
FortiAnalyzer FortiView for analyzing application steering

Although this deployment brief is not FortiAnalyzer-focused, FortiAnalyzer FortiView can be a useful validation and troubleshooting aid once SD-WAN is in place. In particular, the SD-WAN > Application FortiView monitor in FortiAnalyzer consolidates SD-WAN application experience and utilization into a single view, combining key performance indicators such as latency, jitter, packet loss, and retransmissions with traffic utilization insights.

The following examples are taken from a FortiManager which is managing a FortiAnalyzer. See the FortiAnalyzer Admin Guide for more details.



It provides an Application Performance Overview table (with drill-down views for latency, connection stability, retransmissions, and reliability), alongside widgets that show SD-WAN rule utilization, utilization by application per WAN link, and application bandwidth utilization.



Used in this context, the page is best treated as a quick way to confirm that SD-WAN steering is producing the expected end-user experience and to accelerate root-cause analysis when an application's performance degrades.

ASIC Offload Disable

When app-monitor is enabled in a firewall policy, NPU offloading for the firewall policy is automatically disabled. This is required for session-level inspection, which enables Application Performance Monitoring. This can provide unexpected additional overhead on the CPU of an appliance, so APM should be enabled intelligently, and for specific firewall use cases.

In general, avoid enabling app-monitor on firewall policies that:

- Handle high-throughput traffic or very high concurrent session counts
- Are broad in scope and could impact many or most users
- Function as catch-all or last-resort rule

To get the most value from application monitoring:

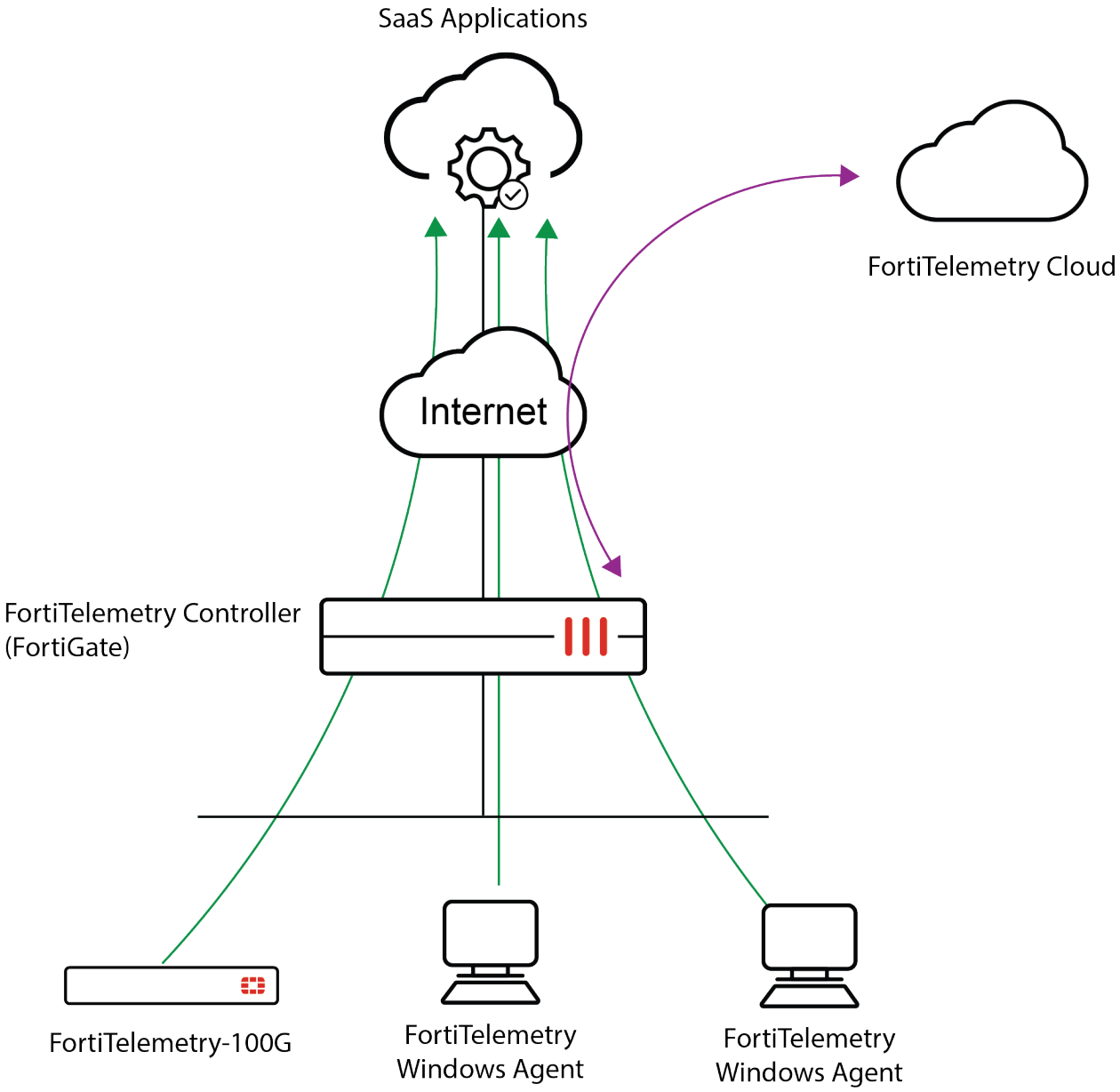
- Create dedicated monitoring policies and scope them to:
  - Specific sources (users/subnets) and/or
  - Specific destinations (applications/servers)

FortiTelemetry

FortiTelemetry provides end-to-end application telemetry monitoring using one FortiGate acting as a FortiTelemetry Controller and one or more FortiTelemetry agents. The controller onboards agents into the Security Fabric, manages telemetry profiles and policies, and provides monitors for viewing application metrics and statistics. Agents continuously emulate and monitor SaaS application experience to generate application-level and network-level performance metrics.

Requirements

FortiTelemetry Controller (FortiGate)



- On-premise, hardware-based FortiGate used as the FortiTelemetry Controller.
- FortiOS 7.6.3 or later.
- At least 4 GB of memory on the hardware FortiGate.
- Network access from the controller to reach FortiTelemetry Cloud.
- Security Fabric Connection access (fabric) enabled on the interface used to connect to agents.
- FortiTelemetry Discovery enabled.

- Controller must be in the same Layer 2 network segment as the agents.

FortiTelemetry agents (hardware and Windows)

- One or more FortiTelemetry agents are required.
- Supported agent types: FortiTelemetry-100G hardware agent and Windows-based software agent.
- Agents must be deployed in the same Layer 2 segment/subnet as the controller's internal/agent-facing interface.
- Windows agent host sizing: at least 4 CPUs and 8 GB RAM (see Release Notes for additional details).

Configure a FortiGate as the Telemetry Controller

Enable the controller (CLI)

```
config system global
    set telemetry-controller enable
end
```

Configure the agent-facing interface (CLI example)

Use the internal/LAN interface that is on the same L2 segment as the agents (example uses port2):

```
config system interface
    edit port2
        set allowaccess ping fabric
        set telemetry-discover enable
        set auto-auth-extension-device disable
    next
end
```

After agent deployment, consider disabling telemetry-discover to reduce exposure to CAPWAP discovery traffic.

Register to a Cloud region and configure certificates

Register the controller to FortiTelemetry Cloud (CLI)

Configure the FortiTelemetry Cloud region and retry interval (current release supports the Global region):

```
config telemetry-controller global
    set region global
```

```
    set retry-interval 120
end
```

Configure certificates (Windows agent only)

A CA certificate must be configured on the controller and a corresponding user certificate must be installed on each Windows agent. This is not required for the FortiTelemetry-100G hardware agent.

1. Create a certificate authority (CA) certificate using your chosen PKI tooling.
2. Upload the CA certificate to the controller FortiGate: *System > Certificates > Create/Import > CA Certificate* (Type: File).
3. Configure the controller to use the CA certificate (CLI):

```
config telemetry-controller global
    set telemetry-ca-certificate "CA_Cert_1"
end
```

4. Create a user certificate for the Windows host (must include the private key) and export it as PFX/p12.
5. On the FortiTelemetry Windows Agent GUI, go to *Settings > Agent Management Certificate* and import/select the certificate.

FortiTelemetry Windows Software Agent

Windows host prerequisite configuration

1. Disable sleep: Windows System Settings > Power & Sleep; set Sleep to Never.
2. Disable NIC power savings: Windows Settings > Network & Internet > Ethernet > Change adapter options; adapter Properties > Configure > Power Management; uncheck “Allow the computer to turn off this device to save power”.
3. Ensure the controller CA is configured and the Windows agent certificate is installed/selected prior to operation.

Install the agent (MSI)

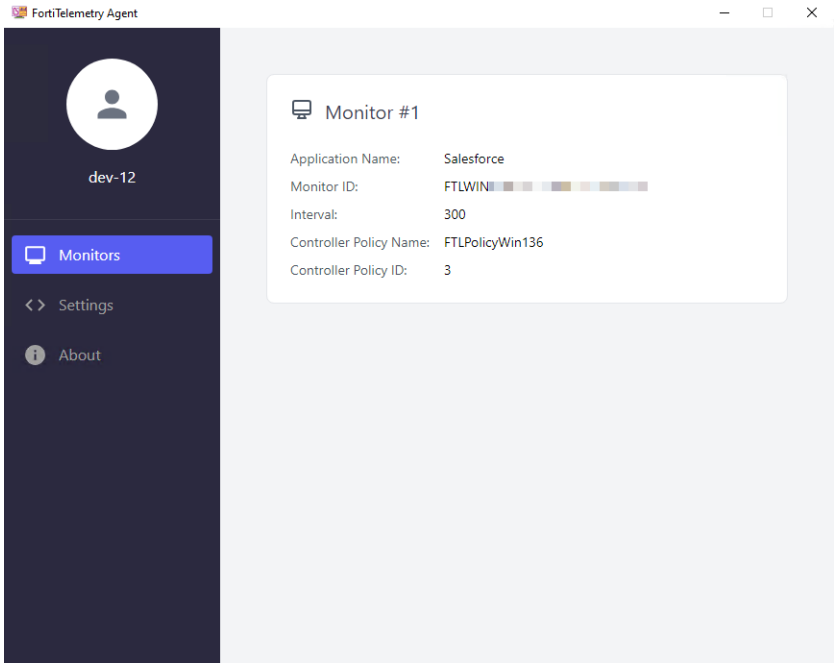
1. Copy the FortiTelemetry agent installer (.msi) to the Windows host.
2. Run the installer and complete the setup wizard (accept license, choose path, Install, Finish).

Validate agent operation

- Use Task Manager to confirm FortiTelemetry agent processes are running; the daemon starts automatically after installation or reboot.
- Default log path: C:\Program Files\Fortinet\FortiTelemetry\output\log

Windows agent GUI overview (for operations)

- Monitor tab: shows assigned monitoring tasks when connected and configured.
- Settings tab: select the network interface used to connect to the controller and the Agent Management Certificate used for DTLS client authentication.
- About tab: shows agent version/serial and controller connectivity details.



Deploy and authorize the FortiTelemetry agent

Discovery method (CAPWAP discovery; manual authorization)

The controller discovers agents using CAPWAP and lists them under the Telemetry fabric connector. Discovered agents must be authorized before use.

Authorize via GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Select the Telemetry connector and click *Edit*.
3. Select the agent, then choose *More* > *Set Status* > *Authorize*.

Authorize via CLI:

```
config telemetry-controller agent
    edit "FT100GTK24000002"
        set authz authorize
```

```
    next
end
```

Pre-configuration method (pre-authorize by serial number)

Pre-create an agent entry using the agent serial number as the name and set authorization to Authorized. When the real agent appears online, it will be auto-authorized.

Pre-authorize via GUI:

1. Go to *Security Fabric* > *Fabric Connectors* > *Telemetry* > *Edit*.
2. Click *Create New* and set *Name* to the agent serial number (Windows agents typically start with FTLWIN; hardware agents start with FT100G).
3. Set *Authorization* to *Authorize* and select an Agent Profile matching the agent model (WINDOWS or FTL100G).

Pre-authorize via CLI (example):

```
config telemetry-controller agent
    edit "FTLWIN8660000001"
        set alias "WINDOWS-108"
        set authz authorized
        set agent-profile "WINDOWS-pre-auth"
    next
end
```

Recommended end-to-end sequence

1. Validate requirements (controller hardware/software, L2 adjacency, cloud reachability).
2. Configure the FortiGate as FortiTelemetry Controller and enable FortiTelemetry visibility in the GUI.
3. Register the controller to the FortiTelemetry Cloud region (Global) and set the retry interval.
4. If using Windows agents: configure CA on the controller and install/import the PFX/p12 certificate on each Windows agent.
5. Install the Windows agent and confirm it is running and able to reach the controller over the L2 segment.
6. Authorize agents (manual authorization after discovery, or pre-authorize by serial number).

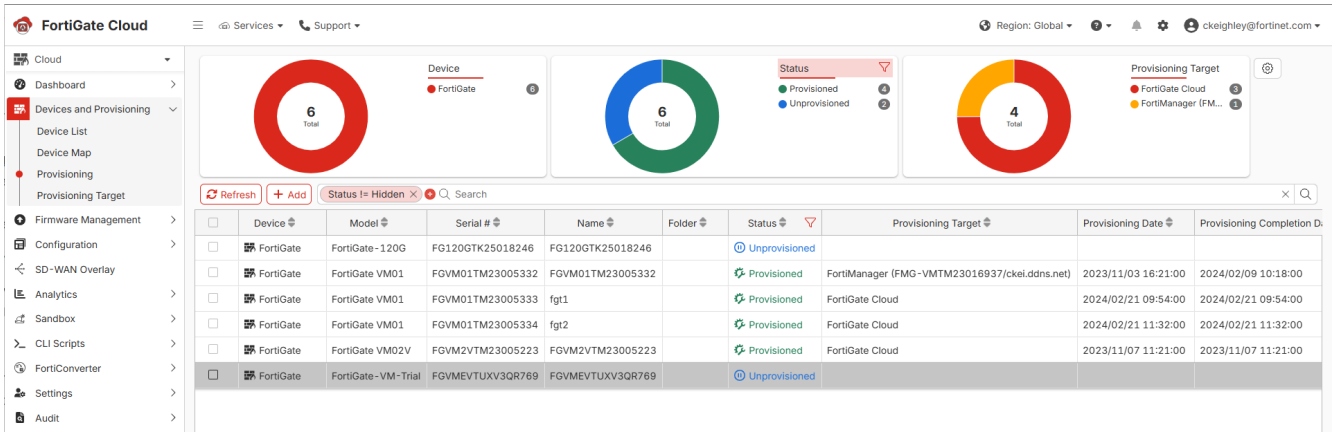
FortiGate Cloud

FortiGate Cloud provides cloud-based onboarding, centralized visibility, and lightweight management workflows for FortiGate devices, including configuration/logging enablement, inventory views, and optional SD-WAN overlay provisioning. Cloud provisioning is the mechanism used to connect a FortiGate to FortiGate Cloud for cloud management and logging, after which you typically enable logging on relevant firewall policies and confirm log upload to FortiGate Cloud.

As the services provided by FortiGate Cloud overlap with the functionality of FortiManager and FortiAnalyzer, administrators should select only one solution to manage their FortiGate deployment, continued configuration (including SD-WAN deployment), and logging.

Cloud Provisioning

Use cloud provisioning to register and connect devices to FortiGate Cloud for ongoing monitoring and management. FortiGate Cloud supports multiple provisioning methods, including FortiCloud key, FortiCloud inventory, and the FortiOS GUI workflow.



Example: Provision a FortiGate to FortiGate Cloud using the FortiCloud key

1. Log in to FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning*, then click *Add*.
3. In the *FortiCloud or FortiDeploy key* field, enter your key value.
4. For *End user type*, select *A non-government user* or *A government user* as required.
5. From the *Partner* dropdown list, select the affiliated Fortinet partner.
6. To provision your FortiGate to FortiGate Cloud after import, enable *Provision after import*.

Scripts may be included as part of provisioning. If utilized, the selected script is executed automatically once the FortiGate establishes a management tunnel with its management server.

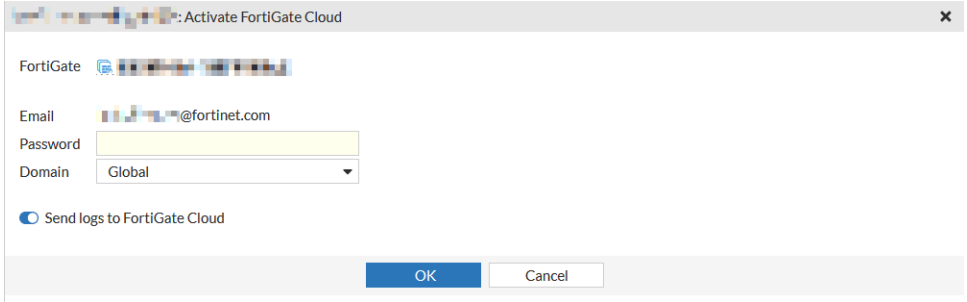
7. Click *OK*.
   After the device is successfully provisioned, the device key becomes invalid. You can only use the key once to provision a device.

Example: Provision a FortiGate to FortiGate Cloud using the inventory

1. Log in to the FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning* , then click *Add*.
3. Select the desired device from the displayed inventory. This displays all assets from the logged-in FortiCloud account. Click *Provision* > *Provision to FortiGate Cloud*.
4. From the *Select Display Timezone for Device* dropdown list, select the desired time zone.
5. Click *Submit*.

Example: Provision a FortiGate to FortiGate Cloud in the FortiOS GUI

1. In the FortiCloud portal, ensure that you have a product entitlement for FortiGate Cloud for the desired FortiGate or FortiWifi.
2. In FortiOS, in the *Dashboard*, in the FortiGate Cloud widget, the *Status* displays as *Not Activated*. Click *Not Activated*.
3. Click the *Activate* button.
4. In the *Activate FortiGate Cloud* panel, the *Email* field is already populated with the FortiCloud account that this FortiGate is registered to.
5. In the *Password* field, enter the password associated with the FortiCloud account.
6. Enable *Send logs to FortiGate Cloud*. Click *OK*.



7. This should have automatically enabled *Cloud Logging*. Ensure that *Cloud Logging* was enabled. If it was not enabled, go to *Security Fabric* > *Fabric Connectors* > *Cloud Logging*, enable it, then set *Type* to FortiGate Cloud.
8. You must set the central management setting to FortiCloud, as this is the initial requirement for enabling device management features.

Example: Configure a FortiGate-VM for FortiGate Cloud

FortiGate-VMs require additional configuration to ensure that they function with FortiGate Cloud. Run the following commands in the FortiOS CLI:

```
config system fortiguard
    unset update-server-location
end
```

Example: Provision Fabric Devices (FortiAP, FortiSwitch, and FortiExtender)

1. Log in to the FortiGate Cloud.
2. Go to *Devices and Provisioning* > *Provisioning*. All FortiAP (FAP), FortiSwitch (FSW), and FortiExtender (FEXT) devices registered in the account's Asset Management portal are displayed on the *Provisioning* page.
3. Select the device(s) to provision and click *Provision*.
4. In the *Provision Device* pane, configure the device and click *OK*.

When a FortiGate is deprovisioned, its connected fabric devices will also be deprovisioned.

If multiple provisioning targets are detected for a Fabric device, a *Conflict Target* pop-up window is displayed, where you can select the intended provisioning target.

When a Fabric device is deprovisioned from its root FortiGate, it is also deauthorized on the FortiGate.

Logging and Analysis

One year of log retention is included for licensed FortiGates, enabling FortiGate Cloud to centrally store and analyze unified threat management (UTM) logs and activity. Advanced analytics are delivered through more than 30 pre-defined reports, alongside real-time log processing that correlates incoming data against a comprehensive database of known threats and malicious patterns. By applying this continuous, contextual analysis, FortiGate Cloud can identify and flag potentially infected endpoints for further investigation. When integrated with Incidents & Events, this capability can also support automated alerting and response, helping streamline detection and remediation workflows.

Example: Scheduled Pre-defined reports

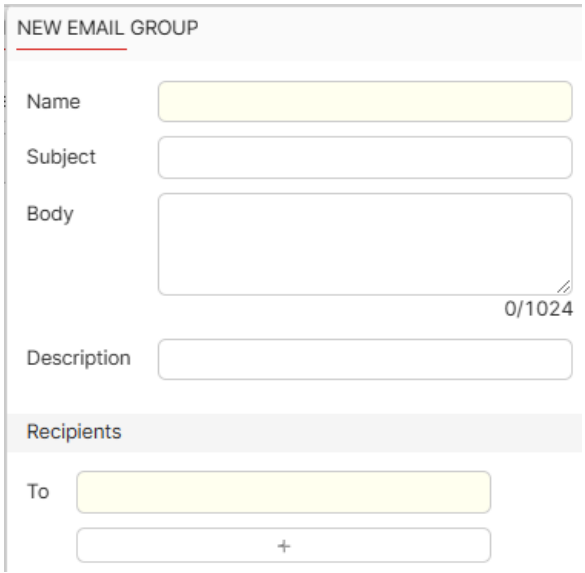
Reports can be run on a defined schedule as well as on-demand. Once the report finishes, it can be sent via Email to one or more email addresses.

To schedule a report:

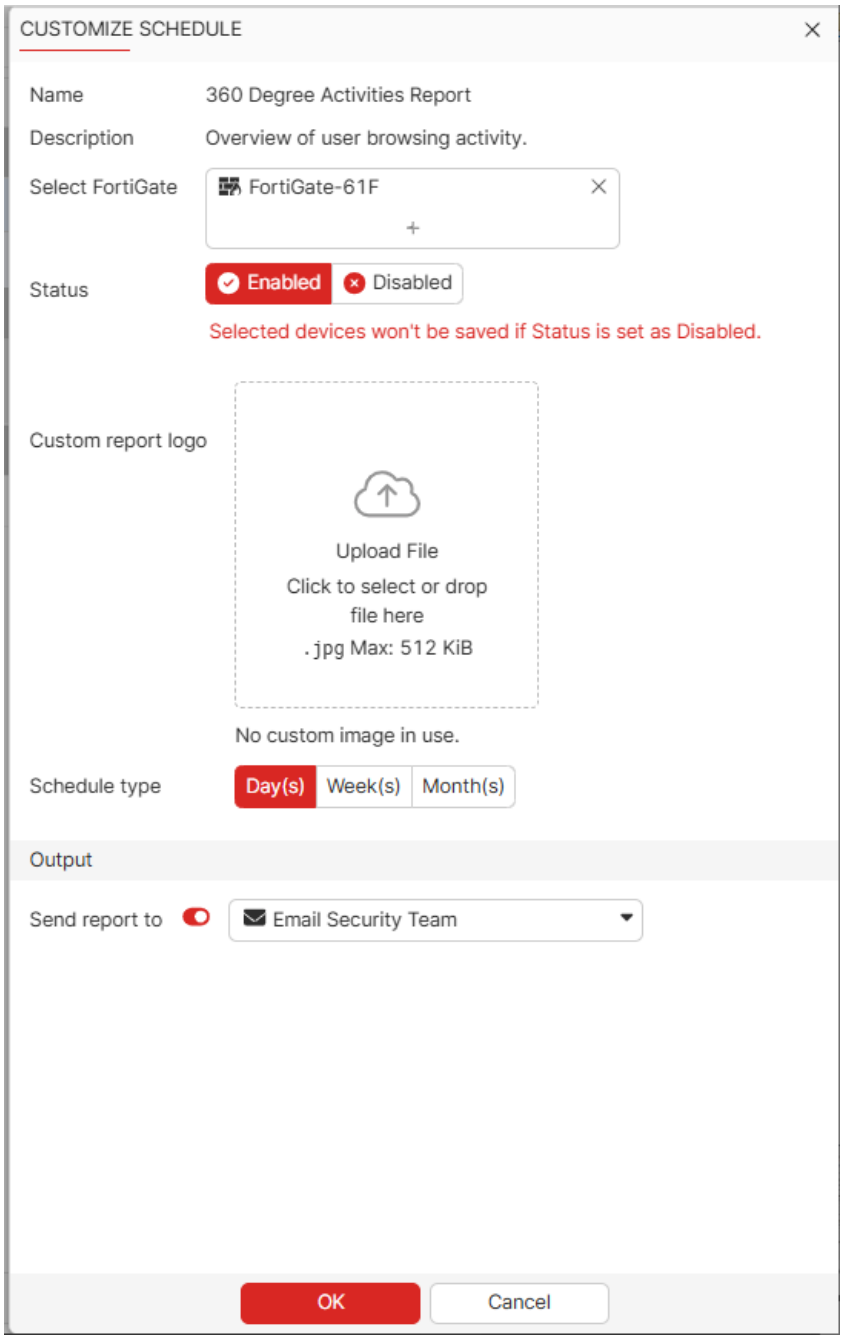
1. Go to *Analytics* > *Reports* > *Scheduled reports*.
2. Select the desired report.
3. Click *Customize*.
4. In the *Select FortiGate* field, select the desired FortiGates to run the report for.
5. If desired, in *Custom report logo*, upload an image as the custom logo for the report.
6. In the *Schedule type* field, configure the desired schedule for the report.
7. If desired, enable *Send report to* and select an email address or email group to send the report to.
8. Click *OK*. FortiGate Cloud generates the report as per the configured schedule. You can view these reports in *Analytics* > *Generated reports*.

To configure an email group to send a report to:

1. Create an email group:
   a. Go to *Analytics* > *Reports* > *Scheduled reports*.
   b. Click *Manage email groups*.
   c. Click *Create*.
   d. In the *Name* field, enter the email group name.
   e. In the *Subject* field, enter the email subject line.
   f. In the *Body* field, enter the email body content.
   g. In the *Description* field, enter the email description.
   h. In the *To* field, enter the email addresses to send the email to.



   i. Click *OK*.
2. Select the desired report, then click *Customize*.
3. Enable the *Send report to* toggle. From the *Send report to* dropdown list, select the desired email group.



4. Click OK.

Example: IoC

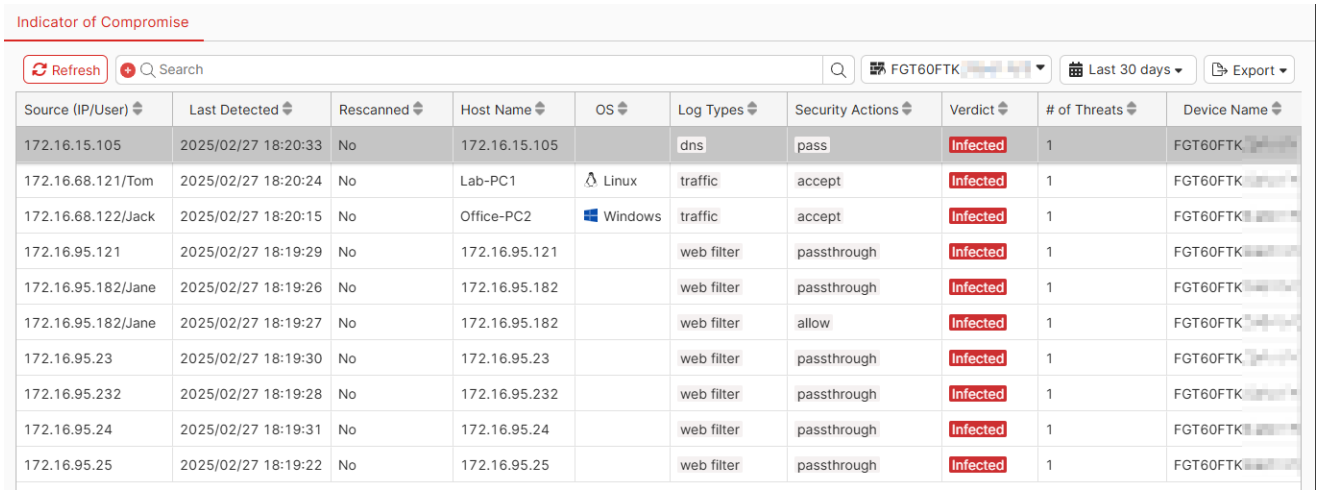
IoC detects the following threat types, based on the evolving FortiGuard database:

Threat type	Description
Malware	Malicious programs residing on infected endpoints

Threat type	Description
Potentially unwanted programs	• Spyware • Adware • Toolbars
Unknown	Threats that the signature detected but does not associate with any known malware

To access IoC:

Go to *Analytics* > *IoC* > *Threats*. This page displays a table of data for any detected threats.



Source (IP/User)	Last Detected	Rescanned	Host Name	OS	Log Types	Security Actions	Verdict	# of Threats	Device Name
172.16.15.105	2025/02/27 18:20:33	No	172.16.15.105		dns	pass	Infected	1	FGT60FTK
172.16.68.121/Tom	2025/02/27 18:20:24	No	Lab-PC1	Linux	traffic	accept	Infected	1	FGT60FTK
172.16.68.122/Jack	2025/02/27 18:20:15	No	Office-PC2	Windows	traffic	accept	Infected	1	FGT60FTK
172.16.95.121	2025/02/27 18:19:29	No	172.16.95.121		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.182/Jane	2025/02/27 18:19:26	No	172.16.95.182		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.182/Jane	2025/02/27 18:19:27	No	172.16.95.182		web filter	allow	Infected	1	FGT60FTK
172.16.95.23	2025/02/27 18:19:30	No	172.16.95.23		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.232	2025/02/27 18:19:28	No	172.16.95.232		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.24	2025/02/27 18:19:31	No	172.16.95.24		web filter	passthrough	Infected	1	FGT60FTK
172.16.95.25	2025/02/27 18:19:22	No	172.16.95.25		web filter	passthrough	Infected	1	FGT60FTK

Events can be reviewed in this menu, and they may be exported to a CSV or JSON file.

You can configure trigger-based automated alerts for IoC events. See Example: Incidents & Events.

Example: Incidents & Events

In *Incidents & Events*, you can generate, monitor, and manage alerts and events from logs.

Incidents	View, edit, and analyze incidents created for events.
Event Monitor	View and monitor events generated by event handlers, and create incidents.
Event Handler	View predefined event handlers and create notification profiles.
Automation	Create event handler stitches for FortiGates. Each stitch specifies what action to automatically take for an event handler on a FortiGate.

Following is a summary of the workflow:

1. Create a notification profile.
2. Create an event handler stitch to combine an event handler with an action.
3. Review events and create incidents.

4. Assign and track incidents.

To create a notification profile:

1. Go to *Analytics > Incidents & Events > Event Handler*.
2. On the *Notification Profile* tab, click *Create New*.
3. Enter a name for the profile.
4. If desired, enable *Email*.
   a. Configure the desired email addresses to send the notification to.
   b. Configure the *Subject* field as desired, then click *OK*.

To create an Event Handler:

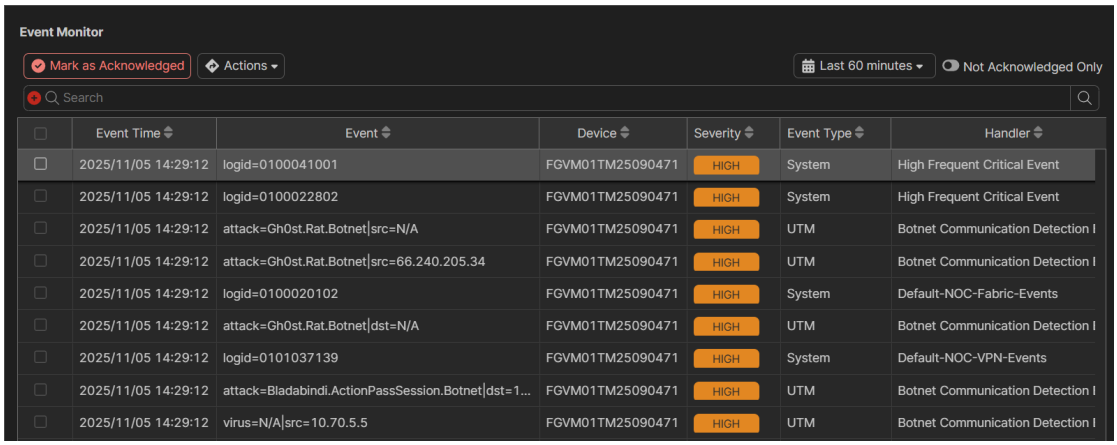
1. Go to *Analytics > Incidents & Events > Event Handler*.
2. In the *Event Handler* tab, click *Create*.
3. Configure the Event Handler details:

Field	Description
Name	Enter the event handler name.
Event Type	Select and event type from the dropdown.
Description	(Optional) Enter a description of the event handler.

4. Configure the event *Rules*.
   a. Click *Create*.
   b. Select the event *Severity* from the dropdown.
   c. *Choose Your Logs*: Select the *Log Type* and *Log Subtype* that you want to monitor for events. Select the *Log Field* to categorize logs into smaller groups based on the chosen log fields.
   d. *Refine Your Logs*: Once logs are grouped, you can refine the data within each group by applying filters with other log fields. Logs that match the filters will be retained within each group.
   e. *Define Event Conditions*: Once you have organized and filtered the logs, set up criteria that enables the system to automatically initiate events when log records reoccur within each group.
5. Click *OK*.

To review events:

After event handlers start generating events, the events display on *Event Monitor*.



Select an incident and click *Analysis*.

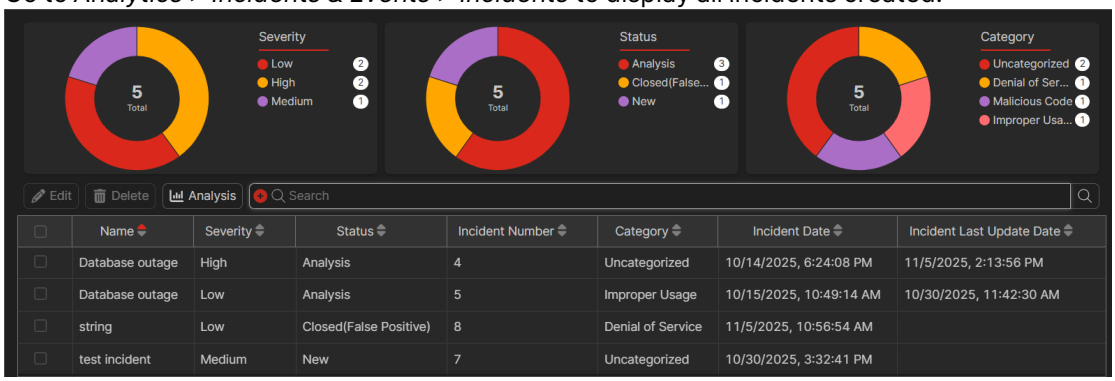
A summary of the incident is displayed as well as the associated event(s).

To create an incident (or add to an existing incident):

1. Go to *Analytics* > *Incidents & Events* > *Event Monitor*.
2. Select one or more incidents, and click *Actions*.
3. Choose one of the following options:
   - Create New Incident
   - Add to Existing Incident

To assign and track incidents:

1. Go to *Analytics* > *Incidents & Events* > *Incidents* to display all incidents created.



2. Select an incident and click *Edit*.
3. Edit the following options, and click *OK*:
   a. Name
   b. Incident Category
   c. Severity
   d. Status
   e. Description
   f. Assigned To

Device List and Device Map

Inventory, Health, and Operations

The FortiGate device list is your primary inventory view and operational cockpit. It provides:

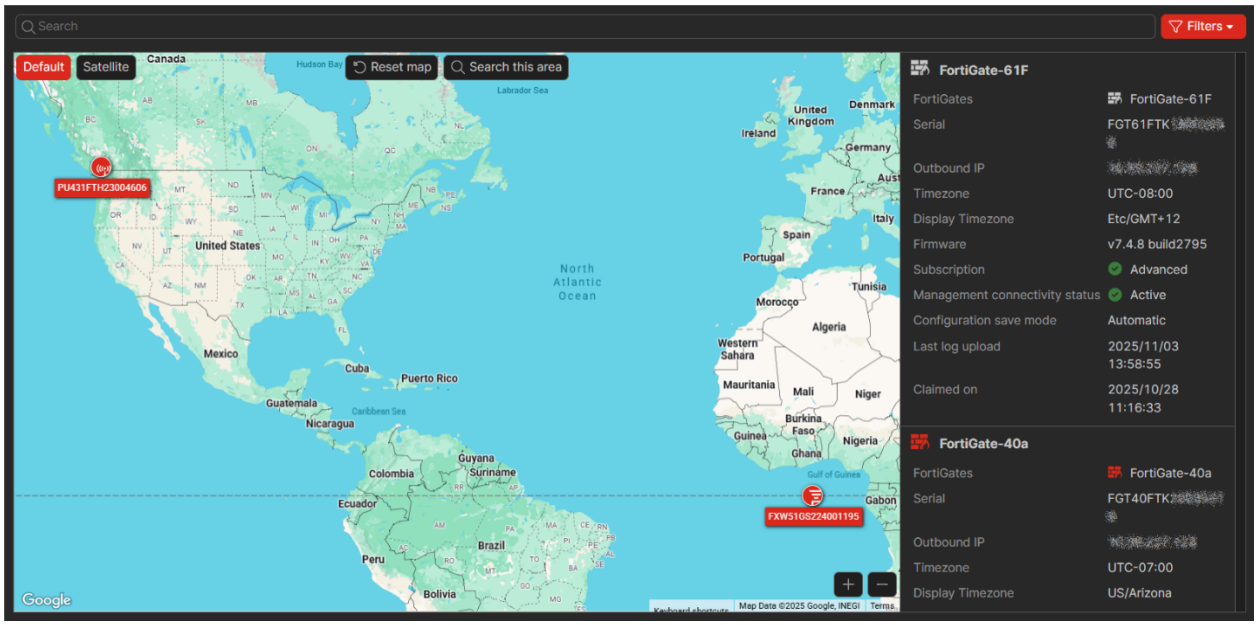
- At-a-glance charts for management connectivity, firmware distribution, and subscription status (including Standard).
- Common actions such as Cloud Access, Export to CSV, and device actions (for example, configuration/diagnostics operations and backup/timezone options).
- Useful operational columns such as firmware/build, connectivity status, resource diagnostics, and timestamps for last backup and last log upload.

FortiAP, FortiSwitch, and FortiExtender device lists provide similar details on respective devices managed by a FortiGate with a FortiGate Cloud Standard subscription.

Device Map (Geographic View & Topology Awareness)

Use Device Map when you need a geographic representation of your deployed devices:

- Shows provisioned devices by geolocation, with a side panel that mirrors key device-list details.
- Lets you zoom/locate devices quickly and reset to a global view.
- For subscribed devices, you can adjust geolocation by dragging a device icon to the correct location; filters allow focusing on specific device types.



SD-WAN Overlay as a service (OaaS)

FortiCloud Overlay-as-a-Service (OaaS) enables centralized orchestration and rapid provisioning of SD-WAN overlays across FortiGate devices using FortiGate Cloud. It provides a simplified, GUI-driven workflow that allows administrators to deploy SD-WAN overlays within a region with minimal manual configuration. The solution leverages FortiCloud-managed overlay hubs and supports a geo-redundant dual-hub architecture, while branch and datacenter FortiGates operate as spokes. Using ADVPN, the overlay dynamically establishes spoke-to-spoke shortcut tunnels when optimal paths are available, reducing unnecessary hub hairpinning and improving traffic efficiency.

During deployment, OaaS automates the configuration of core SD-WAN and overlay components, including IPsec ADVPN tunnels, BGP routing, SD-WAN zones and rules, performance SLAs, policy routes, and required firewall policies. Administrators are guided through prerequisites, topology definition, and provisioning steps via a wizard, with full task visibility in FortiGate Cloud. Access to the feature requires appropriate IAM RBAC permissions and is region-dependent. Once deployment completes, configurations can be validated on the devices, allowing administrators to test connectivity and confirm successful overlay provisioning.

Deployment prerequisites

1. Confirm all site/spoke FortiGates meet the supported baseline (FortiOS 7.4.4 or later).
2. Register and apply an OaaS license for every FortiGate used as a site/spoke (VM or hardware) under the FortiCloud account used for OaaS.
3. Prepare underlay connectivity on every site/spoke: configure WAN IP and default gateway, verify internet reachability, and configure LAN interfaces/subnets.

4. Ensure intended WAN/LAN interfaces are not referenced by existing firewall policies, are not part of existing zones, and the WAN interface is not already bound to an SD-WAN zone.
5. Register each FortiGate with FortiCare and activate FortiGate Cloud so the FortiCloud management tunnel is available for OaaS orchestration.

Planning

1. Overlay network space: validate the reserved overlay subnet does not conflict with existing WAN/LAN addressing; plan an alternate reserved subnet in OaaS Settings if needed.
2. Loopback IP space: define loopback addressing used for performance SLAs, router IDs, and administrative operations.
3. BGP ASN: select a private ASN dedicated to this SD-WAN region and keep it exclusive to this overlay deployment.
4. SLA criteria: define performance objectives and thresholds (for example, steering mode and latency/jitter/loss targets) that will drive SD-WAN behavior.
5. Hub locations: select primary and secondary FortiCloud hub locations to support geo-redundant dual-hub operation.

Firewall policies

1. Understand the default policy posture: OaaS can generate baseline spoke firewall policies that allow overlay traffic using broad/wildcard objects and services.
2. If production segmentation is required, plan to implement Centralized OaaS policies in the portal to restrict traffic to approved subnets/hosts and services.

Configuration steps

1. Register FortiCloud OaaS licenses (and any optional monitoring licenses) and verify each site/spoke FortiGate is entitled.
2. Prepare each site/spoke FortiGate for OaaS: confirm FortiGate Cloud activation, verify WAN/LAN addressing, and re-check interface/policy/zone prerequisites.
3. Access the OaaS portal using the FortiCloud account associated with the licensed devices.
4. Define the SD-WAN hub region by choosing primary and secondary hub locations in the Topology workflow.
5. For each site/spoke: add the site, add the ISP/underlay link, add the LAN/subnet definition, then deploy the SD-WAN configuration and confirm Task Status is successful.
6. Monitor link performance and quality across sites after deployment to validate underlay health and SLA compliance.
7. Apply centralized OaaS policies (if required) to enforce the desired security/segmentation posture.
8. Test and verify connectivity between sites and confirm the expected SD-WAN behavior; remediate any policy or reachability gaps discovered during validation.

Post-deploy validation focus

- Overlay: hub-and-spoke IPsec/ADVPN tunnels to the hubs (and optional shortcuts where applicable).
- Routing: BGP is established and exchanging the expected routes for site LANs.
- SD-WAN: an SD-WAN zone, performance SLAs, and SD-WAN rules are present and selecting links as intended.
- Policy: baseline firewall objects/policies exist; centralized policies are applied if you require restricted traffic flows.

SASE

FortiSASE is a cloud-delivered service that allows clients to securely access the internet with the protection from FortiOS. With FortiSASE, you can ensure to protect remote off-net endpoints and users with the same security policies as when they are on-net, no matter their location. This section demonstrates two common use cases:

- Agent-based SIA, or SIA basic endpoint: Endpoints connect to a FortiSASE tunnel to secure their traffic.
  - Once provisioned, clients are connected through an always-up tunnel connection to ensure FortiSASE scans traffic to the internet.
  - For details, see SIA Agent-based Deployment Guide.
- SPA using FortiGate hub configured for BGP per overlay: FortiSASE remote users access private resources behind FortiGate hub(s) directly through FortiSASE to hub(s) IPsec tunnels.
  - The security points of presence (PoPs) act as spokes to the FortiGate hub (FortiGate SD-WAN hub or FortiSASE SPA hub), relying on IPsec overlays and BGP to secure and route traffic between security PoPs and the networks behind the organization's FortiGate hub.
  - For details, see SPA Deployment Guide using BGP per overlay.

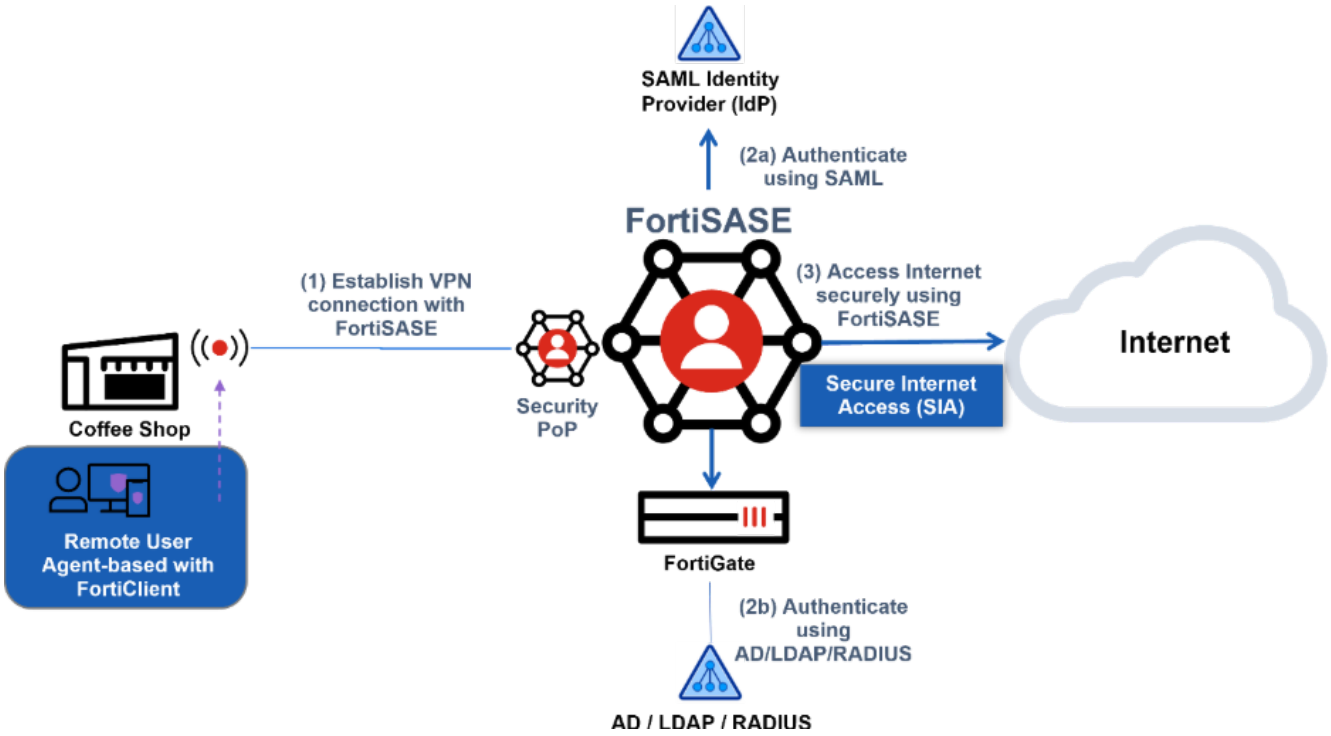
SIA basic endpoint deployment example

> Start with a small pilot group and a minimal policy set (logging enabled) before expanding to larger populations.

FortiSASE Secure Internet Access (SIA) enforces a common security policy for remote users, covering IPS, application control, web/DNS filtering, antimalware, sandboxing, and anti-botnet/C2 protection.

Agent-based SIA is the most common deployment model. FortiClient is installed on Windows or macOS endpoints and establishes a full IPsec tunnel with the FortiSASE FWaaS (Firewall-as-a-Service). All internet traffic and protocols are inspected inline before reaching the internet. Each endpoint connects to the nearest security PoP.

The following deployment example using Entra ID for SAML SSO authentication.



Supported authentication sources:

Method	Where configured
Active Directory / LDAP	Access & authentication > Authentication Sources > LDAP
RADIUS	Access & authentication > Authentication Sources > RADIUS
SAML IdP (e.g. Entra ID)	Access & authentication > Authentication Sources > SSO

Enabling SAML SSO disables other authentication methods (LDAP/RADIUS).

Deployment procedures:

Step	Task
1	Provision FortiSASE instance; select geographic PoP regions; input licenses. See Getting Started.
2	Configure remote authentication (this example uses Entra ID SAML SSO)
3	Configure security policies and profiles
4	Configure DNS settings (default DNS, custom DNS, or split DNS rules)
5	Download and install FortiClient on Windows endpoints
6	Connect FortiClient to FortiSASE using the invitation code

Step	Task
7	Users log in to the FortiSASE tunnel via SAML Login in FortiClient
8	Test and verify internet access and policy enforcement

Configuring Entra ID SAML SSO

1. In FortiSASE, go to *Access & authentication > Authentication Sources > SSO > Agent* and copy the *Entity ID*, *SSO URL*, and *Single Logout URL*.
2. In Azure portal, go to *Entra ID > Enterprise Applications > New Application*, search for *FortiSASE*, create and assign users/groups.
3. Configure SAML by pasting FortiSASE SP values into the Azure *Basic SAML Configuration* fields.
4. From Azure, copy the *Login URL, Entra ID Identifier*, and *Logout URL* back into the FortiSASE SSO wizard. Upload the SAML signing certificate.
5. Set *Digest Method* to *SHA-256*. Use *FortiSASE Default Certificate* for SP (or upload your own to avoid frequent renewals).
6. Send onboarding emails to users via *Onboard Users*. They receive a FortiClient download link and invitation code that can be used for endpoint onboarding.

Configuring Security Profiles

FortiSASE security components are configured at *Security > Traffic > Security profiles* and applied to every *Allow* policy, by default.

Available security features:

Feature	Notes
Antivirus	Enabled via toggle
Web Filter	Customizable categories and overrides
DNS Filter	Domain-level filtering
Intrusion Prevention	IPS signatures
File Filter	Block/allow by file type
Data Loss Prevention	DLP rules
Application Control with Inline-CASB	Requires SSL deep inspection for cloud apps
SSL Inspection	Certificate inspection (default) or deep inspection

SSL Deep Inspection is strongly recommended because it enables FortiSASE to decrypt and inspect HTTPS traffic for malware, phishing, and C2 exfiltration. FortiSASE automatically installs the CA certificate on endpoints, so end users see no browser warnings.

Example granular policy setup (Remote-Home-Office user group): Add these policies via *Security > Traffic > Policies*:

Policy Name	Action	Destination
RemoteHomeOffice-DenyNetflix	Block	*.netflix.com
RemoteHomeOffice-AllowFortinet	Accept	*.fortinet.com
Allow-All	Accept	All

By default, the *Allow-All* policy is already available pre-defined.

Policies are matched top-down. Order matters: Deny rules must precede the catch-all *Allow-All* policy.

Configuring a Security Profile Group and Applying It to a Policy

Security profile groups let you apply different security settings per policy, rather than globally. This is useful when you want a specific security posture for one user group without affecting others.

Example: The *Remote-Home-Office* user group can access **.fortinet.com* via the *RemoteHomeOffice-AllowFortinet* policy. You want to monitor their Cloud/IT application access using Application Control but without enabling Application Control for all other users.

- Before creating a profile group with Application Control enabled, disable Application Control on the default profile group first — otherwise the per-policy override has no effect, since Application Control would already be active globally.

Profile Group	Application Control	Applied To
Default	Disabled (after prerequisite step)	All other policies
Cloud IT	Enabled (Monitor mode)	RemoteHomeOffice-AllowFortinet

- The *Profile Group* field only appears on policies where *Action* is set to *Accept*.

Steps:

1. Go to *Security > Traffic > Security profiles*.
2. From the *Profile Group* dropdown (top right), click *Create*.
3. Name the group (e.g., *Cloud IT*). For *Initial Configuration*, choose:
   a. *Basic* starts with File Filter, DLP, and Application Control disabled; other features enabled.
   b. *Based On* copies settings from an existing profile group.
4. Enable *Application Control* in the new group. By default, this monitors Cloud/IT application access.
5. Apply the profile group to a policy:
   a. Go to *Security > Traffic > Policies*
   b. Select *RemoteHomeOffice-AllowFortinet*
   c. Set *Profile Group* to *Specify* and select *Cloud IT*.

Connecting FortiClient to FortiSASE and provisioning the FortiSASE tunnel

These steps can be followed to onboard end users to FortiSASE. For details, see Getting Started for End Users.

1. Administrator sends an invitation email via *Onboard Users* button from *SSO* page or *Status* dashboard. Email includes download links for Windows/macOS and a unique invitation code.
2. User installs FortiClient and registers to FortiSASE as follows:
   a. Go to *Zero Trust Telemetry > Register with Zero Trust Fabric* and paste the invitation code
   b. Click *Connect*
3. Under *Remote Access*, the tunnel appears as *Secure Internet Access*. User clicks *SAML Login*, authenticates with Entra ID credentials, and if successfully authenticated then the tunnel is established.

Testing Application Control (YouTube Blocking) on user endpoint

Once Application Control is configured to block YouTube either via the default profile or a custom profile group like *Cloud IT* then the end user can verify enforcement from a managed FortiClient endpoint.

Scenario	Configuration used
User in *Remote-Home-Office* group with *Cloud IT* profile applied to their policy	Per-policy Application Control (profile group method)
Application Control defined and enabled on the *Default Profile*	Global Application Control

Test steps:

1. Connect the endpoint to the FortiSASE tunnel via *SAML Login* in FortiClient.
2. Open a browser and navigate to youtube.com.
3. FortiSASE matches the session against the active policy, detects YouTube traffic via Application Control signature matching (IPS protocol decoders), and blocks the connection. This is evident by the browser session timing out.
4. Verify the block in FortiSASE at *Monitoring > Monitors > FortiView Inline-CASB* which lists the cloud traffic detected by SSL deep inspection and Application Control is listed here.

> YouTube is a cloud application and requires SSL deep inspection to be detected by Application Control. Without deep inspection enabled, YouTube traffic will not match cloud application signatures.

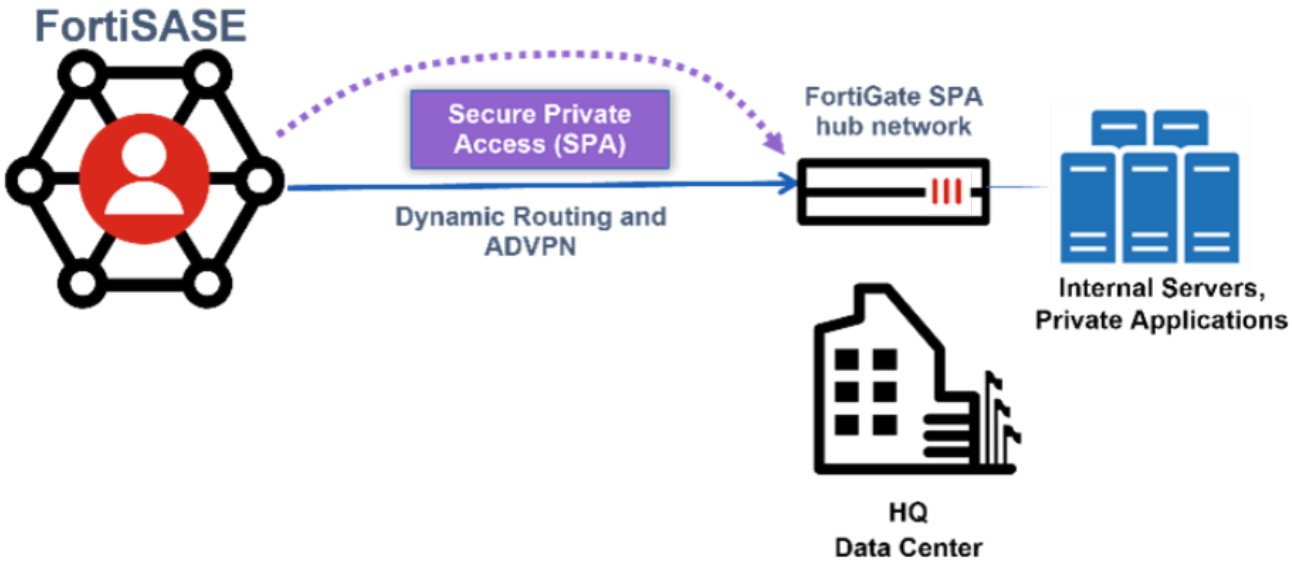
Verifying Connectivity in FortiSASE

The administrator can confirm the end user endpoint connectivity from the FortiSASE portal via the following verification steps:

Verification step	Location in FortiSASE
User online status	Monitoring > Dashboards > Status > User connection monitor
Endpoint online status	Monitoring > Dashboards > Status > Endpoints
Traffic logs	Operations > Logs > Traffic > Internet Access Traffic
Cloud app access (CASB)	Monitoring > Monitors > FortiView Inline-CASB
FortiView sources	FortiView Sources dashboard

SPA using BGP per overlay deployment example

Organizations with resources behind a FortiGate secure private access (SPA) hub can give FortiSASE endpoints access to private TCP- and UDP-based applications. The FortiSASE security PoPs act as spokes in a hub-and-spoke ADVPN topology, using IPsec overlays and iBGP to route traffic.



Supported traffic directions for SPA:

From	To
Remote agents / edge devices	FortiGate hubs (or connected spokes)
FortiGate hubs (or connected spokes)	Remote agents

This example covers the first traffic pairing from remote users to FortiGate hubs, which is the most typical use case.

By default, each FortiSASE PoP allows up to 300 Mbps of aggregate SPA throughput to account for baseline customer SPA hub capacity. If additional traffic is expected in a given region and the customer SPA hub has available bandwidth, you can open a FortiCare Support ticket to increase this SPA throughput.

This example covers the BGP per overlay routing design only (not BGP on loopback) across three hub implementation use cases:

1. SPA with a FortiGate SD-WAN deployment for new or existing SD-WAN hubs managed by FortiManager.
2. FortiGate NGFW to FortiSASE SPA hub conversion for standalone NGFW sites not running SD-WAN.
3. FortiGate NGFW to SPA hub conversion using Fabric Overlay Orchestrator (FOO) for FortiOS 7.2.4+ deployments using the self-orchestrated Security Fabric wizard.

For deployment details for each of these hub implementation use cases, see SPA Deployment Guide using BGP per overlay.

This example demonstrates the FortiGate hub configuration settings required to support SPA in FortiSASE and these settings typically apply to all hub implementation use cases.

FortiGate hub configuration

> Example values for FortiGate network configuration settings are for illustrative purposes only. Do not consider them as recommended settings. You must customize values to match those in your network environment

IPsec settings:

- IKEv2, dialup server mode, mode-cfg enabled
- `auto-discovery-sender enable` (ADVPN)
- `network-overlay enable` with a unique `network-id` per hub
- Pre-shared key per overlay
- Supported Phase 1 proposals: `aes128/256-sha1/sha256`, DH groups 14 and 5
- Supported Phase 2 proposals: `aes128/256-sha1/sha256` plus `aes128/256gcm`, `chacha20poly1305`
- Mode-cfg IP range: minimum /24 (e.g., `10.251.1.1–10.251.1.252/24`); size to customer scale

Sample IPsec CLI configuration

```
config vpn ipsec phase1-interface
   edit VPN1
       set type dynamic
       set interface port1
       set ike-version 2
       set peertype any
       set mode-cfg enable
       set proposal aes256-sha256
       set add-route disable
       set dpd on-idle
       set auto-discovery-sender enable
       set network-overlay enable
       set network-id 1
       set ipv4-start-ip 10.251.1.35
       set ipv4-end-ip 10.251.1.251
       set ipv4-netmask 255.255.255.0
       set psksecret <pre-shared key>
       set dpd-retryinterval 60
   next
end
```

Tunnel Interface

Assign a static IP to the tunnel interface so FortiSASE PoPs can establish BGP peering:

```
config system interface
   edit "VPN1"
       set ip 10.251.1.253 255.255.255.255
       set allowaccess ping
       set type tunnel
       set remote-ip 10.251.1.254 255.255.255.0
       set interface "port1"
   next
end
```

Loopback Interfaces

Two loopbacks are required:

- **Lo-BGP-RID** — BGP router ID for iBGP peering with FortiSASE PoPs (e.g. 10.1.0.254/32)

  ```
  config system interface
      edit "Lo-BGP-RID"
          set vdom "root"
          set ip 10.1.0.254 255.255.255.255
          set allowaccess ping
          set type loopback
      next
  end
  ```

  For the BGP per overlay routing design, this loopback configuration is essentially used for its IP address as BGP router ID only. The iBGP peering is not formed on the loopback as in the *BGP on loopback* routing design.
- **Lo-HC** — Health check target IP for FortiSASE SD-WAN performance SLA (e.g., 10.11.11.11/32)

  ```
  config system interface
      edit "Lo-HC"
          set vdom "root"
          set ip 10.11.11.11 255.255.255.255
          set allowaccess ping
          set type loopback
      next
  end
  ```

BGP Configuration

iBGP peering using neighbor groups and neighbor ranges (matching the mode-cfg IP pool):

```
config router bgp
    set as 65001
    set router-id 10.1.0.254
    set keepalive-timer 5
    set holdtime-timer 15
    set ibgp-multipath enable
    set additional-path enable
```

```
    set cluster-id 10.1.0.254
    set graceful-restart enable
    set additional-path-select 4
    config neighbor-group
        edit "VPN1"
            set capability-graceful-restart enable
            set soft-reconfiguration enable
            set interface "VPN1"
            set next-hop-self enable
            set remote-as 65001
            set additional-path both
            set adv-additional-path 4
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.251.1.0 255.255.255.0
            set neighbor-group "VPN1"
        next
    end
    config network
        edit 1
            set prefix 192.168.111.0 255.255.255.0
        next
    end
end
```

Firewall Policies

Two policies minimum are required to support the IPsec and BGP configuration:

- **BGP**: Allows ICMP PING from the PoP tunnel IP range to the protected LAN.
- **Spoke-to-Hub**: Allows HTTP/HTTPS/SMB/SSH/RDP from the PoP tunnel IP range to protected resources. In example below, no restrictions from specific PoP tunnel IP range has been applied.

```
config firewall policy
    edit 1
        set name "Spoke-to-Hub"
        set srcintf "VPN1"
        set dstintf "port4"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL”
        set logtraffic all
    next
    edit 3
        set name "BGP"
```

```
        set srcintf "VPN1"
        set dstintf "Lo-BGP-RID" "Lo-HC"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

FortiSASE Configuration

Configuration Workflow

1. *Network* > *BGP*: Configure common SPA BGP settings required before creating service connections.
2. *Operations* > *Connectivity* > *Secure private access*: Create one service connection (hub) per FortiGate hub.

Configuring BGP

Go to *Network* > *BGP*.

Key fields:

Field	Description	Example
BGP Routing Design	Must be BGP per overlay for this guide	BGP per overlay
BGP Router ID Subnet	Unused /28+ subnet for PoP loopback BGP router IDs	10.251.1.0/27
SPA hubs belong to	FortiSASE autonomous system (iBGP) or Different autonomous systems (mixed iBGP/eBGP)	FortiSASE autonomous system
FortiSASE ASN	BGP AS number of the hubs	65001
Hub Selection Method	Hub health and priority (default) or BGP MED	Hub health and priority
Health Check IP	Loopback IP on the hub used for SD-WAN SLA health checks	10.11.11.11
BGP Recursive Routing	Enables interhub redundancy when a PoP loses connectivity to its primary hub	Enabled

Configuring Service Connections

Go to *Operations* > *Connectivity* > *Secure private access*.

Key fields per hub:

Field	Description	Example
Name	Hub alias (max 25 chars, alphanumeric + dashes)	Datacenter 1
Remote Gateway	Hub public IP (WAN)	1.2.3.4
Authentication Method	Pre-shared Key or Certificate	Pre-shared key
BGP Peer IP	Hub BGP peer IP (tunnel interface IP)	10.20.1.253
Network overlay ID	Unique per hub; mismatched IDs break ADVPN shortcut failover	2

Up to 12 service connections (hubs) are supported per FortiSASE instance.

Additional Operations

- *Health & Tunnel Status*: View per-hub IPsec, BGP, and health check status from the *Health* button.
- *Editing SLA Thresholds*: Customize latency (default 120 ms), jitter (55 ms), and packet loss (1%) per PoP per hub.
- *Service Connection Priorities*: Assign P1 (highest) or P2 priority per hub per security PoP. Lower cost = higher priority in the SD-WAN rule.
- *Monitoring*: Private access widgets available at *Monitoring > Dashboards > Private access*.

Private Access Security Profile

Configure at *Security > Traffic > Security profiles*. The security settings for private access are identical to internet access profile options.

Verifying SPA traffic flow

Verifying IPsec Tunnels from FortiGate hub:

```
diagnose vpn ike gateway list         # Verify Phase 1 IKE SAs (created/established: 1/1)
diagnose vpn tunnel list              # Verify Phase 2 IPsec SAs
get vpn ipsec tunnel summary          # Confirm selectors up and traffic flowing (non-zero rx/tx)
```

Verifying BGP Routing from FortiGate hub:

```
get router info bgp summary
get router info bgp neighbors <x.x.x.x> advertised-routes
```

Or in the GUI: *Dashboard > Networks > Static & Dynamic Routing widget > BGP Neighbors*.

Verifying Private Access connectivity

By using ping, you can verify access to the FortiGate hub network from FortiSASE remote users, namely, FortiClient users connected to FortiSASE in FortiClient agent-based mode and users behind FortiSASE edge devices.

ping <hub-internal-IP> from a FortiClient-connected Windows endpoint.

Verifying Traffic in FortiSASE Portal

- **Logs**: *Operations > Logs > Traffic > All Internet & Private Access Traffic / Private Access Traffic (To Hubs)*
- **FortiView**: *Monitoring > Monitors > FortiView Sources / Destinations / Policies,* filter by private access destination IP
- **Asset Map**: *Operations > Connectivity > Asset Map*, filter on *Private Access Hub* to see hub status and location

Restricting Access via FortiGate Hub Firewall Policy

As a best practice, access to the FortiGate hub should be restricted to:

- Security PoPs
- Remote users (agent tunnels and edge devices)

To restrict SPA access to security PoPs, update the hub firewall policy to include the IKEv2 mode-cfg address range as a source address object.

1. Confirm the mode-cfg range on the hub:

```
show vpn ipsec phase1-interface | grep ipv4-
```

2. Create an address object (e.g., `SPA-BGP-Spoke-Range`) for the IP range.
3. Add the address object as a source in the existing IPsec-to-LAN firewall policy.

To restrict SPA access to remote users (agent tunnels or edge devices), update the hub firewall policy to include the IKEv2 mode-cfg address range as a source address object.

1. Confirm the IPAM subnet from *Network > IP management > IPAM > IP pools for tunnel and edge devices*.
2. Create an address object (e.g., IPAM-Subnet) for the IPAM subnet.
3. Add the address object as a source in the existing IPsec-to-LAN firewall policy.

FortiGuard Attack Surface

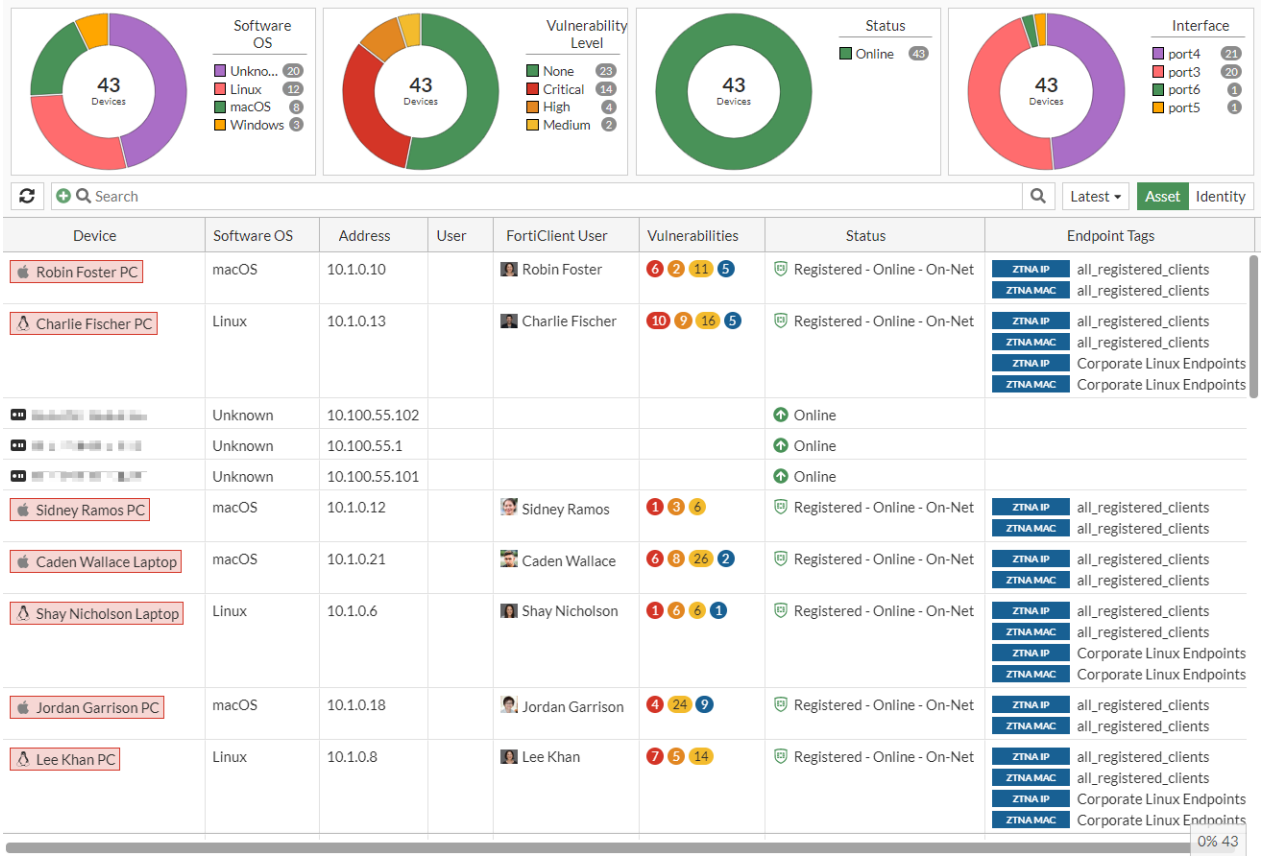
Attack Surface Security Rating (Security Rating) assesses security posture and highlights configuration weaknesses. When combined with IoT detection and vulnerability lookups, it can help identify unmanaged or high-risk devices and guide remediation.

IoT detection service

This service is part of the Attack Surface Security Rating service that allows FortiGate to accurately detect and identify connected IoT devices and to identify vulnerabilities that apply to these devices.

How the service works

1. Enable Device Detection on an interface.
   a. Go to *Network* > *Interfaces* and edit a LAN interface.
   b. Enable *Device detection*.
   c. Click *OK*.
2. FortiGate uses the interface to detect device traffic flow.
3. Upon detecting traffic from an unknown device, FortiGate sends the device data to the FortiGuard collection server.
4. The collection server returns data about the new device to the FortiGuard query server.
5. If the device signature does not appear in the local Device Database (CIDB) or some fields are not complete, FortiGate queries FortiGuard for more information about the device.



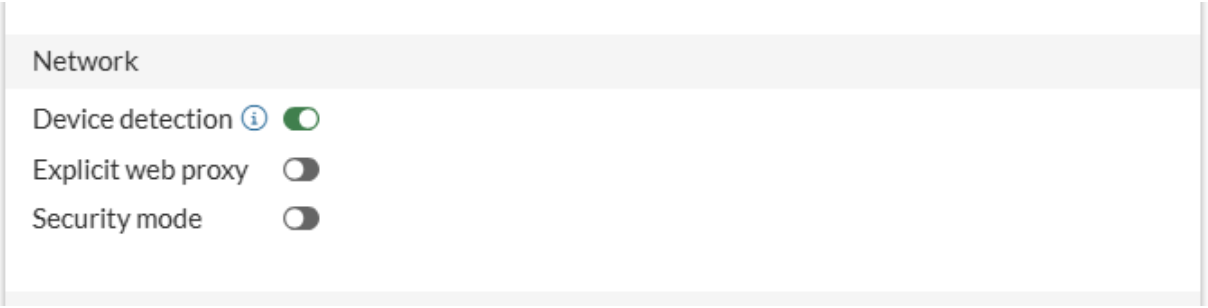
Virtual patching

Virtual patching is a method for mitigating vulnerability exploits against IoT devices by applying patches virtually on the FortiGate. This is done in several steps:

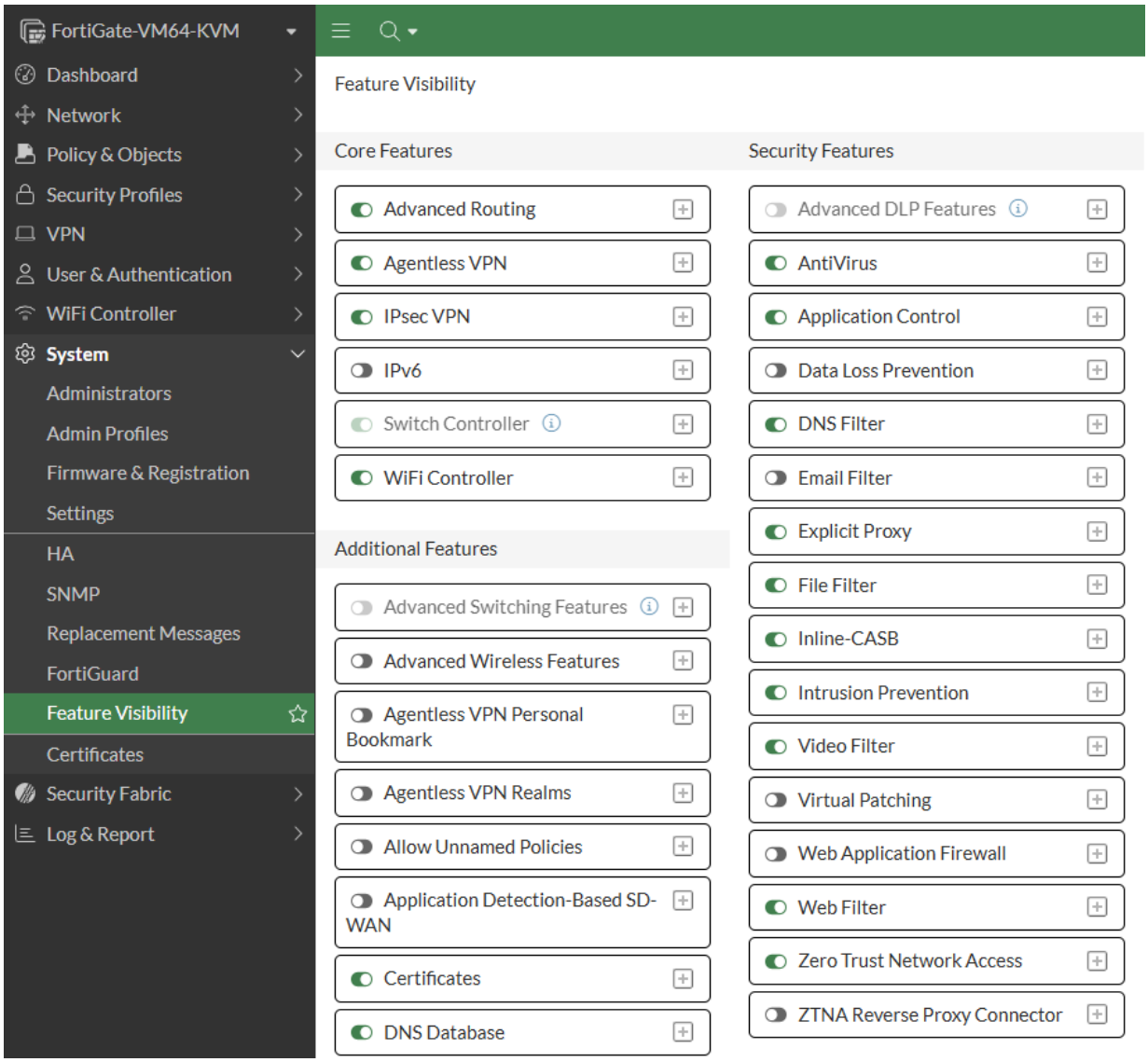
1. A FortiGate uses the Detection Signatures and Service to collect device information from IoT devices that are connected to an interface.
2. The device information is used to perform a vulnerability lookup by querying FortiGuard for device-specific vulnerabilities and mitigation rules.
3. FortiGuard returns virtual patching signatures and IPS signatures.
4. The FortiGate caches the applicable signatures and mitigation rules that apply to each device. The signatures and rules are mapped to the MAC address of the device.
5. When a virtual patching profile is applied to a firewall policy, traffic that enters the firewall policy is subject to signature matching on a per-device basis.
   a. The IPS engine uses the MAC address of the device to match any mitigation rules that should apply.
   b. If the MAC address is in the exempted list, then patching is exempted or skipped.
   c. If the signature rule is in the exempted list, then patching is also exempted or skipped for that signature.
   d. Otherwise, all applicable rules for the device will be applied.

Example: Applying virtual patching to a vulnerable legacy IoT device

1. Enable device detection on port1(LAN):
   a. Go to *Network* > *Interfaces* and edit port2.
   b. In the *Network* section, enable *Device detection*.
   c. Click *OK*.



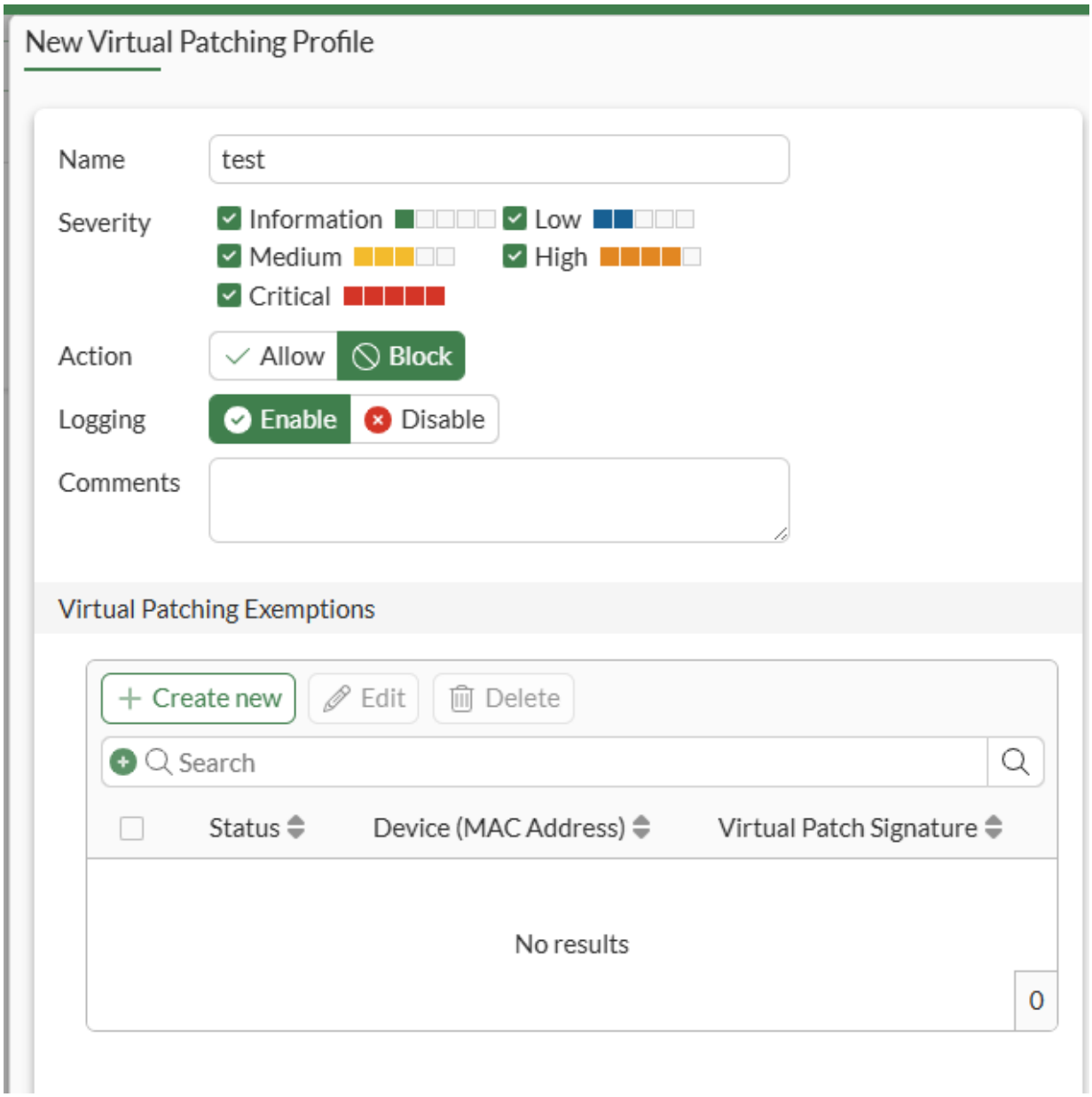
2. Configure the virtual patching profile:
   a. Go to *Security Profiles* > *Virtual Patching* and click *Create New*.
   If Virtual Patching is not present, you must enable the feature visibility under **System > Feature Visibility**.



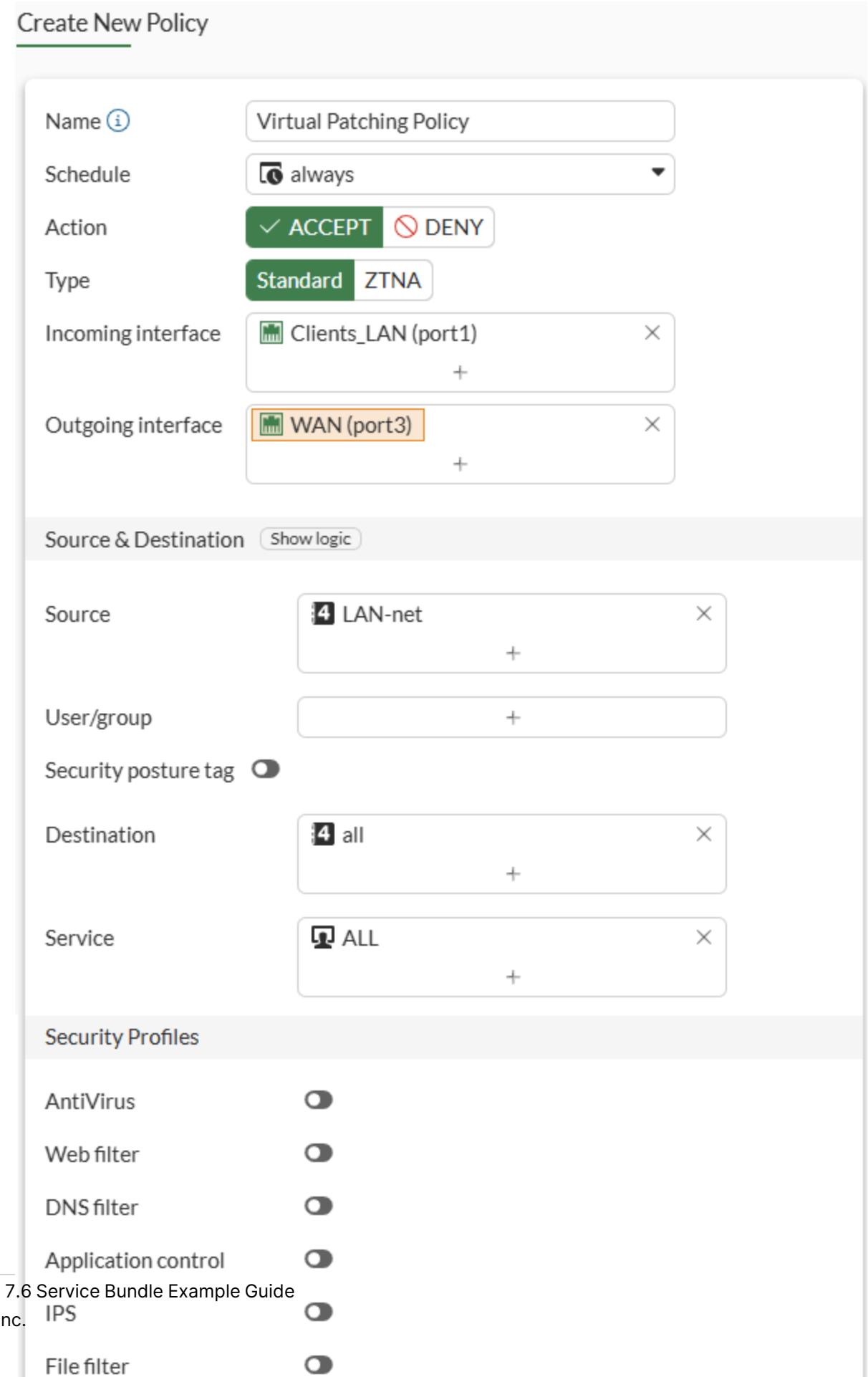
b. Configure the following settings:

Name	test
Severity	Select *Info*, *Low*, *Medium*, *High*, and *Critical*
Action	Block
Logging	Enable

c. Click *OK*.



3. Apply the virtual patching profile to a firewall policy for traffic from port2 to port1:
   a. Go to *Policy & Objects* > *Firewall Policy* and click *Create New*.
   b. In the *Security Profiles* section, enable *Virtual Patching* and select the virtual patch profile (*test*).
   c. Set *SSL Inspection* to a profile that uses deep inspection profile in order to scan SSL encrypted traffic.
   d. Configure the other settings as needed.
   e. Click *OK*.


Create New Policy
Name
Virtual Patching Policy
Schedule
always
Action
ACCEPT
DENY
Type
Standard
ZTNA
Incoming interface
Clients_LAN (port1)
Outgoing interface
WAN (port3)
Source & Destination
Show logic
Source
LAN-net
User/group
Security posture tag
Destination
all
Service
ALL
Security Profiles
AntiVirus
Web filter
DNS filter
Application control
IPS
File filter

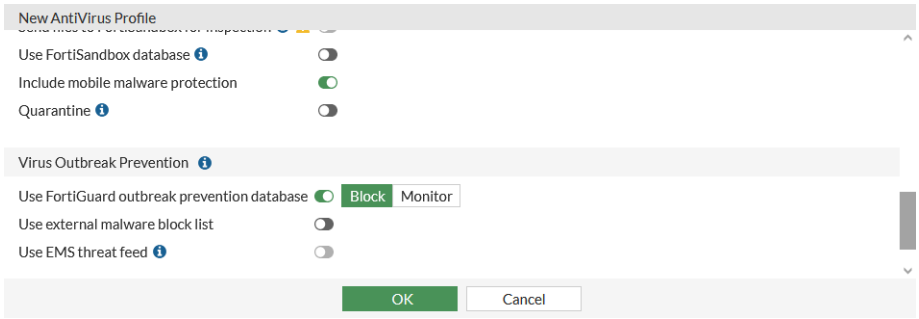
Virus Outbreak Prevention

FortiGuard VOS allows the FortiGate antivirus database to be supplemented with third-party malware hash signatures curated by FortiGuard. This allows VOS to manage zero-day threats effectively. The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. Any signature that is added to FortiGuard becomes immediately active, eliminating the need to wait for AVDB (antivirus database) update. The AVDB queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious. Enabling the AV engine scan is not required to use this feature.

FortiGuard VOS can be used in both proxy-based and flow-based policy inspections across all supported protocols.

Example: Enable FortiGuard outbreak prevention

1. Go to *Security Profiles* > *AntiVirus*.
2. Edit an antivirus profile, or create a new one.
3. Under *Virus Outbreak Prevention*, enable *Use FortiGuard outbreak prevention database* and select *Block* or *Monitor*.



4. Click *OK*.

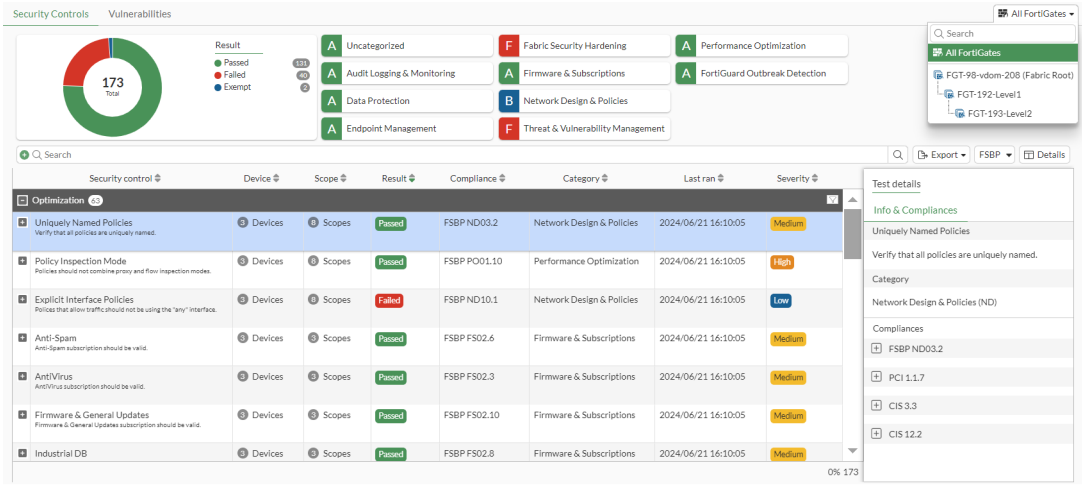
Security Rating

The security rating uses real-time monitoring to analyze your Security Fabric deployment, identify potential vulnerabilities, highlight best practices that can be used to improve the security and performance of your network, and calculate Security Fabric scores.

Security Controls

The Security Controls page provides a quick roll-up of how many checks passed, failed, or were exempt, and breaks results down by category (for example, Audit Logging & Monitoring, Data Protection, and others) with an assigned letter grade for each. Grades are calculated from the percentage of tests passed within that category,

using a standard scale (A ≥ 90%, B = 80–<90%, C = 70–<80%, D = 60–<70%, E = 50–<60%, F < 50%); for example, passing 8 of 10 tests yields an 80% score and a B.

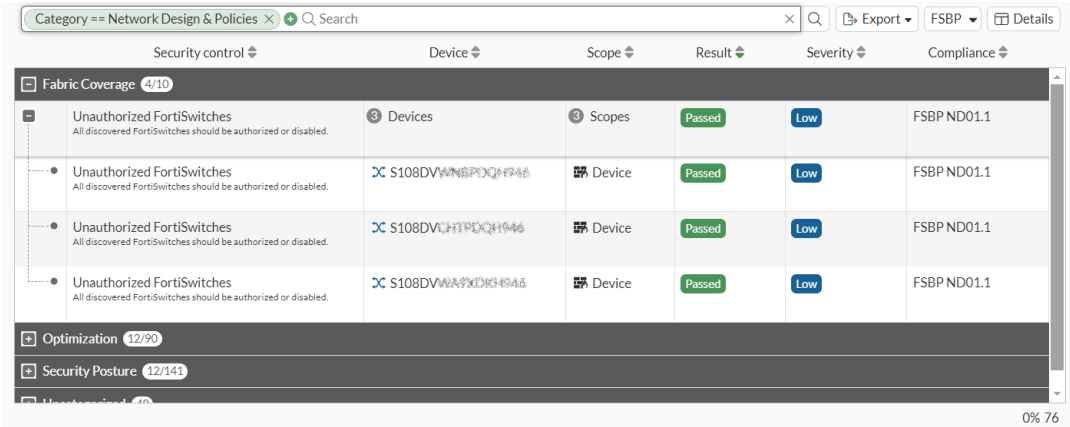


Example: View security controls

1. On the root FortiGate, go to *Security Fabric* > *Security Rating*. The *Security Controls* pane opens.
2. For the graded test categories, hover the cursor over a test category to view the calculation breakdown.
3. For the summary chart, click the *Passed*, *Failed*, or *Exempt* words or associated colors in the chart to filter the report results.

   For example, click *Failed* to display only failed tests in the report.

   Click *Result* to remove the filter, or click the *X* beside the filter in the *Search* bar
4. Expand each security rating category in the report to view its details.

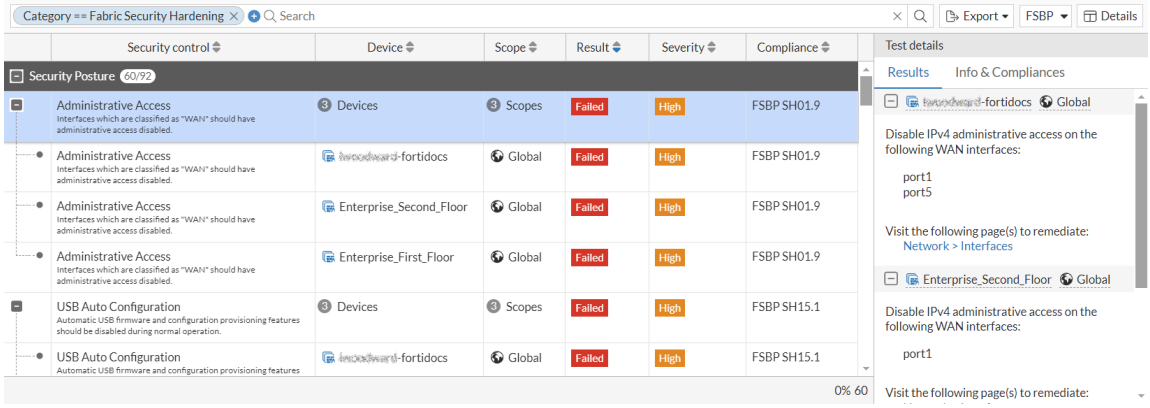


5. In the report, click each row to view its *Test details* pane, which includes two tabs: *Results* and *Info & Compliance*.

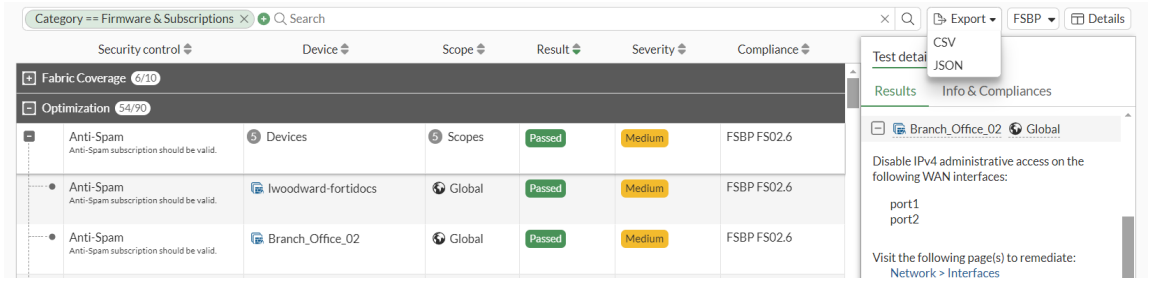
   Click *Details* to hide and display the *Test details* pane for a selected row in the report.

   If a test category failed, the *Results* section includes a link to the GUI page where you can resolve the problem.

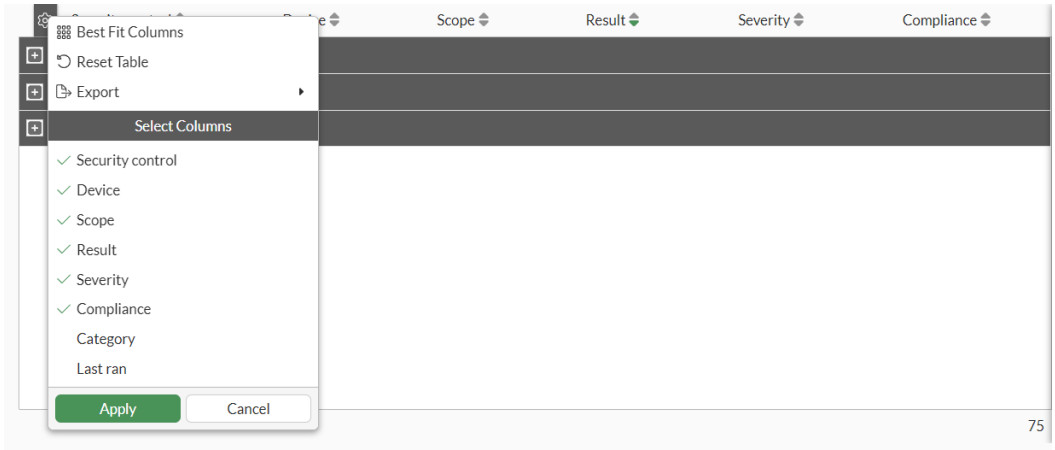
   The *Info & Compliance* tab includes the security controls used for the test and links to specific FSBP, PCI, or CIS compliance policies.



6. Select *FSBP*, *PCI*, or *CIS* to filter the report for the selected compliance policy.
7. Click *Export* to export the report to a CSV or JSON file.

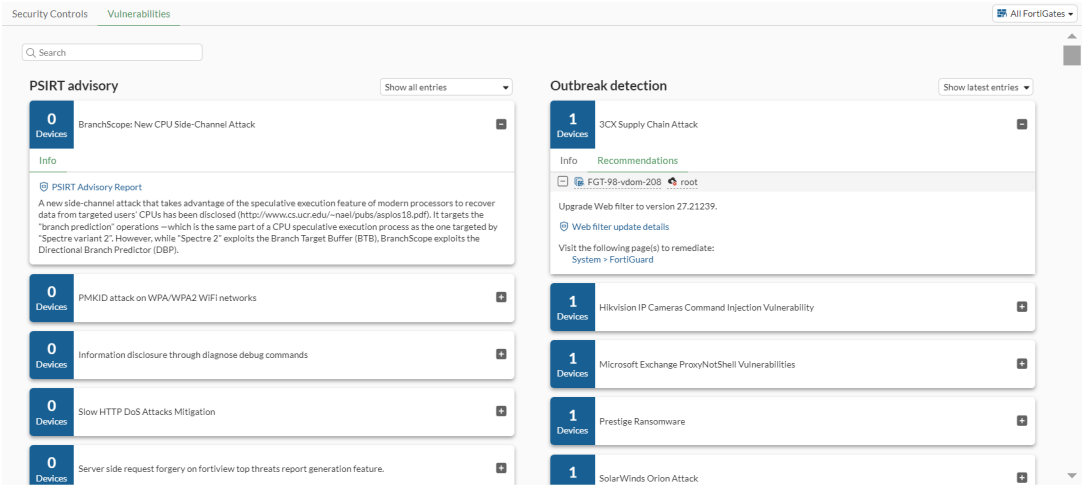


8. Click the gear icon to customize the report table by adding more columns.



Vulnerabilities

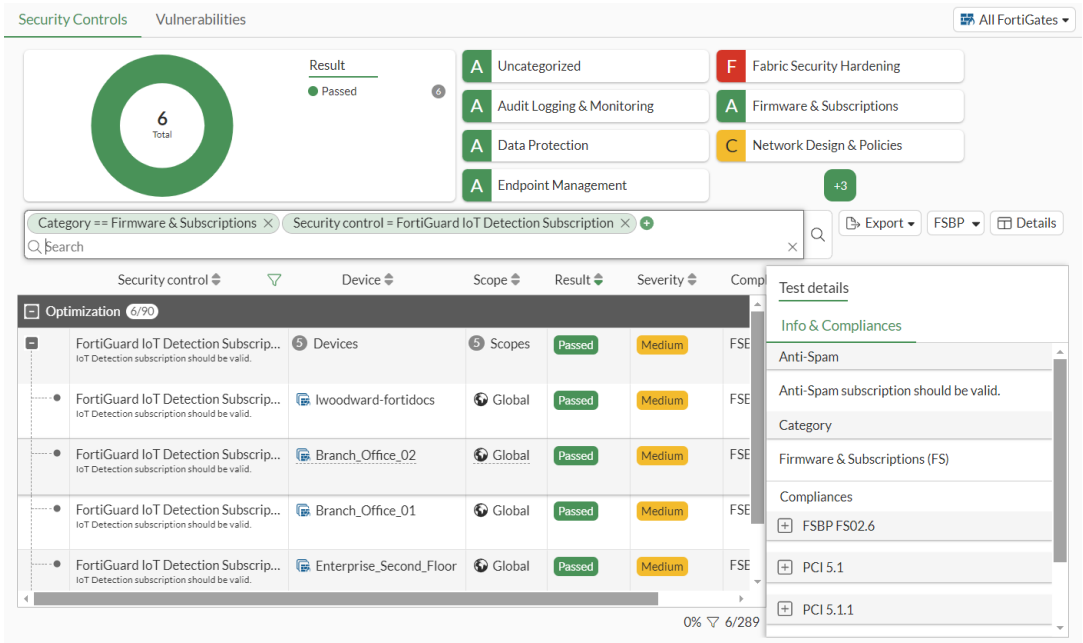
On the *Security Fabric > Security Rating* page, the *Vulnerabilities* tab displays *PSIRT advisory* and *Outbreak detection* entries that are included in the downloaded Security Rating package:



FortiGuard IoT vulnerability-related checks

There are two rating checks in the *Security Posture* report related to IoT vulnerabilities:

- The *FortiGuard IoT Detection Subscription* rating check will pass if the *System > FortiGuard* page shows that the *IoT Detection Definitions* (under the *Attack Surface Security Rating* entitlement) is licensed. In this example, the result is marked as *Passed* because the license is valid.

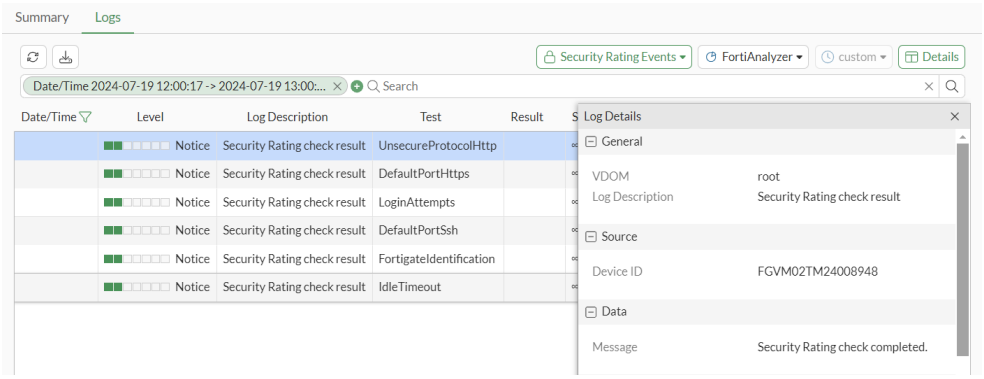


- The *FortiGuard IoT Vulnerability* rating check will fail if any IoT vulnerabilities are found.

Hover over the device name to display the tooltip, which includes an option to *View IoT Vulnerabilities*.

Logging the security rating

The results of past security checks are available on the *Log & Report > System Events* page. Click the *Security Rating Events* card to see the detailed log.



An event filter subtype can be created for the Security Fabric rating so event logs are created on the root FortiGate that summarize the results and show detailed information for the individual tests.

www.fortinet.com