NGFW Deployment

FortiGate

DEFINE / DESIGN / DEPLOY / DEMO

Table of Contents

Change Log 4

Deployment overview 5

- Intended audience 6
- About this guide 6
- Deployment plan 7
- Design concept and consideration 7
  - Port selection for administrative access 7
  - IP addressing scheme 8
  - Physical topology 8
  - VLAN segmentation 8
  - Interface selection on FortiGate 8
  - VLAN-aware managed level 2 switch (FortiSwitch) 8
  - SSL/SSH inspection uses certificate inspection 9
  - Administrative access HTTPS certificate 9
  - WiFi networks 9
- Product prerequisites 9

Deployment procedures 10

- Initial setup 11
  - First connection 12
  - WAN connection 14
  - Management access 14
  - Managed switch connection 18
- System settings 18
  - Configuring system settings 18
  - Configuring log settings 19
  - Configuring a remote RADIUS authentication server 20
- Administrator settings 20
  - Configuring administrator settings 20
  - Configuring RADIUS administrator accounts 21

FortiGate Cloud Sandbox 23

FortiGate objects 24

User group objects 24

Address objects 26

Service objects 28

LANs and LAN segmentation 32

Trunk port 33

VLANs 34

Wireless networks (WLAN) 36

SSIDs 36

AP profile 37

Managed access points (APs) 38

Security 39

Security profiles 39

Firewall policy 42

Security rating check 47

Security Posture 47

Fabric Coverage 48

Optimization 48

More information 50

Products used 50

Documentation references 50

Change Log

Date	Change Description
2022-12-16	Initial release.

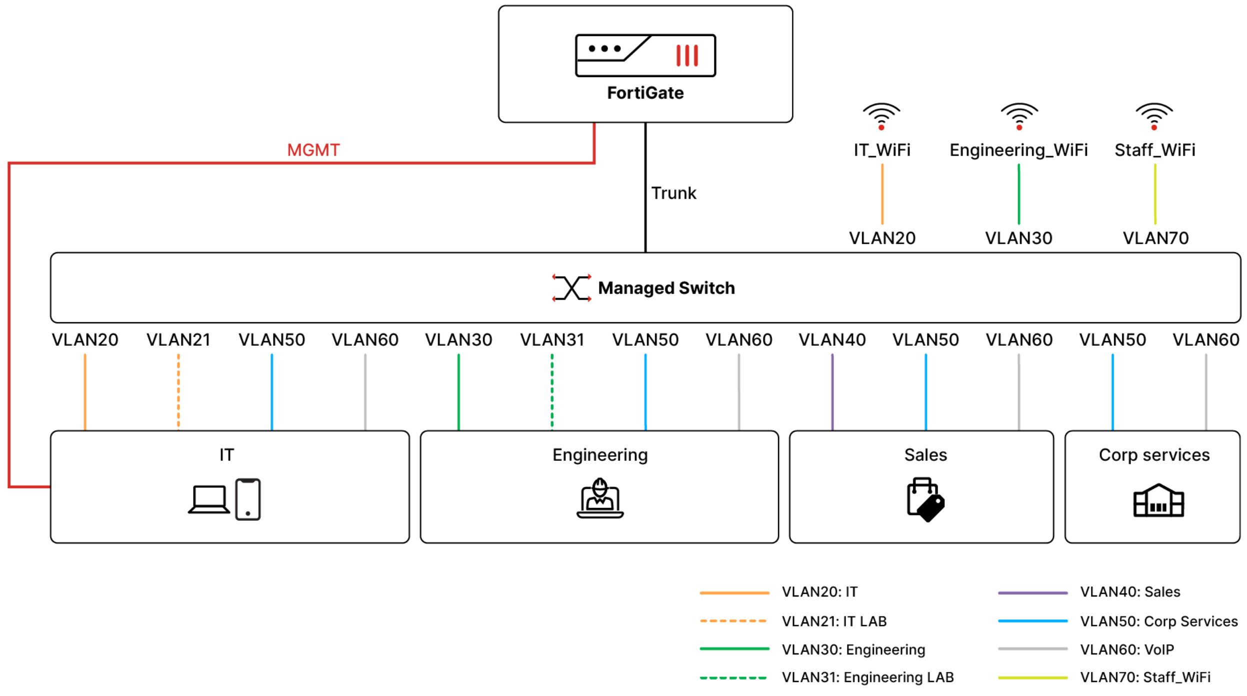
Deployment overview

This document covers Fortinet best practices to deploy a Next Generation Firewall (NGFW) for a small or medium business (SMB) environment. In this case, the customer environment is defined as:

- A small to medium sized business ranging from 20 to 100 employees with several departments
- Single location with a single WAN connection

Following are the goals of the deployment:

- Deploy one FortiGate at the network edge.
- Segment the network for different departments. Only staff, engineering, and IT departments are specified for brevity.
- Provide Next Generation Firewall security by leveraging the Unified Threat Management (UTM) features of the FortiGate.
- Implement security policies for the company by applying appropriate security profiles to firewall policies.
- Configure wireless networks to provide access to department-specific resources.
  Secure wireless networks by using WPA2-Enterprise authentication linked to users on a remote server.
- Send FortiGate logs offsite to FortiGate Cloud.
- Leverage FortiSandbox to inspect suspicious files that do not match any existing virus signatures.
- Harden the FortiGate to restrict management access from external sources.



Intended audience

This guide is primarily created for a technical audience who may be new to configuring FortiGates. The guide assumes a greenfield scenario where the FortiGate may be replacing an existing firewall, but is being configured for the first time. Networking and security fundamentals are assumed. While best practices are applied, customization by the administrator will be required to ensure the final configuration meets the business' needs.

About this guide

The term NGFW is used to describe the combination of traditional firewall features, such as stateful inspection, VPN and packet filtering, with UTM features, such as anti-malware/virus, intrusion prevention, threat intelligence sources, and application awareness and control to name a few.

The deployment configuration detailed in this guide describes one way of configuring a FortiGate to provide security to small and medium businesses. The example is designed for a hypothetical company with typical security needs. The names of the VLANs and IP addresses are generic, and can be adapted for businesses with a different number of employees and departments.

The recommended configuration adheres to Fortinet security best practices and provides a base upon which administrators can add customizations and extensions to better match their needs when implementing additional technologies, such as SD-WAN, FortiSASE, and ZTNA.

Deployment plan

The guide includes the following major sections:

1. Initial setup on page 11
   Connect to the FortiGate, configure internet access, and install the latest firmware.
2. System settings on page 18
   Harden the FortiGate and configure settings, such as logging, certificates, and hostname.
3. Administrator settings on page 20
   Configure the administrator account and access to the FortiGate.
4. FortiGate Cloud Sandbox on page 23
   Enable FortiGate Cloud Sandbox.
5. FortiGate objects on page 24
   Define policy objects, such as addresses and services.
6. LANs and LAN segmentation on page 32
   Define wired networks for the managed switch, such as FortiSwitch.
7. Wireless networks (WLAN) on page 36
   Define wireless networks for the access point, such as FortiAP.
8. Security on page 39
   Configure security profiles and firewall policies.
9. Security rating check on page 47
   Verify of settings with a security rating check.

Design concept and consideration

The NGFW deployment described in this guide was designed to be as extensible as possible. The deployment includes as few products as possible to keep the complexity relatively low. As a result, an administrator can enhance the configuration by adding to it rather than redesigning the configuration to fit their needs.

Additionally, several methods can be used to accomplish a given security requirement. Following is information about choices that were made with some alternatives for your consideration:

- Port selection for administrative access on page 7
- IP addressing scheme on page 8
- Physical topology on page 8
- VLAN segmentation on page 8
- Interface selection on FortiGate on page 8
- VLAN-aware managed level 2 switch (FortiSwitch) on page 8
- SSL/SSH inspection uses certificate inspection on page 9
- Administrative access HTTPS certificate on page 9
- WiFi networks on page 9

Port selection for administrative access

It is best practice to adjust the HTTPS and SSH ports from their defaults. The ports selected should not be ports used by well known applications. For example, TCP/161 is well known for SNMP and should be avoided.

IP addressing scheme

The following criteria was used to choose the IP addressing scheme for the various departments:

- Private addresses (RFC-1918)
- Appropriately sized for the company with consideration for growth
- Ease of recognition (for example, VLAN 20 uses the subnet 192.168.20.0/24)

IP address ranges can be changed based on needs or preference.

Physical topology

For an SMB with 20 to 100 users, two (2) devices per user are assumed, which adds from 40 to 200 devices to the network.

Given the number of devices and subsequent segments, VLANs rather than physical interfaces are used for segmentation. Therefore, besides WAN and MGMT interfaces, which can be accessed directly, all other internal networks are segmented using VLANs.

Also, although this guide demonstrates the use of one (1) managed switch, given the number of possible devices requiring wired connection, it is highly likely that multiple managed switches may be required.

Similarly, where the physical location may be large, multiple FortiAPs may be required to provide sufficient signal and range.

VLAN segmentation

The networks are segmented by department and function. Users in the same department are segmented into the same VLAN, and devices, such as VoIP phones, are segmented by function.

Interface selection on FortiGate

When selecting interfaces on FortiGate for the roles of WAN, LAN, and management, use the port with the name that matches the purpose whenever possible. In this case, wan1 is used for WAN connectivity.

Where a port does not exist with a matching name, select the port which satisfies the needs of the link. For example, if there are 10GE SFP+ ports, and you anticipate a lot of traffic across a particular link, it makes sense to use this port. Ensure you adjust the alias for clarity.

You may also consider aggregating two or more interfaces to increase throughput and add resiliency between the connected devices.

VLAN-aware managed level 2 switch (FortiSwitch)

Although the only requirement for switching is a VLAN-aware managed level 2 (L2) switch, it is highly recommended to utilize a FortiSwitch and leverage the FortiLink interface.

FortiLink allows for single-pane-of-glass management of wired, wireless, and security functions, extending Fortinet UTM features into the network access layer.

Many SMB FortiGates have designated ports (for example, port A and port B) for connecting to a FortiSwitch using FortiLink. This eases the need to configure the trunk port used to connect third-party switches.

Many FortiSwitch devices have PoE capabilities to power FortiAPs or other IoT devices, such as VoIP phones.

SSL/SSH inspection uses certificate inspection

Certificate inspection was chosen because it is easy to deploy. Deep inspection is more thorough and offers better protection; however, it is harder to deploy and maintain. See the *FortiOS 7.0 Administration Guide* for more details on deploying deep inspection.

Consider your company’s security policies when deciding the need for deep inspection. Typically, deep inspection is needed when content within an SSL/TLS protected connection need to be inspected.

Administrative access HTTPS certificate

Automated certificate enrollment was selected to generate the certificate used for administrative HTTPS access due to the ease of setup and maintenance, as well as having a public CA that is trusted by browsers by default.

Alternatively, you could generate a certificate using the FortiGate self-signed CA, or upload a certificate signed by your own private CA or a certificate signed by a public CA.

WiFi networks

The goal of the WiFi networks is to give staff access to corporate resources and the internet. WiFi networks also give specific departments access to their LAB networks.

Following is a summary of the settings used:

- Bridge mode was selected, which allows the FortiAP to share the same subnets with the wired networks. Subsequently, several SSIDs are created that correspond to an SSID for each department.
- WPA2-Enterprise was selected with Windows AD integration through RADIUS.
- LDAP authentication was used.
- Dynamic VLAN assignment uses one SSID.
- Tunnel mode wireless networks were used instead of bridge mode

Product prerequisites

Though the following configuration may be applied to nearly all FortiGate models, the SMB models of 70 through 200 were considered when developing the design.

This guide also utilizes the following products and services:

- FortiGate Cloud
  The free subscription is utilized.
- FortiGate Cloud Sandbox
- Active Directory and LDAP
- RADIUS server (Microsoft Network Policy Server)
- Managed switch (or FortiSwitch)
- FortiAP

Deployment procedures

The deployment procedures are organized into the following sections:

Initial setup on page 11	Describes how to connect to FortiGate after you remove the device from the box, establish a WAN connection, manage access to the FortiGate, and connect a managed switch.
System settings on page 18	Describes how to configure system settings, log settings, and a remote RADIUS authentication server.
Administrator settings on page 20	Describes how to configure administrator settings and administrator accounts for RADIUS.
FortiGate Cloud Sandbox on page 23	Describes how to enable FortiGate Cloud Sandbox.
FortiGate objects on page 24	Describes how to create objects used by FortiGate, such as user groups, address groups, and services.

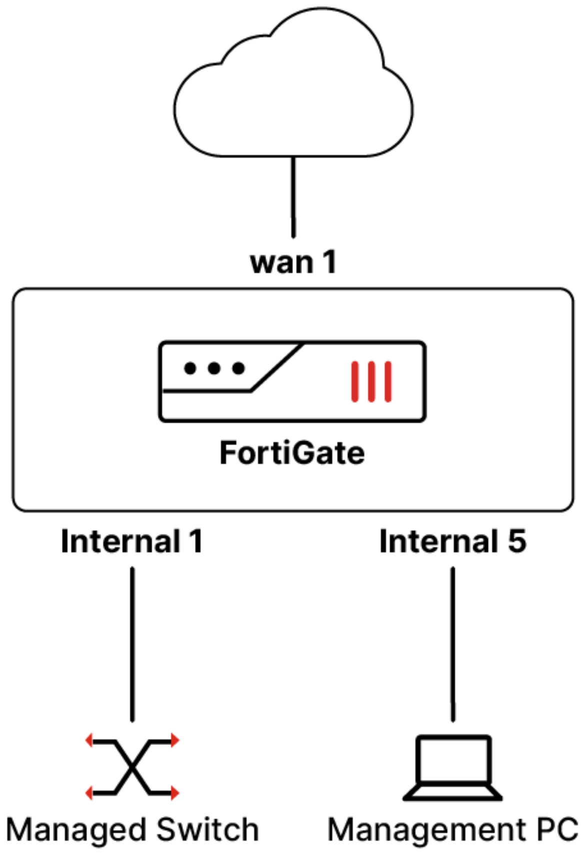
LANs and LAN segmentation on page 32	Describes how to configure LANs, including the trunk port and VLAN definitions.
Wireless networks (WLAN) on page 36	Describes how to configure the WLAN, including SSIDs, AP profiles, and managed APs.
Security on page 39	Describes how to configure security profiles and firewall policies.
Security rating check on page 47	Describes how to review the security rating check.

Initial setup

This section describes how to set up your FortiGate device after removing it from the box. It includes best practices for connecting to the FortiGate for the first time, configuring WAN connectivity, and configuring management access. It includes the following topics:

- First connection on page 12
- WAN connection on page 14
- Management access on page 14
- Managed switch connection on page 18

Once completed, the physical connections will use these interfaces:



First connection

After you remove the FortiGate from the box, you are ready to connect to the device by completing the following steps:

1. Use an Ethernet cable to connect the FortiGate to your PC that will be used to manage the FortiGate. See Connecting FortiGate to your PC on page 12.
2. On your PC, use a browser to connect to the FortiGate GUI and log in. See Connecting to the FortiGate GUI and logging in on page 13.
3. In the FortiGate GUI, complete the *FortiGate Setup* wizard. See Completing the FortiGate Setup wizard on page 13.

Connecting FortiGate to your PC

It is recommended to connect an Ethernet cable between port 2 on the FortiGate and your PC to prepare for removing port 5 and port 1 from the hardware switch later without losing connectivity.

To connect FortiGate to your PC:

1. Use an Ethernet cable to connect port 2 on the FortiGate to your PC.
2. Set your PC network adapter to DHCP.
   Alternatively, you can configure a static IP address on your PC in the range 192.168.1.0/24, excluding the .99 address.

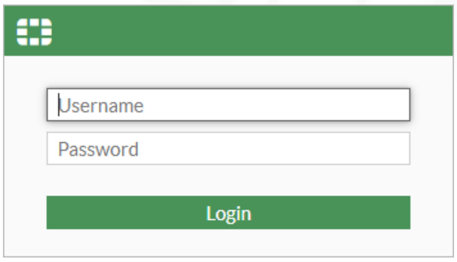
3. Connect to the FortiGate GUI and log in. See Connecting to the FortiGate GUI and logging in on page 13.

Connecting to the FortiGate GUI and logging in

After you connect an Ethernet cable from FortiGate to your PC, you can use a browser to access the FortiGate GUI and log in.

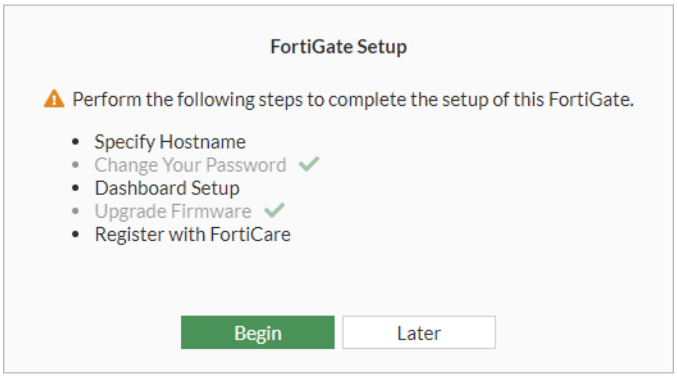
To connect to the FortiGate GUI and log in:

1. In a browser, go to https://192.168.1.99. The FortiGate login page is displayed.



2. Enter the username *admin* with no password, and click *Login*.
3. Configure a password for the admin account by following prompts to gain further access.

   After you log in with the new password, the *FortiGate Setup* wizard is displayed.



FortiGate Setup

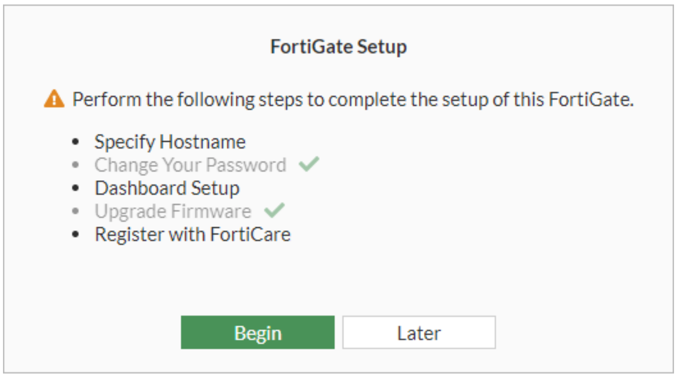
⚠ Perform the following steps to complete the setup of this FortiGate.

- Specify Hostname
- Change Your Password ✓
- Dashboard Setup
- Upgrade Firmware ✓
- Register with FortiCare

4. Complete the FortiGate Setup wizard. See Completing the FortiGate Setup wizard on page 13.

Completing the FortiGate Setup wizard

After you log in to the FortiGate GUI for the first time, the *FortiGate Setup* wizard is displayed. You can click *Later* to complete the wizard later. This topic describes how to click *Begin* and complete the wizard now.



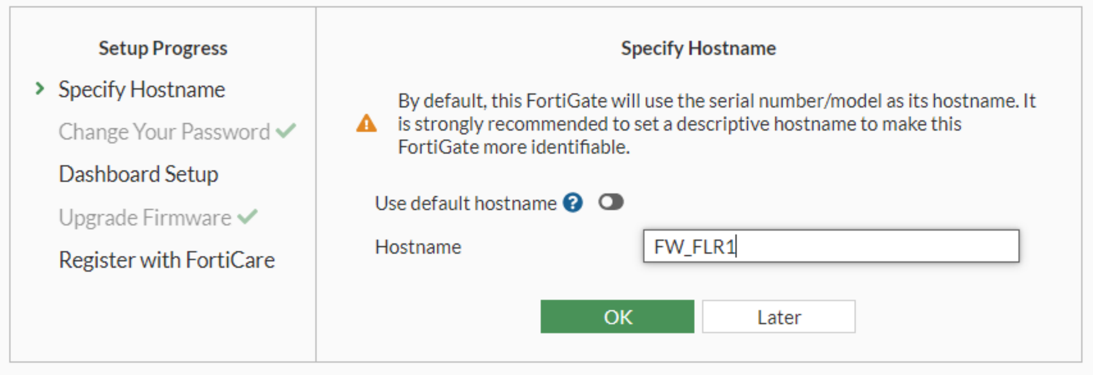
FortiGate Setup

⚠ Perform the following steps to complete the setup of this FortiGate.

- Specify Hostname
- Change Your Password ✓
- Dashboard Setup
- Upgrade Firmware ✓
- Register with FortiCare

To complete the FortiGate Setup wizard:

1. On the *FortiGate Setup* wizard, click *Begin*. The *Specify Hostname* page is displayed.



Setup Progress

› Specify Hostname

Change Your Password ✓

Dashboard Setup

Upgrade Firmware ✓

Register with FortiCare

Specify Hostname

⚠ By default, this FortiGate will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this FortiGate more identifiable.

Use default hostname ?

Hostname: FW_FLR1

2. Enter a hostname, and click *OK*.

   Use a hostname that reflects the location and/or purpose of the FortiGate, such as *FW_FLR1*.

   The *Dashboard setup* page is displayed.
3. Click *OK* to confirm the default dashboard setup.

   You can change the dashboard setup later.

   The *Upgrade Firmware* page is displayed.
4. Upgrade to the latest firmware or to the firmware of your choice, and click *OK*.

   Alternatively you can update the firmware after completing the wizard, if the FortiGate does not have internet connectivity at this time.

   The *Register with FortiCare* page is displayed.
5. If you can provide your FortiGate with internet access, use your FortiCloud credentials to complete registration.

   If the FortiGate does not have internet access, you can register FortiGate on the FortiCloud support portal later. For more information, see the *FortiOS 7.0 Administration Guide*.

WAN connection

Several steps in this document rely on the FortiGate having an established connection to the internet. For this reason, it is assumed that you connect the FortiGate's wan1 port to a modem that provides access to the internet.

FortiGate can be configured as a DHCP client to retrieve a publicly routable IP address and a default gateway route from the modem. Alternatively, you can manually configure the FortiGate to have a static IP address and default static route to your gateway IP address.

Management access

Management access to the FortiGate will be limited to a single physical interface. Although we will use port 5 on the FortiGate (labeled *internal5* on the internal hardware switch in the GUI) for our device model, you can use any interface.

FortiGate models with an internal hardware switch typically have all the interfaces bundled into the switch by default. To use a bundled interface as a separate interface, you must first remove it from the hardware switch.

On the FortiGate device, ports are labeled with numbers, such as 1, 2, 3, and so on. When you log in to the FortiGate GUI, the port numbers also have the following default names:

- Port 1 is named *internal1*.
- Port 2 is named *internal2*.
- ...
- Port 5 is named *internal5*.

Complete the following steps to configure management access:

1. Remove *interface1* and *interface5* from the internal hardware switch. See Removing interfaces from the hardware switch on page 15.
2. Configure *interface5* as the management interface. See Configuring the management interface on page 16.
   Later in the guide, *interface1* will be configured as the trunk port. See Trunk port on page 33.
3. Update your PC connection and settings to continue managing the FortiGate. See Updating your PC on page 17.
4. Edit other interfaces to remove access. See Removing access to interfaces on page 17.

Removing interfaces from the hardware switch

Remove the *interface1* and *interface5* from the internal hardware switch, so you can configure them as a separate interfaces later.

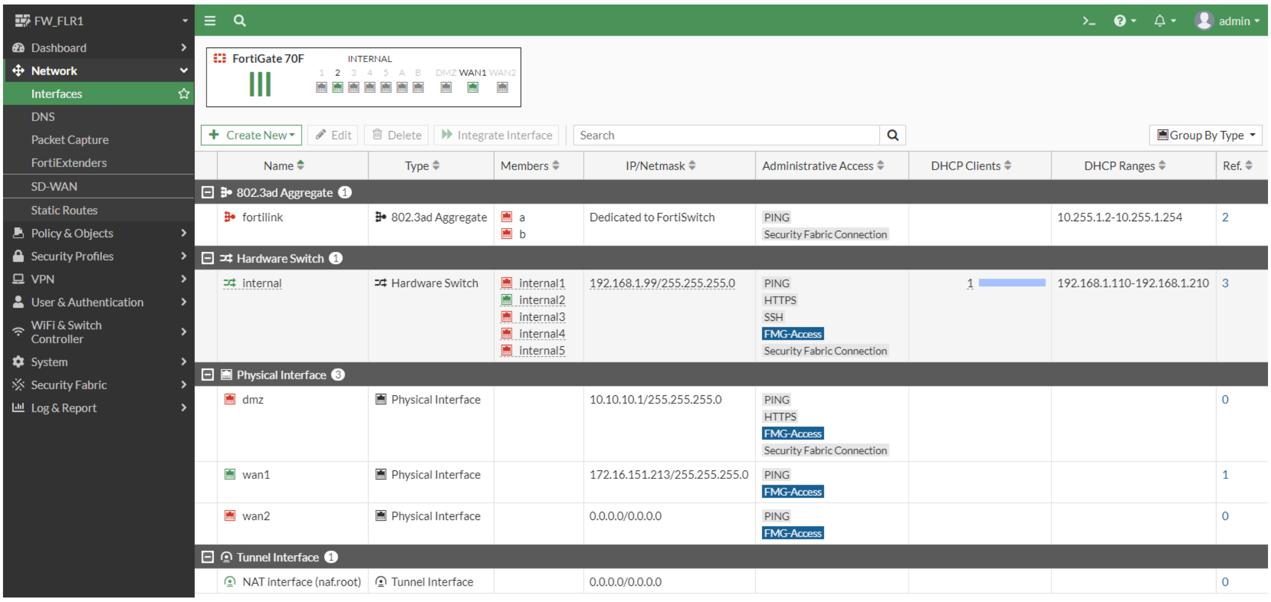
This guide uses *internal1* for the LAN interface and *internal5* for the management interface.

In this example, ports 1 through 5 are displayed under *Hardware Switch* as internal interfaces labeled *internal1*, *internal2*, and so on.

On some FortiGate models, the internal interfaces have the same names, but they are displayed under *VLAN Switch* instead.

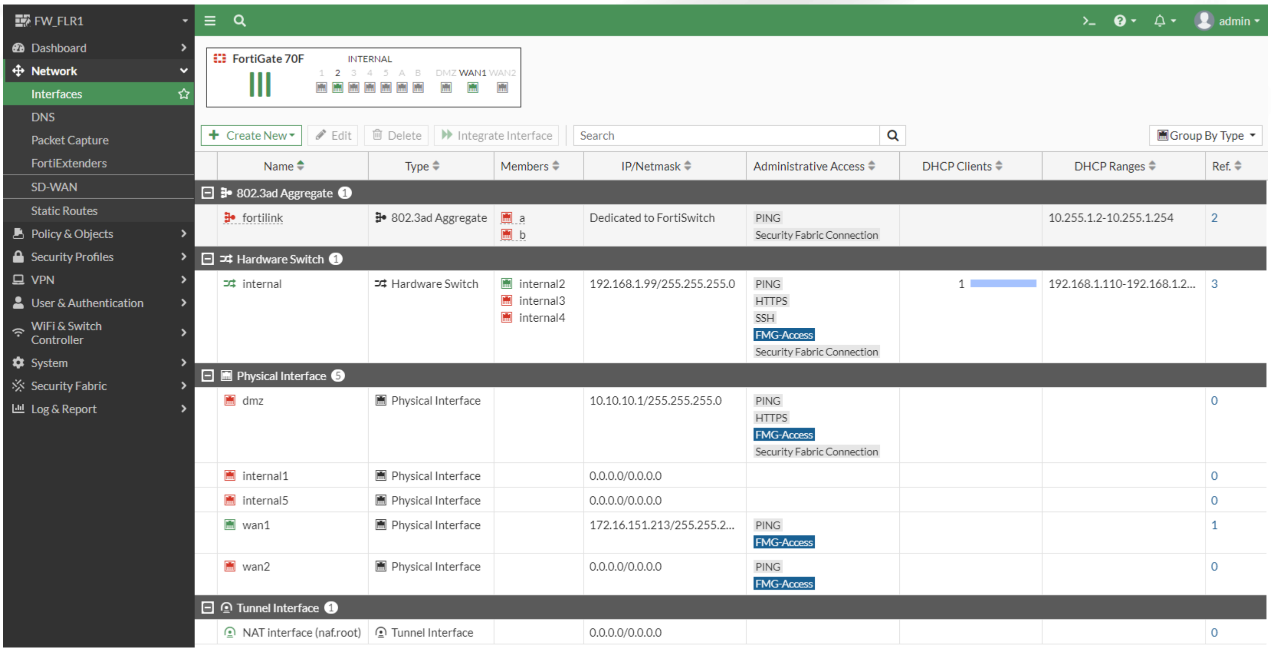
To remove interfaces from the hardware switch:

1. Go to *Network > Interfaces*. The interfaces are displayed.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a b	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Hardware Switch 1							
internal	Hardware Switch	internal1 internal2 internal3 internal4 internal5	192.168.1.99/255.255.255.0	PING HTTPS SSH FMG-Access Security Fabric Connection	1	192.168.1.110-192.168.1.210	3
Physical Interface 3							
dmz	Physical Interface		10.10.10.1/255.255.255.0	PING HTTPS FMG-Access Security Fabric Connection			0
wan1	Physical Interface		172.16.151.213/255.255.255.0	PING FMG-Access			1
wan2	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			0
Tunnel Interface 1							
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

2. Double-click the interface that includes the members named *internal1* and *internal5*.
   In this example, the *Hardware Switch* interface includes the *internal1* and *internal5* member.
   The *Edit Interface* pane is displayed.
3. Beside *internal5*, click the *x* to remove the member from the interface, and then do the same for *internal1*.
4. Click *OK* to save the changes.
   The *internal1* and *internal5* members are removed from the *Hardware Switch* and displayed under *Physical Interfaces*.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate	a b	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Hardware Switch 1							
internal	Hardware Switch	internal2 internal3 internal4	192.168.1.99/255.255.255.0	PING HTTPS SSH FMG-Access Security Fabric Connection	1	192.168.1.110-192.168.1.2...	3
Physical Interface 5							
dmz	Physical Interface		10.10.10.1/255.255.255.0	PING HTTPS FMG-Access Security Fabric Connection			0
internal1	Physical Interface		0.0.0.0/0.0.0.0				0
internal5	Physical Interface		0.0.0.0/0.0.0.0				0
wan1	Physical Interface		172.16.151.213/255.255.2...	PING FMG-Access			1
wan2	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access			0
Tunnel Interface 1							
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

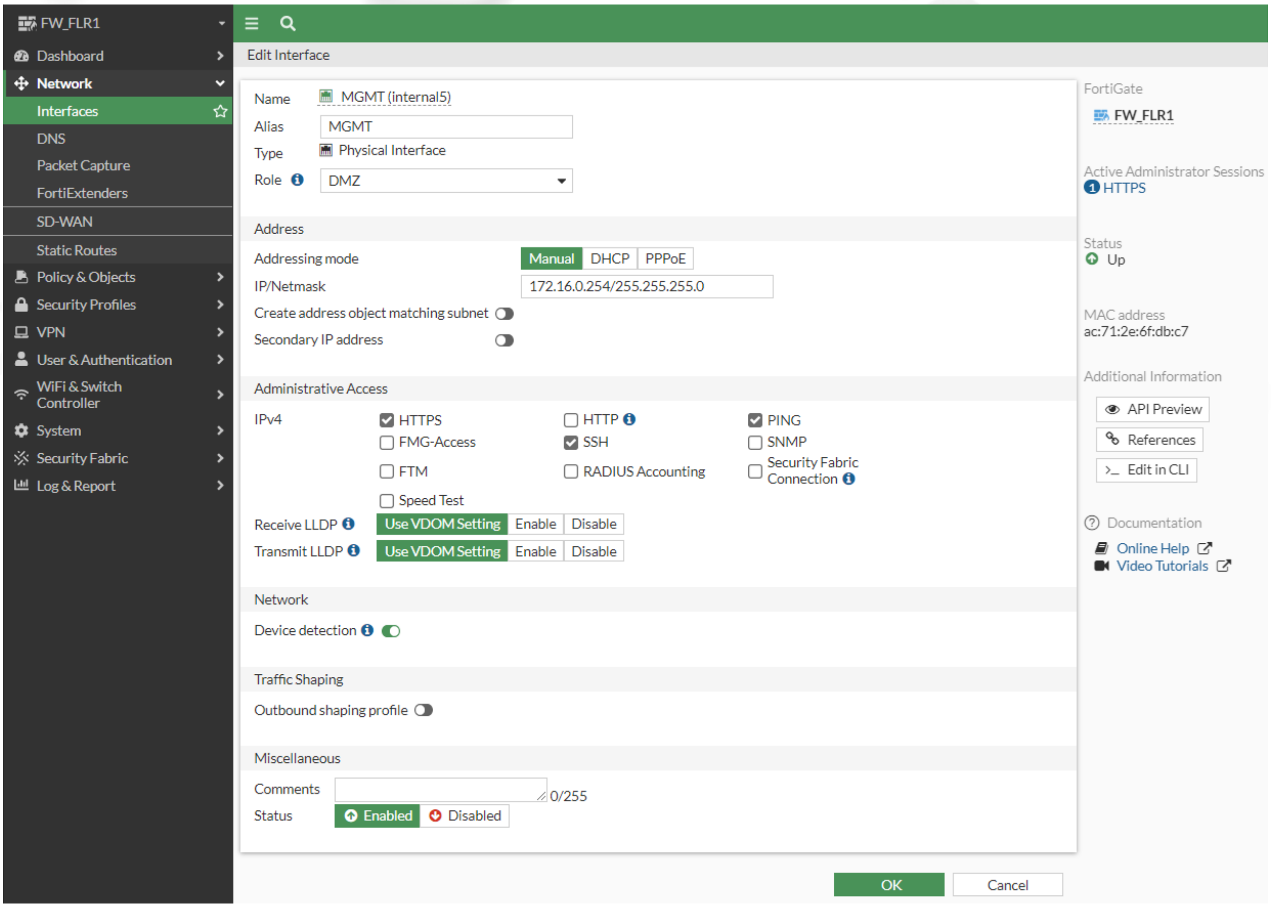
Configuring the management interface

We will configure the *internal5* interface that we removed from the hardware switch as the management interface.

To configure the management interface:

1. On the *Network > Interface* page, double-click the *internal5* interface to open it for editing.
2. Set the following options:

Alias	MGMT
Role	DMZ
IP/Netmask	172.16.0.254/255.255.255.0
Administrative Access	HTTPS, SSH, PING
Device Detection	Enabled



Edit Interface

Name: MGMT (internal5)
Alias: MGMT
Type: Physical Interface
Role: DMZ

Address
Addressing mode: [✓ Manual] DHCP PPPoE
IP/Netmask: 172.16.0.254/255.255.255.0
Create address object matching subnet ○
Secondary IP address ○

Administrative Access
IPv4: ☑ HTTPS ☐ HTTP ☑ PING ☐ FMG-Access ☑ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection ☐ Speed Test
Receive LLDP: [✓ Use VDOM Setting] Enable Disable
Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

Network
Device detection ●

Traffic Shaping
Outbound shaping profile ○

Miscellaneous
Comments: 0/255
Status: [✓ Enabled] Disabled

FortiGate: FW_FLR1
Active Administrator Sessions: 1 HTTPS
Status: Up
MAC address: ac:71:2e:6f:db:c7
Additional Information

3. Click *OK* to save the changes.

Updating your PC

After you configure the *internal5* interface as the management interface on the FortiGate, you must also update settings on your PC.

Access to the FortiGate GUI is temporarily lost during this step.

To configure the management interface:

1. Locate the Ethernet cable between your PC and the FortiGate, and switch the cable from port 1 (the *internal1* interface) on the FortiGate to port 5 (the *MGMT (internal5)* interface) on the FortiGate.
2. On your PC, update the network adapter to *172.16.0.[1-253]/255.255.255.0* with a default gateway of *172.16.0.254*.
3. Use a browser to log back in to the FortiGate GUI. See also Connecting to the FortiGate GUI and logging in on page 13.

Removing access to interfaces

Port 5 (the *MGMT (internal5)* interface) is now configured as the management interface, and your PC is updated to connect to the FortiGate. You are logged in to the FortiGate GUI, and you are now ready to:

- Remove HTTP, HTTPS, and SSH administrative access from all interfaces, except the *MGMT (internal5)* interface.
- Set *Status* to *Disabled* on all interfaces, except for *LAN (internal1)*, *MGMT (internal5)*, and *wan1*. This ensures no other interfaces are susceptible to unauthorized access over a physical connection.

When editing the internal switch interface to remove administrative access, set *IP/Netmask* to *0.0.0.0/0.0.0.0*, disable *DHCP server*, and set *Status* to *Disabled*.

Managed switch connection

A managed switch, such as FortiSwitch, will connect to port1 on the FortiGate. The switch can be connected now or later.

See also LANs and LAN segmentation on page 32.

System settings

Use the *System Settings* module to define parameters related to system access as well as other system-related functions. It is important to customize these settings from defaults to improve device security, ensure proper logging, and allow monitoring of administrative events and other activities.

This section includes the following topics:

- Configuring system settings on page 18
- Configuring log settings on page 19
- Configuring a remote RADIUS authentication server on page 20

Configuring system settings

Before configuring system settings, enable the certificates feature.

To enable certificates:

1. Go to *System > Feature Visibility*.
2. Under *Additional Features*, enable *Certificates*, and click *Apply*.

To configure system settings:

1. Go to *System > Settings*.
2. Set *Time zone* to reflect the location of the FortiGate.
3. Change *HTTPS port* from *443* to an uncommon port number, such as, 9443.
4. For *HTTPS server certificate*, use automated certificate enrollment to leverage the ACME protocol with the Let’s Encrypt service.
   a. Use the dropdown next to *HTTPS server certificate* to select *+Create*.
   b. Select *Use Let’s Encrypt*.
   c. Provide an appropriate name for the certificate.
   d. Set *Domain* to the public FQDN of the FortiGate.
   e. Set *Email* to a valid email address.
   f. Select *Create*.
   For further details on the process, see *FortiOS 7.0 Administration Guide > ACME certificate support*
   .
5. Change the *SSH port* from *22* to an uncommon port number, such as, 9922.

6. Ensure the *Idle timeout* is under 10 minutes. Five (5) minutes is recommended.
   A setting of 10 minutes or less minimizes the amount of time administrators can remain logged in when away from their computer.
7. Enable a password policy for admin with the minimum following values:

Password scope	Admin
Minimum length	8
Minimum number of new characters	0
Character requirements	Enable
Upper case	1
Lower case	1
Number (0-9)	1
Special	1
Allow password reuse	Disable
Password expiration	Disable

8. Disable *VLAN switch mode*.
9. Under *Start Up Settings*, disable *Detect configuration*.
10. Disable *Detect firmware*.
11. Click *Apply*.

Configuring log settings

To configure Log settings:

1. Go to *Security Fabric > Fabric Connectors*, and double-click the *Cloud Logging* tile to open it for editing.
2. Set *Status* to *Enabled*.
3. Set *Type* to *FortiGate Cloud*.
4. Set *Upload option* to *Real Time*.
5. Beside *Account*, click *Activate*.
   a. Provide the account password, and select the geographic location to receive the logs.
   b. Click *OK* to save.
6. In FortiGate Cloud, select your device, and click *Analysis* to review its log and analysis page.
   Under *Event Management > Event* handlers, view the list of pre-defined event handlers, which are used to alert on events when certain logs are detected. It is recommended to enable some event handlers from within FortiGate Cloud. For more information, see the *FortiCloud Admin Guide*.

   Sending logs to FortiGate Cloud improves the local log capabilities of the FortiGate. Even for models with a dedicated disk for logging, centralized logging and reporting with FortiGate Cloud assists with log analysis and correlation tasks and securely stores your logs with greater resiliency and accessibility.
7. In FortiOS, go to *Log & Reports > Log Settings*, and ensure that *Event Logging* is set to All.
   The *Local Traffic Log* setting defines traffic that is destined to the FortiGate interface, or sourced from the FortiGate interface. Typically all local traffic is disabled by default, but to track any unwanted, denied traffic destined to the FortiGate, enable *Log Denied Unicast Traffic*.
8. If your FortiGate includes a logging disk, you can enable the FortiGate to log to the disk too under *Log & Report > Log Settings > Local Log*.
   FortiGate models that end in 1, such as 71F, include a logging disk.

Configuring a remote RADIUS authentication server

A remote authentication server, such as a RADIUS server, can be used with the FortiGate for many purposes, including administrator login, Wireless WPA2-enterprise authentication, and remote VPN user authentication.

Add a RADIUS server to be used for WiFi WPA2-Enterprise authentication.

To configure a remote RADIUS authentication server:

1. Go to *User & Authentication* > *RADIUS Servers*, and click *+Create New*.
2. Enter a name, such as *RADIUS*.
   This guide uses the name *RADIUS*.
3. Set *IP/Name* to the IP address of the RADIUS server.
4. Set *Secret* to the secret of the RADIUS server.
5. Click *Test Connectivity* to verify your credentials.
6. Click *OK* to save the configuration.

Administrator settings

Properly configuring your administrator settings is essential to keeping your FortiGate secure from unwanted and unauthorized access. Having a password policy and enabling MFA are keys to protecting your administrator account.

This section includes the following topics:

- Configuring administrator settings on page 20
- Configuring RADIUS administrator accounts on page 21

Configuring administrator settings

You can edit the default administrator account named *admin*. Alternately you can create a new administrator account, and delete the existing *admin* account. This topic describes how to edit the default *admin* account.

To configure administrator settings in the GUI:

1. Go to *System* > *Administrators*, and double-click the *admin* account to open it for editing.
2. Enable *Two-factor Authentication*, and select *FortiToken*.
3. Set *Token* to one of the available FortiTokens.

FortiGate comes with two (2) free FortiTokens. If you need to apply multi-factor authentication (MFA) to additional users, consider purchasing more tokens or using FortiToken Cloud.

4. Provide an email address or phone number for the activation code:
   - Enter an email address in the *Email Address* box.
   - Enable *SMS* and enter a phone number.

A popup appears at the bottom-right of the pane, indicating the activation code has been sent.

5. Enable *Restrict login to trusted hosts*, and enter your management network, for example, 172.16.0.0/24. This ensures that only users from the trusted network are allowed to log in to the FortiGate.
6. Click *OK*.

The remaining settings must be configured using the command line interface.

Setting	Description
Lockout duration	How long the admin account is locked after repeated, failed login attempts FW_FLR1 # config sys global FW_FLR1 (global) # set admin-lockout-duration 1800 FW_FLR1 (global) # end
Number of failures to trigger the lockout duration	How many failed login attempts before an admin account is locked out FW_FLR1 # config sys global FW_FLR1 (global) # set admin-lockout-threshold [1-10] FW_FLR1 (global) # end
Disable maintainer account	A maintenance account allows users with physical access and knowledge of the FortiGate to log in and perform password resets. FW_FLR1 # config sys global FW_FLR1 (global) # set admin-maintainer disable FW_FLR1 (global) # end

Configuring RADIUS administrator accounts

You may want to configure administrator authentication using RADIUS. First create a user group. Once the user group is defined (and the appropriate settings are configured on your RADIUS server), you can create a RADIUS administrative user.

To create a user group:

1. Go to *User & Authentication* > *User Groups*, and click *+Create New*.
2. Set *Name* to *Admin*.
3. Set *Type* to *Firewall*.
4. Add a remote group:
   a. Click *Add*. The *Add Group Match* pane is displayed.
   b. Set *Remote Server* to *RADIUS*.
   c. Set *Groups* to *Specify*.
   d. Enter *FirewallAdmin*.
   e. Click *OK*. The remote group is displayed.
5. Click *OK* to save the user group.

To create a RADIUS administrator:

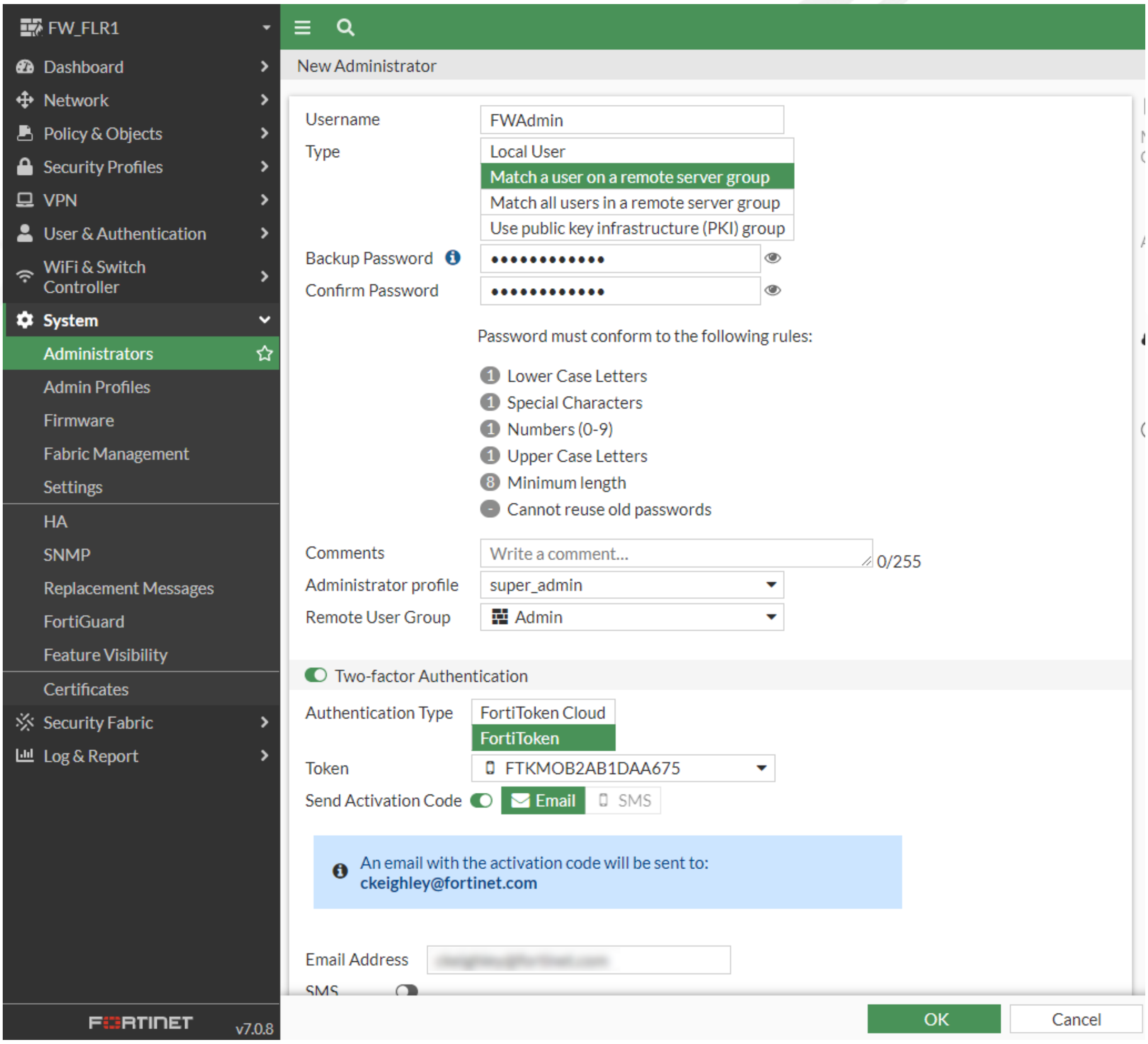
1. Go to *System* > *Administrators*, and click *Create New* > *Administrator*.
2. Enter a name, such as *FWAdmin*, and select *Match a user on a remote server group*.
3. Enter a *Backup Password*. This password is only used when the FortiGate cannot connect to the RADIUS server.
4. Set *Administrator profile* to *super_admin*.
5. Set *Remote User Group* to *Admin*.
6. Enable *Two-factor Authentication*.

⚠ Use caution when implementing MFA on all administrator accounts. If you are unable to provide the token code for all accounts, you may have to reset your FortiGate, and reload your configuration from backup.

As a precaution, consider creating an administrative account with a long and complex password. Write down the password, and keep it in a secure location. Then only use the password if you are locked out from administrator accounts that use MFA.

7. Enable *Restrict login to trusted hosts*.

8. Click *OK*.



Username: FWAdmin

Type:
- Local User
- Match a user on a remote server group
- Match all users in a remote server group
- Use public key infrastructure (PKI) group

Backup Password: ••••••••••••

Confirm Password: ••••••••••••

Password must conform to the following rules:
- 1 Lower Case Letters
- 1 Special Characters
- 1 Numbers (0-9)
- 1 Upper Case Letters
- 8 Minimum length
- - Cannot reuse old passwords

Comments: Write a comment... 0/255

Administrator profile: super_admin

Remote User Group: Admin

Two-factor Authentication

Authentication Type: FortiToken Cloud / FortiToken

Token: FTKMOB2AB1DAA675

Send Activation Code: Email SMS

An email with the activation code will be sent to: **ckeighley@fortinet.com**

Email Address: [redacted]

SMS

FortiGate Cloud Sandbox

A connection from the FortiGate to FortiGate Cloud Sandbox is established when you use the FortiOS CLI to choose a region. FortiGate Cloud Sandbox can be used by antivirus security profiles. See also Creating antivirus profiles on page 40.

For more information about FortiGate Cloud Sandbox, see the *FortiGate Cloud Administration Guide*.

To enable FortiGate Cloud Sandbox:

1. Select a FortiGate Cloud Sandbox region using the CLI:

```
FW_FLR1 # execute forticloud-sandbox region
FW_FLR1 # 0 Europe
FW_FLR1 # 1 Global
FW_FLR1 # 2 Japan
```

```
FW_FLR1 # 3 US
Please select cloud sandbox region[0-3]:
```

2. Go to *FortiGate GUI* > *Security Fabric* > *Fabric Connectors*.
   The *Cloud Sandbox* card reflects the chosen region, and a green arrow displays after the connection is established.

FortiGate objects

We will define all the FortiGate objects we need for our security policies, such as addresses, networks, users, user groups, and services.

User group objects

In addition to the admin user group, the following user groups are defined and use the RADIUS server for authentication:

- Engineering
- Staff
- IT

These groups will be used for wireless authentication, allowing those who belong to the IT and Engineering Active Directory User Groups to access the IT_WiFi and Engineering_WiFi networks respectively, while a third group will allow anyone part of the Staff user group to connect to Staff_WiFi.

IT and Engineering LAB networks are only available on WiFi through their respective networks.

To create user groups on FortiGate:

1. Go to *User & Authentication* > *User Groups*, and click *Create New*.
2. Complete the following options:

Name	Engineering
Type	Firewall

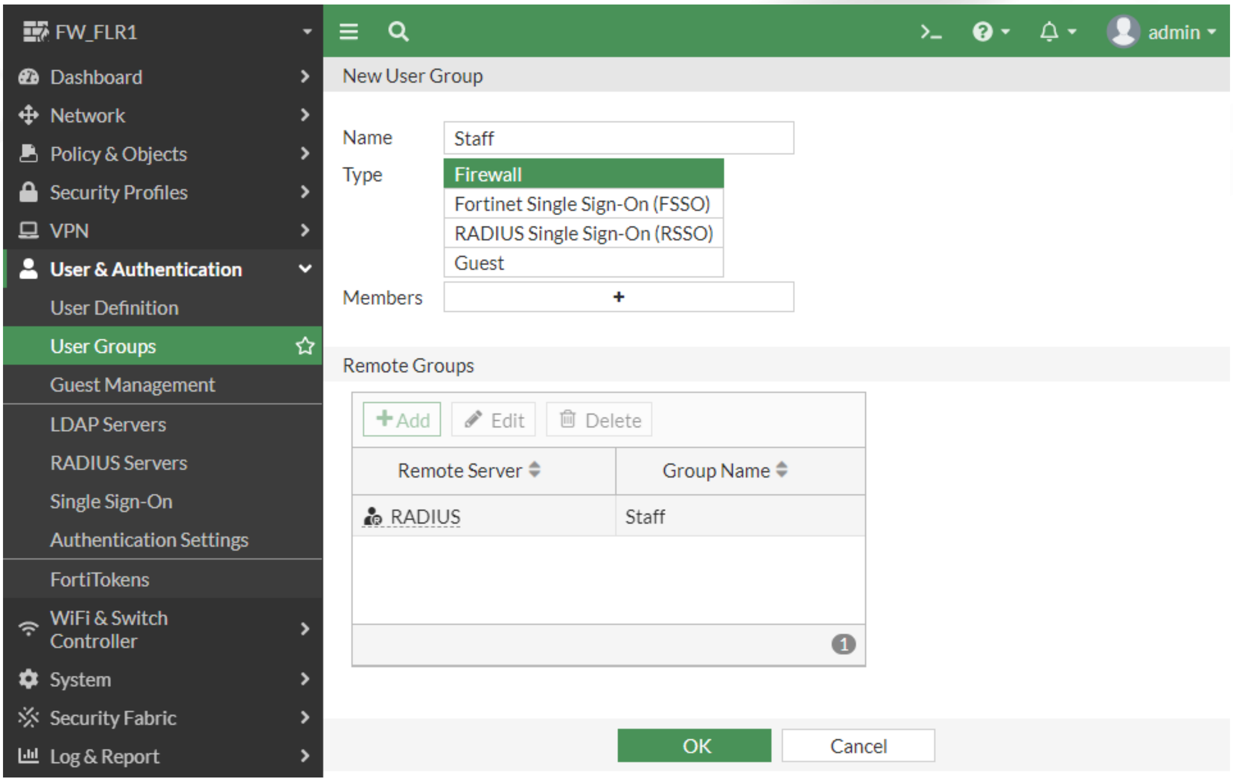
3. In the *Remote Groups* section, click *Add*. The *Add Group Match* pane is displayed.
4. Complete the following options, and click *OK*:

Remote Server	RADIUS
Groups	Click *Specify*, and type *Engineering*.

   The remote group is created.
5. Click *OK*. The new user group is displayed.
6. Repeat this procedure to create a user group named Staff by using the following settings:

Name	Staff

Type	Firewall
Remote Groups	Click *Add*.
Remote Server	Select *RADIUS*.
Groups	Click *Specify*, and type *Staff*.



New User Group

Name: Staff

Type: Firewall (selected) | Fortinet Single Sign-On (FSSO) | RADIUS Single Sign-On (RSSO) | Guest

Members: +

Remote Groups

+Add | Edit | Delete

Remote Server	Group Name
RADIUS	Staff

1

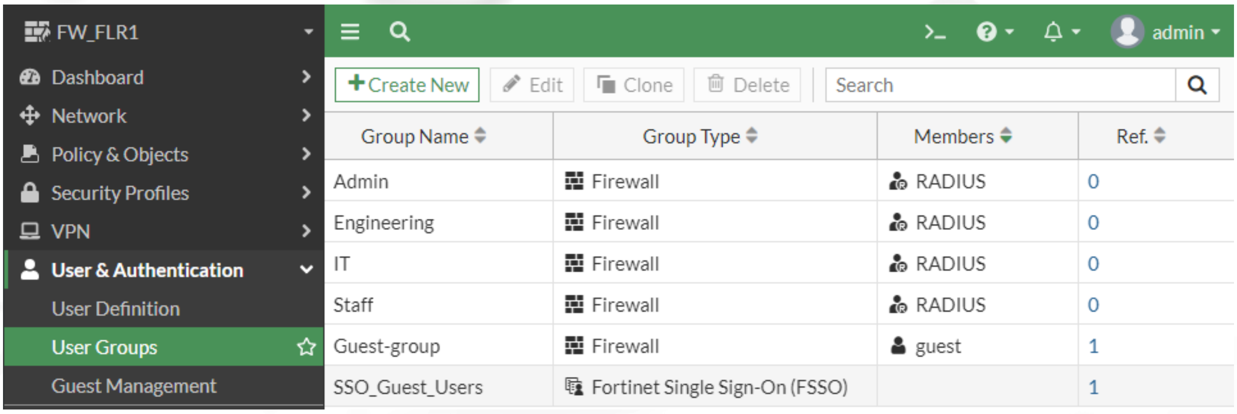
OK | Cancel

The remote group is created.

7. Repeat this procedure to create a user group named IT by using the following settings:

Name	IT
Type	Firewall
Remote Groups	Click *Add*.
Remote Server	Select *RADIUS*.
Groups	Click *Specify*, and type *IT*.

The remote group is created. All groups are displayed.



Group Name	Group Type	Members	Ref.
Admin	Firewall	RADIUS	0
Engineering	Firewall	RADIUS	0
IT	Firewall	RADIUS	0
Staff	Firewall	RADIUS	0
Guest-group	Firewall	guest	1
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

Address objects

Address objects can be defined as subnets, IP ranges, FQDN, geography, dynamic or MAC address.

Complete the following steps to create address objects on FortiGate:

1. Create several address objects. See Creating address objects on page 26.
2. Create an address group to contain the RFC-1918 address objects. See Creating address groups on page 27.

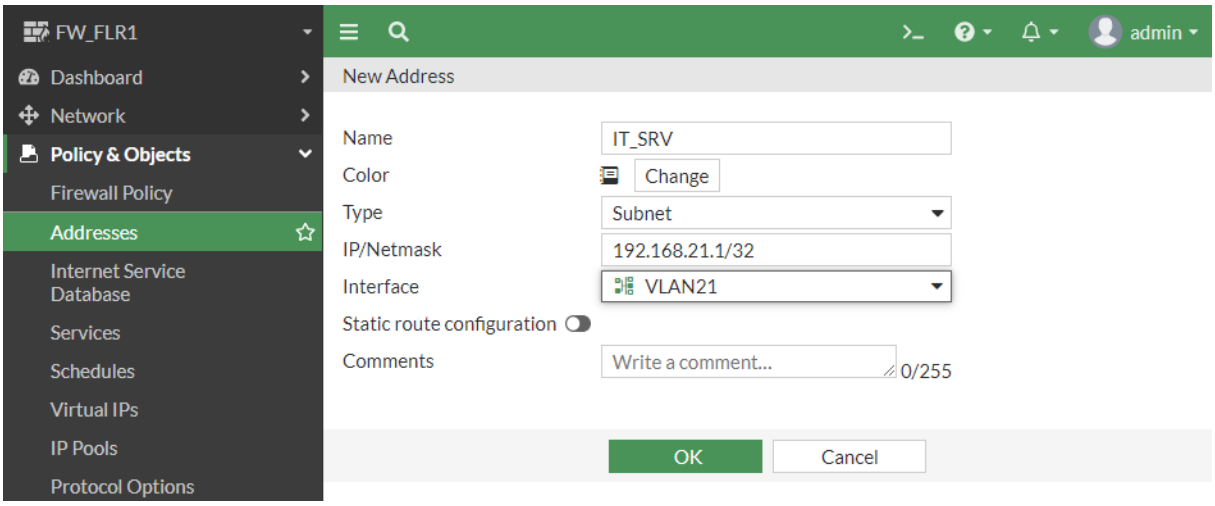
Creating address objects

The address objects used in this configuration are subnets defined as an IP address with a /32 subnet and groups of addresses in the private IP subnet range.

To create address objects on FortiGate:

1. Go to *Policy & Objects > Addresses*, and click *Create New > Address*.
2. Complete the following options:

Name	IT_SRV
IP/Netmask	192.168.21.1/32
Interface	VLAN21



New Address

Name: IT_SRV
Color
Type: Subnet
IP/Netmask: 192.168.21.1/32
Interface: VLAN21
Static route configuration ○
Comments: Write a comment... 0/255

3. Click *OK*. The new address object is created.
4. Repeat this procedure until you create all the following address objects:
   - ENG_SRV

Name	ENG_SRV
IP/Netmask	192.168.31.1/32
Interface	VLAN31

   - CORP_SRV

Name	CORP_SRV
IP/Netmask	192.168.50.1/32
Interface	VLAN50

In this example, all corporate services are hosted on the same IP address. In the event you use multiple servers to provide the services, you will need to create several address objects for various corporate servers or an IP range for a group of contiguous IPs.

   - RFC-1918-10

Name	RFC-1918-10
IP/Netmask	10.0.0.0/8
Interface	any

   - RFC-1918-172

Name	1918-172
IP/Netmask	172.16.0.0/12
Interface	any

   - RFC-1918-192

Name	RFC-1918-192
IP/Netmask	192.168.0.0/16
Interface	any

   The address objects are created.
5. Next, create an address group to contain the address objects. See Creating address groups on page 27.

Creating address groups

After defining the address objects, create an address group named *RFC-1918* to contain the RFC-1918 address objects.

To create an address group:

1. On the *Policy & Objects > Addresses* pane, click *New > Address Group*.
2. Complete the following options:

Group name	RFC-1918
Type	Group
Members	RFC-1918-10 RFC-1918-172 RFC-1918-192

3. Click *OK*.

Service objects

Service objects define specific ports for specific servers. This helps to ensure only required traffic is permitted to access the subnets of the servers hosting the service. If there are multiple services, it is recommended to put them into a group for ease of configuration. For example, if Engineering requires an additional service, you can define this new service, and add it to the existing group to update any references to Engineering servers in your policies.

Complete the following steps to set up service objects:

1. On FortiGate, create service objects. See Creating service objects on page 28.
2. On FortiGate, create service groups to contain the service objects. See Creating service groups on page 29.
3. On a Network Policy Server, configure a RADIUS client for the FortiGate. See Configuring the NPS server RADIUS client on page 30.

Creating service objects

This section describes how to create the following service objects:

- ENG_SRV1
- ENG_SRV2
- IT_SRV1
- IT_SRV2

To create service objects:

1. Go to *Policy & Objects > Services*, and click *Create New > Service*.
2. Complete the following options:

Name	ENG_SRV1
Protocol Type	TCP/UDP/SCTP
Address	192.168.31.1
Destination Port	TCP, 5678

3. Click *OK*. The new address object is created.

4. Repeat this procedure until you create all the following service objects:
   - ENG_SRV2

Name	ENG_SRV2
Protocol Type	TCP/UDP/SCTP
Address	192.168.31.1
Destination Port	TCP, 4678

   - IT_SRV1

Name	IT_SRV1
Protocol Type	TCP/UDP/SCTP
Address	192.168.21.1
Destination Port	TCP, 8765

   - IT_SRV2

Name	IT_SRV2
Protocol Type	TCP/UDP/SCTP
Address	192.168.21.1
Destination Port	TCP, 9765

   The address objects are created.
5. Next, create service groups to contain the service objects. See Creating service groups on page 29.

Creating service groups

After defining the service objects, create the following service groups to contain the objects:

- ENG_SERVICES
- IT_SERVICES

To create service groups:

1. On the *Policy & Objects* > *Services* pane, click *New* > *Service Group*.
2. Complete the following options:

Group name	ENG_SERVICES
Members	ENG_SRV1 ENG_SRV2

3. Click *OK*.
4. Repeat this procedure to create an IT_SERVICES group:

Group name	IT_SERVICES
Members	IT_SRV1 IT_SRV2

5. Next, configure a RADIUS client on a Network Policy Server for the FortiGate. See Configuring the NPS server RADIUS client on page 30.

Configuring the NPS server RADIUS client

On a Network Policy Server, configure a RADIUS client for the FortiGate.

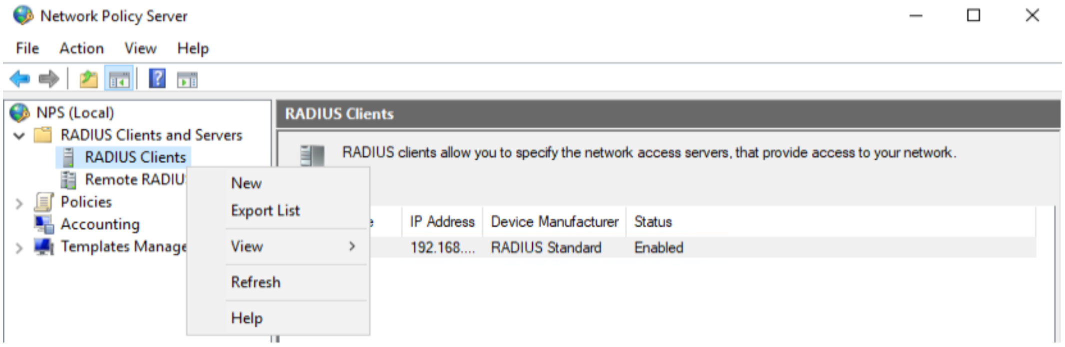
For corporate services, the predefined firewall service group named *Windows AD* is used.

In order to leverage Active Directory (AD) groups to define who belongs to a given user group, the RADIUS server must be configured to return RADIUS AVP Fortinet-Group-Name that matches the group defined in the *User Group > Remote Groups > Radius server > Group Name*.

For more information, see the FortiOS Administration Guide.

To configure the NPS server RADIUS client settings:

1. On a Network Policy server, go to *RADIUS Clients and Servers > RADIUS Clients*.
2. Right-click *RADIUS Clients* to select *New*.

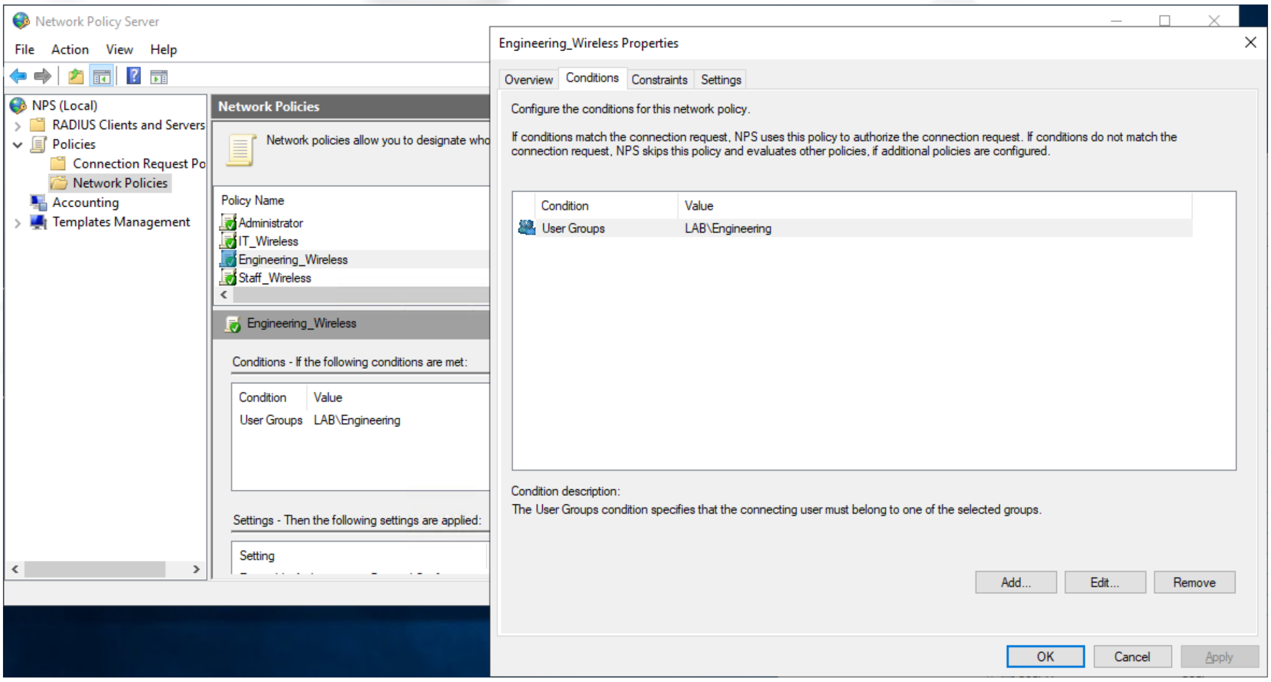


RADIUS clients allow you to specify the network access servers, that provide access to your network.

IP Address	Device Manufacturer	Status
192.168....	RADIUS Standard	Enabled

3. Enter the name, IP address/DNS address, and a secret.
4. Go to *Policies > Network Policies*, and define network policies for each of the following user groups: Engineering, IT, Staff, and Admin.

   Within each policy, the conditions are that the authenticating user belongs to a particular group in AD. (*Policy Properties > Conditions*)



Engineering_Wireless Properties

Overview | Conditions | Constraints | Settings

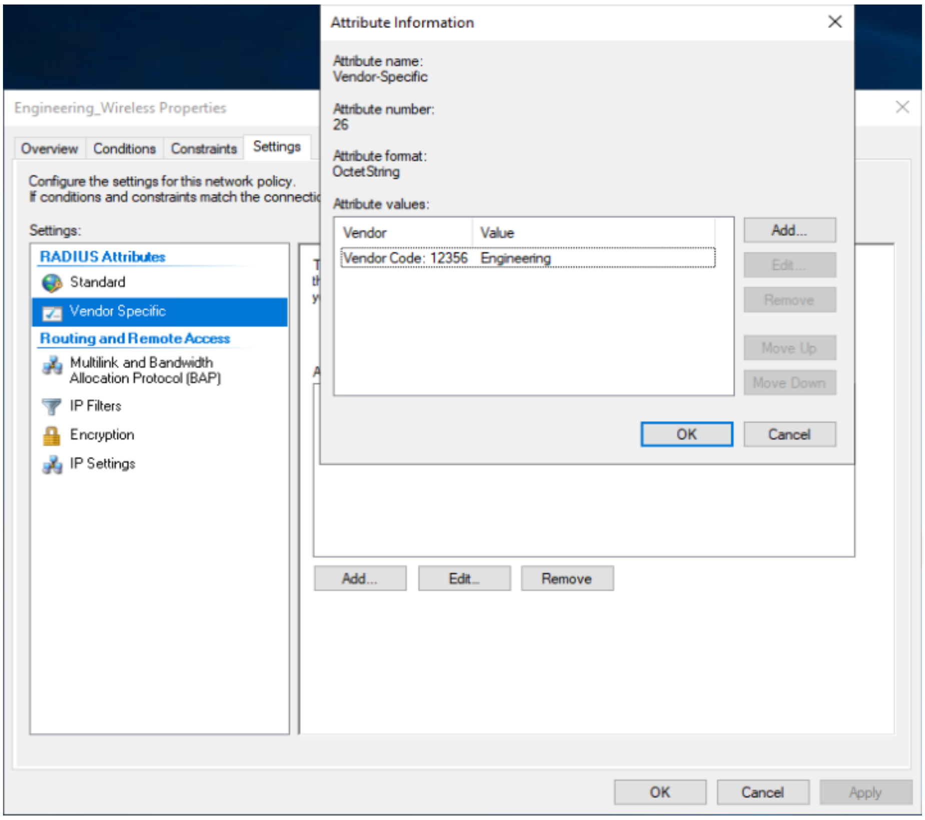
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
User Groups	LAB\Engineering

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

When a user who belongs to this group authenticates, a Vendor-Specific-Attribute (VSA) is configured to return, for example, `Fortinet-Group-Name=IT` (or `Fortinet-Group-Name=Engineering`, and so on).



Attribute Information

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value
Vendor Code: 12356	Engineering

Engineering_Wireless Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connectio
Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
Add...
Edit...
Remove
Move Up
Move Down
OK
Cancel
Apply

FortiGate matches the VSA in the *Groups: Specify* section of the *User Group > Remote Group*. It is a good idea to return a VSA that matches the group, although it is not necessary.

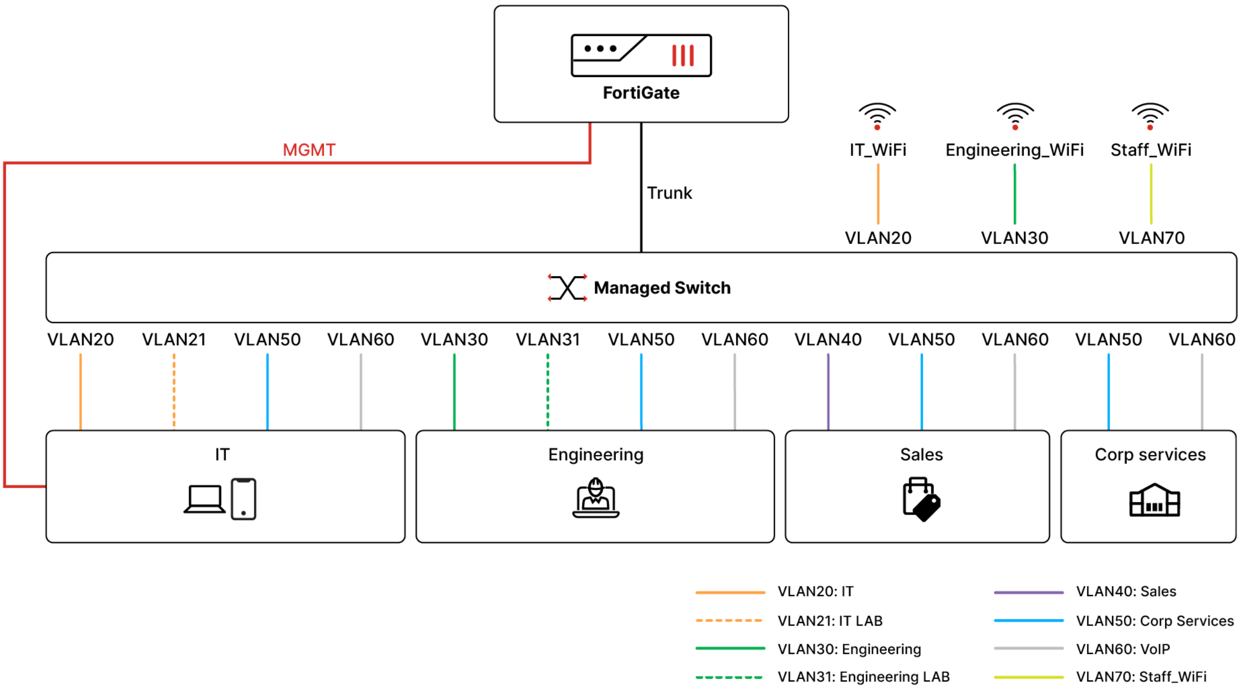
LANs and LAN segmentation

This example company will use the following subnets:

Interface	Purpose	Subnet	DHCP	FortiGate interface address	Address object
MGMT	Management Network	172.16.0.0/24	No	.254	MGMT_net
port1.VLAN20	IT	192.168.20.0/24	Yes	.254	VLAN20 address
port1.VLAN21	IT LAB	192.168.21.0/24	No	.254	VLAN21 address
port1.VLAN30	Engineering	192.168.30.0/24	Yes	.254	VLAN30 address
port1.VLAN31	Engineering LAB	192.168.31.0/24	No	.254	VLAN31 address
port1.VLAN40	Sales	192.168.40.0/24	Yes	.254	VLAN40 address
port1.VLAN50	Corp Services	192.168.50.0/24	Yes	.254	VLAN50 address
port1.VLAN60	VoIP phones	192.168.60.0/24	Yes	.254	VLAN60 address
port1.VLAN70	IoT wireless/Staff WiFi	192.168.70.0/23	Yes	.71.254	VLAN70 address

The subnets used in this guide illustrate the process of creating and using them. You may consider further subnets for devices such as PoS systems, printers, and security cameras to name a few.

Once completed, the topology should be as follows:



Complete the following steps to configure the LAN:

1. If not done already, physically connect your managed switch to the FortiGate trunk port. See Managed switch connection on page 18.
2. Configure the trunk port to connect to the core switch. See Trunk port on page 33.
3. Define and assign the VLANs. See VLANs on page 34.

Trunk port

Configure the trunk port to connect to core switch.

We will use port 1 (the *internal1* interface in the GUI), which was removed from the internal hardware switch earlier in the document. If *internal1* has not been removed, see Removing interfaces from the hardware switch on page 15.

To configure the trunk port:

1. Go to *Network > Interfaces*.
2. Double-click the port that you will use to connect to the core switch to open it for editing.
   In this example, we will use port 1, which is labeled *internal1* in the GUI.
3. Set the following options, and click *OK* to save the changes:

Alias	LAN
Role	LAN
Addressing Mode	Manual
IP/Netmask	Provide an IP address/netmask that the FortiAPs will use to connect to the FortiGate.
DHCP server	Enable to provide addresses in the network.

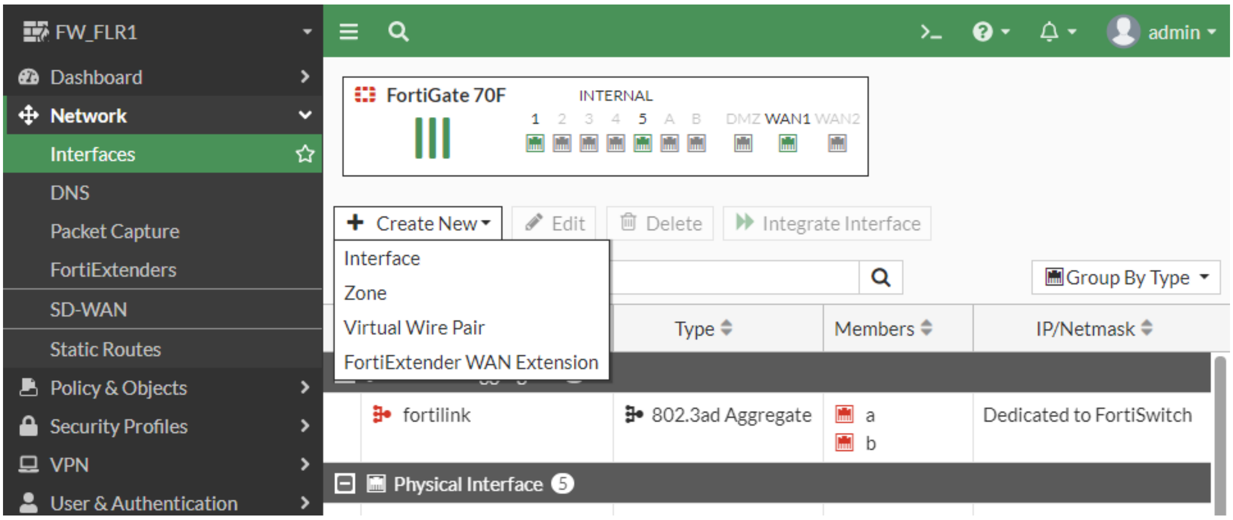
VLANs

Define the following VLANs outlined in LANs and LAN segmentation on page 32:

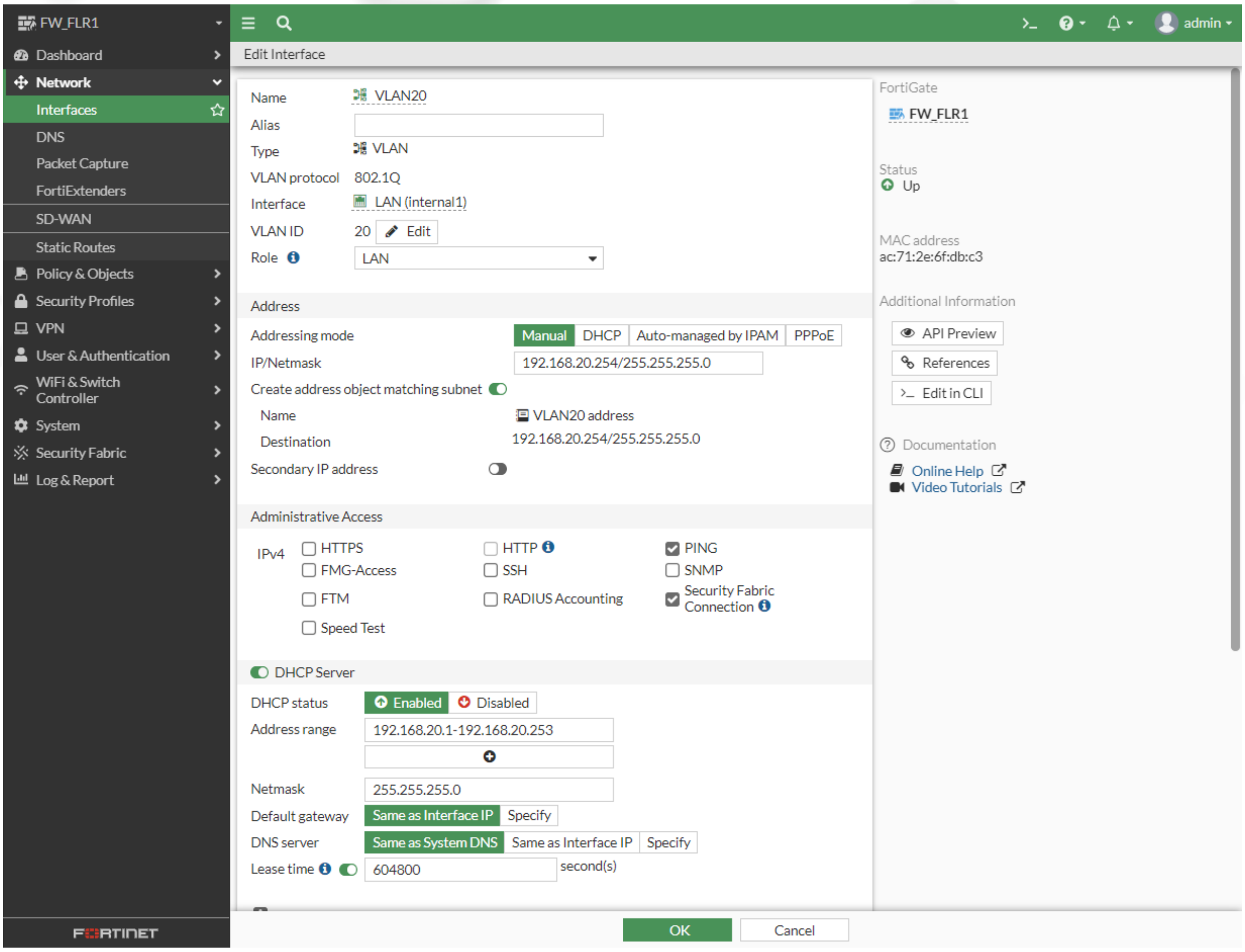
- port1.VLAN20
- port1.VLAN21
- port1.VLAN30
- port1.VLAN31
- port1.VLAN40
- port1.VLAN50
- port1.VLAN60
- port1.VLAN70

To define and assign VLANs:

1. Go to *Network* > *Interfaces*, and click *+Create New* > *Interface*.



2. Enter a name for the VLAN, and select *interface1* for the trunk port.
3. Set the VLAN ID.
4. Configure the *IP/Netmask* to reflect the FortiGate interface address corresponding to the network.
5. Under Administrative Access, enable PING.
6. Enable *DHCP server* to provide a range for the subnet.
   If you have a DNS server, you may elect to update the DNS server option in the DHCP server configuration.



Edit Interface

Name: VLAN20
Alias:
Type: VLAN
VLAN protocol: 802.1Q
Interface: LAN (internal1)
VLAN ID: 20 Edit
Role: LAN

Status: Up
MAC address: ac:71:2e:6f:db:c3
Additional Information

Address

Addressing mode: [✓ Manual] DHCP Auto-managed by IPAM PPPoE
IP/Netmask: 192.168.20.254/255.255.255.0
Create address object matching subnet: ●
Name: VLAN20 address
Destination: 192.168.20.254/255.255.255.0
Secondary IP address: ○

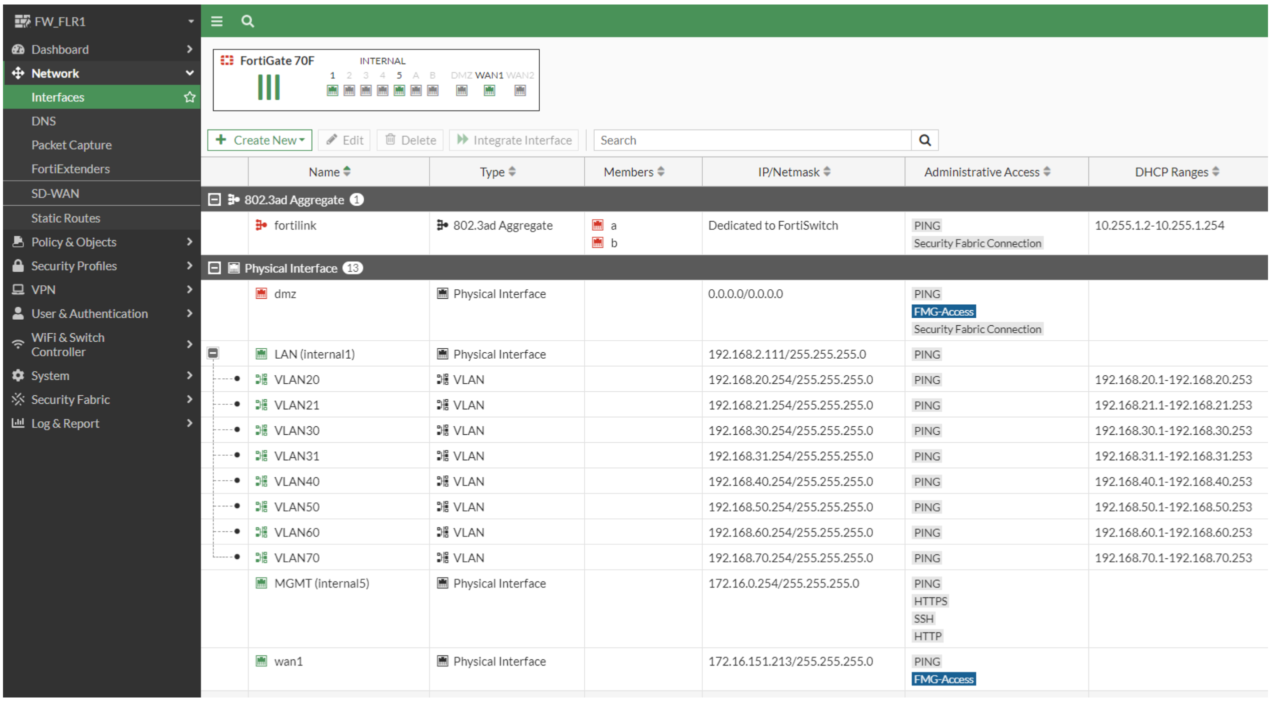
Administrative Access

IPv4
□ HTTPS □ HTTP ☑ PING
□ FMG-Access □ SSH □ SNMP
□ FTM □ RADIUS Accounting ☑ Security Fabric Connection
□ Speed Test

● DHCP Server

DHCP status: [✓ Enabled] Disabled
Address range: 192.168.20.1-192.168.20.253
Netmask: 255.255.255.0
Default gateway: [✓ Same as Interface IP] Specify
DNS server: [✓ Same as System DNS] Same as Interface IP Specify
Lease time ● 604800 second(s)

7. Click *OK*.
8. Repeat this procedure until you create all the VLANs.
   In this guide, the names will remain VLAN20, VLAN 21, and so on for ease of reference.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Ranges
802.3ad Aggregate 1					
fortilink	802.3ad Aggregate	a b	Dedicated to FortiSwitch	PING Security Fabric Connection	10.255.1.2-10.255.1.254
Physical Interface 13					
dmz	Physical Interface		0.0.0.0/0.0.0.0	PING FMG-Access Security Fabric Connection	
LAN (internal1)	Physical Interface		192.168.2.111/255.255.255.0	PING	
VLAN20	VLAN		192.168.20.254/255.255.255.0	PING	192.168.20.1-192.168.20.253
VLAN21	VLAN		192.168.21.254/255.255.255.0	PING	192.168.21.1-192.168.21.253
VLAN30	VLAN		192.168.30.254/255.255.255.0	PING	192.168.30.1-192.168.30.253
VLAN31	VLAN		192.168.31.254/255.255.255.0	PING	192.168.31.1-192.168.31.253
VLAN40	VLAN		192.168.40.254/255.255.255.0	PING	192.168.40.1-192.168.40.253
VLAN50	VLAN		192.168.50.254/255.255.255.0	PING	192.168.50.1-192.168.50.253
VLAN60	VLAN		192.168.60.254/255.255.255.0	PING	192.168.60.1-192.168.60.253
VLAN70	VLAN		192.168.70.254/255.255.255.0	PING	192.168.70.1-192.168.70.253
MGMT (internal5)	Physical Interface		172.16.0.254/255.255.255.0	PING HTTPS SSH HTTP	
wan1	Physical Interface		172.16.151.213/255.255.255.0	PING FMG-Access	

Wireless networks (WLAN)

Like wired networks, wireless networks come in a variety of architectures, with a variety of options for implementation. This section provides a simple way of providing wireless connectivity with some consideration to access control. It is recommended to review the 4-D wireless resource located here for a complete picture and to understand what adjustments can be made to better suit your needs.

Wireless network configuration on the FortiGate is comprised of the following parts:

- SSIDs on page 36
- AP profile on page 37
- Managed access points (APs) on page 38

Some wireless settings must be adjusted, depending on your environment. For example, you may need to adjust wireless settings if there are other competing wireless networks in the area.

SSIDs

We will create SSIDs to support access for the following groups:

- General corporate access (Staff_WiFi)
- IT access (IT_WiFi)
- Engineering access (Engineering_WiFi)

The IT and Engineering SSIDs should only authenticate users who belong to those departments.

To configure SSIDs:

1. Go to *WiFi & Switch Controller > SSIDs*, and click *Create New > SSID*.
2. Complete the following options as needed, then click *OK* to create the SSID named *Staff_WiFi*.

Name	Staff_WiFi
Traffic mode	Bridge
SSID	Staff_WiFi
Security mode	WPA2 Enterprise
Authentication	Local

User group	Staff
Optional VLAN ID	70

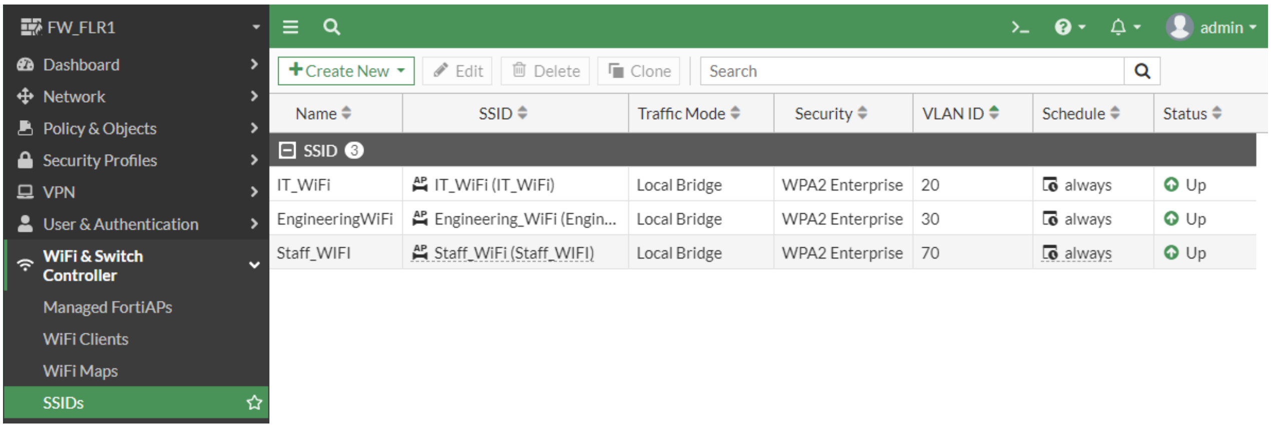
3. Repeat this procedure to create the following additional SSIDs:
   - IT_WiFi

Name	IT_WiFi
Traffic mode	Bridge
SSID	IT_WiFi
Security mode	WPA2 Enterprise
Authentication	Local
User group	IT
Optional VLAN ID	20

   - Engineering_WiFi

Name	Engineering_WiFi
Traffic mode	Bridge
SSID	Engineering _WiFi
Security mode	WPA2 Enterprise
Authentication	Local
User group	Engineering
Optional VLAN ID	30

The SSIDs are created.



Name	SSID	Traffic Mode	Security	VLAN ID	Schedule	Status
IT_WiFi	IT_WiFi (IT_WiFi)	Local Bridge	WPA2 Enterprise	20	always	Up
EngineeringWiFi	Engineering_WiFi (Engin...	Local Bridge	WPA2 Enterprise	30	always	Up
Staff_WIFI	Staff_WiFi (Staff_WIFI)	Local Bridge	WPA2 Enterprise	70	always	Up

AP profile

The AP profile defines the radio settings, such as which channels and SSIDs to broadcast.

To configure an AP profile:

1. Go to *WiFi & Switch controller > FortiAP Profiles*, and *+Create New*.
2. Complete the following options:

Name	Provide a name for the profile. We will use *Corp_Wireless*
Platform	Select the platform of the AP units you are deploying.
Indoor / Outdoor	Leave the location at *Default (Indoor)*.
Country / Region	Adjust if necessary.

3. Define the radio(s):
   We will use two radios to provide both 2.4GHz and 5.0GHz access.
   a. Under *Radio 1*, set the following options:

Mode	Access Point
Radio resource provision	Enable
Band	2.4GHz, 802.11n/g
Channels	All
Transmit power	100%
SSIDs	Bridge

   b. Under *Radio 2*, set the following options:

Mode	Access Point
Radio resource provision	Enable
Band	5GHz, 802.11ac/n/a
Channels	All
Transmit power	100%
SSIDs	Bridge

4. Click *OK*.

Managed access points (APs)

Configure the access point, and then connect the AP to the managed switch. If the AP is not automatically authorized, authorize it.

You can configure the AP before you connect it to the managed switch.

To configure the managed AP:

1. On FortiGate, go to *WiFi & Switch Controller > Managed FortiAPs*, and click *Create New > Managed AP*.
2. Set the following options:

Serial Number	Provide the serial number of the AP.
Name	Enter a descriptive name. It is recommended to include the physical location in the AP name.
FortiAP profile	Select the FortiAP profile created earlier (*Corp_Wireless*).

3. Click *OK* to save.

To connect the managed AP:

1. On your managed switch, select a port for the FortiAP connection, and configure the interface as a trunk to allow the three VLANs used in the three SSIDs (20, 30, 70).
2. Physically connect the FortiAP to the switch port.
   Shortly after, the device will appear in the *WiFi & Switch Controller > Managed FortiAPs* pane on FortiGate.

To authorize the managed AP:

1. On FortiGate go to the *WiFi & Switch Controller > Managed FortiAPs*.
2. Right-click the FortiAP, and click *Authorize*, if it was not automatically authorized .

Security

When implementing security and access control, administrators must be aligned with the business and security needs of the company. This may be different for each company, depending on the industry and sector in which they operate. A financial institute will have stricter security controls than a small logistics company for example. Key differentiators are the value of the data held and the services provided.

Therefore, it is important for businesses to assess and evaluate their data and infrastructure and build security policies around that. What are the most important data and where are they stored? This can be user data, code, other digital assets, and intellectual property. Who can access these data? What are possible vectors in which these data can be stolen or compromised? What are services that the company provides? Where are these hosted? What are possible vectors in which these servers can be hacked?

In our hypothetical software engineering company, servers and services that store important data are either in the IT lab or Engineering lab. Therefore, these networks have restrictive access.

On another note, company policies might exist about internet access and the type of content that can be accessed. These policies should be considered by type of users and devices that will access the internet.

On the FortiGate, security is managed by customizing security profiles and firewall policies. The next sections demonstrate the recommendations for our hypothetical company.

Security profiles

Use the following procedures to create security profiles:

AntiVirus	See Creating antivirus profiles on page 40.
Web Filter	See Creating web filter profiles on page 40.
DNS	See Creating DNS Filter profiles on page 41.
Application Control	See Creating application control profiles on page 42.
Intrusion Prevention	See Creating intrusion prevention profiles on page 42.
VoIP	See Creating VoIP profiles on page 42.

Creating antivirus profiles

Clone the default antivirus profile to create a new profile, and then configure the settings.

To configure antivirus profiles:

1. Go to *Security Profiles > AntiVirus*.
2. Select the default profile, and click *Clone*.
3. Type a name for the clone, such as *CORP_AV*, and click *OK*. The new profile is created.
4. Double-click the new profile to open it for editing, and set the following options:

Name	CORP_AV
Inspected Protocols	• HTTP • SMTP • POP3 • IMAP • FTP
AntiVirus scan	Enable
Send files to FortiSandbox for inspection	Suspicious Files Only
APT Protection Options	Enable
Use FortiSandbox database	Enable
Include mobile malware protection	Enable
Quarantine	Enable
FortiGuard outbreak prevention database	Block

5. Click *OK* to save the changes.

Creating web filter profiles

Clone the default web filter profile to create a new profile, and then configure the settings.

To configure web filter profiles:

1. Go to *Security Profiles > Web Filter*.
2. Select the default profile, and click *Clone*.
3. Type a name for the clone, such as *CORP_WF*, and click *OK*. The new profile is created.

4. Double-click the new profile to open it for editing, and set the following options:

Name	CORP_WF
FortiGuard Category Based Filter	Enable
Pre-configured filters	- In the *Potentially Liable* category, adjust each filter to have an action of *Block*. - In the *Adult/Mature Content* category, adjust each filter to have an action of *Block*. - In the *Bandwidth Consuming* category, adjust each filter to have an action of *Block*. - In the *Security Risk* category, adjust each filter to have an action of *Block*.
Static URL Filter	- Enable *Block invalid URLs*. - Enable *Block malicious URLs discovered by FortiSandbox*

5. Click *OK* to save the changes.

Creating DNS Filter profiles

Clone the default DNS Filter profile to create a new profile, and then configure the settings.

To configure DNS Filter profiles:

1. Go to *Security Profiles > DNS Filter*.
2. Select the default profile, and click *Clone*.
3. Type a name for the clone, such as *CORP_DNS*, and click *OK*. The new profile is created.
4. Double-click the new profile to open it for editing, and set the following options:

Name	CORP_DNS
Redirect botnet C&C requests to Block Portal	Enable
FortiGuard Category Based Filter	Enable
Pre-configured filters	- In the *Adult/Mature Content* category, adjust each filter to have an action of *Redirect to Block Portal*. - In the *Bandwidth Consuming* category, adjust the first four (4) filters to have an action of *Redirect to Block Portal*. - In the *Bandwidth Consuming* category, adjust the remaining filters to have an action of *Monitor*. - In the *General Interest – Business* category, adjust each filter to have an action of *Monitor*. - In the *General Interest – Personal* category, adjust each filter to have an action of *Monitor*. - In the *Potentially Liable* category, adjust each filter to have an action of *Redirect to Block Portal*.

5. Click *OK* to save the changes.

Creating application control profiles

Clone the default application control profile to create a new profile, and then configure the settings.

To configure application control profiles:

1. Go to *Security Profiles > Application Control*.
2. Select the default profile, and click *Clone*.
3. Type a name for the clone, such as *CORP_AC*, and click *OK*. The new profile is created.
4. Double-click the new profile to open it for editing, and set the following options:

Name	CORP_AC
All Categories	Adjust to *Monitor*.
P2P	Adjust to *Block*.
Proxy	Adjust to *Block*.

5. Click *OK* to save the changes.

Creating intrusion prevention profiles

Clone the default intrusion prevention profile to create a new profile, and then configure the settings.

To configure intrusion prevention profiles:

1. Go to *Security Profiles > Intrusion Prevention*.
2. Select the default profile, and click *Clone*.
3. Type a name for the clone, such as *CORP_IP*, and click *OK*. The new profile is created.
4. Double-click the new profile to open it for editing, and set the following options:

Name	CORP_IP
Block malicious URLs	Enable
Default filter (for SEV 3,4,5)	Adjust *Action* from *Default* to *Block*.
Scan Outgoing Connections to Botnet Sites	Adjust from *Disable* to *Block*.

5. Click *OK* to save the changes.

Creating VoIP profiles

You must use the CLI to create VoIP profiles.

Create a VoIP profile named CORP_VOIP, and ensure the configuration matches requirements for your VOIP service.

For details, see the *FortiOS Administration Guide*.

Firewall policy

Use the following procedures to create firewall policies for the different types of network traffic:

Corporate to internet	See Creating a corporate to internet policy on page 43.
Lab to internet	See Creating a lab to internet policy on page 43.
Phones to server	See Creating a phones to server policy on page 44.
IoT to internet	See Creating an IOT to internet policy on page 45.
Employee corporate services	See Creating an employee corporate services policy on page 45.
Engineering to engineering lab	See Creating an engineering to engineering lab policy on page 46.
IT to IT lab	See Creating an IT to IT lab policy on page 46.

Creating a corporate to internet policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	CORP_to_INTERNET
Incoming Interface	VLAN20, VLAN30, VLAN40
Outgoing Interface	WAN1
Source	IT_net, ENG_net, SALES_net
Destination*	!RFC-1918
Service	ALL
Schedule	Always
Action	Accept
NAT	Use Outgoing Interface Address
Security Profiles	CORP_AV, CORP_WF, CORP_DNS, CORP_AC, CORP_IP
Logging Options	All Sessions

* After saving the policy, right-click it to select >_Edit in CLI. From the CLI, enter set dstaddr-negate enable. This will change the destination to NOT RFC-1918 addresses.

Creating a lab to internet policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	LAB_to_INTERNET
Incoming Interface	VLAN21, VLAN31

Outgoing Interface	WAN1
Source	IT _LAB_net, ENG_LAB_net
Destination	!RFC-1918
Service	ALL
Schedule	Always
Action	Accept
NAT	Use Outgoing Interface Address
Security Profiles	You may use the same profiles as the above policies, however it may be necessary to adjust some profiles to allow for less restrictions as necessitated by the lab requirements.
Logging Options	All Sessions

Creating a phones to server policy

To create a firewall policy:

1. Go to *Policy & Objects* > *Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	PHONES_to_SERVER
Incoming Interface	VLAN60
Outgoing Interface	VLAN50
Source	VOIP_net
Destination	CORP_SRV ^
Service	VOIP *
Schedule	Always
Action	Accept
NAT	NO
Security Profiles	CORP_VOIP
Logging Options	All Sessions

* There are several VoIP services built in to the FortiGate. You should select the protocol(s) used by your company (for example, SIP, H323, and so on).

^ If you are using an external VoIP service, you must adjust the destination and outgoing interface to reflect the server location.

Creating an IOT to internet policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	IOT_to_INTERNET
Outgoing Interface	WAN1
Source	IOT_net
Destination	!RFC-1918
Service	ALL
Schedule	Always
Action	Accept
NAT	Use Outgoing Interface Address
Security Profiles	You may use the configured CORP_ profiles; however, it may be necessary to increase security here to account for staff BYOD, which may not have the same security measures as corporate provided devices (for example, antivirus, patching, and so on).
Logging Options	All Sessions

Creating an employee corporate services policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	EMPLOYEE_CORP_SERVICES
Incoming Interface	VLAN20, VLAN30, VLAN40,VLAN70
Outgoing Interface	VLAN50
Source	SALES_net, ENG_net, SALES_net, IOT_net
Destination	CORP_SRV
Service	Windows AD
Schedule	Always
Action	Accept
NAT	NO
Security Profiles	CORP_AV, CORP_WF, CORP_DNS, CORP_AC, CORP_IP
Logging Options	All Sessions

Creating an engineering to engineering lab policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	Engineering_to_ENG_LAB
Incoming Interface	VLAN30
Outgoing Interface	VLAN31
Source	ENG_net
Destination	ENG_LAB_net
Service	ENG_SERVICES
Schedule	Always
Action	Accept
NAT	NO
Security Profiles	CORP_AV, CORP_WF, CORP_DNS, CORP_AC, CORP_IP
Logging Options	All Sessions

Creating an IT to IT lab policy

To create a firewall policy:

1. Go to *Policy & Objects > Firewall Policy*, and click *Create New*.
2. Set the following options, and click *OK*:

Name	IT_to_IT_LAB
Incoming Interface	VLAN20
Outgoing Interface	VLAN21
Source	IT_net
Destination	IT_LAB_net
Service	IT_SERVICES
Schedule	Always
Action	Accept
NAT	NO
Security Profiles	CORP_AV, CORP_WF, CORP_DNS, CORP_AC, CORP_IP
Logging Options	All Sessions

Security rating check

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

You can run the security rating check by navigating to *Security Fabric > Security Rating*, and selecting *Run Now* in the top right.

The security rating is divided into the following categories: Security Posture, Fabric Coverage, and Optimization.

After completing the deployment guide, the following security best practices will be met:

- Security Posture on page 47
- Fabric Coverage on page 48
- Optimization on page 48

Security Posture

Explicit Interface Policies	Polices that allow traffic should not use the *any* interface.
Admin Password Policy	A password policy should be set up for system administrators.
LAN Segment Servers	Servers should be placed behind interfaces classified as *DMZ*.
Endpoint Registration	Interfaces that are classified as *LAN* and are used by a policy should have Security Fabric Connection enabled.
DNS Helper	Ensure that a DNS session helper is configured for wildcard FQDN address resolvability.
LDAP Server Identity Check	Verify that `server-identity-check` is enabled for LDAP servers to ensure certificate validation takes place. While this is the default option in a clean install, it may not be set if upgrading from older FortiOS releases.
Unsecure Protocol - HTTP	Interfaces currently in use should not allow HTTP administrative access.
Unsecure Protocol - Telnet	Interfaces that are classified as *WAN* and are used by a policy should not allow Telnet administrative access.
Valid HTTPS Certificate - Administrative GUI	The administrative GUI should use a valid and secure certificate.
Interface Classification	All interfaces used by a policy should be classified as either *LAN*, *WAN*, or *DMZ*.
Detect Botnet Connections	Interfaces that are classified as *WAN* and are used by a policy should use an IPS sensor that blocks or monitors outgoing connections to botnet sites.
Device Discovery	Interfaces that are classified as *LAN* or *DMZ* and are used by a policy should have device detection enabled.
Centralized Logging & Reporting	Logging and reporting should be done in a centralized place.

FortiClient Vulnerabilities	All registered FortiClient devices should have no critical vulnerabilities.
Compatible Firmware	All devices in the Security Fabric should have compatible firmware versions.

One best practice is not met due to the missing dependency of a FortiSwitch:

VLAN Management	Non-FortiLink interfaces should not have multiple VLANs configured on them.

Fabric Coverage

FortiAP Firmware Versions	Non-FortiLink interfaces should not have multiple VLANs configured on them.
FortiCare Support	Appropriate devices should be registered with FortiCare and have valid support coverage.
Anti-Spam	Anti-Spam subscription should be valid.
AntiVirus	AntiVirus subscription should be valid.
Firmware & General Updates	Firmware & General Updates subscription should be valid.
IPS	IPS subscription should be valid.
Outbreak Prevention	Outbreak Prevention subscription should be valid.
Web Filtering	Web Filtering subscription should be valid.
Third Party Router & NAT Devices	No third-party router or NAT devices should be detected in the network.
Unauthorized FortiAPs	All discovered FortiAPs should be authorized or disabled.
Advanced Threat Protection	Suspicious files should be submitted to FortiSandbox appliance or FortiGate Cloud Sandbox for inspection.
Compatible Firmware	All devices in the Security Fabric should have compatible firmware versions.
FortiSandbox	All FortiGates in the Security Fabric can connect to their configured FortiSandbox.

One best practice is not met due to the missing dependency of an additional subscription:

Security Rating	Security Rating subscription should be valid.

Optimization

Managed Switch Capacity Exceeded on FortiGate	Number of managed FortiSwitch devices should not exceed 80% of the FortiGate's maximum capacity (table size).
FortiSwitch Strict Tunnel Mode	Should enable strict tunnel mode to enforce switch controller to use cipher set in FortiOS.

Policy Inspection Mode	Policies should not combine proxy and flow inspection modes.
Compatible Firmware	All devices in the Security Fabric should have compatible firmware versions.
Unused Policies	All policies should be used.

More information

This section outlines the products used in this guide and provides links to additional documentation.

Products used

The following Fortinet product models and firmware were used in this guide:

Product	Model	Firmware
FortiGate	70F	7.0.9
FortiGate Cloud		
FortiGate Cloud Sandbox		
FortiAP	U312EV	6.2.4

Documentation references

FortiGate

- FortiOS 7.2 Administration Guide:
  - Configuring FortiAnalyzer Cloud services
  - Security rating
  - RADIUS servers
  - Restricting RADIUS user groups to match selective users on the RADIUS server
- Best practices:
  - Logging and reporting
  - Security profiles
  - SSL/TLS deep inspection
  - Security rating

FortiAP

- FortiAP / FortiWiFi 7.2 Configuration Guide:
  - Wireless network configuration

Solution Hub

- FortiCloud

4-D Resources

- Secure Access: Wireless

www.fortinet.com

01-700-858757-20221216