

DO NOT REPRINT
© FORTINET



FortiGate Security Study Guide

for FortiOS 7.2

FORTINET®
Training Institute

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

<https://www.fortinet.com/nse-training>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

<https://helpdesk.training.fortinet.com/support/home>



TABLE OF CONTENTS

Change Log.....	4
01 Introduction and Initial Configuration.....	5
02 Firewall Policies.....	47
03 Network Address Translation.....	94
04 Firewall Authentication.....	134
05 Logging and Monitoring.....	172
06 Certificate Operations.....	213
07 Web Filtering.....	251
08 Application Control.....	293
09 Antivirus.....	338
10 Intrusion Prevention and Denial of Service.....	381
11 Security Fabric.....	422

Change Log

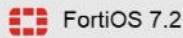
This table includes updates to the *FortiGate Security 7.2 Study Guide* dated 6/13/2022 to the updated document version dated 8/23/2022.

Change	Location
Various formatting fixes	Entire Guide
Fixed notes ("The DNS connection matches central SNAT "policy ID 2")	Lesson 3 slide 28
Fixed check mark on knowledge check, question 2	Lesson 7 slide 8

DO NOT REPRINT**© FORTINET**

FortiGate Security

Introduction and Initial Configuration



Last Modified: 13 June 2022

In this lesson, you will learn about FortiGate administration basics and the components within FortiGate that you can enable to extend functionality. This lesson also includes details about how and where FortiGate fits into your existing network architecture.

DO NOT REPRINT**© FORTINET**

Lesson Overview



High-Level Features



Setup Decisions



Basic Administration



Fundamental Maintenance

In this lesson, you will explore the topics shown on this slide.

DO NOT REPRINT**© FORTINET**

High-Level Features

Objectives

- Identify the platform design features of FortiGate
- Identify features of FortiGate in virtualized networks and the cloud
- Understand FortiGate security processing units (SPU)

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying the platform design features of FortiGate, FortiGate features in virtualized networks and the cloud, as well as the FortiGate security processing units, you will be able to describe the fundamental components of FortiGate and explain the types of tasks that FortiGate can perform.

DO NOT REPRINT**© FORTINET**

The Modern Context of Network Security

- Firewalls are more than gatekeepers on the network perimeter
- Today's firewalls are designed in response to multifaceted and multidevice environments with no identifiable perimeter:
 - Mobile workforce
 - Partners accessing your network services
 - Public and private clouds
 - Internet of things (IoT)
 - Bring your own device (BYOD)
- Firewalls are expected to perform different functions within a network
 - Different deployment modes:
 - Distributed enterprise firewall
 - Next-generation firewall
 - Internal segmentation firewall
 - Data center firewall
 - DNS, DHCP, web filter, intrusion prevention system (IPS), and so on



© Fortinet Inc. All Rights Reserved.

4

In the past, the common way of protecting a network was securing the perimeter and installing a firewall at the entry point. Network administrators used to trust everything and everyone inside the perimeter.

Now, malware can easily bypass any entry-point firewall and get inside the network. This could happen through an infected USB stick, or an employee's compromised personal device being connected to the corporate network. Additionally, because attacks can come from inside the network, network administrators can no longer inherently trust internal users and devices.

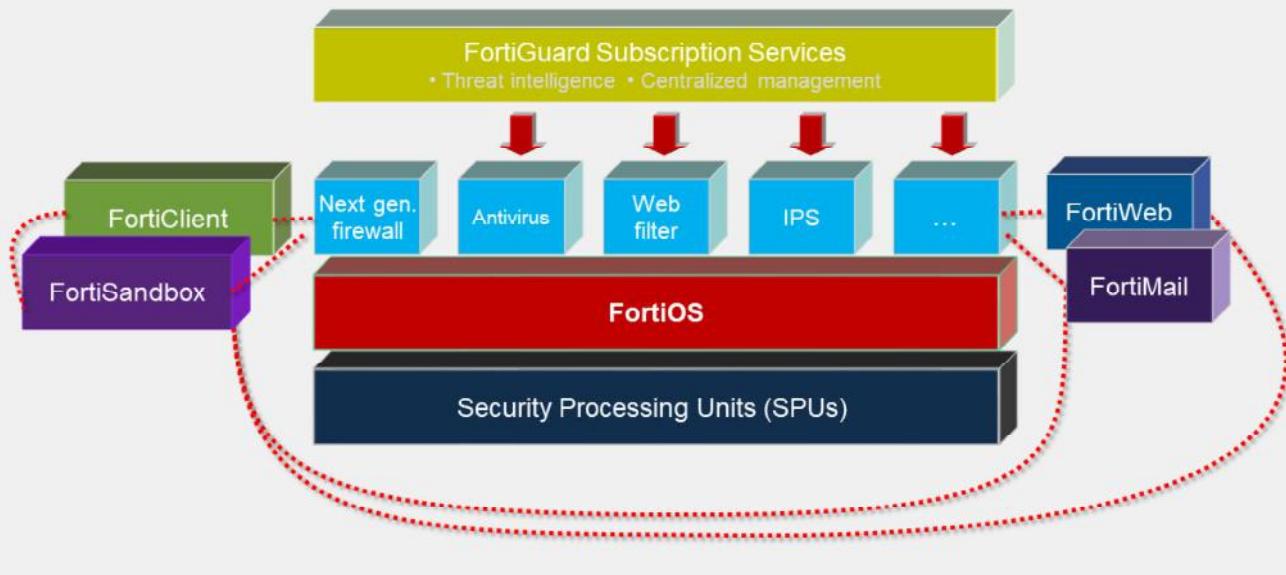
What's more, today's networks are highly complex environments whose borders are constantly changing. Networks run vertically from the LAN to the internet, and horizontally from the physical network to a private virtual network and to the cloud. A mobile and diverse workforce (employees, partners, and customers) accessing network resources, public and private clouds, the IoT, and BYOD programs all conspire to increase the number of attack vectors against your network.

In response to this highly complex environment, firewalls have become robust multifunctional devices that counter an array of threats to your network. Thus, FortiGate can act in different modes or roles to address different requirements. For example, FortiGate can be deployed as a data center firewall whose function is to monitor inbound requests to servers and to protect them without increasing latency for the requester. Or, FortiGate can be deployed as an internal segmentation firewall as a means to contain a network breach.

FortiGate can also function as DNS and DHCP servers, and be configured to provide web filter, antivirus, and IPS services.

DO NOT REPRINT
© FORTINET

Platform Design



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

5

In the architecture diagram shown on this slide, you can see how FortiGate platforms add strength, without compromising flexibility. Like separate, dedicated security devices, FortiGate is still *internally* modular. Plus:

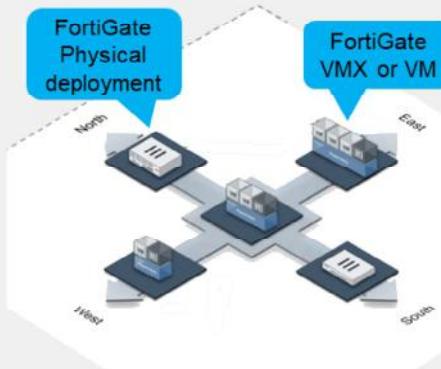
- **Devices add duplication.** Sometimes, dedication *doesn't* mean efficiency. If it's overloaded, can one device borrow free RAM from nine others? Do you want to configure policies, logging, and routing on 10 separate devices? Does 10 times the duplication bring you 10 times the benefit, or is it a hassle? For smaller to midsize businesses or enterprise branch offices, unified threat management (UTM) is often a superior solution, compared to separate dedicated appliances.
- **FortiGate hardware isn't just off-the-shelf.** It's carrier-grade. Most FortiGate models have one or more specialized circuits, called ASICs, that are engineered by Fortinet. For example, a CP or NP chip handles cryptography and packet forwarding more efficiently. Compared to a single-purpose device with only a CPU, FortiGate can have dramatically better performance. This is especially critical for data centers and carriers where throughput is business critical.
(The exception? Virtualization platforms—VMware, Citrix Xen, Microsoft, or Oracle Virtual Box—have general-purpose vCPUs. But, virtualization might be worthwhile because of other benefits, such as distributed computing and cloud-based security.)
- **FortiGate is flexible.** If all you need is fast firewalling and antivirus, FortiGate won't require you to waste CPU, RAM, and electricity on other features. In each firewall policy, you can enable or disable UTM and next-generation firewall modules. Also, you won't pay more to add VPN seat licenses later.
- **FortiGate cooperates.** A preference for open standards instead of proprietary protocols means less vendor lock-in and more choice for system integrators. And, as your network grows, FortiGate can leverage other Fortinet products, such as FortiSandbox and FortiWeb, to distribute processing for deeper security and optimal performance—a total Security Fabric approach.

DO NOT REPRINT

© FORTINET

Topology in the Cloud

- Deploy FortiGate in **virtualized networks**
 - FortiGate VM – Same features as physical appliance except SPUs
- VMs or physical appliances
 - Configuration is essentially the same



FortiGate VM Specifications

Licenses	Max. 1 / 2 / 4 / 8 vCPU
Hypervisor	VMware, Hyper-V, KVM, Citrix Xen Server, Open Source Xen, Azure, Amazon AWS BYOL & on-demand
Memory	Max. 1/4/8/12 GB
10/100/1000 Interfaces	2-4 virtual NICs
Storage Capacity	40+ GB

FortiGate VMs have the same features as physical FortiGate devices, *except* for hardware acceleration. Why? First, the hardware abstraction layer software for hypervisors is made by VMware, Xen, and other hypervisor manufacturers, *not* by Fortinet. Those other manufacturers don't make the Fortinet proprietary SPU chips. But there is another reason, too. The purpose of generic virtual CPUs and other virtual chips for hypervisors is to abstract the hardware details. That way, all VM guest OSs can run on a common platform, no matter the different hardware on which the hypervisors are installed. Unlike vCPUs or vGPUs that use generic, *non-optimal* RAM and vCPUs for abstraction, SPU chips are specialized *optimized* circuits. Therefore, a virtualized ASIC chip would not have the same performance benefits as a physical SPU chip.

If performance on equivalent hardware is less, you may wonder why anyone would use a FortiGate VM. In large-scale networks that change rapidly and may have many tenants, equivalent processing power and distribution may be achievable using larger amounts of cheaper, general purpose hardware. Also, trading some performance for other benefits may be worth it. You can benefit from faster network and appliance deployment and teardown.

Either VMs or physical appliances (low or high-end models), the configuration of the security instances is essentially identical, using same FortiOS version and FortiGuard real-time threat intelligence.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which is a more accurate description of a modern firewall?
 - A. A device that inspects network traffic at an entry point to the internet and within a simple, easily defined network perimeter
 - B. A multifunctional device that inspects network traffic from the perimeter or internally, within a network that has many different entry points

2. Which solution specific to Fortinet enhances performance and reduces latency for specific features and traffic?
 - A. Acceleration hardware, called SPUs
 - B. Increased RAM and CPU power

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Fundamental Maintenance

Good job! You now understand some of the high-level features of FortiGate.

Now, you will learn how to perform the initial setup of FortiGate and learn about why you might decide to use one configuration over another.

DO NOT REPRINT
© FORTINET

Setup Decisions

Objectives

- Identify the factory default settings
- Understand the FortiGate relationship with FortiGuard and distinguish between live queries and package updates

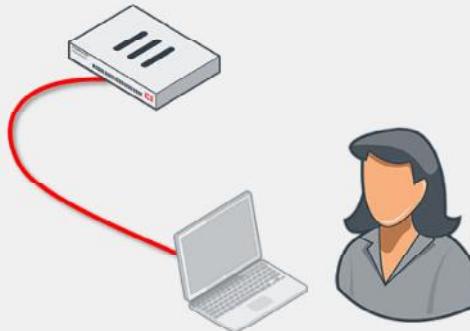
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in setting up FortiGate, you will be able to use the device effectively in your own network.

DO NOT REPRINT**© FORTINET**

Factory Default Settings

- IP: 192.168.1.99/24
 - MGMT interface on high-end and mid-range models
 - Port1 or internal interface on entry-level models
- PING, HTTPS, and SSH protocol management enabled
- Built-in DHCP server is enabled on port1 or internal interface
 - Only on entry-level models that support DHCP server
- Default login:
User: admin
Password: (blank)
 - Both are case sensitive
 - Modify the default (blank) password
- Can access FortiGate on the CLI
 - Console: without network
 - CLI console widget and terminal emulator, such as PuTTY or Tera Term



Network address translation (NAT) mode is the default operation mode. What are the other factory default settings? After you've removed FortiGate from its box, what do you do next?

Now you'll take a look at how you set up FortiGate.

Attach your computer network cable to port1 or the internal switch ports (on the entry-level model). For high-end and mid-range models, connect to the MGMT interface. In most entry-level models, there is a DHCP server on that interface, so, if your computer's network settings have DHCP enabled, your computer should automatically get an IP, and you can begin setup.

To access the GUI on FortiGate or FortiWifi, open a web browser and visit <https://192.168.1.99>.

The default login information is public knowledge. Never leave the default password blank. Your network is only as secure as your FortiGate admin account. Once you logged in with default login details, you'll see a message to change the default blank password for the admin user password. Before you connect FortiGate to your network, you should set a complex password. You'll also be asked to apply additional configuration such as hostname, dashboard setup, register with FortiCare, and so on.

All FortiGate models have a console port and/or USB management port. The port provides CLI access without a network. You can access the CLI using the CLI console widget on the GUI, or from a terminal emulator, such as PuTTY or Tera Term.

DO NOT REPRINT
© FORTINET

FortiGuard Subscription Services

- Internet connection and contract required
- Provided by FortiGuard Distribution Network (FDN)
 - Major data centers in North America, Asia, and Europe
 - Or, from FDN through your FortiManager
 - FortiGate prefers the data center in nearest time zone, but will adjust by server load
- Package updates: FortiGuard antivirus and IPS
 - update.fortiguard.net
 - TCP port 443 (SSL)
- Live queries: FortiGuard web filtering, DNS filtering, and antispam
 - service.fortiguard.net for proprietary protocol on UDP port 53 or 8888
 - securewf.fortiguard.net for HTTPS over port 443, 53 or, 8888
- FortiOS uses FortiGuard server for DNS request
 - By default, uses DNS over TLS (DoT) to secure dns traffic



Some FortiGate services connect to other servers, such as FortiGuard, in order to work. FortiGuard Subscription Services provide FortiGate with up-to-date threat intelligence. FortiGate uses FortiGuard by:

- Periodically requesting packages that contain a new engine and signatures
- Querying the FDN on an individual URL or host name

By default, the FortiGuard server location is set to anywhere FortiGate selects a server based on server load, from any part of the world. However, you have the option to change the FortiGuard server location to USA. In this case, FortiGate selects a USA-based FortiGuard server.

Queries are real-time; that is, FortiGate asks the FDN every time it scans for spam or filtered websites. FortiGate queries, instead of downloading the database, because of the size and frequency of changes that occur to the database. Also, you can select queries to use UDP or HTTPs for transport; the protocols are not designed for fault tolerance, but for speed. So, queries require that your FortiGate device has a reliable internet connection.

Packages, like antivirus and IPS, are smaller and don't change as frequently, so they are downloaded (in many cases) only once a day. They are downloaded using TCP for reliable transport. After the database is downloaded, their associated FortiGate features continue to function, even if FortiGate does not have reliable internet connectivity. However, you should still try to avoid interruptions during downloads—if your FortiGate device must try repeatedly to download updates, it can't detect new threats during that time.

When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers.

DO NOT REPRINT**© FORTINET**

FortiGuard Subscription Services (Contd)

- FortiGuard third party SSL certificate verification and OCSP stapling check
 - Default FortiGuard access mode is *anycast*
 - Optimize the routing performance to the FortiGuard servers
 - FortiGate gets a single IP address for the domain name of each FortiGuard service
 - FortiGuard servers query the CA OCSP responder every four hours
 - Enforce a connection to use protocol HTTPS and port 443

Server	Domain name and IP address
Object download	globalupdate.fortinet.net - 173.243.140.6
Querying service (webfiltering, antispam)	globalguardservice.fortinet.net - 173.243.140.16
FortiGate Cloud logging	globallogctrl.fortinet.net - 173.243.132.25
FortiGate Cloud management	globalmgrctrl.fortinet.net - 173.243.132.26
FortiGate Cloud messaging	globalmsgctrl.fortinet.net - 173.243.132.27
FortiGate Cloud sandbox	globalaptctrl.fortinet.net - 184.94.112.22
The productapi used by OVPN registration and GUI icon download	globalproductapi.fortinet.net - 66.35.17.252

Now, third-party SSL certificate verification and OCSP stapling check has been implemented for all FortiGuard servers. By default, the FortiGuard access mode is *anycast* on FortiGate, to optimize the routing performance to the FortiGuard servers. The FortiGuard server has one IP address to match its domain name. FortiGate connects with a single server address, regardless of where the FortiGate device is located.

The domain name of each FortiGuard service is the common name in the certificate of that service. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that FortiGate can always validate the FortiGuard server certificate efficiently. FortiGate will complete the TLS handshake only with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status results in a failed SSL connection.

The FortiGuard servers query the OCSP responder of the CA every four hours and update its OCSP status. If FortiGuard is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days.

FortiGate aborts the connection to the FortiGuard server if:

- The CN in the server certificate does not match the domain name resolved from the DNS.
- The OCSP status is not good.
- The issuer-CA is revoked by the root-CA.

The FortiGuard access mode *anycast* setting forces the rating process to use protocol HTTPS, and port 443. The table on this slide shows a list of some of the FortiGuard servers and their domain names and IP addresses.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which protocol does FortiGate use to download antivirus and IPS packages?
 A. UDP
 B. TCP

2. How does FortiGate check content for spam or malicious websites?
 A. Live queries to FortiGuard over UDP or HTTPS
 B. Local verification using a downloaded web filter database locally on FortiGate

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Fundamental Maintenance

Good job! You now understand how to perform the initial setup of FortiGate and why you might decide to use one configuration over another. Now, you will learn about basic administration.

DO NOT REPRINT**© FORTINET**

Basic Administration

Objectives

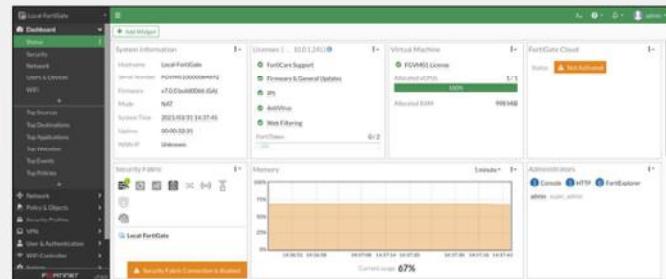
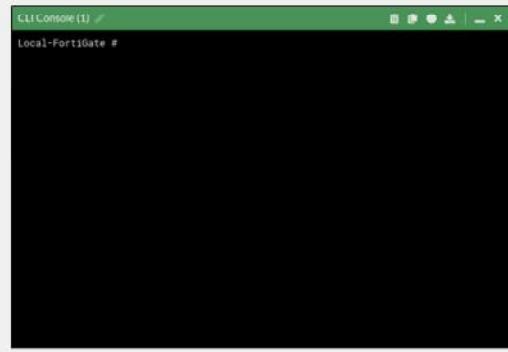
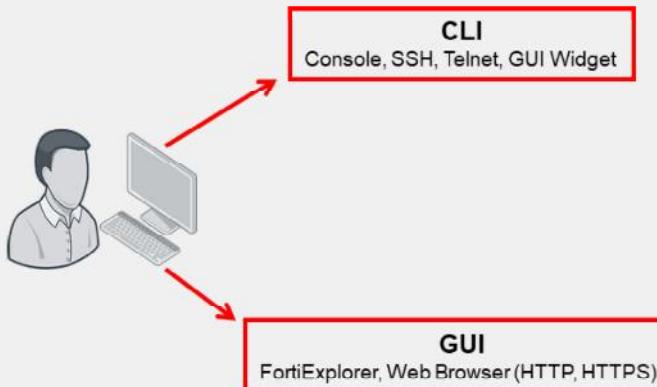
- Manage administrator profiles
- Manage administrative users
- Define the configuration method for administrative users
- Define and describe VDOMs
- Control administrative access to the FortiGate GUI and CLI
- Manage specific aspects of the network interfaces
- Describe VLANs and VLAN tagging
- Enable the DHCP and DNS services on FortiGate

After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic administration, you will be able to better manage administrative users and implement stronger security practices around administrative access.

DO NOT REPRINT
© FORTINET

Administration Methods



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

16

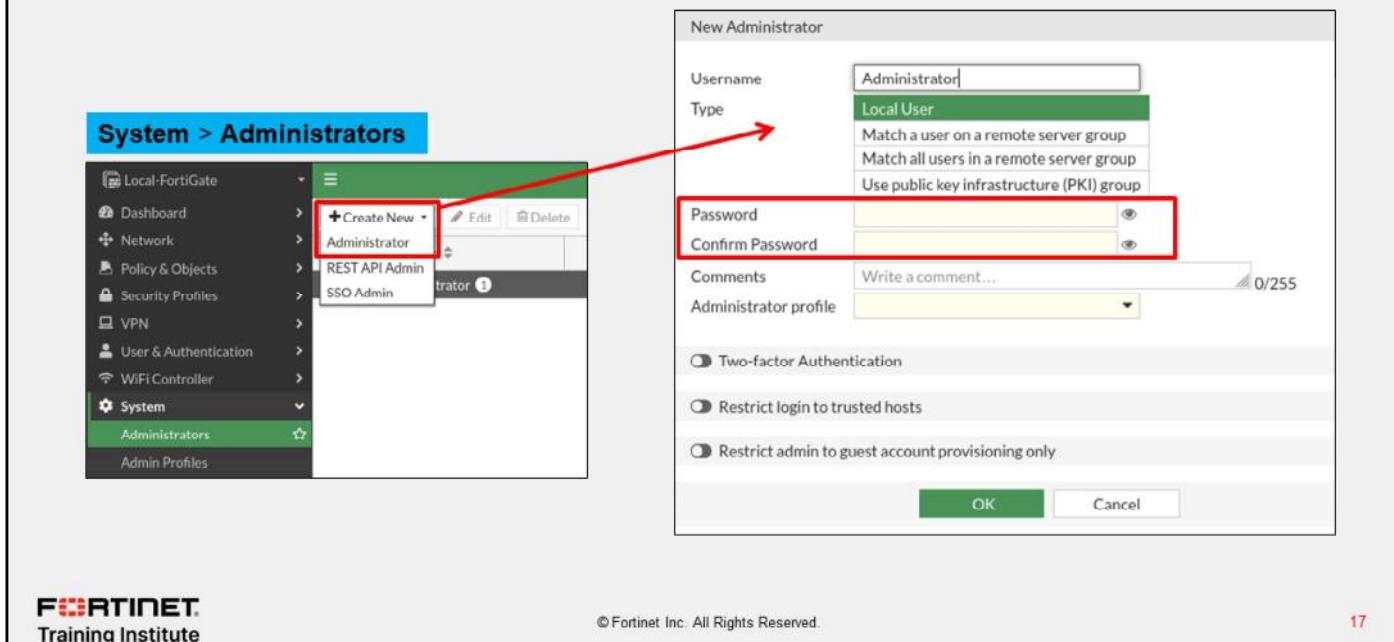
Most features are available on both the GUI and CLI, but there are a few exceptions. You can't view reports on the CLI. Also, advanced settings and diagnostic commands for super users are usually not available on the GUI.

As you become more familiar with FortiGate, and especially if you want to script its configuration, you might want to use the CLI in addition to the GUI. You can access the CLI through either the JavaScript widget on the GUI named **CLI Console**, or through a terminal emulator such as Tera Term (<http://ttssh2.sourceforge.jp/index.html.en>) or PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>). Your terminal emulator can connect through the network—SSH or telnet—or the local console port.

SNMP and some other administrative protocols are also supported, but they are read-only. You can't use them for basic setup.

DO NOT REPRINT
© FORTINET

Create an Administrative User



The screenshot shows the FortiGate Management Interface. On the left, there is a navigation tree under 'System > Administrators'. A red arrow points from the 'Create New' button in the tree to a larger window titled 'New Administrator' on the right. The 'New Administrator' window contains fields for 'Username' (set to 'Administrator'), 'Type' (set to 'Local User'), 'Password', and 'Confirm Password'. Below these are several optional checkboxes: 'Two-factor Authentication', 'Restrict login to trusted hosts', and 'Restrict admin to guest account provisioning only'. At the bottom are 'OK' and 'Cancel' buttons.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

Whichever method you use, start by logging in as admin. Begin by creating separate accounts for other administrators. For security and tracking purposes, it is a best practice for each administrator to have their own account.

In the **Create New** drop-down list, you can select either **Administrator** or **REST API Admin**. Typically, you will select **Administrator** and then assign an **Administrator Profile**, which specifies that user's administrative permissions. You could select **REST API Admin** to add an administrative user who would use a custom application to access FortiGate with a REST API. The application would allow you to log in to FortiGate and perform any task that your assigned **Administrator Profile** permits.

Other options not shown here, include:

- Instead of creating accounts on FortiGate itself, you could configure FortiGate to query a remote authentication server.
- In place of passwords, your administrators could authenticate using digital certificates that are issued by your internal certification authority server.

If you do use passwords, ensure that they are strong and complex. For example, you could use multiple interleaved words with varying capitalization, and randomly insert numbers and punctuation. Do not use short passwords, or passwords that contain names, dates, or words that exist in any dictionary. These are susceptible to brute force attack. To audit the strength of your passwords, use tools such as L0phcrack (<http://www.l0phcrack.com/>) or John the Ripper (<http://www.openwall.com/john/>). Risk of a brute force attack is increased if you connect the management port to the internet.

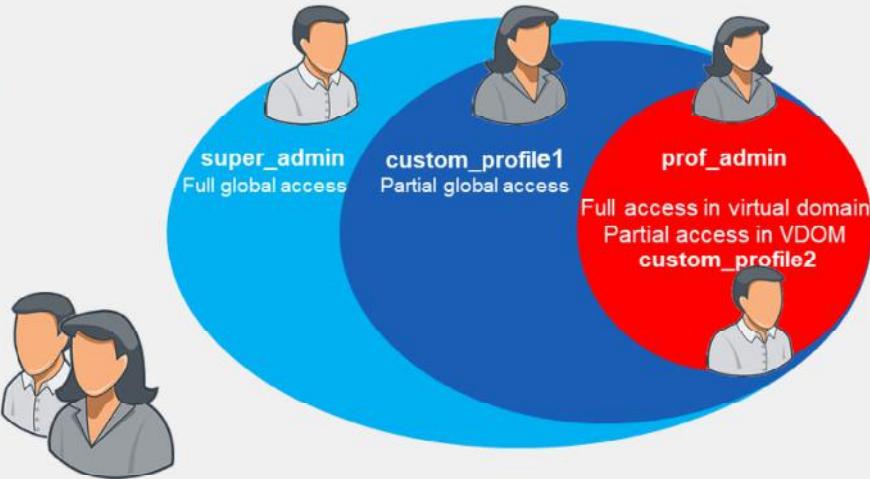
In order to restrict access to specific features, you can assign permissions.

DO NOT REPRINT
© FORTINET

Administrator Profiles

- Permissions

- Hierarchy



When assigning permissions to an administrator profile, you can specify read-and-write, read-only, or none to each area.

By default, there is a special profile named **super_admin**, which is used by the account named **admin**. You can't change it. It provides full access to everything, making the **admin** account similar to a root **superuser** account. The **prof_admin** is another default profile. It also provides full access, but unlike **super_admin**, it applies only to its virtual domain—not the global settings of FortiGate. Also, you can change its permissions.

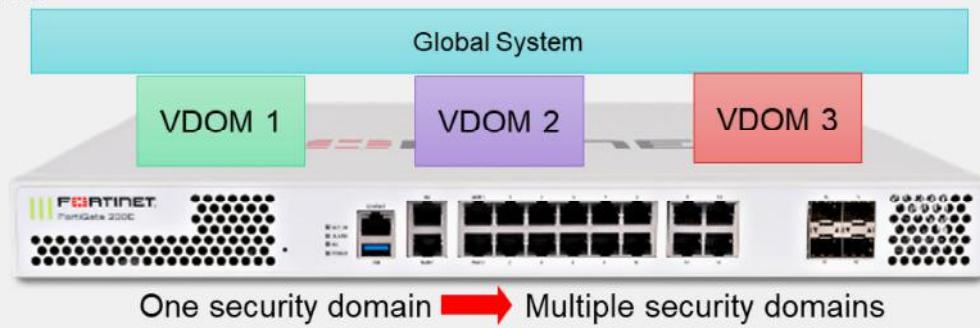
You aren't required to use a default profile. You could, for example, create a profile named **auditor_access** with read-only permissions. Restricting a person's permissions to those necessary for his or her job is a best practice, because even if that account is compromised, the compromise to your FortiGate device (or network) is not total. To do this, create administrator profiles, then select the appropriate profile when configuring an account.

The **Override Idle Timeout** feature allows the `admintimeout` value, under `config system accprofile`, to be overridden per access profile. You can configure administrator profiles to increase inactivity timeout and facilitate use of the GUI for central monitoring. Note that you can do this on a per-profile basis, to prevent the option from being unintentionally set globally. So, what are the effects of administrator profiles?

It's actually more than just read or write access. Depending on the type of administrator profile that you assign, an administrator may not be able to access the entire FortiGate device. For example, you could configure an account that can view only log messages. Administrators may not be able to access global settings outside their assigned virtual domain either. Virtual domains (VDOMs) are a way of subdividing the resources and configurations on a single FortiGate. Administrators with a smaller scope of permissions cannot create, or even view, accounts with more permissions.

DO NOT REPRINT
© FORTINET

VDOMs



- VDOMs split FortiGate into multiple virtual devices
 - They employ independent security policies, routing tables, and so on
- Packets are confined to same VDOM
- By default, FortiGate supports up to 10 VDOMs
 - High-end models allow for the purchase of additional VDOMs

What if, more than segmenting your network, you want to subdivide policies and administrators into multiple security domains?

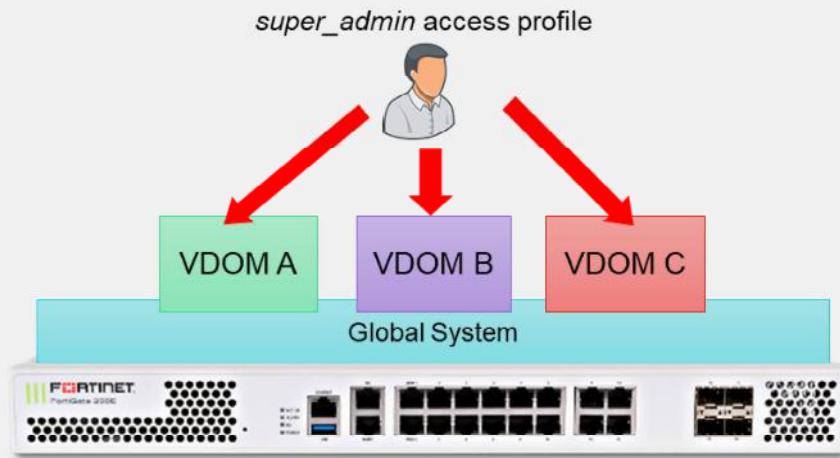
In that case, you can enable FortiGate VDOMs, which split your FortiGate into multiple logical devices. Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, UTM inspection, and secure communication devices.

DO NOT REPRINT**© FORTINET**

VDOM Administration

- Only the account named **admin** or accounts with the **super_admin** profile can configure and back up all VDOMs

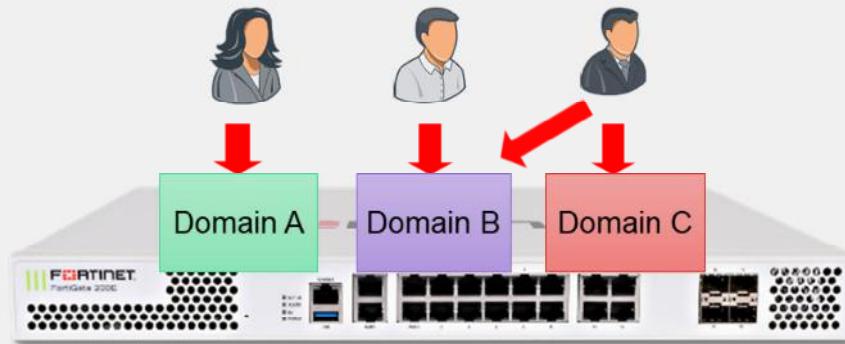


If you want to grant access to all VDOMs and global settings, select **super_admin** as the access profile when configuring the administrator account. Similar to the account named **admin**, this account can configure all VDOMs.

DO NOT REPRINT
© FORTINET

Per-VDOM Administration

- Other administrators can access only their *assigned* VDOMs
 - Cannot access the global settings



In most cases, you start by creating one administrator account per VDOM. That administrator is chiefly responsible for that domain, including the configuration backups of that VDOM. In larger organizations, you may need to make multiple VDOM administrators. You can assign multiple administrators to each VDOM. You can subdivide permissions using access profiles, in order to follow best practices for segregation of duties.

The converse is also possible. If required, you can assign an administrator to multiple VDOMs.

DO NOT REPRINT**© FORTINET**

Resetting a Lost Admin Password

User: maintainer

Password: bcpb<serial-number>

All letters in <serial-number> *must* be upper case, for example, FGT60

- All FortiGate appliance models and some other Fortinet device types
- No maintainer procedure in VM, revert to snapshot or reprovision VM
- Only after hard power cycle
 - Soft cycle (reboot) does not work for security reasons
- Only during first 60 seconds *after boot* (varies by model)
 - **Tip:** Copy serial number into the terminal buffer, then paste
- Only through hardware console port
 - Requires physical access for security reasons
 - If compliance/risk of physical access requires, you can disable maintainer

```
config sys global  
    set admin-maintainer disable  
end
```



© Fortinet Inc. All Rights Reserved.

22

What happens if you forget the password for your `admin` account, or a malicious employee changes it?

This recovery method is available on all FortiGate devices and even some non-FortiGate devices, like FortiMail. There is no maintainer procedure in the VM. The administrator must revert to a snapshot or reprovision the VM and restore the configuration. It's a *temporary* account, only available through the local console port, and only after a hard reboot—disrupting power by unplugging or turning off the power, then restoring it. You must physically shut off FortiGate, then turn it back on, not reboot it through the CLI.

The `maintainer` login is available for login only for about 60 seconds after the restart completes (or less time on older models).

If you cannot ensure physical security, or have compliance requirements, you can disable the `maintainer` account. Use caution if you disable `maintainer` and then lose your `admin` password, because you cannot recover access to your FortiGate device. In order to regain access in this scenario, you will need to reload the device. This will reset to the device to its factory default settings.

DO NOT REPRINT

© FORTINET

Administrative Access—Trusted Sources

The screenshot illustrates the configuration and enforcement of trusted hosts for administrative access. On the left, a configuration dialog shows the 'Restrict login to trusted hosts' option selected, with 'Trusted Host 1' set to '10.0.1.10/32'. A red arrow points from this configuration to a table on the right where the 'System Administrator' entry is shown with 'Trusted Hosts' set to '10.0.1.10/32'. Below this, a callout box states: 'If admin attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message'. On the right, a login screen shows an 'Authentication failure' message, indicating that an attempt to log in from a different IP address was unsuccessful.

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator	10.0.1.10/32	super_admin	Local	Disabled

If admin attempts to log in to the FortiGate GUI from any IP other than 10.0.1.10, they receive this message

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

23

Another way to secure FortiGate is to define the hosts or subnets that are trusted sources from which to log in.

In this example, we have configured 10.0.1.10 as the only trusted IP for **admin** from which **admin** logs in. If **admin** attempts to log in from a machine with any other IP, they will receive an authentication failure message.

Note that if trusted hosts are configured on all administrators and an administrator is trying to log in from an IP address that is not set on any of the trusted hosts for any administrators, then the administrator will not get the login page but rather will receive the message: "Unable to contact server".

If you leave any IPv4 address as 0.0.0.0/0, it means that connections from any source IP will be allowed. By default, 0.0.0.0/0 is the configuration for the administrator, although you may want to change this.

Notice that each account can define its management host or subnet differently. This is especially useful if you are setting up VDOMs on FortiGate, where the VDOM administrators may not even belong to the same organization. Be aware of any NAT that occurs between the desired device and FortiGate. You can easily prevent an administrator from logging in from the desired IP address if it is later NATed to another address before reaching FortiGate, thus defeating the purpose of the trusted hosts.

DO NOT REPRINT
© FORTINET

Administrative Access—Ports and Password

- Port numbers are customizable
- Using only secure access (SSH, HTTPS) is recommended
- Default **Idle timeout** is five minutes

The screenshot shows the 'System > Settings' interface. The 'Administration Settings' section includes fields for HTTP port (80), Redirect to HTTPS (disabled), HTTPS port (443), HTTPS server certificate (self-sign), SSH port (22), Telnet port (23), and Idle timeout (5 minutes). The 'Password Policy' section includes fields for Password scope (Admin selected), Minimum length (8), Minimum number of new characters (0), Character requirements (disabled), Allow password reuse (disabled), and Password expiration (disabled).

You may also want to customize the administrative protocols port numbers.

You can choose whether to allow concurrent sessions. You can use concurrent sessions to avoid accidentally overwriting settings, if you usually keep multiple browser tabs open, or accidentally leave a CLI session open without saving the settings, then begin a GUI session and accidentally edit the same settings differently.

For better security, use only secure protocols, and enforce password complexity and changes.

The **Idle timeout** setting specifies the number of minutes before an inactive administrator session times out (default is five minutes). A shorter idle timeout is more secure, but increasing the timer can help reduce the chance of administrators being logged out while testing changes.

You can override the idle timeout setting per administrator profile using the **Override Idle Timeout** setting.

You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. The **Override Idle Timeout** setting allows the **admintimeout** value, under **config system accprofile**, to be overridden per access profile.

Note that you can do this on a per profile basis, to avoid the option from being unintentionally set globally.

DO NOT REPRINT
© FORTINET

Administrative Access—Protocols

- Enable acceptable management protocols on each interface independently:
 - Separate IPv4 and IPv6
 - IPv6 options hidden by default
- Also protocols where FortiGate is the destination IP:
 - Security Fabric Connection:
 - CAPWAP
 - FortiTelemetry
 - FMG-Access
 - FTM
 - RADIUS Accounting
- LLDP Support
 - Detecting an upstream Security Fabric FortiGate through LLDP

You've defined the management subnet—that is, the trusted hosts—for each administrator account. How do you enable or disable management protocols?

This is specific to each interface. For example, if your administrators connect to FortiGate only from port3, then you should disable administrative access on all other ports. This prevents brute force attempts and also insecure access. Your management protocols are HTTPS, HTTP, PING, and SSH. By default, the HTTP and TELNET option is not visible on the GUI.

Consider the location of the interface on your network. Enabling PING on an internal interface is useful for troubleshooting. However, if it's an external interface (in other words, exposed to the internet), then the PING protocol could expose FortiGate to a DoS attack. You should disable protocols that do not encrypt data flow, such as HTTP and TELNET. IPv4 and IPv6 protocols are separate. It's possible to have both IPv4 and IPv6 addresses on an interface, but only respond to pings on IPv6.

Security Fabric connection includes CAPWAP and FortiTelemetry. Protocols like FortiTelemetry are *not* for administrative access, but, like GUI and CLI access, they are protocols where the packets have FortiGate as a destination IP. Use the FortiTelemetry protocol specifically for managing FortiClient and the Security Fabric. Use the CAPWAP protocol for FortiAP, FortiSwitch, and FortiExtender when they are managed by FortiGate. Use the FMG-Access protocol specifically for communicating with FortiManager when that server is managing multiple FortiGate devices. Use the RADIUS accounting protocol when FortiGate needs to listen for and process RADIUS accounting packets for single sign-on authentication. FTM, or FortiToken Mobile push, supports second-factor authentication requests from a FortiToken mobile app.

When you assign the interface roles LAN or WAN to the appropriate interfaces, your FortiGate uses the Link Layer Discovery Protocol (LLDP) to detect if there's an upstream FortiGate in your network. If FortiGate discovers an upstream FortiGate, you're prompted to configure the upstream FortiGate device to join the Security Fabric.

DO NOT REPRINT

© FORTINET

Interface IPs

- In NAT mode, you can't use interfaces until they have an IP address:
 - Manually assigned
 - Automatic
 - DHCP
 - PPPoE

Network > Interfaces

Edit Interface

Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> Auto-managed by FortiIPAM
IP/Netmask	0.0.0.0/0.0.0.0
Secondary IP address	<input type="checkbox"/>

Edit Interface

Name	port5
Alias	
Type	Physical Interface
VRF ID	0
Role	Undefined
Address	
Addressing mode	<input type="radio"/> Manual <input checked="" type="radio"/> DHCP <input type="radio"/> Auto-managed by FortiIPAM
Retrieve default gateway from server	<input type="checkbox"/>
Distance	5
Override Internal DNS	<input type="checkbox"/>

When FortiGate is operating in NAT mode, every interface that handles traffic must have an IP address. When in NAT mode, FortiGate can use the IP address to source the traffic, if it needs to start or reply to a session, and as a destination address for devices trying to contact FortiGate or route traffic through it. There are multiple ways to get an IP address:

- Manually
- Automatically, using either DHCP or PPPoE (available on the CLI)

DO NOT REPRINT
© FORTINET

Interface Role Compared to Alias

- Role defines interface settings typically grouped together:
 - Prevents accidental misconfiguration
 - Four types:
 - WAN
 - LAN
 - DMZ
 - Undefined (show all settings)
 - Not in list of policies
- Alias is a friendly descriptor for the interface:
 - Used in list of policies to label interfaces by purpose

Network > Interfaces

Edit Interface

Name:	port3
Alias:	Internal_Network
Type:	Physical Interface
VRF ID:	0
Role:	LAN
Address:	10.0.1.254/255.255.255.0
IP/Netmask:	Secondary IP address

Policy & Objects > Firewall Policy

Create New **Edit** **Delete**

Name	From	To	Source	Destination
Full_Access	Internal_Network (port3)	port1	LOCAL_SUBNET	all
Implicit Deny	any	any	all	all

How many times have you seen network issues caused by a DHCP server—not client—enabled on the WAN interface?

You can configure the interface role. The roles shown on the GUI are the usual interface settings for that part of a topology. Settings that do not apply to the current role are hidden on the GUI. (All settings are always available on the CLI regardless of the role.) This prevents accidental misconfiguration.

For example, when the role is configured as **WAN**, there is no DHCP server and device detection configuration available. Device detection is usually used to detect devices internally on your LAN.

If there is an unusual case, and you need to use an option that's hidden by the current role, you can always switch the role to **Undefined**. This displays all options.

To help you remember the use of each interface, you can give them aliases. For example, you could call port3 **internal_network**. This can help to make your list of policies easier to comprehend.

DO NOT REPRINT

© FORTINET

VLANs



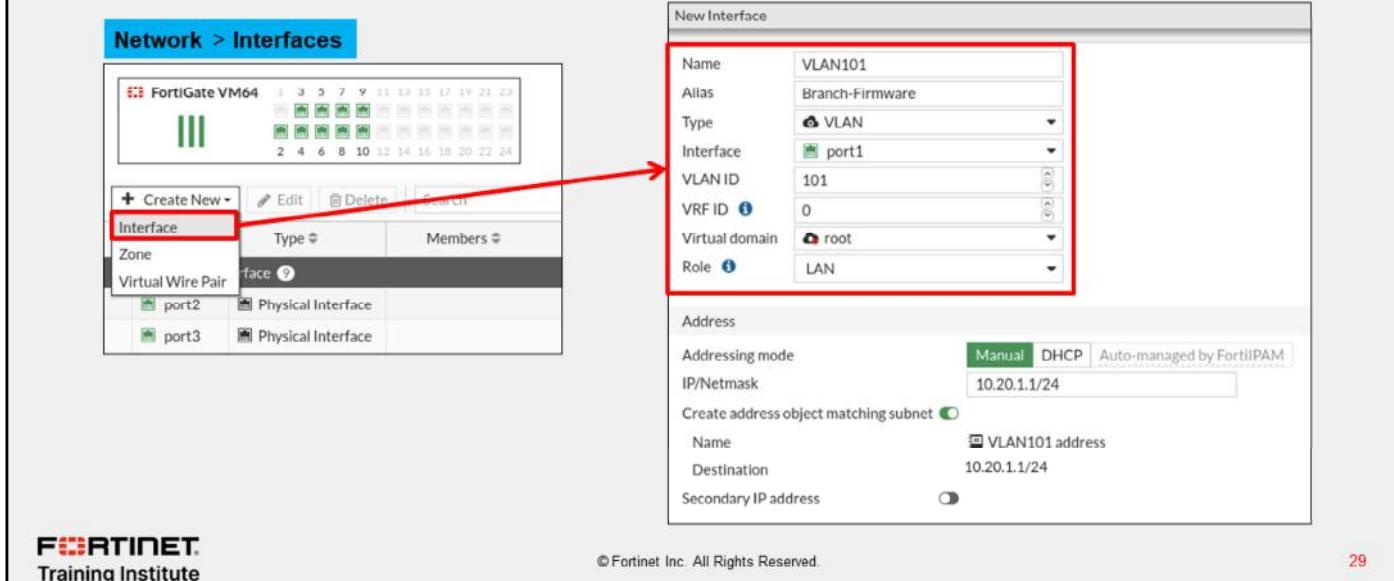
- *Logically* subdivide your physical Layer 2 network into smaller segments
 - Each segment forms a separate broadcast domain
 - VLAN tags added to frames to identify their network segments

VLANs split your physical LAN into multiple, logical LANs. In NAT operation mode, each VLAN forms a separate broadcast domain. Multiple VLANs can coexist in the same physical interface, provided they have different VLAN IDs. In this way, a physical interface is split into two or more logical interfaces. A tag is added to each Ethernet frame to identify the VLAN to which it belongs.

DO NOT REPRINT
© FORTINET

Creating VLANs

- Frames sent or received by the physical interface segment are never tagged; they belong to the *native VLAN*



The screenshot shows the FortiGate VM64 interface configuration screen. On the left, under 'Network > Interfaces', there is a table with columns for Interface, Type, and Members. A red arrow points from the 'Create New' button at the top left of this table to a larger 'New Interface' dialog box on the right. The 'New Interface' dialog has the following fields filled in:

Name	VLAN101
Alias	Branch-Firmware
Type	VLAN
Interface	port1
VLAN ID	101
VRF ID	0
Virtual domain	root
Role	LAN

Below these fields, there is an 'Address' section with an 'Addressing mode' dropdown set to 'Manual', an IP/Netmask field containing '10.20.1.1/24', and a 'Create address object matching subnet' checkbox. Underneath, there are fields for 'Name' (VLAN101 address) and 'Destination' (10.20.1.1/24), with a 'Secondary IP address' checkbox.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

29

To create a VLAN using the GUI, click **Create New**, select **Interface**, and then, in the **Type** drop-down list, select **VLAN**. You must specify the VLAN ID and the physical interface to which the VLAN will be bound. Frames that belong to interfaces of that type are always tagged. On the other hand, frames sent or received by the physical interface segment are never tagged. They belong to what is called the *native VLAN* (VLAN ID 0).

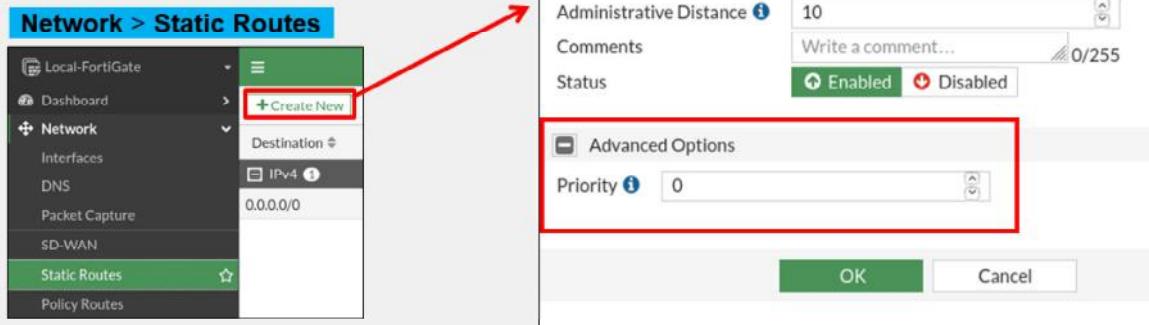
Note that in a multi-VDOM environment, the physical interface and its VLAN sub-interface can be in separate VDOMs.

DO NOT REPRINT

© FORTINET

Static Gateway

- Must be at least one default gateway
- If the interface is DHCP or PPPoE, the gateway can be added dynamically



Before you integrate FortiGate into your network, you should configure a default gateway.

If FortiGate gets its IP address through a dynamic method such as DHCP or PPPoE, then it should also retrieve the default gateway.

Otherwise, you must configure a static route. Without this, FortiGate will not be able to respond to packets outside the subnets directly attached to its own interfaces. It probably also will not be able to connect to FortiGuard for updates, and may not correctly route traffic.

You should make sure that FortiGate has a route that matches all packets (destination is 0.0.0.0/0), known as a default route, and forwards them through the network interface that is connected to the internet, to the IP address of the next router.

Routing completes the basic network settings that are required before you can configure firewall policies.

DO NOT REPRINT
© FORTINET

FortiGate as a DHCP Server

The screenshot shows the FortiGate Management Interface with three main windows:

- Edit Interface (port3):** Shows port3 configured as a Physical Interface with Role set to LAN. Address mode is Manual (HCP). IP address is 10.0.129.4.
- DHCP Server (port3):** Shows the built-in DHCP server enabled with address range 10.0.1.1-10.0.1.253, netmask 255.255.255.0, and lease time 604800 seconds. It also lists various provisioning options like NTP, DNS, and additional DHCP options.
- Create New IP Address Assignment Rule:** A modal dialog for creating a new rule. It includes fields for Type (MAC Address or DHCP Relay Agent), Description, Match Criteria (MAC address), Action (Assign IP, Block, Reserve IP), and IP (0.0.0.0).

A red arrow points from the "IP Address Assignment Rules" section in the DHCP Server window to the "Create New" button in the modal dialog.

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

31

Wireless clients are not the only ones that can use FortiGate as their DHCP server.

For an interface (such as port3), select the **Manual** option, enter a static IP, and then enable the **DHCP Server** option. Options for the built-in DHCP server appear, including provisioning features, such as DHCP options and IP address assignment rules. You can also block specific MAC addresses from receiving an IP address.

Note that the screenshot on the middle of the slide shows that you can create IP address assignment rules in the **IP Address Assignment Rule** section. The **IP Address Assignment Rule** section allows you to assign, block or reserve the IP address to the host. It also allows you to select actions for unknown MAC addresses. The default action is **Assign IP**; however, you can change the default action type to **Assign IP** or **Block**.

DO NOT REPRINT**© FORTINET**

FortiGate as a DNS Server

- Resolves DNS lookups from the internal network:
 - Enabled per interface
 - Not appropriate for internet service because of load, and therefore should not be public facing
- One DNS database can be shared by all FortiGate interfaces:
 - Can be separate per VDOM
- Resolution methods:
 - Forward: relay requests to the next server (in DNS settings)
 - Non-recursive: use FortiGate DNS database only to try to resolve queries
 - Recursive: use FortiGate DNS database first; relay unresolvable queries to next server (in DNS settings)



© Fortinet Inc. All Rights Reserved.

32

You can configure FortiGate to act as your local DNS server. You can enable and configure DNS separately on each interface.

A local DNS server can improve performance for your FortiMail device or other devices that use DNS queries frequently. If your FortiGate device offers DHCP to your local network, you can use DHCP to configure those hosts to use FortiGate as both the gateway and DNS server.

FortiGate can answer DNS queries in one of three ways:

- Forward: relays all queries to a separate DNS server (that you have configured in **Network > DNS**); that is, it acts as a DNS relay instead of a DNS server.
- Non-Recursive: replies to queries for items in the FortiGate DNS databases and does not forward unresolvable queries.
- Recursive: replies to queries for items in the FortiGate DNS databases and forwards all other queries to a separate DNS server for resolution.

You can configure all modes on the GUI or CLI.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. How do you restrict logins to FortiGate from only specific IP addresses?
 - A. Change the FortiGate management interface IP address.
 - B. Configure a trusted host.

2. As a best security practice when configuring administrative access to FortiGate, which protocol should you disable?
 - A. Telnet
 - B. SSH

3. When configuring FortiGate as a DNS server, which resolution method uses only the FortiGate DNS database to try to resolve queries?
 - A. Non-recursive
 - B. Recursive

DO NOT REPRINT**© FORTINET**

Lesson Progress

**High-Level Features****Setup Decisions****Basic Administration****Fundamental Maintenance**

Good job! You now have the knowledge needed to carry out some basic administrative tasks. You also know how to enable DHCP and DNS services on FortiGate.

Now, you will learn about fundamental maintenance.

DO NOT REPRINT**© FORTINET**

Fundamental Maintenance

Objectives

- Back up and restore system configuration files
- Understand the restore requirements for plaintext and encrypted configuration files
- Identify the current firmware version
- Upgrade firmware
- Downgrade firmware

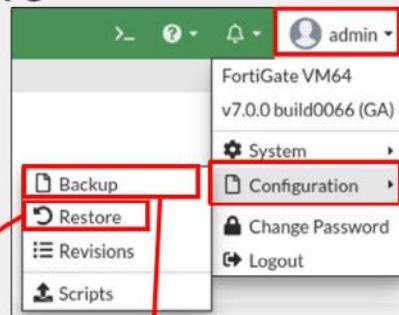
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the basic maintenance of FortiGate, you will be able to perform the vital activities of backing up and restoring configurations, upgrading and downgrading firmware, and ensuring that FortiGate remains reliably in service throughout its lifecycle.

DO NOT REPRINT
© FORTINET

Configuration File—Backup and Restore

- Configuration can be saved to an external device
 - Optional encryption
 - Can back up automatically
 - Upon logout
 - Not available on all models
- To restore a previous configuration, upload file
 - Reboots FortiGate



Restore System Configuration

Restore from Local PC USB Disk

File

Password

Backup System Configuration

Backup to Local PC USB Disk

Encryption

Password

Confirm password

Now that FortiGate has basic network settings and administrative accounts, you will learn how to back up the configuration. In addition to selecting the destination of the backup file, you can choose to encrypt or not to encrypt the backup file. Even if you choose not to encrypt the file, which is the default, the passwords stored in the file are hashed, and, therefore, obfuscated. The passwords that are stored in the configuration file would include passwords for the administrative users and local users, and preshared keys for your IPSec VPNs. It may also include passwords for the FSSO and LDAP servers.

The other option is to encrypt the configuration file with a password. Besides securing the privacy of your configuration, it also has some effects you may not expect. After encryption, the configuration file cannot be decrypted without the password and a FortiGate of the same model and firmware. This means that if you send an encrypted configuration file to Fortinet technical support, even if you give them the password, they cannot load your configuration until they get access to the same model of FortiGate. This can cause unnecessary delays when resolving your ticket.

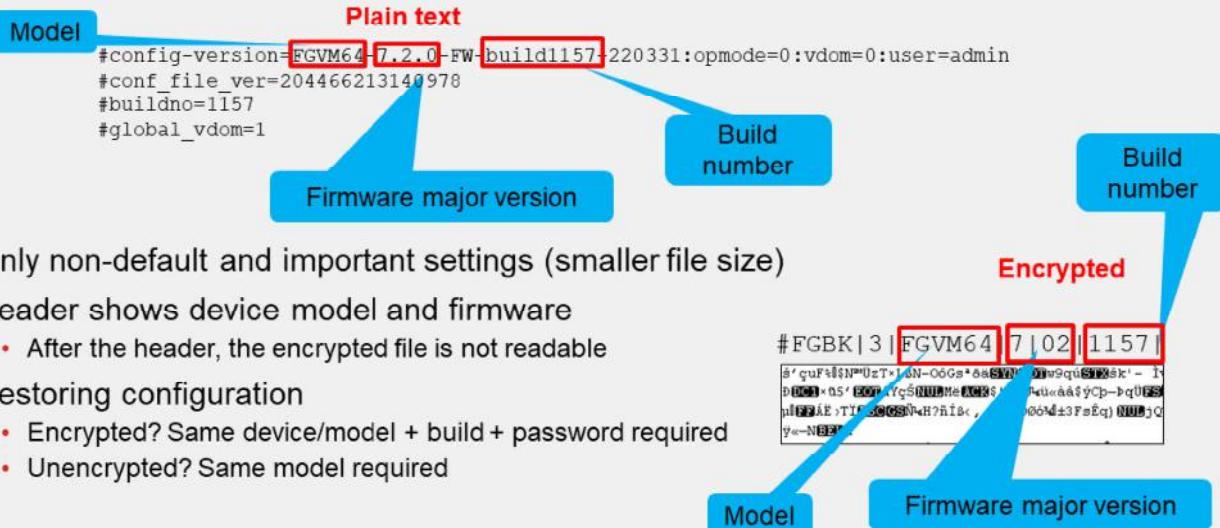
If you enable virtual domains (VDOMs), subdividing the resources and configuration of your FortiGate device, each VDOM administrator can back up and restore their own configurations. You don't have to back up the entire FortiGate configuration, however, it is still recommended.

Backups are needed to help speed up the return to production in the event of an unforeseen disaster that damages FortiGate. Having to recreate hundreds of policies and objects from scratch takes a significant amount of time, while loading a configuration file on a new device takes much less.

Restoring a configuration file is very similar to backing one up and restarts FortiGate.

DO NOT REPRINT
© FORTINET

Configuration File Format



If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a cleartext header that contains some basic information about the device. The example on this slide shows what information is included. To restore an encrypted configuration, you must upload it to a FortiGate device of the same model and firmware, then provide the password.

To restore an unencrypted configuration file, you are required to match only the FortiGate model. If the firmware is different, FortiGate will attempt to upgrade the configuration. This is similar to how it uses upgrade scripts on the existing configuration when upgrading firmware. However, it is still recommended to match the firmware on FortiGate to the firmware listed in the configuration file.

Usually, the configuration file contains only non-default settings, plus few default, yet crucial, settings. This minimizes the size of the backup, which could otherwise be several megabytes in size.

DO NOT REPRINT
© FORTINET

Configuration File Format (Contd)

- Support YAML
- Configuration can be backedup and restored by CLI only

```

• # execute backup yaml-config {ftp | tftp} <filename> server [username]
  [password]
• # execute restore yaml-config {ftp | tftp} <filename> server [username]
  [password]

```

```

config system global
  set admintimeout 480
  set alias "FortiGate-100F"
end
config system settings
  set default-voip-alg-mode kernel-helper-based
  set gui-dynamic-routing enable
end
config system interface
  edit "port1"
    set vdom "root"
    set ip 204.126.10.3 255.255.254.0
    set allowaccess ping
    config secondaryip
      edit 1
        set ip 204.126.10.2 255.255.255.0
        set allowaccess ping
    end

```

Default Format

```

config_system_global:
  admintimeout:480
  alias:FortiGate-100F
config_system_settings:
  default-voip-alg-mode: kernel-helper-based
  gui-dynamic-routing: enable
config_system_interface:
  - port1:
    vdom: root
    ip: "204.126.10.3 255.255.254.0"
    allowaccess: ping
    secondaryip:
      - 0:
        ip: "204.126.10.2 255.255.255.0"
        allowaccess: ping

```

YAML Format

YAML format becomes more and more popular often use to create configuration files. FortiOS now supports YAML format, you can take a backup as well as restore YAML configuration file using CLI commands. You must provide server type: ftp or tftp, filename, server IP address, and user credential's to backup or restore configuration file in YAML format.

This slide shows the sample configuration to understand the difference between the default file format and YAML format.

DO NOT REPRINT

© FORTINET

Upgrade Firmware

- You can view the current firmware version on the dashboard or in **System > Fabric Management** (or on the CLI: get system status)
- If there is an updated firmware version, you are notified
- Firmware can be updated by clicking **Upgrade** and then selecting the **All Upgrades** or **File Upload** option
- Make sure you read the *Release Notes* to verify the upgrade path and other details

The screenshot shows two windows from the FortiGate GUI. The top window is titled "System > Fabric Management". It displays two circular dashboards: one for "Device Type" (FortiGate) showing 1 total, and another for "Upgrade Status" showing 1 total and "Up to date". Below these are buttons for "Fabric Upgrade" (highlighted with a red box), "Upgrade", "Register", and "Authorize". A search bar and filter options for Device, Status, Registration Status, and Firmware Version are also present. The bottom window is titled "FortiGate Upgrade" and shows the current version as "v7.2.0 build1157 (Feature)". It has tabs for "Select Firmware" (highlighted with a red box), "Latest", "All Upgrades", "All Downgrades", and "File Upload". A green message bar at the bottom states "The firmware is up to date."

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

39

You can view the current firmware version in multiple places on the FortiGate GUI. When you first log in to FortiGate, the landing page is the dashboard. You can see the firmware version in the **System** widget. This information is also found at **System > Fabric Management**. And, of course, you can retrieve the information on the CLI using the command `get system status`.

If a new version of the firmware is available, you are notified on the dashboard and on the **Fabric Management** page. The **Fabric Management** page allows administrators to manage the firmware running on each FortiGate, FortiAP, and FortiSwitch in the Security Fabric, and to authorize and register these Fabric devices.

You can use **Upgrade** option to upgrade firmware of the selected device. The **Fabric Upgrade** option upgrades firmware for the root FortiGate as well as Fabric devices. You can also use this option to upgrade firmware for a non-Security Fabric FortiGate with managed FortiSwitch and FortiAP devices. The **Fabric Upgrade** option uses released firmware images from FortiGuard.

You can also use the **Register** option to register a selected device to FortiCare and an **Authorize** option to authorize a selected device for use in security fabric.

Remember to read the *Release Notes* to make sure that you understand the supported upgrade path. The *Release Notes* also provide pertinent information that may affect the upgrade.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When restoring an encrypted system configuration file, in addition to needing the FortiGate model and firmware version from the time the configuration file was produced, what must you also provide?
 A. The password to decrypt the file
 B. The private decryption key to decrypt the file

2. Which document should you consult to increase the chances of success before upgrading or downgrading firmware?
 A. Cookbook
 B. Release Notes

DO NOT REPRINT**© FORTINET**

Lesson Progress



High-Level Features



Setup Decisions



Basic Administration



Fundamental Maintenance

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify key FortiGate features, services, and built-in servers
- ✓ Identify the relationship between FortiGate and FortiGuard
- ✓ Identify the factory defaults, basic network settings, and console ports
- ✓ Execute basic administration, such as creating administrative users and permissions
- ✓ Define and describe VDOMs
- ✓ Execute backup and restore tasks and discuss the requirements for restoring an encrypted configuration file
- ✓ Initiate an upgrade of the firmware



© Fortinet Inc. All Rights Reserved.

42

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how and where FortiGate fits into your network and how to perform basic FortiGate administration.

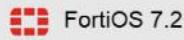
DO NOT REPRINT

© FORTINET



FortiGate Security

Firewall Policies



FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn about firewall policies and how to apply them to allow and deny traffic passing through FortiGate. At its core, FortiGate is a firewall, so almost everything that it does to your traffic is linked to your firewall policies.

DO NOT REPRINT

© FORTINET

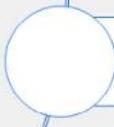
Lesson Overview



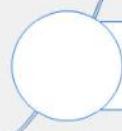
Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

Firewall Policies

Objectives

- Identify components of firewall policies
- Identify how FortiGate matches traffic to firewall policies

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in identifying the different components of firewall policies, and recognizing how FortiGate matches traffic with firewall policies and takes appropriate action, you will have a better understanding of how firewall policies interact with network traffic.

DO NOT REPRINT

© FORTINET

What Are Firewall Policies?

- Policies define:
 - Which traffic matches them
 - How to process matching traffic
- When a new IP session packet arrives, FortiGate:
 - Starts at the top of the list to look for a policy match
 - Applies the first matching policy

Implicit Deny

- No matching policy? FortiGate drops packet

Policy & Objects > Firewall Policy											
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log		
1	Internet_Access_ISP1	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All		
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default SSL deep-inspection	All		
0	Implicit	all	all	always	ALL	DENY	Disabled				

Implicit Deny



To begin, you will learn what firewall policies are.

Any traffic passing through a FortiGate must be associated with a firewall policy. A policy is a set of instructions that controls traffic flow through the FortiGate. These instructions determine where the traffic goes, how it's handled, and whether it's allowed to pass through the FortiGate. In summary, firewall policies are sets of rules that specify which traffic is allowed through the FortiGate and what FortiGate should do when traffic matches a policy.

Should the traffic be allowed? FortiGate bases this decision on simple criteria. FortiGate analyzes the source of the traffic, the destination IP address, and the service. If the policy does not block the traffic, FortiGate begins a more computationally expensive security profile inspection—often known as Unified Threat Management (UTM)—such as antivirus, application control, and web filtering, if you've chosen it in the policy. These inspections block the traffic if there is a security risk, for example, if the traffic contains a virus. Otherwise, the traffic is allowed.

Will network address translation (NAT) be applied? Is authentication required? Firewall policies also determine the answers to these questions. After processing is finished, FortiGate forwards the packet toward its destination.

FortiGate looks for the matching firewall policy from *top to bottom* and, if a match is found, the traffic is processed based on the firewall policy. If no match is found, the traffic is dropped by the default **Implicit Deny** firewall policy.

DO NOT REPRINT**© FORTINET**

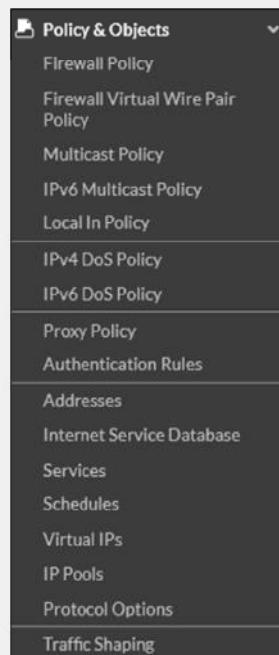
Components and Policy Types

Objects used by policies

- Interface and zone
- Address, user, and internet service objects
- Service definitions
- Schedules
- NAT rules
- Security profiles

Policy types

- Firewall Policy (IPv4, IPv6)
- Firewall Virtual Wire Pair Policy (IPv4, IPv6)
- Proxy Policy
- Multicast Policy
- Local-in Policy
- DoS Policy (IPv4, IPv6)
- Traffic Shaping



Each policy matches traffic and applies security by referring to the objects that you've defined, such as addresses and profiles.

Common policy types are:

- Firewall Policy: A firewall policy consists of set of rules that control traffic flow through FortiGate.
- Firewall Virtual Wire Pair Policy: A virtual wire pair policy is used to control the traffic between the interfaces in a virtual wire pair.
- Multicast Policy: A multicast policy allows multicast packets to pass from one interface to another.
- Local In Policy: A local-in policy controls the traffic to a FortiGate interface and can be used to restrict administrative access.
- DoS Policy: A denial-of-service (DoS) policy checks for the anomalous patterns in the network traffic that arrives at a FortiGate interface.

By default, only **Firewall Policy** is visible under **Policy and Object**. Other policies are available based on the interface configurations and advanced features enabled through **Feature Visibility**.

In this lesson, you will learn about IPv4 firewall policies, because they are the most commonly used policies.

DO NOT REPRINT
© FORTINET

How Are Policy Matches Determined?

Incoming and outgoing interfaces ✓

Source: IP address, user, internet services ✓

Destination: IP address or internet services ✓

Services ✓

Schedules ✓

Action = **ACCEPT** or **DENY**

Policy & Objects > Firewall Policy

Name	<input type="text"/>
Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="button" value="+"/>
Destination	<input type="button" value="+"/>
Schedule	<input type="button" value="always"/>
Service	<input type="button" value="+"/>
Action	<input checked="" type="button" value="ACCEPT"/> <input type="button" value="DENY"/>

© Fortinet Inc. All Rights Reserved.

FORTINET
Training Institute

6

When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:

- **Incoming Interface**
- **Outgoing Interface**
- **Source**: IP address, user, internet services
- **Destination**: IP address or internet services
- **Service**: IP protocol and port number
- **Schedule**: Specific times to apply policy

If the traffic matches a firewall policy, FortiGate applies the action configured in the firewall policy:

- If the **Action** is set to **DENY**, FortiGate drops the session.
- If the **Action** is set to **ACCEPT**, FortiGate allows the session and applies other configured settings for packet processing, such as user authentication, source NAT, antivirus scanning, web filtering, and so on.

When FortiGate receives traffic, it evaluates the packet's source IP address, destination IP address, and the requested service (protocol and port number). It also checks the incoming interface and the outgoing interface it needs to use. Based on this information, FortiGate identifies the firewall policy and evaluates the traffic. If the traffic matches the policy, then FortiGate applies the action (Accept/Deny) defined in the policy.

For example, to block incoming FTP traffic to all but a few FTP servers, define the addresses of the FTP servers as the destination, and select FTP as the service. You probably *wouldn't* specify a source (often any location on the internet is allowed) or schedule (FTP servers are usually always available, day or night). Finally, set the **Action** setting to **ACCEPT**.

DO NOT REPRINT

© FORTINET

Simplify—Interfaces and Zones

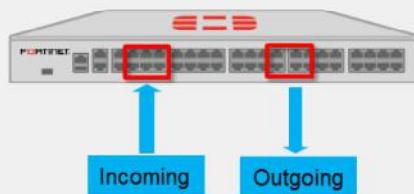
- The incoming and outgoing interfaces can function as individual interfaces or you can create a zone, which is a logical group of interfaces
- To match policies with traffic, select one or more interfaces

Network > Interfaces

	Type	Members	IP/Netmask
Interface	Physical Interface		10.200.1.1/255.255.255.0
Zone	Physical Interface		10.200.2.1/255.255.255.0
Virtual Wire Pair	Physical Interface		10.0.1.254/255.255.255.0
	Physical Interface		0.0.0.0.0.0.0
	Physical Interface		172.16.100.3/255.255.255.0
Tunnel Interface			
Zone	DMZ	port4 port5 port6 port7	

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.



7

To begin describing how FortiGate finds a policy for each packet, let's start with the interfaces.

Packets arrive on an incoming, or ingress, interface. Routing determines the outgoing, or egress, interface. In each policy, you *must* set a source and destination interface; even if one or both are set to **any**. Both interfaces must match the policy's interface criteria in order to be a successful match.

For example, if you configure policies between port3 (LAN) ingress and port1 (WAN) egress and a packet arrives on port2, the packet will *not* match your policies and, therefore, would be dropped because of the implicit deny policy at the end of the list. Even if the policy is from port3 (LAN) ingress to any egress, the packet would still be dropped because it did not match the incoming interface.

To simplify policy configuration, you can group interfaces into logical zones. For example, you could group port4 to port7 as a DMZ. You can create zones on the **Interfaces** page. However, you should note that you cannot reference an interface in a zone individually, and, if you need to add the interface to the zone, you must remove all references to that interface (for example, firewall policies, firewall addresses, and so on). If you think you might need to reference interfaces individually, you should set multiple source and destination interfaces in the firewall policy, instead of using zones.

DO NOT REPRINT
© FORTINET

Selecting Multiple Interfaces or Any Interface

- Disabled by default
 - Cannot select multiple interfaces or any interface in firewall policy on the GUI
- Can be made visible in the GUI

The screenshot illustrates the configuration of a firewall policy and the enabling of multiple interface policies.

Policy & Objects > Firewall Policy

New Policy
 Name: Single_Interface
 Incoming Interface: port4
 Outgoing Interface: port5

A callout bubble points to the Outgoing Interface dropdown with the text "Multiple interface policies disabled".

System > Feature Visibility

Multiple Interface Policies
 Allow the configuration of policies with multiple source/destination interfaces.

An arrow points from the "Multiple Interface Policies" checkbox to the "Policy & Objects > Firewall Policy" screen.

Policy & Objects > Firewall Policy

New Policy
 Name: Multiple_Interface
 Incoming Interface: port9, port10
 Outgoing Interface: any

A callout bubble points to the Outgoing Interface dropdown with the text "Multiple interface policies enabled".

Fortinet Training Institute

© Fortinet Inc. All Rights Reserved.

8

By default, you can select only a single interface as the incoming interface and a single interface as the outgoing interface. This is because the option to select multiple interfaces, or **any** interface in a firewall policy, is disabled on the GUI. However, you can enable the **Multiple Interface Policies** option on the **Feature Visibility** page to disable the single interface restriction.

You can also specify multiple interfaces, or use the **any** option, if you configure a firewall policy on the CLI, regardless of the default GUI setting.

It is also worth mentioning that when you choose the **any** interface option, you cannot select multiple interfaces for that interface. In the example shown on this slide, because **any** is selected as the outgoing interface, you cannot add any additional interfaces, because **any** interface implies that all interfaces have already been selected.

DO NOT REPRINT

© FORTINET

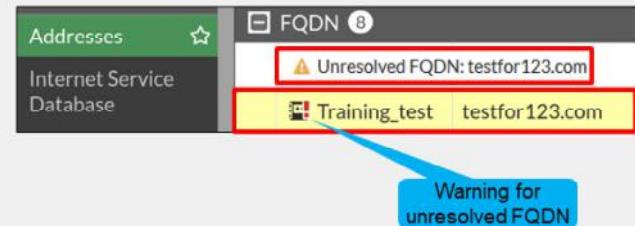
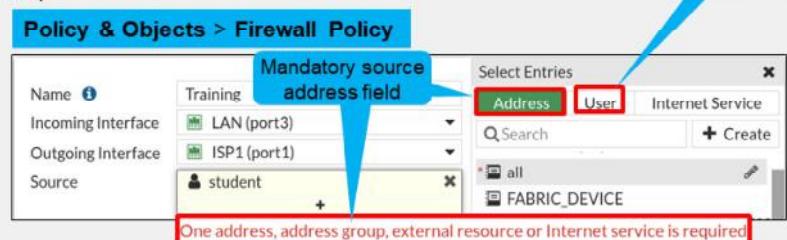
Matching by Source

- Must specify at least one source (address or internet service database (ISDB) object)

- IP address or range
- Subnet (IP/netmask)
- FQDN
- Geography
- Dynamic
 - Fabric connector address
- MAC Address Range

- May specify:

- Source user—individual user or user group
- This may refer to:
 - Local firewall accounts
 - Accounts on a remote server (for example, Active Directory, LDAP, RADIUS)
 - FSSO
 - Personal certificate (PKI-authenticated) users



The next match criteria that FortiGate considers is the packet's source.

In each firewall policy, you *must* select a source address object. Optionally, you can refine your definition of the source address by *also* selecting a user, or a user group, which provides a much more granular match, for increased security. You can also select ISDB objects as the source in the firewall policy, which you will learn about later in this lesson.

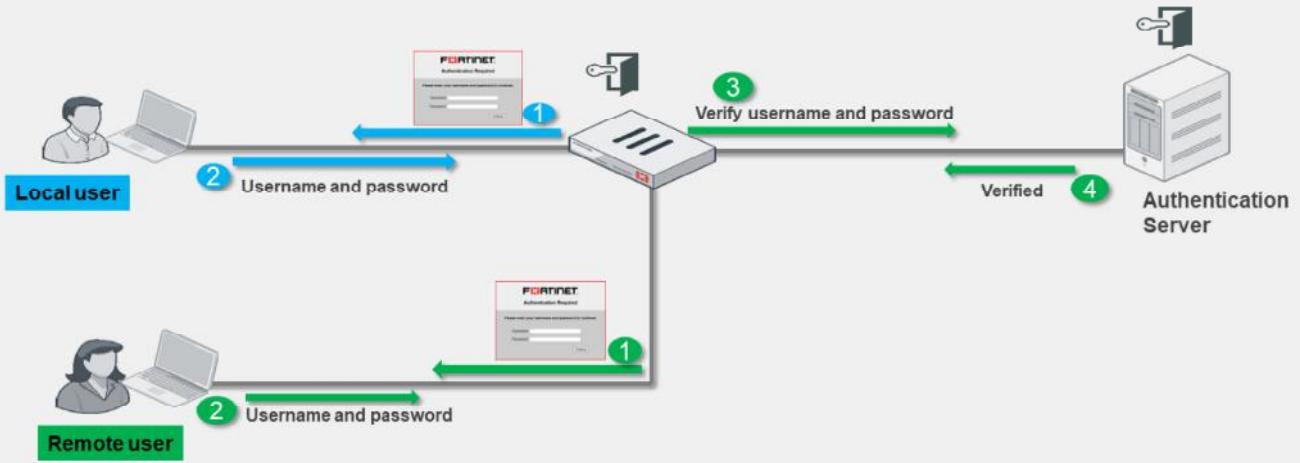
When selecting a fully qualified domain name (FQDN) as the source address, it must be resolved by DNS and cached in FortiGate. Make sure FortiGate is configured properly for DNS settings. If FortiGate is not able to resolve an FQDN address, it will present a warning message, and a firewall policy configured with that FQDN may not function properly.

DO NOT REPRINT

© FORTINET

Source—User Identification

- Confirms identity of user
- Access to network is provided after confirming user credentials



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

10

If a user is added as part of the source, FortiGate must verify the user before allowing or denying access based on the firewall policy. There are different ways that a user can authenticate.

For local users, the username and password is configured *locally* on FortiGate. When a local user authenticates, the credentials that they enter must match the username and password configured locally on FortiGate.

For a remote user (for example, LDAP or RADIUS), FortiGate receives the username and password from the remote user and passes this information to the authentication server. The authentication server verifies the user login credentials and updates FortiGate. After FortiGate receives that information, it grants access to the network based on the firewall policy.

A Fortinet single sign-on (FSSO) user's information is retrieved from the domain controller. Access is granted based on the group information on FortiGate.

DO NOT REPRINT
© FORTINET

Example—Matching Policy by Source

- Source as internet service database (ISDB) objects
- Matches by source address, user

Policy & Objects > Firewall Policy

Name:	Training
Incoming Interface:	port3
Outgoing Interface:	port1
Source:	<input checked="" type="checkbox"/> LOCAL SUBNET <input checked="" type="checkbox"/> student

Policy & Objects > Firewall Policy

Name:	Training
Incoming Interface:	port3
Outgoing Interface:	port1
Source:	<input checked="" type="checkbox"/> Amazon-AWS

User Address Internet Service

© Fortinet Inc. All Rights Reserved.
11

In the example shown on this slide, source selectors identify the specific subnet and user group. Remember, user is an optional object. The user object is used here to make the policy more specific. If you wanted the policy to match more traffic, you would leave the user object undefined.

You can also use internet service (ISDB) objects as a source in the firewall policy. There is an either/or relationship between internet service objects and source address objects in firewall policies. This means that you can select either a source address or an internet service, but not both.

DO NOT REPRINT**© FORTINET**

Matching by Destination

Like source, destination criteria can use:

- Address objects:
 - Subnet (IP or netmask)
 - IP address or address range
 - FQDN
 - DNS query used to resolve FQDN
 - Geography
 - Country defines addresses by ISP's geographical location
 - Database updated periodically through FortiGuard
 - Dynamic
 - Fabric connector address
- Internet service database (ISDB) objects

Like the packet's source, FortiGate also checks the destination address for a match.

You can use address objects or ISDB objects as destinations in the firewall policy. The address object may be a host name, IP subnet, or range. If you enter an FQDN as the address object, make sure that you've configured your FortiGate device with DNS servers. FortiGate uses DNS to resolve those FQDN host names to IP addresses, that appear in the IP header.

You can also choose geographic addresses, which are groups or ranges of addresses that are assigned to a country. FortiGuard is used to update these objects.

Why is there is no option to select a user? The user identification is determined at the ingress interface, and packets are forwarded only to the egress interface after the user is successfully authenticated.

DO NOT REPRINT

© FORTINET

Internet Service

- Database that contains IP addresses, IP protocols, and port numbers used by the most common internet services
 - Regularly updated through FortiGuard
- Can be used as **Source** or **Destination** in the firewall policy

Policy & Objects > Internet Service Database

Name	Direction	Number of Entries
Alibaba-SSH	Destination	4,347
Alibaba-Web	Destination	4,347
Amazon-AWS	Both	14,015
Amazon-AWS.WorkSpaces.Gateway	Destination	27
Amazon-DNS	Destination	41,821
Amazon-FTP	Destination	41,821

Policy & Objects > Firewall Policy

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. On the left, there's a configuration form with fields for Name (Training), Incoming Interface (port3), Outgoing Interface (port1), Source (all), Destination (all), and Schedule (always). On the right, there's a 'Select Entries' panel titled 'Address' with 'Internet Service' selected. A list of entries includes Facebook-SSH, Facebook-Web (highlighted in yellow), Facebook-Whatsapp, Fastly-CDN, Forcepoint-Forcepoint.Cloud, Fortinet-DNS, Fortinet-FortiCloud, and Fortinet-FortiGuard. A red box highlights the 'Facebook-Web' entry in the list. A red arrow points from this box to a red box on the configuration form containing the message: 'Addresses/groups cannot be mixed with Internet services'.

Internet Service is a database that contains a list of IP addresses, IP protocols, and port numbers used by the most common internet services. FortiGate periodically downloads the newest version of this database from FortiGuard. You can select these as **Source** or **Destination** in the firewall policy.

What happens if you need to allow traffic to only a few well-known public internet destinations, such as Dropbox or Facebook?

When configuring your firewall policy, you can use **Internet Service** as the destination in a firewall policy, which contains all the IP addresses, ports, and protocols used by that service. For the same reason, you cannot mix regular address objects with ISDB objects, and you cannot select services on a firewall policy. The ISDB objects already have services information, which is hardcoded.

Compared with address objects, which you need to check frequently to make sure that none of the IP addresses have changed or appropriate ports are allowed, internet services helps make this type of deployment easier and simpler.

DO NOT REPRINT
© FORTINET

Geographic-Based Internet Service Database

- Allows users to define ISDB objects based on a country, region, and city
- Objects can be used in firewall policies for more granular control over the location of the parent ISDB object

The screenshot shows the FortiGate UI for managing Geographic-Based Internet Services. At the top left, a blue header bar says "Policy & Objects > Internet Service Database". Below it is a toolbar with buttons for "+ Create New", "Edit", and "Delete". A red box highlights the "Geographic Based Internet Service" entry in the list. A red arrow points down from this entry to a "New Internet Service" dialog box. This dialog box has two main sections: configuration settings on the left and service details on the right. The configuration section includes fields for Name (Training-Location-ISDB), Type (Predefined, Geographic Based selected), Primary Internet Service (Google-Other), Country/Region (United Kingdom), Region (England), and City (Birmingham). The right section shows the Primary Internet Service Name (Google-Other), Primary Internet Service ID (65536), Direction (Destination), and a link to "Entries" with a "View/Edit Entries" button. A red box highlights the "View/Edit Entries" button. At the top right of the dialog box is a table titled "Google-Other" with three entries:

IP	Port	Protocol	Status
62.24.215.76 - 62.24.215.79	1 - 65535	TCP	Enabled
62.24.215.76 - 62.24.215.79	1 - 65535	UDP	Enabled
62.24.215.81 - 62.24.215.83	1 - 65535	TCP	Enabled

At the bottom left of the UI is the FORTINET Training Institute logo. At the bottom center is the copyright notice "© Fortinet Inc. All Rights Reserved." and at the bottom right is the page number "14".

Geographic-based ISDB objects allow users to define a country, region, and city. These objects can be used in firewall policies for more granular control over the location of the parent ISDB object.

ISDB objects are referenced in policies by name, instead of by ID.

DO NOT REPRINT**© FORTINET**

Internet Service Database (ISDB)—Updates

- You can disable ISDB updates so they occur only during a change control window
 - Control ISDB updates by using CLI command:

```
# config system fortiguard
    set update-ffdb [enable | disable]
next
end
```

- Once ISDB updates are disabled, other scheduled FortiGuard updates do not update ISDB
- By default, ISDB updates are enabled



© Fortinet Inc. All Rights Reserved.

15

You can disable ISDB updates, so they occur only during a change control window. Once ISDB updates are disabled, other scheduled FortiGuard updates for IPS, AV, and so on, do not update ISDB. By default, ISDB updates are enabled.

DO NOT REPRINT

© FORTINET

Scheduling

- Policies apply only during specific times and on specific days
 - Example: A less restrictive *lunch time* policy
 - The default schedule applies all the time
- Recurring
 - Happens at the same time during specified day(s) of the week



- One-time
 - Happens only once

Policy & Objects > Schedules

New Schedule

Type	<input checked="" type="radio"/> Recurring	<input type="radio"/> One Time
Name	Maintenance	
Color	<input checked="" type="radio"/> Change	
Days	<input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday	
All Day	<input checked="" type="radio"/>	
Start Time	12:00:00,000 AM	
Stop Time	12:00:00,000 AM	

Policy & Objects > Schedules

New Schedule

Type	<input checked="" type="radio"/> Recurring	<input type="radio"/> One Time
Name	Maintenance	
Color	<input checked="" type="radio"/> Change	
Start Date	04/21/2021	06:58:00,000 PM
End Date	04/21/2021	07:58:00,000 PM
Pre-expiration event log	<input checked="" type="radio"/>	
Number of days before	1	

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

16

Schedules add a time element to the policy. For example, you might use a policy to allow backup software to activate at night, or create a test window for a remote address that is allowed for testing purposes.

Schedules can be configured and use a 24-hour time clock. There are a few configuration settings worth mentioning:

- Recurring:** If you enable **All Day**, traffic will be allowed for 24 hours for the days selected. When configuring recurring schedules, if you set the stop time earlier than the start time, the stop time will occur the next day. For example, if you select Sunday as the day, 10:00 as the start time, and 09:00 as the stop time, the schedule will stop on Monday at 09:00. If the start and stop time are identical, the schedule will run for 24 hours.
- One-time:** The start date and time must be earlier than the stop date and time. You can also enable **Pre-expiration event log**, which will generate an event log N number of days before the schedule expires, where N can be from 1 to 100 days.

FortiGate Security 7.2 Study Guide

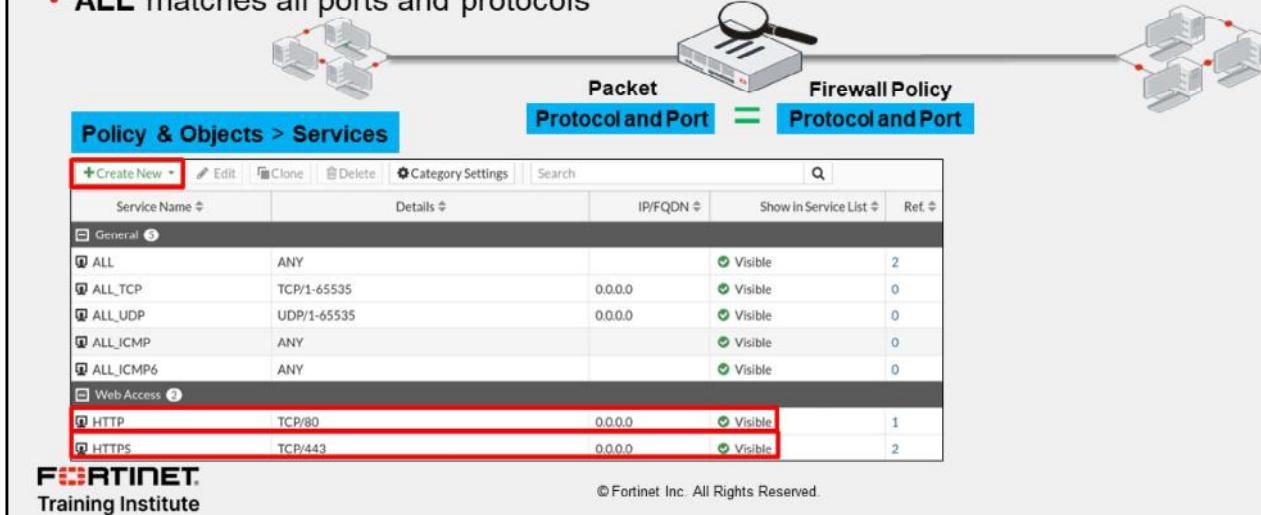
62

DO NOT REPRINT

© FORTINET

Matching by Service

- Service determines matching transmission protocol (UDP, TCP, and so on) and port number
- Can be predefined or custom
- **ALL** matches all ports and protocols



Another criterion that FortiGate uses to match policies is the packet's service.

At the IP layer, protocol numbers (for example, TCP, UDP, SCTP, and so on) together with source and destination ports, define each network service. Generally, only a destination port (that is, the server's listening port) is defined. Some legacy applications may use a specific source port, but in most modern applications, the source port is randomly identified at transmission time, and therefore is not a reliable way to define the service.

For example, the predefined service object named HTTP is TCP destination port 80, and the predefined service object named HTTPS is TCP destination port 443. However, the source ports last for only a short time and, therefore, are not defined.

By default, services are grouped together to simplify administration by categories. If the predefined services don't meet your organizational needs, you can create one or more new services, service groups, and categories.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. What criteria does FortiGate use to match traffic to a firewall policy?
 A. Source and destination interfaces
 B. Security profiles

2. What must be selected in the **Source** field of a firewall policy?
 A. At least one address object or ISDB
 B. At least one source user and one source address object

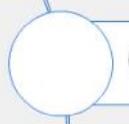
DO NOT REPRINT

© FORTINET

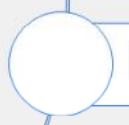
Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand the components used in firewall policies and matching criteria used by FortiGate.

Now, you'll learn how to configure firewall policies.

DO NOT REPRINT**© FORTINET**

Configuring Firewall Policies

Objectives

- Restrict access and make your network more secure using security profiles
- Configure logging

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring firewall policies, you will be able to apply the correct settings, such as security profiles, logging, and traffic shaping, to firewall policies on FortiGate, and make your network more secure.

DO NOT REPRINT

© FORTINET

Configuring Firewall Policies

- Mandatory policy name when creating on GUI
 - Can relax the requirement by enabling **Allow Unnamed Policies**

- Flat GUI view allows:
 - Select by clicking
 - Drag-and-drop

```
config firewall policy
edit 1
  set name "Training"
  set uid 2204966e-47f7-51..
```

Universally unique identified (UUID)

The screenshot shows the FortiGate Firewall Policy configuration screen. A callout points to the 'Name' field with the text 'Enabled by default MUST specify unique name'. Another callout points to the 'Source' section with the text 'Highlights selected entry'. To the right, a 'Select Entries' dialog box is open, showing a list of entries under 'Address' tab. The entry 'LOCAL_CLIENT' is highlighted with a yellow background.

Name	Incoming Interface	Outgoing Interface	Source	Destination	Schedule	Service	Action
Training	LAN (port3)	ISP1 (port1)	LOCAL_CLIENT	all	always	ALL	✓ ACCEPT

Select Entries
 Address (17)
 all
 FABRIC_DEVICE
 FIREWALL_AUTH_PORTAL_ADDRESS
 FORTINET
 gmail.com
 LINUX_ETH1
 LOCAL_CLIENT
 LOCAL_SUBNET

When you configure a new firewall policy on the GUI, you *must* specify a unique name for the firewall policy because it is enabled by default, while it is optional on the CLI. This helps the administrator to quickly identify the policy that they are looking for. However, you can make this feature optional on the GUI on the **Feature Visibility** page by enabling **Allow Unnamed Policies**.

Note that if a policy is configured without a policy name on the CLI, and you modify that existing policy on the GUI, you *must* specify a unique name. The FortiGate flat GUI view allows you to select interfaces and other objects by clicking or dragging and dropping from the list populated on the right side.

You can select **Internet Service** as the source. **Internet Service** is a combination of one or more addresses and one or more services associated with a service found on the internet, such as an update service for software.

There are many other options that you can configure in the firewall policy, such as firewall and network options, security profiles, logging options, and enabling or disabling a policy.

When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer.

When creating firewall policies, remember that FortiGate is a stateful firewall. As a result, you need to create only one firewall policy that matches the direction of the traffic that initiates the session. FortiGate will automatically remember the source-destination pair and allow replies.

DO NOT REPRINT

© FORTINET

Security Profiles

- Firewall policies limit access to configured networks
- Security profiles configured in firewall policies protect your network by:
 - Blocking threats
 - Controlling access to certain applications and URLs
 - Preventing specific data from leaving your network

Policy & Objects > Firewall Policy

Security Profiles	
AntiVirus	AV default
Web Filter	WEB default
Video Filter	VF New Profile
DNS Filter	DNS default
Application Control	APP default
IPS	IPS default
File Filter	FF default
VoIP	VOIP default
Web Application Firewall	WAF default
SSL Inspection	SSL deep-inspection

Default profile not available, you need to manually create a profile

One of the most important features that a firewall policy can apply is security profiles, such as IPS and antivirus. A security profile inspects each packet in the traffic flow, where the session has already been conditionally accepted by the firewall policy.

When inspecting traffic, FortiGate can use one of two methods: flow-based inspection or proxy-based inspection. Different security features are supported by each inspection type.

Note that by default, the **Video Filter**, **VOIP**, and **Web Application Firewall** security profile option is not visible in the policy page on the GUI. You need to enable them on the **Feature Visibility** page.

DO NOT REPRINT

© FORTINET

Logging

- By default, set to **Security Events**
 - Generates logs based on applied security profile only
- Can change to **All Sessions**

Accept

Logging Options

Log Allowed Traffic	<input checked="" type="radio"/> Security Events <input type="radio"/> All Sessions
Generate Logs when Session Starts	<input checked="" type="checkbox"/>
Capture Packets	<input checked="" type="checkbox"/>

Deny

Log Violation Traffic

```
config system setting
    set ses-denied-traffic [disable | enable]
end
config system global
    set block-session-timer [1-300]
end
```

If you have enabled logging in the policy, FortiGate generates traffic logs after a firewall policy closes an IP session.

By default, **Log Allowed Traffic** is enabled and set to **Security Events** and generates logs for only the applied security profiles in the firewall policy. However, you can change the setting to **All Sessions**, which generates logs for all sessions.

If you enable **Generate Logs when Session Starts**, FortiGate creates a traffic log when the session begins. FortiGate also generates a second log for the same session when it is closed. But remember that increasing logging decreases performance, so use it only when necessary.

During the session, if a security profile detects a violation, FortiGate records the attack log immediately. To reduce the number of log messages generated and improve performance, you can enable a session table entry of dropped traffic. This creates the denied session in the session table and, if the session is denied, all packets of that session are also denied. This ensures that FortiGate does not have to do a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation.

This option is in the CLI, and is called `ses-denied-traffic`. You can also set the duration for block sessions. This determines how long a session will be kept in the session table by setting `block-session-timer` in the CLI. By default, it is set to 30 seconds.

If the GUI option **Generate Logs when Session Starts** is not displayed, this means that your FortiGate device does not have internal storage. This option is on the CLI, regardless of internal storage, and is called `set logtraffic-start enable`.

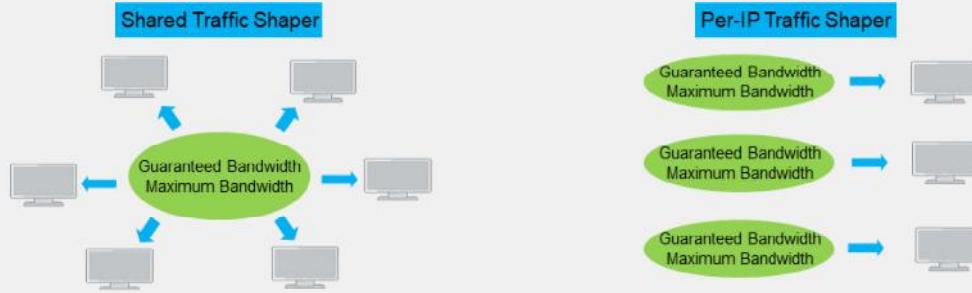
DO NOT REPRINT

© FORTINET

Traffic Shapers

- Rate limiting is configurable
 - In bandwidth and out bandwidth
 - Defines maximum and guaranteed bandwidth

Policies & Objects > Traffic Shaping Policy



You can configure two types of traffic shapers: shared and per IP.

A shared shaper applies a total bandwidth to all traffic using that shaper. The scope can be per policy or for all policies referencing that shaper. FortiGate can count the packet rates of ingress and egress to police traffic.

FortiGate allows you to create three types of traffic shaping policies:

- Shared policy shaping: bandwidth management of security policies
- Per-IP shaping: bandwidth management of user IP addresses
- Application control shaping: bandwidth management by application

When creating traffic shaping policies, you must ensure that the matching criteria is the same as the firewall policies you want to apply shaping to. Note that these apply equally to TCP and UDP, and UDP protocols may not recover as gracefully from packet loss.

DO NOT REPRINT
© FORTINET

Consolidated IPv4 and IPv6 Policy Configuration

- IPv4 and IPv6 policies are combined into a single consolidated policy, instead of separate policies
- The IP version of the sources and destinations in a policy must match
- Single policy table for GUI
- Different IP addresses and IP pool for IPv4 and IPv6

Policy & Objects > Firewall Policy										
ID	Name	From	To	Source	Destination	Schedule	Action	NAT	Security Profiles	IPv4 + IPv6
34		port4	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> no-inspection
44		port4	port3	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Disabled	<input checked="" type="checkbox"/> certificate-inspection <input checked="" type="checkbox"/> All
99		port3	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> no-inspection <input checked="" type="checkbox"/> UTM
91		port2	port2	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> no-inspection <input checked="" type="checkbox"/> UTM
222		port2	port1	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all6	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input checked="" type="checkbox"/> ipv4-ippool-1 <input checked="" type="checkbox"/> ipv6-ippool-1	<input checked="" type="checkbox"/> certificate-inspection <input checked="" type="checkbox"/> UTM
0	Implicit Deny	<input type="checkbox"/> any	<input type="checkbox"/> any	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> all <input checked="" type="checkbox"/> all	<input checked="" type="checkbox"/> always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> DENY		<input checked="" type="checkbox"/> Disabled

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

25

By default, IPv4 and IPv6 policies are combined into a single consolidated policy, rather than creating and maintaining two different policy sets for IPv4 and IPv6.

You can share the **Incoming Interface**, **Outgoing Interface**, **Schedule**, and **Service** fields with both IPv4 and IPv6. For source addresses, destination addresses, and IP pool, you must select addresses for both IPv4 and IPv6.

While configuring a consolidated firewall policy, you can configure a policy with IPv4 source addresses, IPv4 destination addresses, and an IPv4 IP pool, without specifying any IPv6 references. You can also configure the policy with the same behavior for IPv6. However, if you want to combine IPv4 and IPv6, you must select both IPv4 addresses and IPv6 addresses in the **Source** and **Destination** address fields in the firewall policy. The IP version of the sources and destinations in a policy must match. For example, a policy cannot have only an IPv4 source and an IPv6 destination. The policy table in the GUI can be filtered to show policies with IPv4, IPv6, or IPv4 and IPv6 sources and destinations.

Note that, by default, the **IPv6** option is not visible in the policy table on the GUI. You must enable **IPv6** on the **Feature Visibility** page.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. To configure a firewall policy, you must include a firewall policy name when configuring using the ____.
 A. CLI
 B. GUI

2. What is the purpose of applying security profiles to a firewall policy?
 A. To allow access to specific subnets
 B. To protect your network from threats, and control access to specific applications and URLs

DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand how to configure firewall policies on FortiGate.

Next, you'll learn how to manage and fine-tune settings for firewall policies.

DO NOT REPRINT**© FORTINET**

Managing Firewall Policies

Objectives

- Identify policy list views
- Understand the use of policy IDs
- Identify where an object is referenced

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managing firewall policies, you will be able to understand the use of the policy ID of a firewall policy. Also, you will be able to pinpoint object usage, and simplify policies using object groups.

DO NOT REPRINT

© FORTINET

Policy List—Interface Pair View and By Sequence

- **Interface Pair View**

- Lists policies by ingress and egress interfaces (or zone) pairings

Can view **By Sequence** also

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
Fortinet	port3	port1	always	Web Access	ACCEPT	Enabled	no-inspection	UTM
Full_Access	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All
Backup_Access	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM

- **By Sequence (only)**

- If policies are created using multiple source and destination interfaces or any interface

Name	From	To	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes
Fortinet	port3	port1	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT	Enabled	no-inspection	UTM
Full_Access	port3	port1	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All
Any Interface	port3	any	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM
Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled

Firewall policies appear in an organized list. The list is organized either in **Interface Pair View** or **By Sequence**.

By default, the policy list appears in **Interface Pair View**. Each section contains policies in the order that they are evaluated for matching traffic and are arranged by ingress-egress interface pair. Alternatively, you can view your policies as a single, comprehensive list by selecting **By Sequence** at the top of the page. In this view the policies are also listed in the order in which they are evaluated for traffic matching, but they are not grouped.

In some cases, you cannot choose the view. For example, if you use multiple source or destination interfaces, or the **any** interface in a firewall policy, you cannot separate policies into sections by interface pairs—some would be triplets or more. In this case, policies always appear in a single list (**By Sequence**).

To help you remember the use of each interface, you add aliases by editing the interface on the **Network** page. For example, you could call port1 *ISP1*. This can help to make your list of policies easier to understand.

DO NOT REPRINT
© FORTINET

Real-Time Policy Status

- Real-time policy status update
 - ID
 - Last used
 - First used
 - Active sessions
 - Hit count
 - Total bytes
 - Current bandwidth
 - Usage graph

The screenshot shows the 'Edit Policy' screen for a policy named 'Internet_Access_ISP1'. The policy details include:

- Name:** Internet_Access_ISP1
- Incoming Interface:** LAN (port3)
- Outgoing Interface:** ISP1 (port1)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)

Inspection Mode: Flow-based (selected)

Firewall / Network Options:

- NAT: Enabled
- IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool
- Preserve Source Port: Enabled
- Protocol Options: PROT default

Statistics (since last reset):

ID	1
Last used	0 second(s) ago
First used	46 minute(s) ago
Active sessions	3
Hit count	198
Total bytes	196.44 kB
Current bandwidth	0 B/s

Graph options: Bytes, Packets, Hit Count (selected)

Reset Counters button is highlighted with a blue arrow.

At the bottom right of the interface, there is a red '30' icon.

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

When you edit the policy, policy information will be visible.

This feature is very useful if an administrator wanted to check the policy usage, such as last used, first used, hit count, active sessions, and so on.

DO NOT REPRINT

© FORTINET

Policy ID

- Firewall policies are primarily ordered on a top-down basis
- Policy IDs are identifiers:
 - The policy ID is assigned by the system when the rule is created
 - The ID number never changes as rules move higher or lower in the sequence
 - Policy IDs are not displayed by default on the GUI

```
config firewall policy
edit <policy_id>
end
```

Policy ID

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Action	NAT
	port3 → port1 2					
2	Block_FTP	all	all	always	FTP DENY	
1	Full_Access	LOCAL_SUBNET	all	always	ALL ACCEPT Enabled	
	port3 → port2 1					
3	DMZ	DMZ	all	always	ALL ACCEPT Enabled	

```
config firewall policy
edit 2
  set name "Block_FTP"
...
next
  edit 1
    set name "Full_Access"
```

An important concept to understand about how firewall policies work is the precedence of order, or, if you prefer a more recognizable term, first come, first served.

Policy IDs are identifiers. By default, policy IDs are not displayed on the policy list GUI. You can add a policy ID column using the **Configure Table** settings icon.

FortiGate automatically assigns a policy ID when you create a new firewall policy on the GUI. The policy ID never changes, even if you move the rule higher or lower in the sequence.

If you enable **Policy Advanced Options**, then you can manually assign a policy ID, while creating a new policy. If a duplicate entry is found, the system produces an error, so you can assign a different available policy ID number.

Policy Advanced Options is not available on the GUI by default, you must enable it on the **Feature Visibility** page.

DO NOT REPRINT
© FORTINET

Simplify—Groups of Addresses or Services

- You can reference address and service objects individually, or use groups to simplify policy configuration

The screenshot illustrates the simplification of firewall policy configuration through the use of object groups. At the top, a policy rule is shown for traffic from port3 to port2, accepting all traffic always. It references the 'Web_FTP' service group, which contains DNS, FTP, HTTP, and HTTPS services. Below this, two dialog boxes are displayed: 'New Address Group' containing 'Local_LANS' with members Lan1 and Lan2, and 'New Service Group' containing 'Web-FTP' with members DNS, FTP, HTTP, and HTTPS. Arrows point from the 'Lan1' and 'Lan2' entries in the address group to their respective members in the service group. In the final policy view at the bottom, the 'Web_FTP' service group is used instead of individual service icons.

To simplify administration, you can group service and address objects. Then, you can reference that group in the firewall policy, instead of selecting multiple objects each time, or making multiple policies.

This slide shows that four services are used to configure the policy: HTTP, HTTPS, FTP, and DNS. DNS is used by browsers to resolve URLs to IP addresses because people remember domain names for websites instead of IP addresses. If you need to make many policies for web and FTP traffic, then it makes sense to create a service object named **Web-FTP**. That way, you don't have to manually select all four services each time you make a policy. Policies can reference the **Web-FTP** service group instead.

Also, you can consolidate source addresses in source groups.

DO NOT REPRINT

© FORTINET

Object Usage

- Allows for faster changes to settings
- Reference column shows if the object is being used
 - Links directly to the referencing object

The screenshot illustrates the FortiGate GUI interface for managing objects. On the left, a configuration window titled 'Edit Policy' shows a rule for 'Internet_Access_ISP1' with source and destination set to 'all'. A callout 'Number of times object used' points to a modal window titled 'Usage of Address: all' which lists its references. The modal includes tabs for 'Edit', 'View List', 'View Properties', 'Current Usage' (which is highlighted), and 'Possible Uses'. The 'Current Usage' tab shows 'Object Name: Internet_Access_ISP1 (1) [2 References]' and 'Ref.: 1'. Another callout 'Referenced by policy ID' points to the 'Internet_Access_ISP1' row in the main table. On the right, a table titled 'Policy & Objects > Addresses' shows an IP range 'LOCAL_SUBNET' and an address object 'all' with a reference count of 5. A callout 'Reference of group' points to the 'all' row in the table. Below the table is a detailed properties window for 'Properties of Firewall Policy: 1'.

Name	Details	Interface	Type	Ref.
IP Range/Subnet 12				
LOCAL_SUBNET	10.0.1.0/24		Address	1
all	0.0.0.0/0		Address	5

Attribute	Value	Policy
policyid	1	
status	enable	
name	Internet_Access_ISP1	
uuid	b11ac58c-791b-51e7-4	
srcintf.name	port3	
dstintf.name	port1	
srcaddr.name	all	
dstaddr.name	all	

You've just seen several component objects that can be reused as you make policies. What if you want to delete an object?

If an object is being used, you can't delete it. First, you *must* reconfigure the objects that are currently using it. The GUI provides a simple way to find out where in the FortiGate's configuration an object is being referenced. Take a look at the numbers in the **Ref** column. They are the number of places where that object is being used. The number is actually a link, so if you click it, you can see which objects are using it.

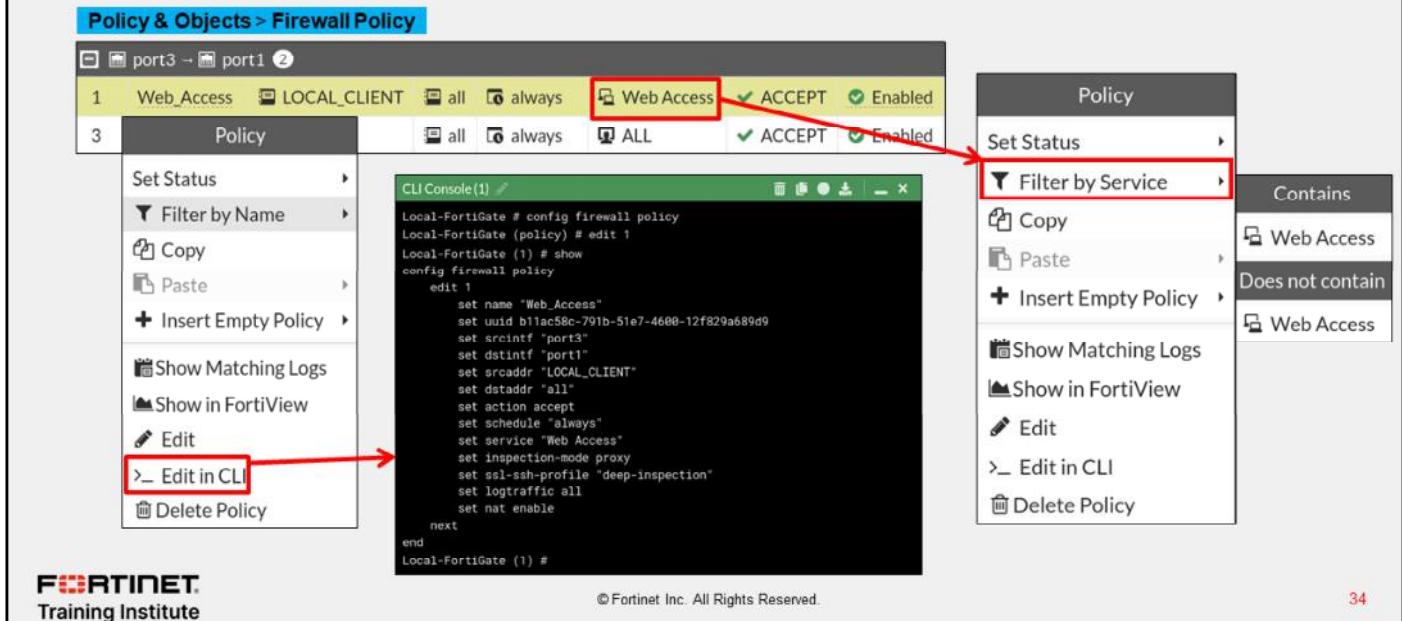
In the example shown on this slide, the **all** address object is being used by the **Training** address group and three firewall policies. If you select a firewall policy, you can use the **Edit**, **View List**, and **View Properties** tabs.

- Edit:** allows you to edit the selected object. In this example, it shows the edit page for the firewall policy ID 1.
- View List:** allows you to view selected objects in its category. In this example, it will show you the list of all the firewall policies.
- View Properties:** shows where the object is used in that configuration. In this example, address object **all** is being used in the destination address and source address of that firewall policy.

DO NOT REPRINT
© FORTINET

Firewall Policy—Fine Tuning

- Right-click menu contains various options to add and modify policies



You can right-click any firewall policy to see different menu options to edit or modify the policy. The options include enabling or disabling a firewall policy, inserting firewall policies (above or below), copying and pasting policies, and cloning reverse (only if NAT is disabled on that policy).

Clicking **Edit in CLI** opens the CLI console for the selected firewall policy or object. It shows the configured settings on the CLI and can modify the selected firewall policy or object directly on the **CLI Console**.

DO NOT REPRINT

© FORTINET

Filter Column

- You can use filters in each column to filter firewall policies

Policy & Objects > Firewall Policy

The screenshot shows the 'Firewall Policy' table in the FortiGate GUI. A search dialog is open over the table, specifically targeting the 'Name' column. The search term 'FTP' is entered, and the 'Contains' option is selected. An 'Apply' button is visible at the bottom of the dialog. A red arrow points from the 'Name' column header in the main table to the 'Name' column header in the search dialog. Below the search dialog, the main table displays a single policy row for 'FTP'.

ID	Name	Source	Destination	Schedule	Service	Action
1	Training1	port3 → port1	all	always	ALL_ICMP	ACCEPT
2	FTP	all	all	always	FTP	ACCEPT
3	Training2	port3 → port1	all	always	ALL_ICMP	ACCEPT
0	Implicit Deny	port3 → port1	all	always	ALL	DENY

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

35

You can filter firewall policies on the GUI using filters in each column. You can add the **ID** column and then click the **ID** column filter icon to filter and search policies based on policy id numbers. You can click the **Name** filter icon to search policies based on policy name, and so on.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. If you configure a firewall policy with the **any** interface, you can view the firewall policy list only in which view? _____.
 A. The By Sequence View
 B. The Interface Pair View

DO NOT REPRINT

© FORTINET

Lesson Progress



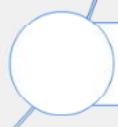
Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Good job! You now understand how to manage firewall policies on FortiGate.

Now, you'll learn about best practices and troubleshooting related to firewall policies.

DO NOT REPRINT**© FORTINET**

Best Practices and Troubleshooting

Objectives

- Identify naming restrictions for firewall policies and objects
- Reorder firewall policies for correct matching
- Demonstrate how to find matching policies for traffic type

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in knowing firewall policy restrictions and using policy matching techniques, you will be able to apply best practices and basic troubleshooting techniques when working with firewall policies.

DO NOT REPRINT**© FORTINET**

Naming Rules and Restrictions

- Most firewall object name fields accept up to 35 characters
- Supported characters in a firewall object name:
 - Numbers: 0 to 9
 - Letters: A to Z (uppercase and lower case)
 - Special characters: hyphen - and underscore _
 - Spaces
 - Avoid using spaces in general
- Some special characters are supported in passwords, comments, replacement messages, and so on
 - < > () # " " ^ ^

Policy & Objects > Addresses

New Address	
Category	Address IPv6 Address Multicast Address IPv6 Multicast Address
Name	Training(LAN) <small>Invalid characters: < > () # " "</small>
Color	<input type="button" value="Change"/>
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	<input type="checkbox"/> any
Static route configuration	<input checked="" type="radio"/>
Comments	Write a comment... <small>0/255</small>

When configuring names for firewall objects, only specific characters are supported. For example, Training (LAN) is not a valid name for an address object because it includes special characters that are not supported. Although spaces are supported in the names, as a best practice, avoid using spaces in names. Instead, use a hyphen or underscore. Using spaces can cause issues when trying to modify on the CLI, or troubleshooting.

However, many special characters are supported in passwords, comments, replacement messages, and so on.

DO NOT REPRINT
© FORTINET

Best Practices

- Test policies in a maintenance window before deploying in production
 - Test policy for a few IP addresses, users, and so on
- Be careful when editing, disabling, or deleting firewall policies and objects
 - Changes are saved and activated immediately
 - Resets active sessions
- Create firewall policies to match as specifically as possible
 - Example: Restrict firewall policies based on source, destination, service
 - Use proper subnetting for address objects
- Analyze and enable appropriate settings on a per-policy basis
 - Security profiles
 - Logging settings



© Fortinet Inc. All Rights Reserved.

40

Always plan a maintenance window and create a test case for a few IP addresses and users, before implementing configuration changes in the production network. Any configuration changes made using the GUI or CLI take effect immediately, and can interrupt service.

As a best practice, try to configure firewall policies as specifically as possible. This helps to restrict access to only those resources. For example, use correct subnets when configuring address objects.

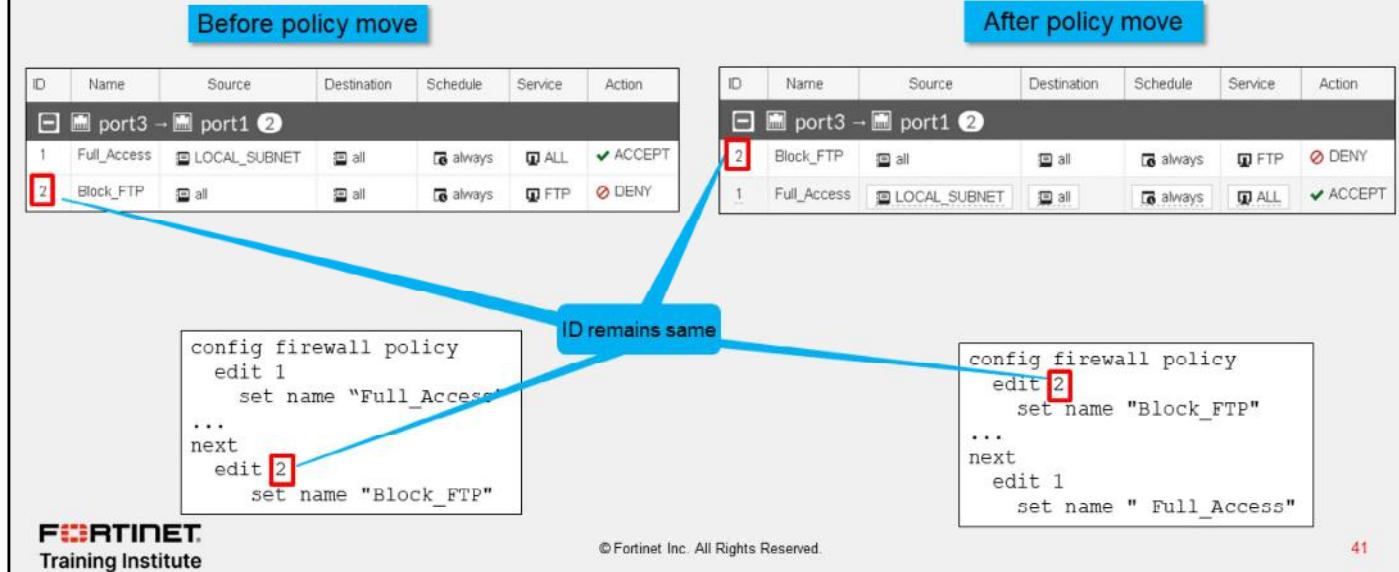
Another setting worth mentioning is security profiles. Security profiles help to provide appropriate security for your network. Proper logging configuration can also help you to analyze, diagnose, and resolve common network issues.

DO NOT REPRINT

© FORTINET

Adjusting Policy Order

- On the GUI, drag-and-drop



Remember you learned that only the first matching policy applies? Arranging your policies in the *correct position* is important. It affects which traffic is blocked or allowed. In the section of the applicable interface pair, FortiGate looks for a matching policy, beginning at the top. So, you should put more specific policies at the top; otherwise, more general policies will match the traffic first, and more granular policies will never be applied.

In the example shown on this slide, you're moving the **Block_FTP** policy (ID 2) that matches only FTP traffic, to a position above a more general **Full_Access** (accept everything from everywhere) policy. Otherwise, FortiGate would always apply the first matching policy in the applicable interface pairs—**Full_Access**—and never reach the **Block_FTP** policy.

When moving the policies across the policy list, policy IDs remain unchanged.

Note that FortiGate assigns the next highest available ID number as policies are created.

Note that policy IDs are identifiers and are not displayed by default on the policy list GUI. You can add a policy **ID** column using the **Configure Table** settings icon.

DO NOT REPRINT**© FORTINET**

Combining Firewall Policies

- Check the settings before combining firewall policies
 - Source and destination interfaces
 - Source and destination addresses
 - Services
 - Schedules
 - Security profiles
 - Logging
 - NAT rules

Can combine Policy ID 1 and 2 by combining services

Make decisions for logging settings when combining Policy ID 1 and 2

Policy & Objects > Firewall Policy

ID	Name	Source	Destin...	Schedule	Service	Action	NAT	Security Profiles	Log
port3 → port1 ②									
2	Training2	LOCAL	all	always	FTP Web Access	✓ ACCEPT ✓ Enabled	AV default WEB default SSL deep-inspection	UTM	
1	Training1	LOCAL	all	always	ALL_ICMP	✓ ACCEPT ✓ Enabled		All	

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved.

42

In order to optimize and consolidate firewall policies, always check all configured settings. In the example shown on this slide, the two firewall policies have differences in terms of services, security profiles, and logging settings. You can consolidate these two firewall policies by combining services and choosing appropriate logging settings.

If you select **Security Events** (UTM) for the logging settings, traffic logs will not be generated for **ALL_ICMP** traffic.

Note that the **ALL_ICMP** service is not subject to web filter and antivirus scans, which means that applying these security profiles to the ICMP traffic will result in the traffic passing through without being inspected.

DO NOT REPRINT**© FORTINET**

Policy Lookup (GUI)

- Identify matching policy without real traffic
 - Does not generate any packets
- Searches matching policy based on input criteria
 - Source interface
 - Protocol
 - Requires more granular input criteria
 - Source IP address
 - Destination IP/FQDN
- Policy lookup checks
 - Reverse path forward (RPF)
 - Destination NAT, if matching virtual IP
 - Route lookup, to resolve destination interface

Policy & Objects > Firewall Policy

The screenshot shows a 'Policy & Objects > Firewall Policy' window with a 'Policy Lookup' dialog. The dialog contains the following fields:

Incoming Interface	any
IP Version	IPv4
Protocol	IP
Protocol Number	1-255
Source	IP Address
Destination	IP Address/FQDN

At the bottom of the dialog are 'Search' and 'Close' buttons.

You can find a matching firewall policy based on the policy lookup input criteria. Policy lookup creates a packet flow over FortiGate without real traffic. From this, policy lookup can extract a policy ID from the flow trace and highlight it on the GUI policy configuration page.

Depending on the protocol you select (for example, TCP, UDP, IP, ICMP, and so on), you need to define other input criteria. For example, when you select TCP as the protocol, you need to define the source address, source port (optional), destination port, and destination address. When you select ICMP as the protocol, you need to define the ICMP type/code, source address, and destination address.

When FortiGate is performing policy lookup, it performs a series of checks on ingress, stateful inspection, and egress, for the matching firewall policy, from top to bottom, before providing results for the matching policy.

Note that if the firewall policy status is set to **disabled**, the policy lookup skips the disabled policy and checks for the next matching policy in the list.

When FortiGate is in Transparent mode, it does not support the policy lookup function.

DO NOT REPRINT
© FORTINET

Policy Lookup Example (GUI)

- Highlights matching policy after search

Policy & Objects > Firewall Policy

Policy Lookup

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	all	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	ALL_ICMP Web Access	ACCEPT	Enabled

Search

ID	Name	Source	Destination	Schedule	Service	Action	NAT
1	Training1	LOCAL_CLIENT	all	always	ALL_ICMP	ACCEPT	Enabled
2	FTP	all	all	always	FTP	ACCEPT	Enabled
3	Training2	LOCAL_SUBNET	Fortinet_FQDN	always	ALL_ICMP Web Access	ACCEPT	Enabled

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

44

Based on the input criteria, after clicking **Search**, the trace result is selected and highlighted on the **Firewall Policy** page.

Why didn't policy **ID #1** or **ID #2** match the input criteria?

Because policy **ID #1** status is set to **disable**, policy lookup skips the disabled policy. For firewall policy **ID #2**, it doesn't match the destination port specified in the policy lookup matching criteria.

DO NOT REPRINT

© FORTINET

Knowledge Check

1. Which of the following naming formats is correct when configuring a name for a firewall address object?
 A. Good_Training
B. Good(Training)

2. What is the purpose of the policy lookup feature on FortiGate?
 A. To find a matching policy based on input criteria
B. To block traffic based on input criteria

DO NOT REPRINT

© FORTINET

Lesson Progress



Firewall Policies



Configuring Firewall Policies



Managing Firewall Policies



Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

DO NOT REPRINT**© FORTINET**

Review

- ✓ Identify components of firewall policies
- ✓ Identify how FortiGate matches traffic to firewall policies
- ✓ Restrict access and make your network more secure using security profiles
- ✓ Configure logging
- ✓ Identify policy list views
- ✓ Understand the use of policy IDs
- ✓ Identify where an object is referenced
- ✓ Identify naming restrictions for firewall policies and objects
- ✓ Reorder firewall policies for correct matching
- ✓ Demonstrate how to find matching policies for traffic type



© Fortinet Inc. All Rights Reserved.

47

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure, use, and manage firewall policies.

DO NOT REPRINT

© FORTINET



FortiGate Security

Network Address Translation



Last Modified: 23 August 2022

In this lesson, you will learn how to configure network address translation (NAT) and use it to implement source NAT (SNAT) and destination NAT (DNAT) for the traffic passing through FortiGate.

DO NOT REPRINT

© FORTINET

Lesson Overview



Introduction to NAT



Firewall Policy NAT



Central NAT



Best Practices and Troubleshooting

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT

© FORTINET

Introduction to NAT

Objectives

- Understand NAT and port address translation (PAT)
- Understand the different configuration modes available for NAT

After completing this section, you should be able to achieve the objectives shown on this slide.

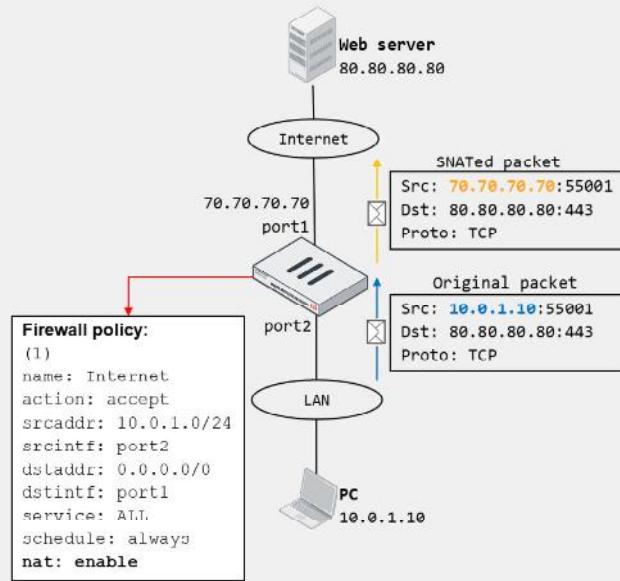
By demonstrating competence in understanding how NAT and PAT work, and the available NAT configuration modes, you will be well-positioned to plan the implementation of NAT in your network.

DO NOT REPRINT

© FORTINET

NAT

- Method of translating IP addresses in a packet
 - If ports are also translated, it is called PAT
- Benefits:
 - Real address is hidden from external networks
 - Prevents depletion of public IP address space
 - Private address space flexibility
- Types:
 - SNAT
 - Translates source IP address and source port
 - Enabled on firewall policy or using central SNAT rules
 - DNAT
 - Translates destination IP address and destination port
 - Requires VIP object on firewall policy
 - In central NAT, no need to reference VIP on firewall policy
- NAT64 and NAT46
 - Translates IPv6 to IPv4, and the reverse
- NAT66
 - NAT between two IPv6 networks



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

4

NAT is a method that enables a NAT device such as a firewall or router, to translate (or map) the IP address in a packet to another IP address, usually for connectivity purposes. If the port information in the packet is also translated, then the translation method is called PAT. NAT provides the following benefits:

- Security: The real address of a device is hidden from external networks.
- Public address depletion prevention: Hundreds of computers can share the same public IPv4 address.
- Private address flexibility: The addresses can stay the same, even if ISPs change. You can reuse private addresses in multiple networks.

There are two types of NAT: SNAT and DNAT. In SNAT, a NAT device translates the source IP address and source port in a packet. In DNAT, a NAT device translates the destination IP address and destination port. You can configure FortiGate to perform SNAT and DNAT as follows:

- For SNAT, you enable NAT on the matching firewall policy. Alternatively, you can enable central NAT to configure central SNAT rules for the VDOM.
- For DNAT, you configure virtual IPs (VIPs) and then reference them on the matching firewall policy. If you enable central NAT, you configure central DNAT rules and VIP objects for DNAT.

The example on this slide shows the most common use case for NAT: SNAT. FortiGate, acting as a NAT device, translates the private IP address assigned to the PC to the public address assigned by your ISP. The private-to-public source address translation is needed for the PC to access the internet web server.

NAT64 and NAT46 refer to the methods that translate an IPv6 address to an IPv4 address and the reverse, respectively. They enable you to communicate IPv6 networks with IPv4 networks, and the reverse. NAT66 consists of translating addresses between two IPv6 networks.

DO NOT REPRINT**© FORTINET**

Configuration Modes for NAT

- There are two ways to configure SNAT and DNAT:
 - Firewall policy NAT
 - You configure SNAT and DNAT on firewall policies
 - SNAT uses the outgoing interface address or configured IP pool
 - DNAT uses the configured VIP as the destination address
 - Central NAT
 - You configure SNAT and DNAT per virtual domain
 - It applies to multiple firewall policies, based on SNAT and DNAT rules
 - Configure SNAT rule in central SNAT policy
 - Configure DNAT using DNAT and VIP objects

You configure NAT using firewall policy NAT mode or central NAT.

When you use firewall policy NAT mode, you must configure SNAT and DNAT for each firewall policy.

When you use central NAT, you configure NAT per virtual domain by configuring SNAT and DNAT rules. The result is that SNAT and DNAT settings automatically apply to multiple firewall policies, as opposed to each firewall policy in firewall policy NAT.

As a best practice, when you use central NAT, you should configure specific SNAT and DNAT rules so that they match only the desired firewall policies in your configuration.

Both firewall policy NAT and central NAT produce the same results; however, some deployment scenarios are best suited to firewall policy NAT and some are best suited to central NAT.

Firewall policy NAT is suggested for deployments that include relatively few NAT IP addresses and where each NAT IP address would have separate policies and security profiles. Central NAT is suggested for more complex scenarios where multiple NAT IP addresses have identical policies and security profiles, or in next generation firewall (NGFW) policy mode, where the appropriate policy may not be determined at the first packet.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is a benefit of using NAT?

- A. Prevents depletion of IPv4 public address
- B. Enhanced content inspection

2. Which statement about NAT66 is true?

- A. It is used to translate addresses between two IPv6 networks.
- B. It is used to translate addresses between two IPv4 networks.

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

Good job! You now know about NAT.

Now, you'll learn about firewall policy NAT.