



FortiGate Administrator

Firewall Policies and NAT

FortiOS 7.4

Last Modified: 8 May 2024

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.

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.

Firewall Policies

Objectives

- Configure IPv4 firewall policy
- Monitor traffic logs from firewall policy
- Choose inspection modes for 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.

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	NAT	AV default WEB default SSL deep-inspection	UTM
2	Internet_Access_ISP2	all	all	always	ALL	ACCEPT	NAT	AV default WEB default SSL deep-inspection	UTM
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.

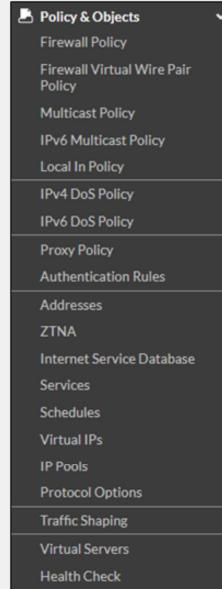
Components and Policy Types

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 (IPv4, IPv6)
- 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.

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)

Name	Value
Incoming Interface	LAN (port3)
Outgoing Interface	ISP1 (port1)
Source	LOCAL_CLIENT
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Select Entries

Address	User	Internet Service
ADDRESS (17)		
all		
FABRIC_DEVICE		
FIREWALL_AUTH_PORTAL_ADDRESS		
gmail.com		
LOCAL_CLIENT		
LOCAL_SUBNET		
LOCAL_WINDOWS		

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.

You can configure 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.

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	Full_Access
Incoming Interface	LAN (port3)
Outgoing Interface	ISP1 (port1)
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL

Action: **✓ ACCEPT** **✗ DENY**

FORTINET
Training Institute
© Fortinet Inc. All Rights Reserved.
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
- **Schedule**: Specific times to apply policy
- **Service**: IP protocol and port number

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**.

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

Policy & Objects > Firewall Policy

Create New Policy

Name	Single_Interface
Incoming Interface	port4
Outgoing Interface	port5

Multiple interface policies disabled

System > Feature Visibility

Multiple Interface Policies

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

Policy & Objects > Firewall Policy

Create New Policy

Name	Multiple.Interfaces
Incoming Interface	port7 port8
Outgoing Interface	any

Multiple interface policies enabled

© Fortinet Inc. All Rights Reserved. 7

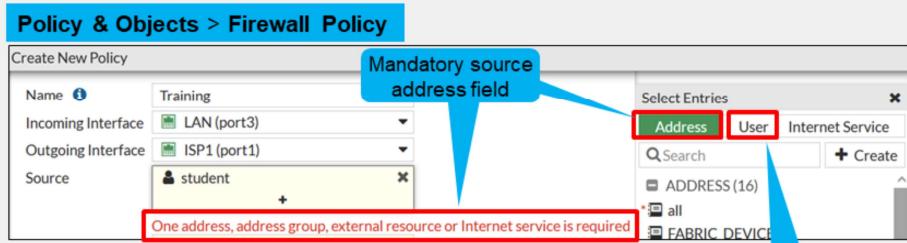
By default, you can select only a single interface as the incoming interface and a single interface as the outgoing interface. This is because the option to select multiple interfaces, or **any** interface in a firewall policy, is disabled on the GUI. However, you can enable the **Multiple Interface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

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
- ISDB and geography are valid with a valid support contract



One address, address group, external resource or Internet service is required

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.

FortiGate devices with valid FortiCare support contract receive up-to-date information to use the ISDB and geography database and use them as firewall objects.

Example—Matching Policy by Source

- Matches by source address, user
- Source as ISDB objects

The screenshot shows the 'Policy & Objects > Firewall Policy' interface. A policy named 'Training' is selected. In the 'Source' field, two entries are listed: 'LOCAL SUBNET' and 'student'. The 'student' entry is highlighted with a red box. Below the interface, two blue callout boxes point to these entries: one labeled 'User' pointing to 'student', and another labeled 'Address' pointing to 'LOCAL SUBNET'.

The screenshot shows the same 'Policy & Objects > Firewall Policy' interface. The 'Source' field now contains 'Alibaba-Alibaba.Cloud' and 'Amazon-AWS', both highlighted with red boxes. To the right, a 'Select Entries' sidebar is open, showing a list of objects including 'Internet Service'. The 'Internet Service' option is highlighted with a green box. A blue callout box points from the 'Internet service' label to the 'Internet Service' entry in the sidebar.

FORTINET
Training Institute
© Fortinet Inc. All Rights Reserved.
9

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 ISDB objects as a source in the firewall policy. There is an either/or relationship between ISDB 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.

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
- 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.

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	Profile	Status	Action
AntiVirus	AV default	<input checked="" type="checkbox"/>	
Web Filter	WEB default	<input checked="" type="checkbox"/>	
Video Filter	VF video_filter	<input checked="" type="checkbox"/>	
DNS Filter	DNS default	<input checked="" type="checkbox"/>	
Application Control	APP default	<input checked="" type="checkbox"/>	
IPS	IPS default	<input checked="" type="checkbox"/>	
File Filter	FILE default	<input checked="" type="checkbox"/>	
Email Filter	EMAIL default	<input checked="" type="checkbox"/>	
DLP Profile	DLP default	<input checked="" type="checkbox"/>	
SSL Inspection	SSL deep-inspection	<input type="checkbox"/>	
Decrypted Traffic Mirror		<input type="checkbox"/>	

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 options are not visible on the policy page on the GUI. You need to enable them on the **Feature Visibility** page.

Policy ID

- Firewall policies are primarily ordered on a top-down basis
- Policy IDs are identifiers:
 - The system assigns policy ID when the rule is created
 - The ID number never changes as rules move higher or lower in the sequence

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

Policy & Objects > Firewall Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT
	LAN (port3) → DMZ (port2)	1					
3	DMZ	4 all	4 all	always	ALL	✓ ACCEPT	✓ NAT
	LAN (port3) → ISP1 (port1)	2					
2	Block_FTP	4 all	4 all	always	FTP	✗ DENY	
1	Full_Access	4 LOCAL_SUBNET	4 all	always	ALL	✓ ACCEPT	✓ NAT
	Implicit	1					

Policy ID

```
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. You can add or remove the 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.

Policy List—Interface Pair View and By Sequence

- **Interface Pair View**

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

ID	Name	Source	Destination	Schedule	Action	NAT	Type	Security	Bytes
1	LAN (port3) → DMZ (port2)	all	all	always	ALL	ACCEPT	NAT	Standard	no-inspection
3	DMZ	all	all	always	FTP	DENY		Standard	no-inspection
2	LAN (port3) → ISP1 (port1)	all	all	always	ALL	ACCEPT	NAT	Standard	no-inspection
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT	NAT	Standard	no-inspection

- **Sequence Grouping View and By Sequence**

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

ID	Name	From	To	Source	Destination	Schedule	Action	NAT	Bytes
1	Block_FTP	LAN (port3)	ISP1 (port1)	all	all	always	FTP	DENY	0 B
1	Full_Access	LAN (port3)	ISP1 (port1)	LOCAL_SUBNET	all	always	ALL	ACCEPT	0 B
3	DMZ	LAN (port3)	DMZ (port2)	DMZ	all	always	ALL	ACCEPT	0 B

Firewall policies appear in an organized list. The list is organized as one of **Interface Pair View**, **Sequence Grouping 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 **Sequence Grouping View** or **By Sequence** at the top of the page. In these two views, the policies are also listed in the order in which they are evaluated for traffic matching—they are grouped as uncategorized in **Sequence Grouping View** layout. You can create new labels to group firewall policies as necessary to organize the firewall policies with the sequence order in mind.

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.

Adjusting Policy Order

- On the GUI, drag-and-drop

Before policy move

ID	Name	From	To	ID
1	Full_Access	LAN (port3) DMZ (port2)	ISP1 (port1)	4 4
2	Block_FTP	LAN (port3)	ISP1 (port1)	4
3	DMZ	LAN (port3)	DMZ (port2)	4

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

After policy move

ID	Name	From	To	ID
2	Block_FTP	LAN (port3)	ISP1 (port1)	4 a
1	Full Access	LAN (port3) DMZ (port2)	ISP1 (port1)	4 b
3	DMZ	LAN (port3)	DMZ (port2)	4 c

ID remains same

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

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.

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	Destination	Schedule	Service	Action	NAT	Type	Security Profiles	Logs	Bytes	
	LAN (port3) → ISP1 (port1) ②											
1	Full_Access	LOCAL_SUBNET DMZ	all	always	Web Access FTP	✓ ACCEPT	✓ NAT	Standard	AV default WEB default SSL deep-inspection	UTM	28.95 kB	
2	ICMP	all	all	always	ALL ICMP	✓ ACCEPT	✓ NAT	Standard	SSL no-inspection	All	0 B	
Implicit 1												
0	Implicit Deny	all	all	always	ALL	✗ DENY				Disabled	58.21 kB	

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.

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
 - Re-evaluate 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

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.

Inspection Modes on Firewall Policies

- Enabling profiles has an impact on firewall throughput
- FortiGate kernel inspect sessions to enforce filtering (for example, web filter)
- Selecting the FortiGate inspection modes on firewall policies:
 - Flow-based
 - Default mode
 - Optimize performance
 - Proxy-based
 - Processed by CPU
 - Provides thorough inspection
 - Support advanced features like *safe search*

Policy & Objects > Firewall Policy

Create New Policy

Name	Internet_Access
Type	Standard ZTNA
Incoming Interface	LAN (port3) <input type="button" value="X"/>
	+ <input type="button" value=""/>
Outgoing Interface	ISP1 (port1) <input type="button" value="X"/>
	+ <input type="button" value=""/>
Source	LOCAL_SUBNET <input type="button" value="X"/>
	+ <input type="button" value=""/>
Destination	all <input type="button" value="X"/>
	+ <input type="button" value=""/>
Schedule	always <input type="button" value=""/>
Service	ALL <input type="button" value="X"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
<input type="button" value="Inspection Mode"/> Flow-based Proxy-based	

Enabling the security profiles on the FortiGate impacts on firewall resources and throughput. Packets are sent to the kernel or main CPU to enforce filtering. FortiOS supports flow-based and proxy-based inspection in firewall policies and security profiles.

Depending on your requirements, you can select inspection mode, but it is useful to know some differences and how it can impact the firewall performance. Flow-based inspection identifies and blocks threats in real time as FortiOS identifies them typically requires lower processing resources than proxy-based inspection. It is recommended to apply flow-based inspection to policies that prioritize traffic throughput.

Proxy-based inspection involves buffering traffic and examining it as a whole before determining an action. Having all the data to analyze allows for the examination of more data points than flow-based inspection. Some advanced features like usage quota, safe search, and web-profile override are also supported in proxy-based inspection.

Inspection Modes—Proxy-based Visibility

- Proxy-based inspection mode is available on most FortiGate devices
- Some security profiles are available only in proxy-based inspection mode, such as:
 - Video Filter
 - Inline CASB
 - ICAP
 - Web Application Firewall
 - Data Leak Prevention (available on CLI)
- Low-end platforms with 2 GB of RAM or less do not display the option on the GUI
 - Firewall inspection mode setting is not available on GUI—only on CLI
 - GUI option is available on low-end platforms when enabled on CLI:

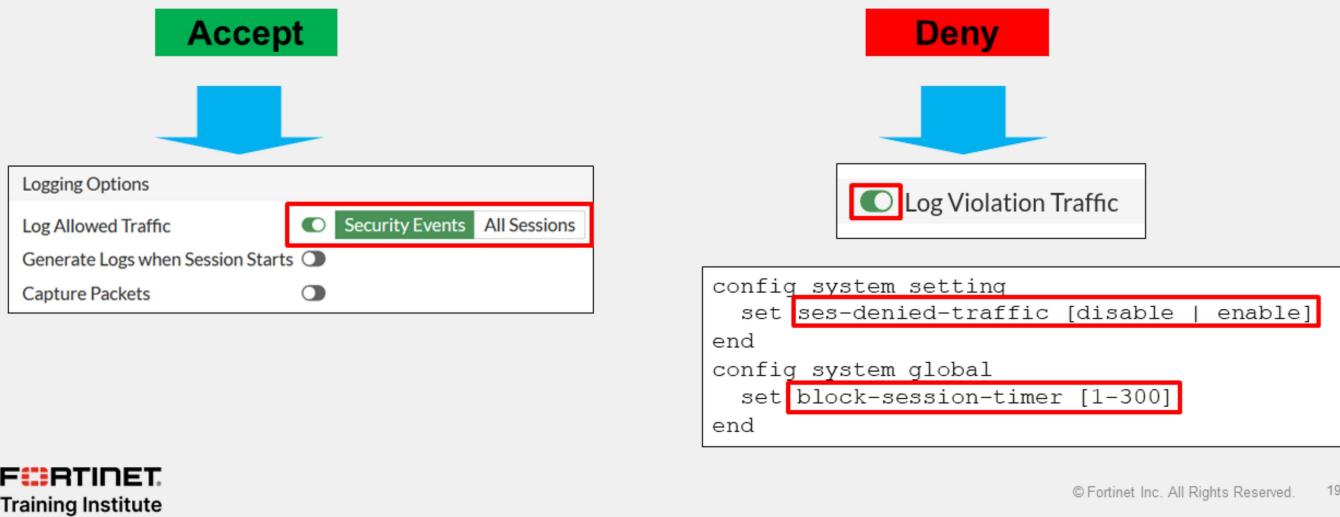
```
config system settings
    set gui-proxy-inspection enable
end
```

By default, low-end FortiGate platforms with RAM of 2 GB or less do not show proxy-based settings on the GUI for firewall policies and security profiles. This is to reduce memory usage on these platforms as the RAM is designed to serve the purpose of the low-end FortiGate and also to maximize security using flow-based security inspection across FortiGate.

The option to configure proxy-based inspection mode on firewall policies and security profiles is available using the CLI command `config system settings`.

Logging

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 19

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 only for 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 perform a policy lookup for each new packet matching the denied session, which reduces CPU usage and log generation.

The CLI command is `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. Regardless of internal storage, the CLI command is set `logtraffic-start enable`.

Monitor Traffic Logs

- FortiGate supports storing all type of logs in several log devices
 - FortiGate local and cloud
 - FortiAnalyzer local and cloud
 - Syslog
- View traffic logs in **Log & Report > Forward Traffic**
 - Apply filter to display relevant logs
 - Select the source of logs
 - Specify the historical time frame
- Right-click firewall policy and view matching traffic logs

The screenshot shows two windows from the FortiGate Management Interface:

- Log & Report > Forward Traffic**: A table displaying network traffic logs. The columns include Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID. The table shows various log entries such as NTP, HTTPS, and TCP/53 requests.
- Policy & Objects > Firewall Policy**: A list of firewall policies. A context menu is open over the first policy (ID 1), with the "Show matching logs" option highlighted.

A blue callout bubble points to the "Show matching logs" option in the context menu, stating: "Only logs matching the firewall policy are displayed in the forward traffic logs page". Another blue callout bubble points to the search bar at the top of the Log & Report page, stating: "Apply the filter desired to reduce irrelevant log entries".

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 20

Logging on FortiGate records the traffic that passes through, starts from, or ends on FortiGate. It records the actions during the traffic scanning process. FortiGate supports sending all log types to several log devices including its local storage which is subject to the disk available on different FortiGate models.

You can view traffic logs in **Log & Report > Forward Traffic**. Apply the filter needed to display the logs and then enter the policy UUID in the filter field to display records that match the firewall policy. Select the source of the logs and specify the historical time frame to reduce irrelevant log entries.

You can also view the logs by right-clicking the firewall policy, and then clicking on **Show matching logs**.

Geographic-Based Internet Service Database

- By default, ISDB updates are enabled
- 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

Policy & Objects > Internet Service Database

Edit Internet Service

Name	Training-Location-ISDB	Primary Internet Service Name Google-Other
Type	Predefined Geographic Based	Primary Internet Service ID 65536
Primary Internet Service	Google-Other	Direction Both
Country/Region	United States	Entries
Region	California	
City	Sunnyvale	

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.

Knowledge Check

1. Which 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
 B. At least one source user and one source address object

3. 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

NAT

Objectives

- Configure SNAT
- Configure a firewall policy to perform DNAT using VIP

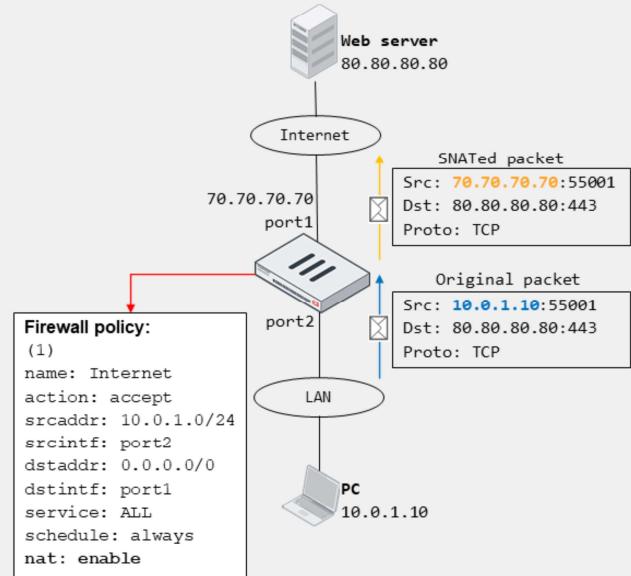
Now, you'll learn about NAT with firewall policies.

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

By demonstrating competence in these areas, you will be able to configure firewall policies and apply appropriate SNAT and DNAT, and understand how it is applied to the traffic traversing through FortiGate.

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
 - DNAT**
 - Translates destination IP address and destination port
 - Requires VIP object on firewall policy



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.
- For DNAT, you configure virtual IPs (VIPs) and then reference them on the matching firewall policy.

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.

Firewall Policy SNAT

- There are two ways to SNAT traffic:
 - Using the outgoing interface address
 - Using the dynamic IP pool

Policy & Objects > Firewall Policy

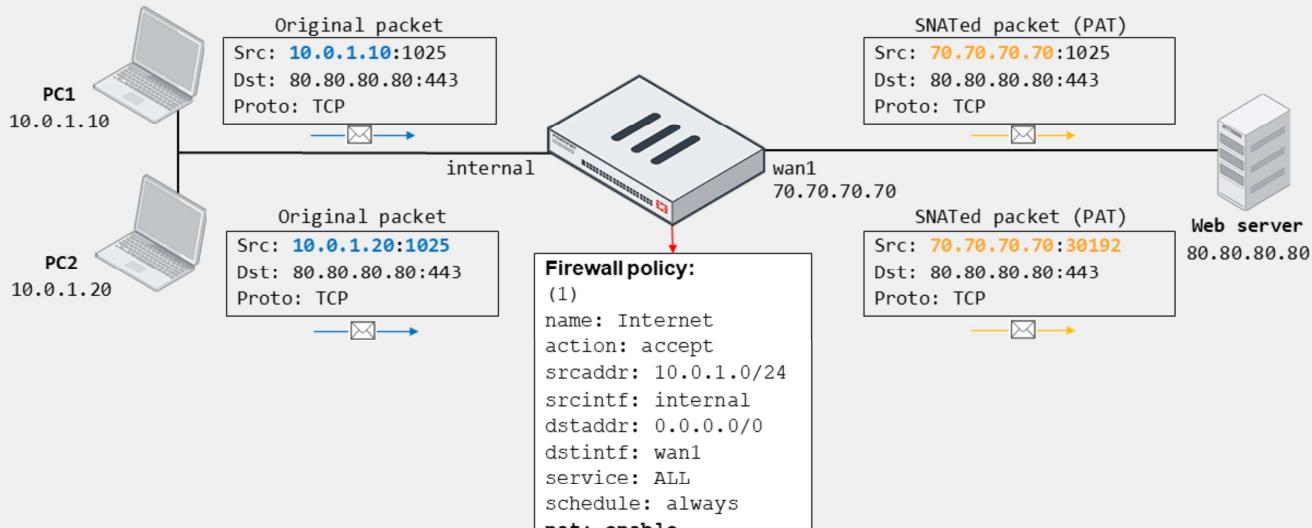
Create New Policy

Name	Full_Access
Type	Standard ZTNA
Incoming Interface	LAN (port3)
Outgoing Interface	ISP1 (port1)
Source	LOCAL_SUBNET
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input checked="" type="radio"/> Proxy-based
Firewall/Network Options	
NAT	<input checked="" type="radio"/>
IP Pool Configuration	<input type="radio"/> Use Outgoing Interface Address <input checked="" type="radio"/> Use Dynamic IP Pool
Preserve Source Port	<input type="radio"/>
Protocol Options	PROT default

To configure a firewall policy, you can enable SNAT in the firewall and network options section. There are two options to select and choose how SNAT should work:

1. To use the outgoing interface IP address: Packets matching the firewall policy translate the IP address in a packet to another IP address, usually for connectivity purposes.
2. To use the dynamic IP pool: This is dynamic SNAT which allows FortiGate to map private IP addresses to the first available public address from a pool of addresses.

Firewall Policy SNAT Using the Outgoing Interface



When you select **Use Outgoing Interface Address** on the matching firewall policy, FortiGate uses the egress interface address as the NAT IP for performing SNAT.

If there are multiple devices behind FortiGate, FortiGate performs many-to-one NAT. This is also known as PAT. FortiGate assigns to each connection sharing the egress interface address a port number from a pool of available ports. The assignment of a port enables FortiGate to identify packets associated with the connection and then perform the corresponding translation. This is the same behavior as the overload IP pool type, which you will also learn about.

Optionally, you may select a fixed port, in which case the source port translation is disabled. With a fixed port, if two or more connections require the same source port for a single IP address, only one connection is established.

The example on this slide shows two PCs behind FortiGate that share the same public IP address (70.70.70.70) to access the internet web server 80.80.80.80. Because **Use Outgoing Interface Address** is enabled on the firewall policy—set `nat enable` on the CLI—the source IP address of the PCs is translated to the egress interface address. The source port, however, is not always translated. It depends on the available ports and the connection 5-tuple. In the example shown on this slide, FortiGate translates the source port of the connection from PC2 only. Otherwise, the two connections would have the same information on the session table for the reply traffic, which would result in a session clash.

IP Pools

- IP pools define a single IP address or a range of IP addresses to be used as the source address for the duration of the session
- IP pools are usually configured in the same range as the interface IP address
- There are four types of IP pools:
 - Overload (default)
 - One-to-one
 - Fixed port range
 - Port block allocation

Useful for CGN

Policy & Objects > IP Pools

New Dynamic IP Pool

Name	<input type="text"/>
Comments	<input type="text"/> Write a comment... /255
Type	<input checked="" type="radio"/> Overload <input type="radio"/> One-to-One <input type="radio"/> Fixed Port Range <input type="radio"/> Port Block Allocation
External IP address/range	<input type="text"/> 0.0.0.0-0.0.0
NAT64	<input type="checkbox"/>
ARP Reply	<input type="checkbox"/>

Policy & Objects > Firewall Policy

Edit Policy

Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY
Inspection Mode	Flow-based <input checked="" type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input checked="" type="checkbox"/>
IP Pool Configuration	<input type="checkbox"/> Use Outgoing Interface Address <input checked="" type="checkbox"/> Use Dynamic IP Pool <input checked="" type="radio"/> INTERNAL-HOST-EXT-IP <input type="checkbox"/>

Fortinet
Training Institute

© Fortinet Inc. All Rights Reserved.

27

IP pools allow sessions leaving the FortiGate firewall to use NAT. An IP pool defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session. These assigned addresses are used instead of the IP address assigned to that FortiGate interface.

IP pools are usually configured in the same range as the interface IP address.

When you configure the IP pools that will be used for NAT, there is a limitation that you must take into account. If the IP addresses in the IP pool are different from the IP addresses that are assigned to the interfaces, communications based on those IP addresses *may fail if the routing is not properly configured*. For example, if the IP address assigned to an interface is 172.16.100.1/24, you cannot choose 10.10.10.1 to 10.10.10.50 for the IP pool unless you configure appropriate routing.

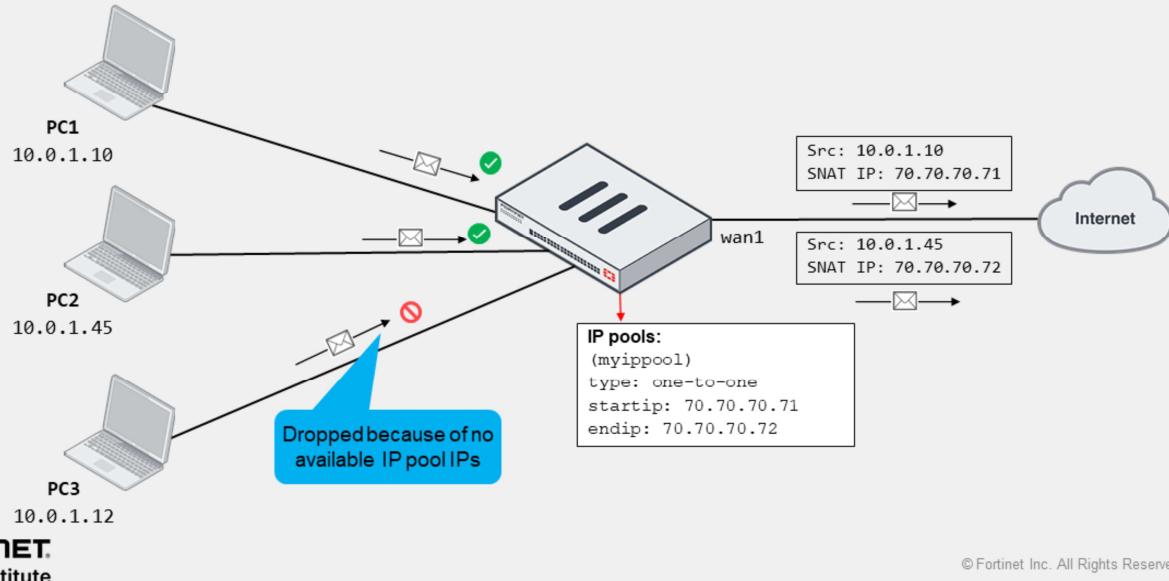
There are four types of IP pools that you can configure on the FortiGate firewall:

- Overload
- One-to-one
- Fixed port range
- Port block allocation

The fixed port range and port block allocation types are more common carrier-grade NAT (CGN) deployments.

IP Pool Type—One-to-One

- Assigns an IP pool address to an internal host on a first-come, first-served basis
 - Packets from unserved hosts are dropped if there are no available addresses in the IP pool



© Fortinet Inc. All Rights Reserved.

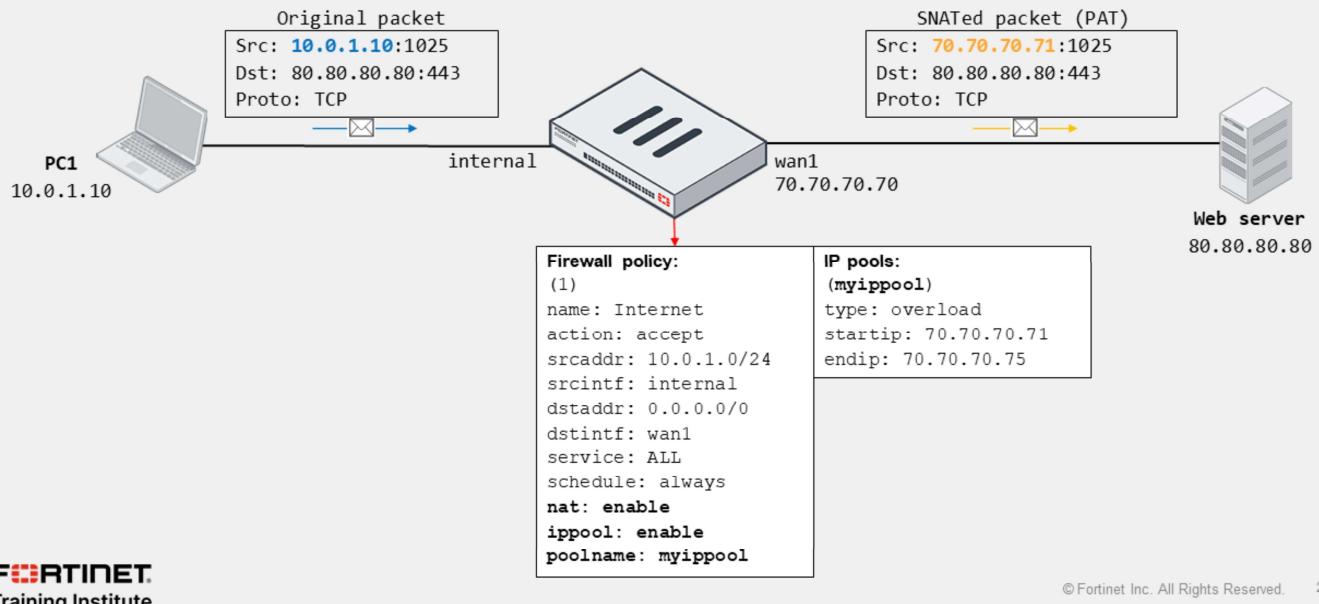
28

In the one-to-one pool type, FortiGate assigns an IP pool address to an internal host on a first-come, first-served basis.

There is a single mapping of an internal address to an external address. That is, an IP pool address is not shared with any other internal host, thus the name one-to-one. If there are no more addresses available in the IP pool, FortiGate drops packets from unserved hosts.

The example on this slide shows three internal hosts accessing the internet. PC1 and PC2 packets are received first by FortiGate and, therefore, served with addresses 70.70.70.71 and 70.70.70.72, respectively. However, FortiGate drops packets sourced from PC3 because they arrived last, which is when there are no more available addresses in the IP pool to choose from.

IP Pool Type—Overload



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 29

If you use an IP pool, the source address is translated to an address from that pool, rather than the egress interface address. The larger the number of addresses in the pool, the greater the number of connections that the pool can support.

The default IP pool type is overload. In the overload IP pool type, a many-to-one or many-to-few relationship and port translation is used.

In the example shown on this slide, source IP 10.0.1.10 is translated to the address 70.70.70.71, which is one of the addresses defined in the IP pool (70.70.70.71 – 70.70.70.75).

VIPs

- DNAT objects
- Default type is **Static NAT**
 - One-to-one mapping, applies to both:
 - Ingress traffic (DNAT; use internal IP as NAT IP)
 - Egress traffic (SNAT; use external IP as NAT IP)
 - Reference IP addresses or FQDN objects (set **Type** to **FQDN**)
- Enable **Port Forwarding** to:
 - Redirect traffic destined to external IP and port to mapped internal address and port
 - Reuse external IP on multiple VIPs

The screenshot shows two configuration screens from the FortiGate management interface:

- Policy & Objects > Virtual IPs**: A form for creating a new Virtual IP object named "VIP-INTERNAL-HOST". It specifies "port1" as the interface, "Static NAT" as the type, and "100.64.100.22" as the external IP address/range. The "Map to" field contains "10.1.1.10".
- Policy & Objects > Firewall Policy**: A form for creating a new firewall policy named "Web Server Access". It defines "port1" as the incoming interface and "port3" as the outgoing interface. The "Source" is set to "all". Under "Destination", there is a list containing "VIP-INTERNAL-HOST". The "Action" section includes "ACCEPT" and "DENY" buttons.

A red arrow points from the "VIP-INTERNAL-HOST" entry in the Destination list of the Firewall Policy screen to the "VIP used as destination in firewall policy" callout box.

FORTINET
Training Institute

30

VIPs are DNAT objects. For sessions matching a VIP, the destination address is translated; usually a public internet address is translated to the private network address of a server. VIPs are selected in the firewall policy **Destination** field.

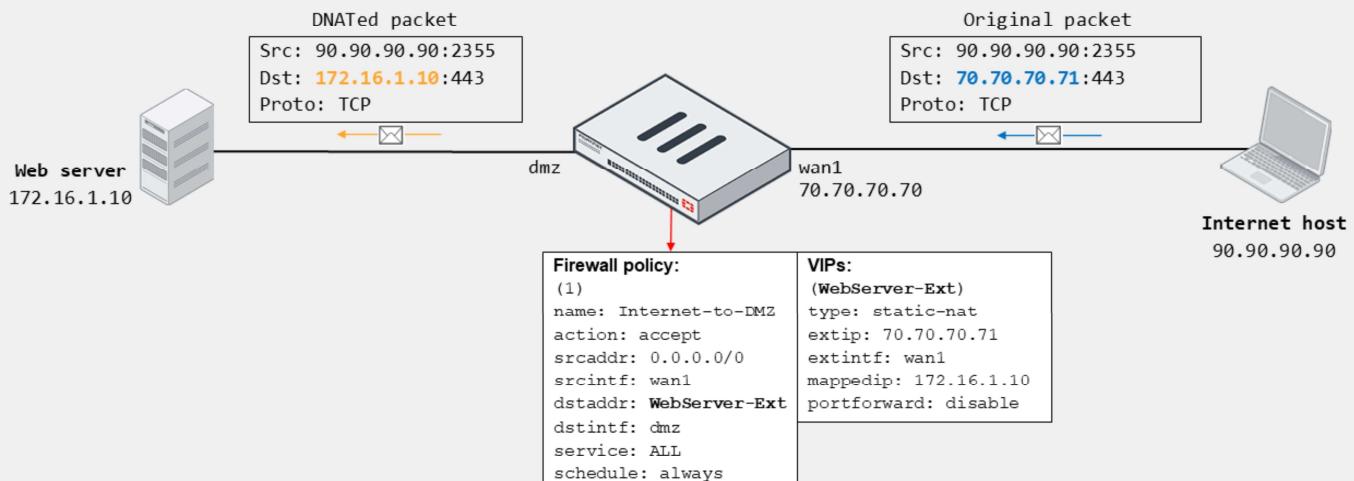
The default VIP type is **Static NAT**. This is a one-to-one mapping. This means that:

1. FortiGate performs DNAT on ingress traffic destined to the external IP address defined in the VIP, regardless of the protocol and port of the connection, provided the matching firewall policy references the VIP as **Destination**.
2. FortiGate uses as NAT IP the external IP address defined in the VIP when performing SNAT on all egress traffic sourced from the mapped address in the VIP, provided the matching firewall policy has NAT enabled. That is, FortiGate doesn't use the egress interface address as NAT IP.

Note that you can override the behavior described in step 2 by using an IP pool. You can also select **FQDN** as **Type**. When you select **FQDN**, you can configure FQDN address objects as external and internal IP addresses. This enables FortiGate to automatically update the external and internal IP addresses used by the VIP in case the FQDN resolved address changes.

Optionally, you can enable **Port Forwarding** on the VIP to instruct FortiGate to redirect the traffic matching the external address and port in the VIP to the mapped internal address and port. When you enable port forwarding, FortiGate no longer performs one-to-one mapping. This means that you can reuse the same external address and map it to different internal addresses and ports provided the external port is unique. For example, you can configure a VIP so connections to the external IP 70.70.70.70 on port 8080 map to the internal IP 192.168.0.70 on port 80. You can then configure another VIP so connections to the external IP 70.70.70.70 on port 8081 map to the internal IP 192.168.0.71 on port 80.

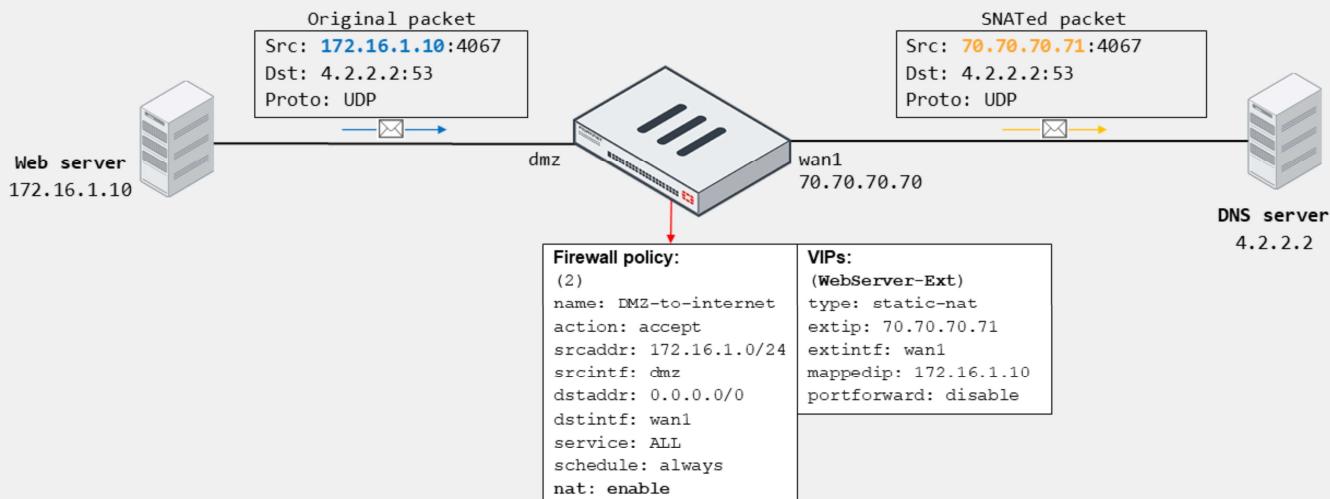
VIP Example—Static NAT—Incoming Connection



In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the WebServer-Ext VIP as destination. Because the VIP is configured as static NAT and has port forwarding disabled, then FortiGate translates the destination address of the packet to 172.16.1.10 from 70.70.70.71. Note that the destination port doesn't change because port forwarding is disabled.

Also note that the external interface address is different from the external address configured in the VIP. This is not a problem as long as the upstream network has its routing properly set. You can also enable ARP reply on the VPN (enabled by default) to facilitate routing on the upstream network. You will learn more about ARP reply in this lesson.

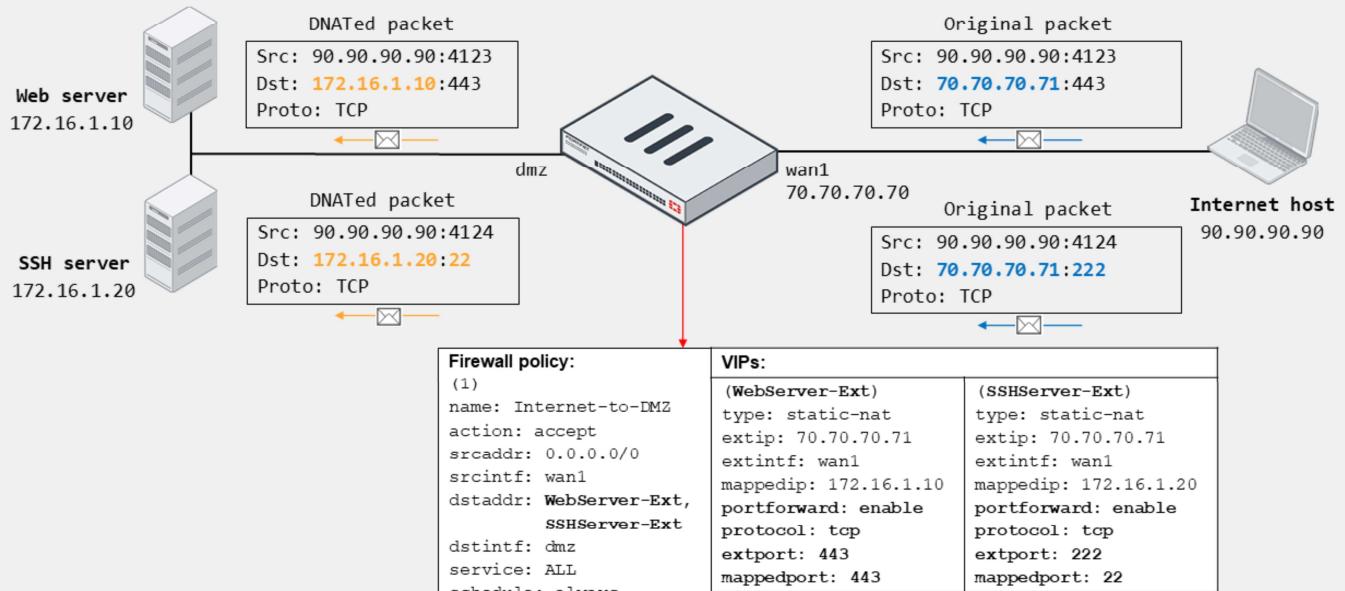
VIP Example—Static NAT—Outgoing Connection



Now, suppose that the internal web server (172.16.1.10) initiates a DNS connection to the internet DNS server (4.2.2.2). On FortiGate, the traffic matches the firewall policy ID 2, which has `nat` enabled. Because the source address matches the internal address of the VIP, and because the VIP is configured as static NAT with port forwarding disabled, FortiGate translates the source address of the packet to 70.70.70.71 from 172.16.1.10. Note that FortiGate doesn't have to perform PAT because the static NAT VIP equals one-to-one mapping. That is, the external IP is used by the web server only for SNAT.

Also note that FortiGate uses the VIP external address for SNAT if the VIP is referenced in an incoming firewall policy. That is, if you don't configure firewall policy ID 1, which is shown on the previous slide, or if you disable the firewall policy, then FortiGate doesn't automatically use the external IP for translating the source address of the web server. Instead, FortiGate uses the egress interface address (70.70.70.70).

VIP Example—Port Forwarding—Incoming Connection



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 33

The example on this slide shows how FortiGate handles two incoming connections to the same external address, but on different ports. FortiGate forwards each connection to a different internal host based on the VIP mapping settings. This is possible because port forwarding is enabled on the VIPs, which enables FortiGate to redirect the external traffic to the corresponding internal address and port, while using the same external address.

Both connections match the firewall policy ID, which references two VIPs as destination. The HTTPS connection matches the WebServer-Ext VIP, and the SSH connection matches the SSHServer-Ext VIP. Note that for the SSH connection, FortiGate also translates the destination port to 22 from 222.

Although not shown on this slide, outgoing connections sourced from the web and SSH server would result in FortiGate using as NAT IP the egress interface address for SNAT, providing there is a matching firewall policy with `nat` enabled.

VIP—Matching Policies

- Default behavior: Firewall address objects do not match VIPs
 - Doesn't block an egress-to-ingress connection, even when the deny policy is at the top of the list
- VIP policy (WAN to LAN)

ID	Name	Source	Destination	Schedule	Service	Action
port1 → port3 ②						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_Access	all	Web_Server	always	HTTP HTTPS	ACCEPT

- Two solutions:
 - Enable `match-vip` on the deny policy
 - Set the VIP as destination

```
config firewall policy
  edit <deny policy ID>
    set match-vip enable
  next
end
```

Setting available only
when policy action is set
to deny

```
config firewall policy
  edit <deny policy ID>
    set dstaddr <VIP>
  next
end
```

In FortiOS, VIPs and firewall address objects are completely different. They are stored separately with no overlap. This means that, by default, firewall address objects do not match VIPs.

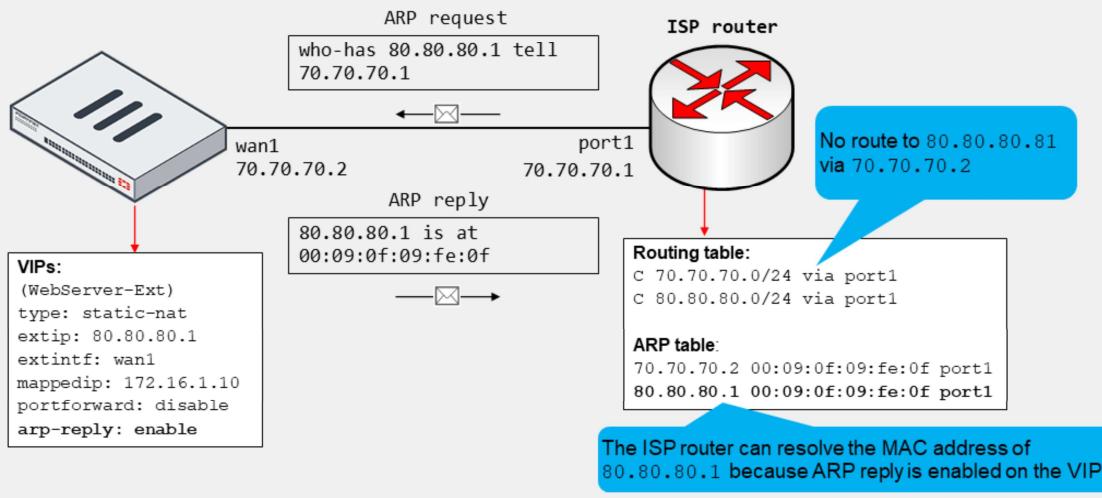
In the example shown on this slide, the destination of the first firewall policy is set to **all**. Even though this means all destination addresses (`0.0.0.0/0`), by default, this doesn't include the external addresses defined on the VIPs. The result is that traffic destined to the external address defined on the **Web_Server** VIP skips the first policy and matches the second policy instead.

But what if you want the first policy to block all incoming traffic to all destinations, including the traffic destined to any VIPs?. This is useful if your network is under attack, and you want to temporarily block all incoming external traffic. You can do this by enabling `match-vip` on the first firewall policy. Enabling `match-vip` instructs FortiGate to also check for VIPs during policy evaluation. Note that the `match-vip` setting is available only when the firewall policy action is set to **DENY**.

In case you want to block only traffic destined to one or more VIPs, you can reference the VIPs as the destination address on the deny firewall policy.

ARP Reply Option in VIPs and IP Pools

- Enabled by default; instructs FortiGate to reply to ARP requests for external address
- Sometimes required to overcome routing misconfigurations
 - Example:



When you configure a VIP or an IP pool, ARP reply is enabled by default. When ARP reply is enabled, FortiGate replies to incoming ARP requests for the external address configured in the VIP and IP pools.

Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next-hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled.

Consider the example shown on this slide, which shows an internet connection between FortiGate and an ISP router. The example also shows a simplified version of the ISP router routing table and ARP table.

The ISP assigns the FortiGate administrator the public subnet 80.80.80.0/24 to deploy internet-facing services. The administrator configured the VIP shown on this slide to provide internet users with access to the company web server. While testing, the administrator confirms that internet users can reach the web server at 80.80.80.1.

However, the administrator is likely unaware that having ARP reply enabled was key for a successful connectivity. The reason is that the ISP router doesn't have a route in its routing table to access the 80.80.80.0/24 subnet through the 70.70.70.2 gateway. Instead, the routing table contains a connected route for the subnet through port1. The result is that the ISP router generates ARP requests out of port1 to resolve the MAC address of any of the addresses in the 80.80.80.0/24 subnet. Nonetheless, because FortiGate responds to ARP requests for the external address in the VIP, the ISP router is able to resolve the MAC address successfully.

NAT Implementation Best Practices

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IP addresses of each IP pool
 - Ensure that the IP pool address range does not overlap with addresses assigned to FortiGate and hosts
 - If internal and external users are accessing the same servers, configure your DNS service so internal users resolve to the destination internal address
- Don't configure a NAT rule for inbound traffic unless it is required by an application
- Schedule maintenance window to make changes on NAT configuration

Use the following best practices when implementing NAT:

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IP addresses of each IP pool.
 - Ensure that the IP pool address range does not overlap with addresses assigned to FortiGate interfaces or to any hosts on directly connected networks.
 - If you have internal and external users accessing the same servers, configure your DNS services so internal users resolve to use the destination internal address instead of its external address defined in the VIP.
- Don't configure a NAT rule for inbound traffic unless it is required by an application.
 - For example, if there is a matching NAT rule for inbound SMTP traffic, the SMTP server might act as an open relay.
- You must schedule a maintenance window when making changes to NAT mode configuration since making changes could create a network outage.

Knowledge Check

1. What is the default IP pool type?

- A. One-to-one
- B. Overload

2. Which of the following is the default VIP type?

- A. static-nat
- B. load-balance

Review

- ✓ Configure IPv4 firewall policy
- ✓ Monitor traffic logs from firewall policy
- ✓ Choose inspection modes for firewall policies
- ✓ Configure SNAT
- ✓ Configure a firewall policy to perform DNAT using VIP

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 and NAT on FortiGate.