

DO NOT REPRINT**© FORTINET**

Firewall Policy NAT

Objectives

- Configure a firewall policy to perform SNAT and DNAT (VIP)
- Apply SNAT with IP pools
- Configure DNAT with VIPs or a virtual server

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.

DO NOT REPRINT**© FORTINET**

Firewall Policy SNAT

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

Policy & Objects > Firewall Policy

Edit Policy

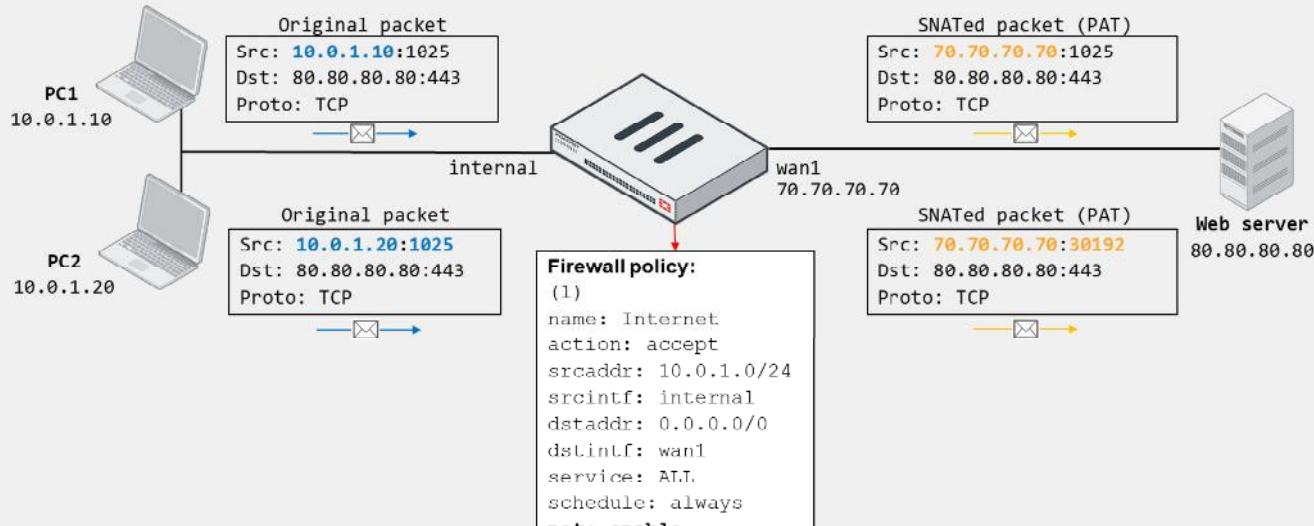
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT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

There are two ways to configure firewall policy SNAT:

- Use the outgoing interface address.
- Use the dynamic IP pool.

DO NOT REPRINT
© FORTINET

Firewall Policy SNAT Using the Outgoing Interface



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

10

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.

DO NOT REPRINT

© FORTINET

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" value="Write a comment..."/>
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" value="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	<input type="text" value="port3"/>
Outgoing Interface	<input type="text" value="port1"/>
Source	<input type="text" value="LOCAL_SUBNET"/>
Destination	<input type="text" value="all"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY
Inspection Mode	<input type="radio"/> Flow-based <input checked="" type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input 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"/>

IP pools are a mechanism that 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 interface(s), 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 appropriate routing is configured.

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

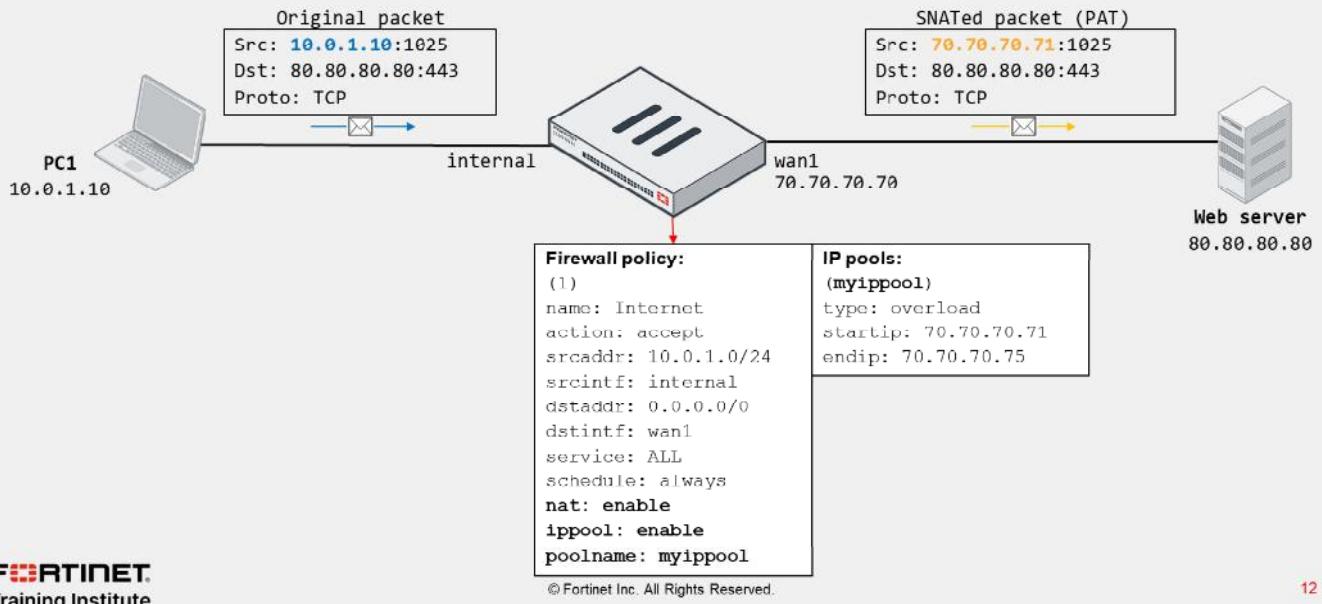
- Overload
- One-to-one
- Fixed port range
- Port block allocation

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

DO NOT REPRINT

© FORTINET

IP Pool Type—Overload



12

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.

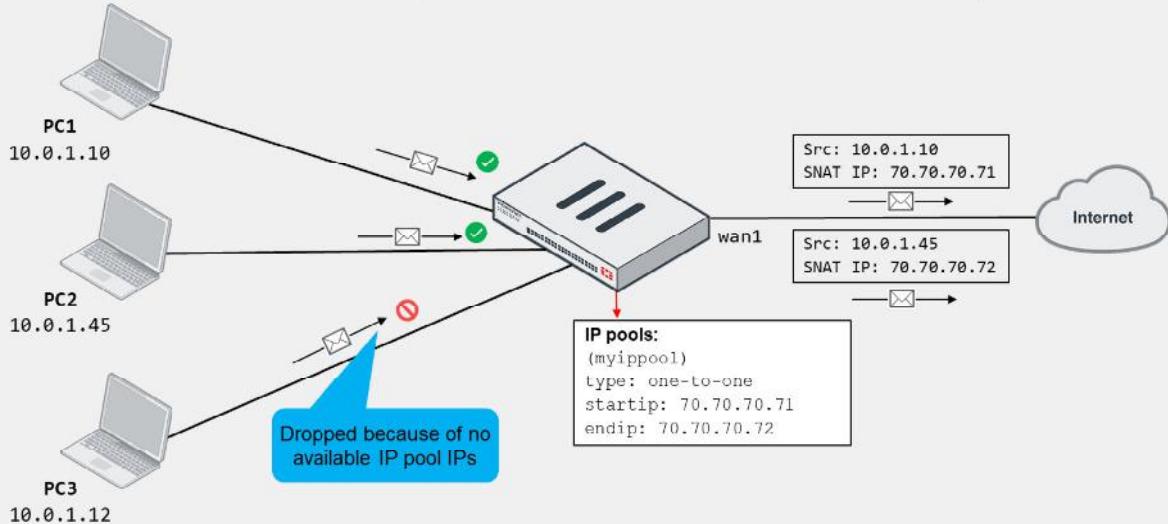
The default IP pool type is overload. In the overload IP pool type, a many-to-one or many-to-few relationship and port translation is used.

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).

DO NOT REPRINT
© FORTINET

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
 Training Institute

© Fortinet Inc. All Rights Reserved.

13

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

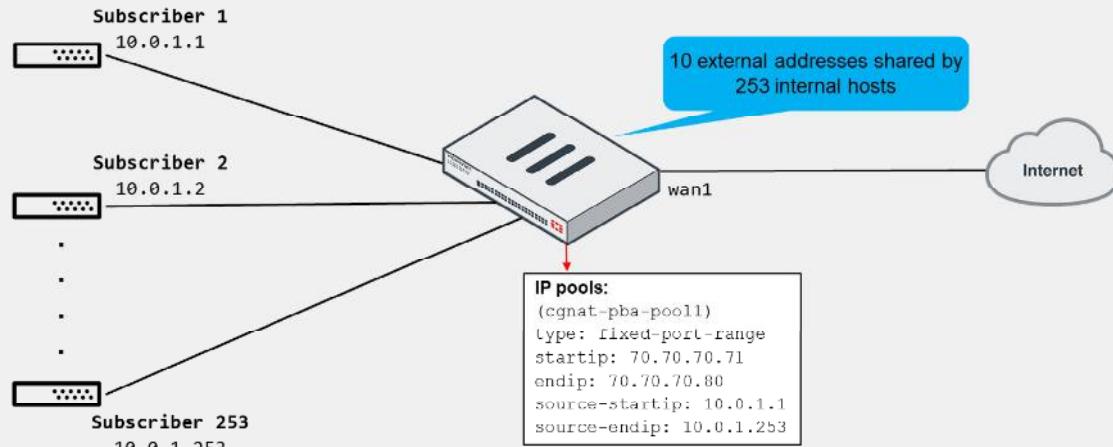
There is a single mapping of an internal address to an external address. That is, an IP pool address is not shared with any other internal host, thus the name one-to-one. If there are no more addresses available in the IP pool, FortiGate drops packets from unserved hosts.

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.

DO NOT REPRINT
© FORTINET

IP Pool Type—Fixed Port Range

- Useful for service providers in CGN environments
 - Ability to identify the subscriber of a connection by public IP address and port (no traffic log required)



ISPs must be able to identify the subscriber responsible for a given connection should authorities require it. If the ISP performs NAT to subscriber traffic, then the traffic will share one or more public addresses. One way to track the traffic and, therefore, the NAT details for each connection, is by logging them. However, this can result in a huge number of resources that the ISP needs to dedicate for logging purposes only.

Another option is to deploy a CGN-focused feature such as a fixed port range IP pool. Fixed port range IP pools enable administrators to track connections by public address and port without having to log every session. When you configure a fixed port range IP pool, you indicate a range of external IP addresses that FortiGate uses to perform NAT on traffic sourced from a range of internal IP addresses. It is called fixed port range because FortiGate calculates the port block size and the number of available port blocks for the IP pool based on the number of configured internal and external IP addresses. FortiGate then allocates one or more port blocks to internal hosts when performing NAT, which is what enables the administrator to track connections without having to log them.

The example on this slide shows a fixed port range IP pool. The internal address range 10.0.1.1 to 10.0.1.253 maps to the external address range 70.70.70.71 to 70.70.70.80. That is, FortiGate shares ten external addresses with 253 internal addresses.

DO NOT REPRINT
© FORTINET

IP Pool Type—Fixed Port Range (Contd)

- Port block size and the number of available port blocks by external address:

```
# diagnose firewall ippool list
list ippool info:(vf=root)
ippool cgnat-pba-pool1: id=1, block-sz=2323, num-block=1, fixed-port=no, use=2
    nat ip-range=70.70.70.71-70.70.70.80 start-port=5117, num-pba-per-ip=26
    source ip-range=10.0.1.1-10.0.1.253 deterministic NAT
    clients=0, inuse-NAT-IPs=0
    total-PBAs=260, inuse-PBAs=0, expiring-PBAs=0, free-PBAs=100.00%
    allocate-PBA-times=0, reuse-PBA-times=0

# diagnose firewall ippool-fixed-range list natip 70.70.70.71
ippool name=cg nat-pba-pool1, ip shared num=26, port num=2323
internal ip=10.0.1.1, nat ip=70.70.70.71, range=5117~7439
internal ip=10.0.1.2, nat ip=70.70.70.71, range=7440~9762
...
internal ip=10.0.1.26, nat ip=70.70.70.71, range=63192~65514

# diagnose firewall ippool-fixed-range list natip 70.70.70.71 5900
ippool name=cg nat-pba-pool1, ip shared num=26, port num=2323
internal ip=10.0.1.1, nat ip=70.70.70.71, range=5117~7439
```

Check block size and number of blocks for IP pool

Detailed external address and port assignment per internal address

Add source port to obtain specific port block for internal address

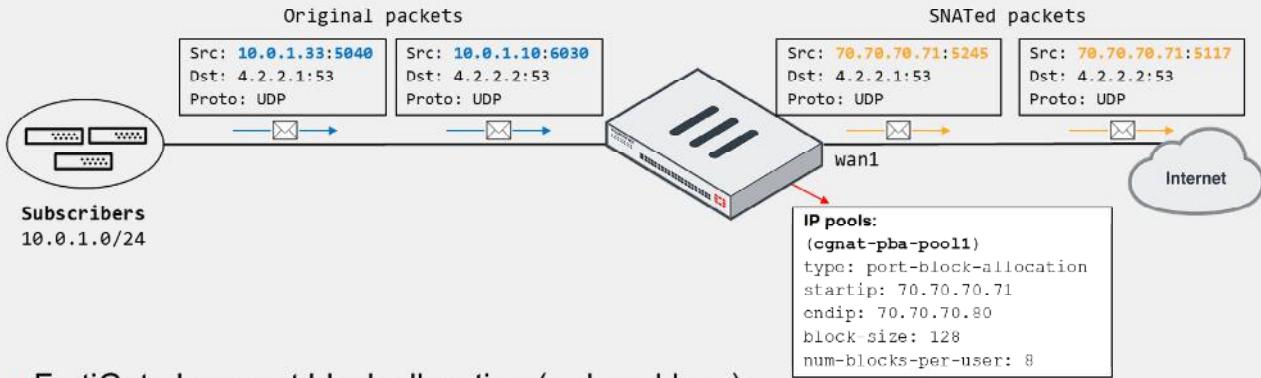
You can use the `diagnose firewall ippool list` command to identify the block size and number of blocks assigned to each external address in the fixed port range IP pool.

You can also use the `diagnose firewall ippool-fixed-range list natip` command to view detailed external address and port assignment information per internal address, as shown on this slide. The result is that you can identify subscribers by providing the public address and port of a connection.

DO NOT REPRINT
© FORTINET

IP Pool Type—Port Block Allocation

- FortiGate allocates a block size and number per host for a range of external addresses
 - Another useful option for CGN



- FortiGate logs port block allocation (reduced logs):

```
System event logs:
action="ippool-create" saddr="10.0.1.33" nat=70.70.70.71 portbegin=5245 portend=5372 poolname="cgnat-pba-pool1"
action="ippool-create" saddr="10.0.1.10" nat=70.70.70.71 portbegin=5117 portend=5244 poolname="cgnat-pba-pool1"
```

The port block allocation IP pool is also a useful option for CGN. It give administrators a more flexible way to control user port allocation for NAT. Unlike the fixed port range IP pool, which requires you to define internal and external IP address ranges, with port block allocation, you define the external IP address range only. You must also indicate the block port size and the number of blocks that FortiGate allocates to each host (or source IP address). The result is that each source IP address is limited to the number of blocks and ports configured in the IP pool, thus preventing port exhaustion caused by a few hosts.

For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator. The administrator can then look at the system event logs to identify internet connections made by a device should the authorities require such information. That is, like the fixed port block case, the administrator doesn't have to log the traffic for connection identification purposes.

The example on this slide shows how port block allocation assignment takes place. FortiGate allocates port blocks on a first-come, first-served basis. The port block allocation is made when FortiGate receives a packet from unserved hosts. In the example, 10.0.1.10 and 10.0.1.33 are unserved hosts that try to access the internet. FortiGate then allocates the port blocks to each host and performs the respective SNAT on traffic. Upon allocation, FortiGate also generates system event logs with the port block allocation details to inform the administrator.

Note that the system event logs shown on this slide have been cut to fit the slide.

DO NOT REPRINT

© FORTINET

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 windows. The top window, 'Policy & Objects > Virtual IPs', displays a 'New Virtual IP' form. The 'Name' field is 'VIP-INTERNAL-HOST', 'VIP type' is 'IPv4', 'Interface' is 'port1', 'type' is 'Static NAT', 'External IP address/range' is '100.64.100.22', and 'Map to' is '10.0.1.10'. The bottom window, 'Policy & Objects > Firewall Policy', shows a 'New Policy' configuration. In the 'Destination' field, 'VIP INTERNAL HOST' is selected. A blue callout box with the text 'VIP used as destination in firewall policy' points to this selection. A red arrow points from the 'VIP INTERNAL HOST' entry in the destination field to the 'VIP INTERNAL HOST' entry in the 'Map to' field of the Virtual IP form.

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:

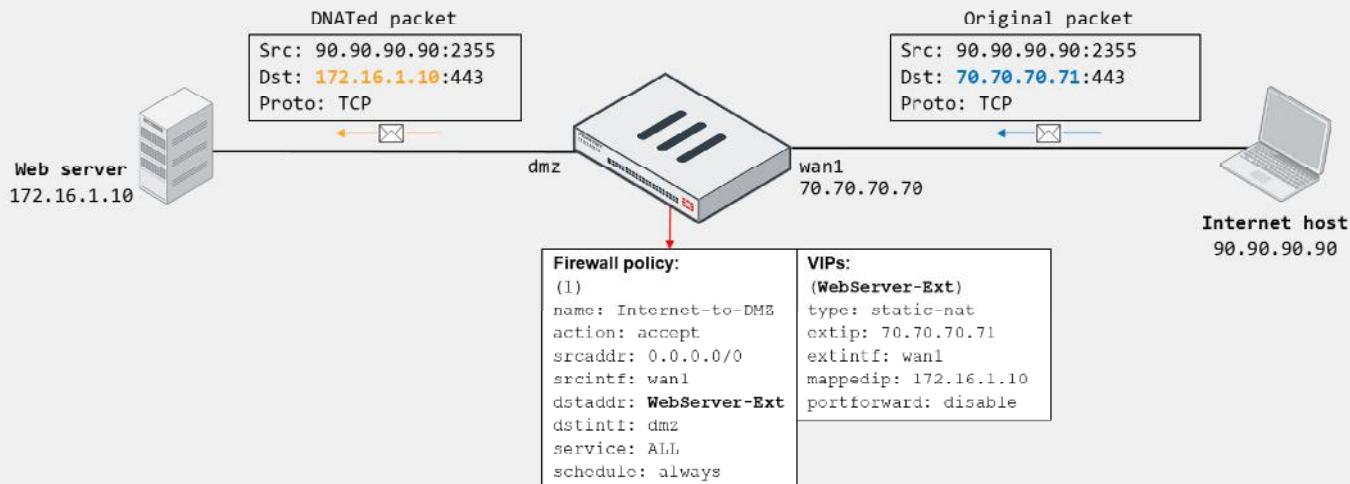
1. FortiGate performs DNAT on ingress traffic destined to the external IP address defined in the VIP, regardless of the protocol and port of the connection, provided the matching firewall policy references the VIP as **Destination**.
2. FortiGate uses as NAT IP the external IP address defined in the 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.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Incoming Connection

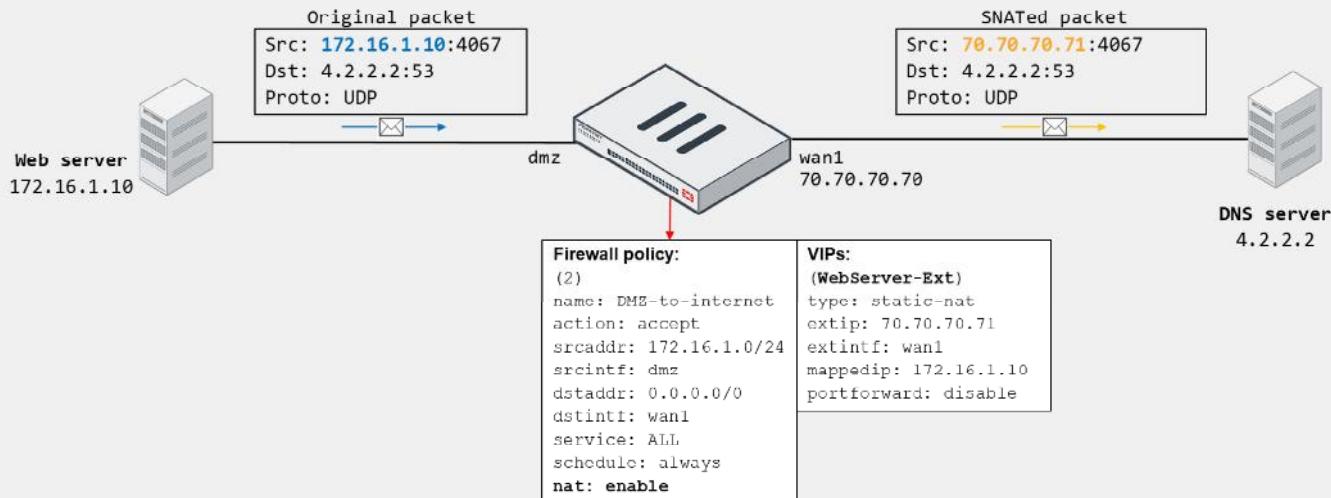


In the example shown on this slide, the internet host initiates a connection to 70.70.70.71 on TCP port 443. On FortiGate, the traffic matches the firewall policy ID 1, which references the WebServer-Ext VIP as destination. Because the VIP is configured as static NAT and has port forwarding disabled, 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.

DO NOT REPRINT
© FORTINET

VIP Example—Static NAT—Outgoing Connection

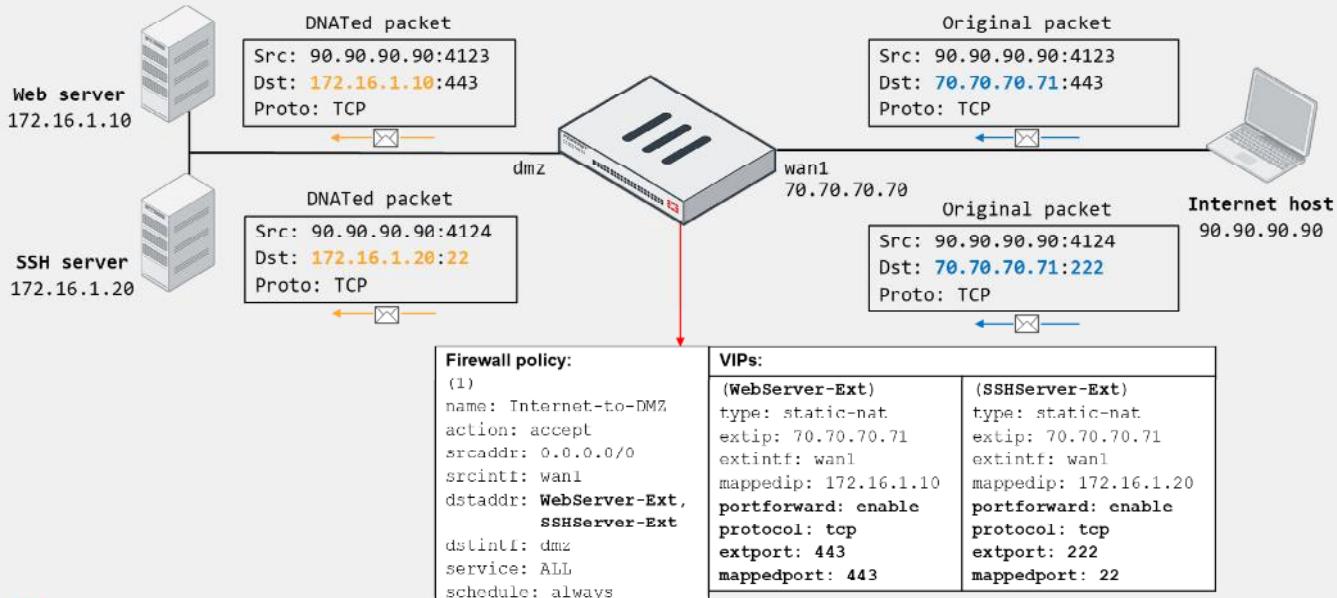


Now, suppose that the internal web server (172.16.1.10) initiates a DNS connection to the internet DNS server (4.2.2.2). On FortiGate, the traffic matches the firewall policy ID 2, which has `nat` enabled. Because the source address matches the internal address of the VIP, and because the VIP is configured 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).

DO NOT REPRINT
© FORTINET

VIP Example—Port Forwarding—Incoming Connection



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

20

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.

DO NOT REPRINT

© FORTINET

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
WAN (port1) → LAN (port3) 2						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

Action = DENY

- Two solutions:

- Enable **match-vip** on the deny policy

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

Setting available only
when policy action is set
to deny

- Set the VIP as destination

```
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.

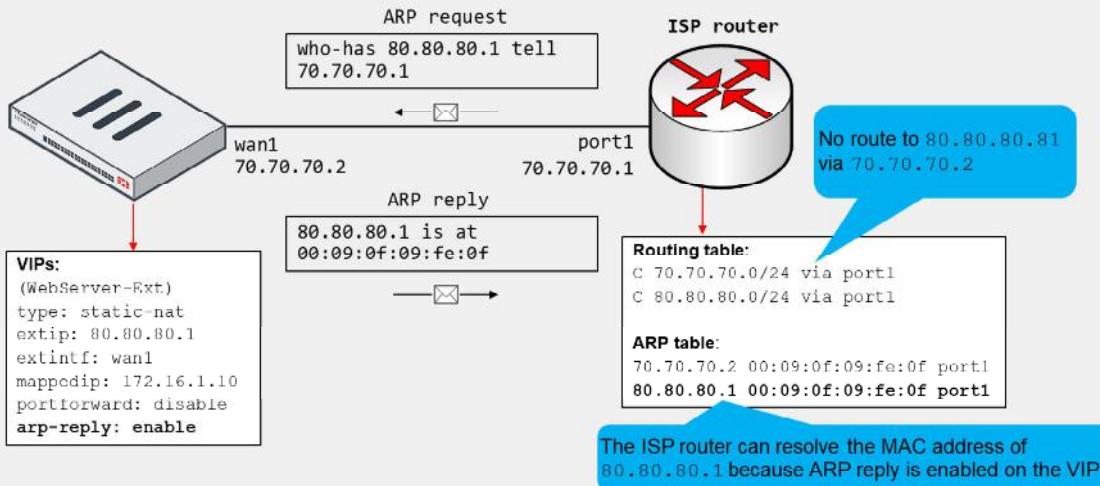
But what if you want the first policy to block all incoming traffic to all destinations, including the traffic destined to any VIPs? This is useful if your network is under attack, and you want to temporarily block all incoming external traffic. You can do this by enabling **match-vip** on the first 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.

DO NOT REPRINT
© FORTINET

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:



FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

22

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.

DO NOT REPRINT**© FORTINET**

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

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Introduction to NAT****Firewall Policy NAT****Central NAT****Best Practices and Troubleshooting**

Good job! You now understand firewall policy NAT.

Now, you'll learn about central NAT.

DO NOT REPRINT

© FORTINET

Central NAT

Objectives

- Configure central NAT

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

By demonstrating competence in configuring central NAT to perform SNAT and DNAT, you will be able to use NAT on a more granular level to control IP address, protocol, and port translation.

DO NOT REPRINT

© FORTINET

Central NAT

- Enable or disable on the GUI or CLI (default = disable)

System > Settings > Central SNAT

NGFW Mode **Profile-based** Policy-based

Central SNAT

```
config system settings
    set central-nat enable
end
```

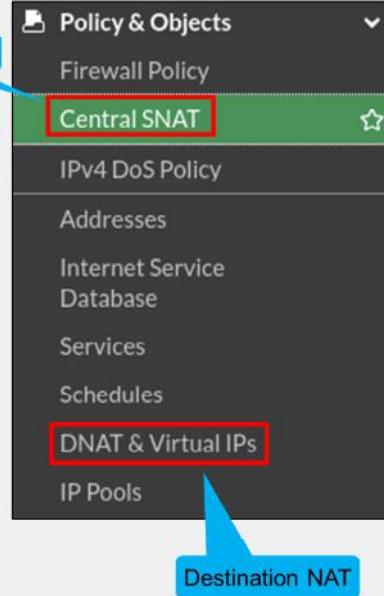
Source NAT

Enable central NAT from GUI or CLI

- Must remove VIP and IP pool references from existing policies

```
# config system settings
(settings) # set central-nat enable
Cannot enable central-nat with firewall policy using vip (id=2).
```

- Once enabled, these two options are available on the GUI:
 - Central SNAT
 - DNAT & Virtual IPs
- Central SNAT is mandatory for NGFW policy-based mode



By default, central NAT is disabled. You can enable it on the CLI or the GUI. After central NAT is enabled, the following two options are available to be configured on the GUI:

- Central SNAT**
- DNAT & Virtual IPs**

What happens if you try to enable central NAT, but there are still IP pools or VIPs configured in firewall policies?

The CLI does not allow this and presents a message referencing the firewall policy ID with the VIP or IP pool. You *must* remove VIP or IP pool references from existing firewall policies in order to enable central NAT.

Central SNAT is mandatory for the new NGFW policy-based mode. This means SNAT behaves only according to the NAT settings found by clicking **Policy & Objects > Central SNAT**.

DO NOT REPRINT

© FORTINET

Central SNAT

- Configure SNAT on central SNAT policies
 - Useful for advanced SNAT
 - Firewall policy and central SNAT policy segregation
 - Simplifies firewall policy configuration
- Central SNAT policy matching criteria:
 - Incoming interface
 - Outgoing interface
 - Source address
 - Destination address
 - Protocol
 - Source port (explicit port mapping)
- SNAT policies are evaluated from top to bottom
 - If no match is found, traffic is not SNATed

Policy & Objects > Central SNAT

New Policy

Incoming Interface	port3	x
Outgoing Interface	port1	x
Source Address	LOCAL_SUBNET	x
Destination Address	all	x

NAT

NAT NAT IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Protocol any TCP UDP SCTP Specify 6

Explicit port mapping

Comments 0/1023

Enable this policy

When you enable central NAT, you configure SNAT on the central SNAT page on the FortiGate GUI.

The main benefit of using central NAT for SNAT is firewall policy and central SNAT policy segregation. This is particularly useful for advanced SNAT configurations comprising multiple networks and IP pools. Instead of enabling NAT and selecting IP pools on firewall policies, you configure SNAT policies for all the accepted traffic by the firewall policies. This way, you focus your firewall policy configuration on what kind of traffic to accept, and your SNAT policies on what portion of the accepted traffic to translate and the SNAT mapping to follow. The result is that you simplify your firewall policy configuration by removing the SNAT settings from it.

When you configure SNAT policies, you can configure the following matching criteria:

- Incoming interface
- Outgoing interface
- Source address
- Destination address
- Protocol
- Source port (explicit port mapping)

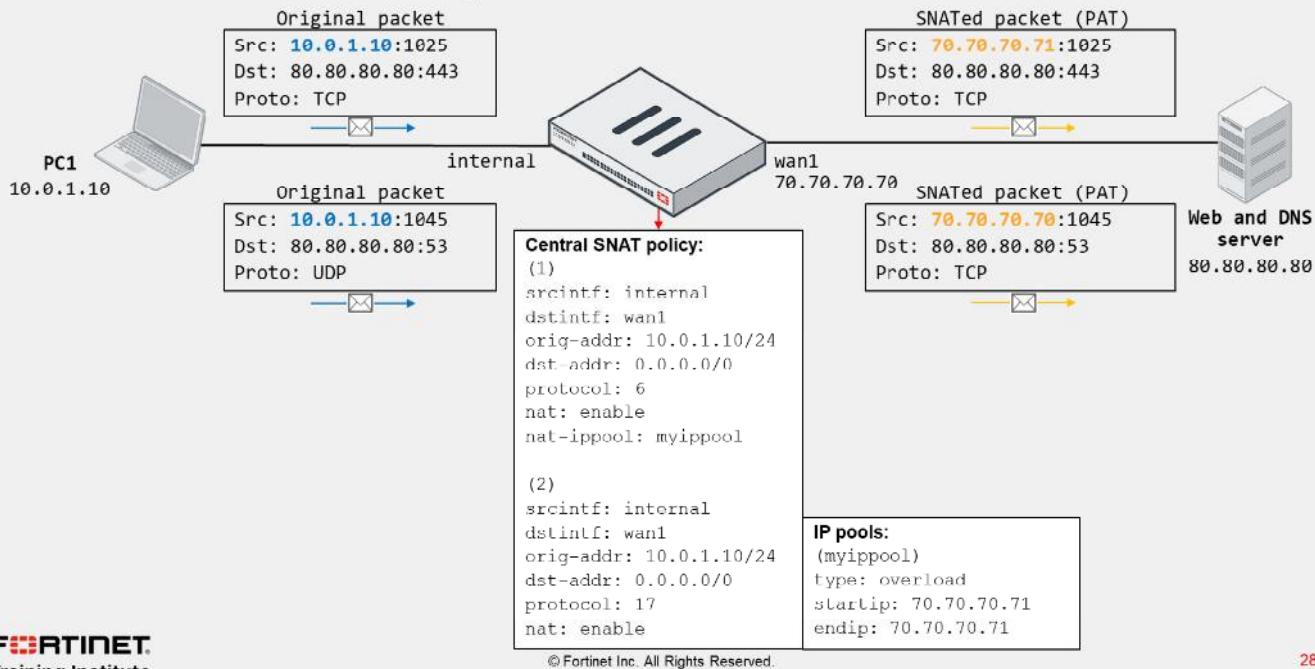
You must also indicate whether you want to perform SNAT using the outgoing interface address or an IP pool. Note that if you enable central NAT mode, FortiGate doesn't perform SNAT on traffic unless you configure the corresponding matching central SNAT policy. Similarly, if the traffic doesn't match any of the configured SNAT policies, FortiGate doesn't perform SNAT on the traffic either.

Like firewall policies, SNAT policies are processed from *top to bottom* and, if a match is found, the source address and source port are translated based on the central SNAT policy mapping settings.

DO NOT REPRINT

© FORTINET

Central SNAT Example



28

In the example shown on this slide, PC1 (10.0.1.10) initiates two connections to the external server (80.80.80.80). The HTTPS connection matches central SNAT policy ID 1 and, therefore, the source address is translated to the IP pool address (70.70.70.71). The DNS connection matches central SNAT policy ID 2, which doesn't reference an IP pool. The result is that the source address of the DNS connection is translated to the external interface address (70.70.70.70).

Although not shown on this slide, there are firewall policies configured that accept both connections.

Now, what if PC1 initiates an ICMP connection to the server? Because there is no matching central SNAT policy, then FortiGate wouldn't perform SNAT for the ICMP connection.

DO NOT REPRINT

© FORTINET

Central DNAT and VIPs

- Kernel has DNAT rules based on configured VIPs
 - You no longer reference VIPs in firewall policies
- Firewall policy
 - Destination address must match the VIP mapped address
 - DNAT takes place before firewall policy lookup

Policy & Objects > DNAT and Virtual IPs

Edit DNAT & Virtual IP

DNAT & VIP type: IPv4 DNAT

Name: VIP-INTERNAL-HOST

Comments: Write a comment... 0/255

Status: Disable to exclude VIP from DNAT

Network

Interface: port1

Type: Static NAT

Source interface filter:

External IP address/range: 70.70.70.71

Map to

IPv4 address/range: 10.0.1.10

Optional Filters

Port Forwarding

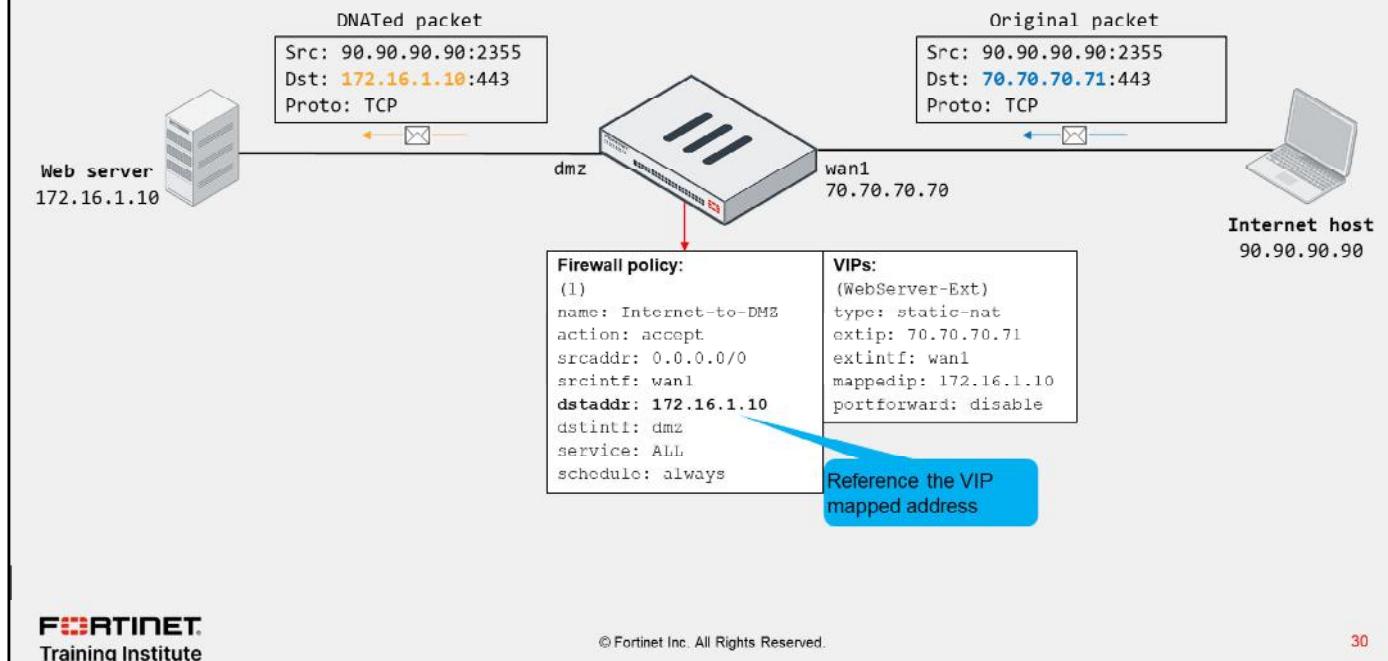
When you enable central NAT, you no longer reference VIPs on firewall policies. Instead, FortiGate automatically creates a rule in the kernel to perform DNAT for the matching traffic based on the configured VIPs. You configure the VIPs on the **DNAT and Virtual IPs** page.

Like in the central SNAT case, you must also have a matching firewall policy that accepts the traffic you want to DNAT. However, instead of referencing the VIP, you reference the mapped internal address as destination in the firewall, and *not* the external address. This is because for ingress traffic, DNAT takes place before the firewall policy lookup. That is, FortiGate considers the translated destination address during the firewall policy lookup process.

In central NAT mode, VIPs take effect right after you create them. In case you want to exclude a VIP from DNAT, you can disable the object on the FortiGate GUI by using the **Status** button.

DO NOT REPRINT
© FORTINET

DNAT and VIPs Example



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

30

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 web server internal address (172.16.1.10) as the 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 you configure the firewall policy to match the VIP mapped address as the destination, and *not* the VIP external address.

DO NOT REPRINT**© FORTINET**

Disabling Central NAT

- Disable central NAT on the FortiGate CLI:

```
config system settings
    set central-nat disable
end
```

- When disabled, FortiGate stops performing NAT on traffic
 - FortiGate requires NAT configuration on firewall policies
- Configure SNAT by enabling NAT on firewall policy
 - Optionally, reference IP pool
- Configure DNAT by referencing VIP as destination on firewall policy



© Fortinet Inc. All Rights Reserved.

31

You can disable central NAT on the FortiGate CLI by disabling `central-nat` under `config system settings`.

However, note that when you disable central NAT, FortiGate stops performing NAT on traffic because it now requires the NAT configuration to be applied on the corresponding firewall policies. For FortiGate to perform SNAT, you must enable NAT on the respective firewall policy and, optionally, reference the IP pool. For DNAT, you must reference the VIP object as the destination on the corresponding firewall policies.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statement is true?

- A. Central NAT is not enabled by default.
- B. Both central NAT and firewall policy NAT can be enabled together.

2. What happens if there is no matching central SNAT policy or no central SNAT policy configured?

- A. The egress interface IP is used.
- B. NAT is not be applied to the firewall session.

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

Good job! You now understand central NAT.

Now, you'll learn about best practices and troubleshooting NAT.

DO NOT REPRINT**© FORTINET**

Best Practices and Troubleshooting

Objectives

- Identify common NAT issues by reviewing traffic logs
- Monitor NAT sessions using diagnose commands
- Use NAT implementation best practices

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

By demonstrating competence in using traffic logs, diagnose commands, and best practices for NAT implementation, you should be able to monitor and troubleshoot common NAT issues, and successfully implement NAT in your network.

DO NOT REPRINT**© FORTINET**

Monitoring NAT Sessions With Diagnose Commands

- `diagnose firewall ippool-all list`
 - Lists all the configured NAT IP pools with NAT IP range and type

```
# diagnose firewall ippool-all list
vdom:root owns 1 ippool(s)
name:myippol
type:overload
nat-ip-range:10.200.1.100-10.200.1.100
```



© Fortinet Inc. All Rights Reserved.

35

You can run the `diagnose firewall ippool-all list` command to display the configured IP pools and their settings.

DO NOT REPRINT

© FORTINET

Monitoring NAT Sessions With Diagnose Commands (Contd)

- diagnose firewall ippool-all stats <Optional IP Pool name>
 - Lists stats for all of the IP pools:
 - NAT sessions per IP pool
 - Total TCP sessions per IP pool
 - Total UDP sessions per IP pool
 - Total others (non-TCP and non-UDP) sessions per IP pool

```
# diagnose firewall ippool-all stats EXT
name: EXT
type: overload
startip: 10.200.1.100
endip: 10.200.1.100
total ses: 100
tcp ses: 75
udp ses: 20
other ses: 5
```

Command shows only stats of IP pool named EXT

```
# diagnose firewall ippool-all stats
vdom:root owns 2 ippool(s)
name: EXT
type: overload
startip: 10.200.1.100
endip: 10.200.1.100
total ses: 100
tcp ses: 75
udp ses: 20
other ses: 5
```

Command shows stats of all IP pools

```
name: Training
type: one-to-one
startip: 10.200.1.50
endip: 10.200.1.60
total ses: 10
tcp ses: 8
udp ses: 2
other ses: 0
```

The `diagnose firewall ippool-all stats` command shows the stats for all IP pools.

The `stats` command provides the following data and information:

- NAT sessions per IP pool
- Total TCP sessions per IP pool
- Total UDP sessions per IP pool
- Total others (non-TCP and non-UDP) sessions per IP pool

Optionally, you can filter the output for a specific IP pool by using the name of the IP pool.

DO NOT REPRINT**© FORTINET**

NAT Implementation Best Practices

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IPs 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 switch from one NAT mode to another



© Fortinet Inc. All Rights Reserved.

37

Use the following best practices when implementing NAT:

- Avoid misconfiguring an IP pool range:
 - Double-check the start and end IPs 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 to switch from central NAT mode to firewall policy NAT mode, or from firewall policy NAT mode to central NAT mode. Switching between NAT modes can create a network outage.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. An administrator wants to check the total number of TCP sessions for an IP pool named INTERNAL. Which CLI command should the administrator use?
 A. diagnose firewall ippool-all stats INTERNAL
 B. diagnose firewall ippool-all list INTERNAL

DO NOT REPRINT

© FORTINET

Lesson Progress



Introduction to NAT

Firewall Policy NAT

Central NAT

Best Practices and Troubleshooting

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Understand NAT and PAT
- ✓ Understand the different configuration modes for NAT
- ✓ Configure a firewall policy to perform SNAT and DNAT (VIPs)
- ✓ Configure central NAT
- ✓ Use traffic logs to identify common NAT issues and monitor NAT sessions using session diagnose commands
- ✓ Use NAT implementation best practices

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

By mastering the objectives covered in this lesson, you learned how to understand and configure NAT so that you can use it in your network.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Security

Firewall Authentication

FortiOS 7.2

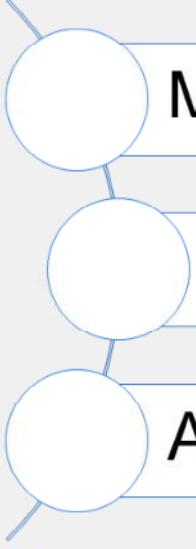
Last Modified: 13 June 2022

In this lesson, you will learn about using authentication on the firewall policies of FortiGate.

DO NOT REPRINT

© FORTINET

Lesson Overview



Methods of Firewall Authentication

User Groups

Authentication Using Firewall Policies

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

DO NOT REPRINT**© FORTINET**

Methods of Firewall Authentication

Objectives

- Describe firewall authentication
- Identify the different methods of firewall authentication available on FortiGate devices
- Identify supported remote authentication servers
- Understand the roles of LDAP and RADIUS
- Describe active and passive authentication and order of operations

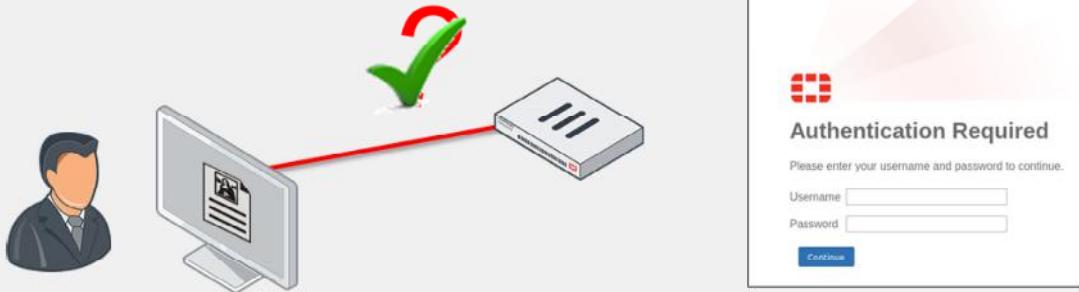
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in methods of firewall authentication, you will be able to describe and identify the supported methods of firewall authentication available on FortiGate.

DO NOT REPRINT**© FORTINET**

Firewall Authentication

- Includes the authentication of users and user groups
 - It is more reliable than just IP address and device-type authentication
 - Users must authenticate by entering valid credentials
- After FortiGate identifies the user or device, FortiGate applies firewall policies and profiles to allow or deny access to each specific network resource



 **Authentication Required**

Please enter your username and password to continue.

Username

Password

Traditional firewalling grants network access by verifying the source IP address and device. This is inadequate and can pose a security risk because the firewall cannot determine who is using the device to which it is granting access.

FortiGate includes authentication of users and user groups. As a result, you can follow individuals across multiple devices.

Where access is controlled by a user or user group, users must authenticate by entering valid credentials (such as username and password). After FortiGate validates the user, FortiGate applies firewall policies and profiles to allow or deny access to specific network resources.

DO NOT REPRINT**© FORTINET**

FortiGate Methods of Firewall Authentication

- Local password authentication
 - Username and password stored on FortiGate
- Server-based password authentication (also called remote password authentication)
 - Password stored on a POP3, RADIUS, LDAP, or TACACS+ server
- Two-factor authentication
 - Enabled on top of an existing method
 - Requires something you know and something you have (token or certificate)



© Fortinet Inc. All Rights Reserved.

5

FortiGate supports multiple methods of firewall authentication:

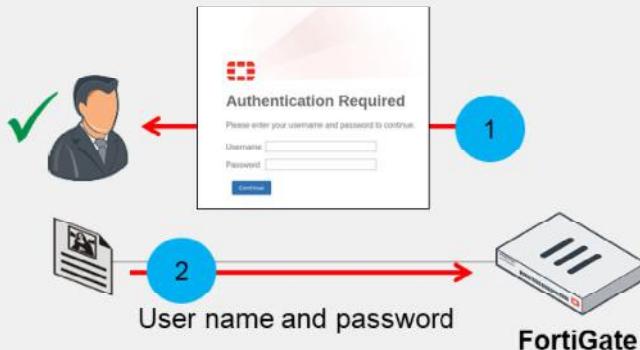
- Local password authentication
- Server-based password authentication (also called remote password authentication)
- Two-factor authentication
This is a system of authentication that is enabled on top of an existing method—it cannot be enabled without first configuring one of the other methods. It requires something you know, such as a password, and something you have, such as a token or certificate.

During this lesson, you will learn about each method of firewall authentication in detail.

DO NOT REPRINT
© FORTINET

Local Password Authentication

- User accounts stored locally on FortiGate
 - Works well for single FortiGate installations



User & Authentication > User Definition

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Username: Student

Password: *****

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Two-factor Authentication

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

User Account Status: Enabled

User Group: (radio button)

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

6

The simplest method of authentication is local password authentication. User account information (username and password) is stored locally on the FortiGate device. This method works well for a single FortiGate installation.

Local accounts are created on the **User Definition** page where a wizard takes you through the process. For local password authentication, select **Local User** as the user type and create a username and password. If desired, you can also add email and SMS information to the account, enable two-factor authentication, and add the user to a preconfigured user group.

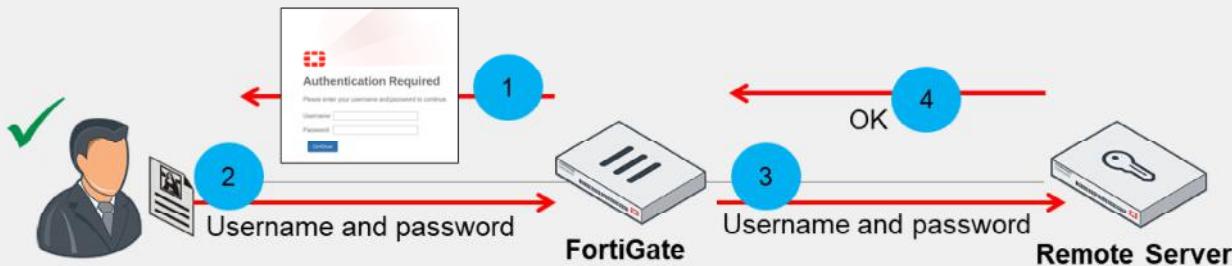
After you create the user, you can add the user—or any preconfigured user group in which the user is a member—to a firewall policy, in order to authenticate. You will learn about user groups and firewall policies in this lesson.

DO NOT REPRINT

© FORTINET

Server-Based Password Authentication

- Accounts are stored on a remote authentication server
- Administrators can do one of the following:
 - Create an account for the user locally, and specify the server to verify the password
 - Add the authentication server to a user group
 - All users in that server become members of the group



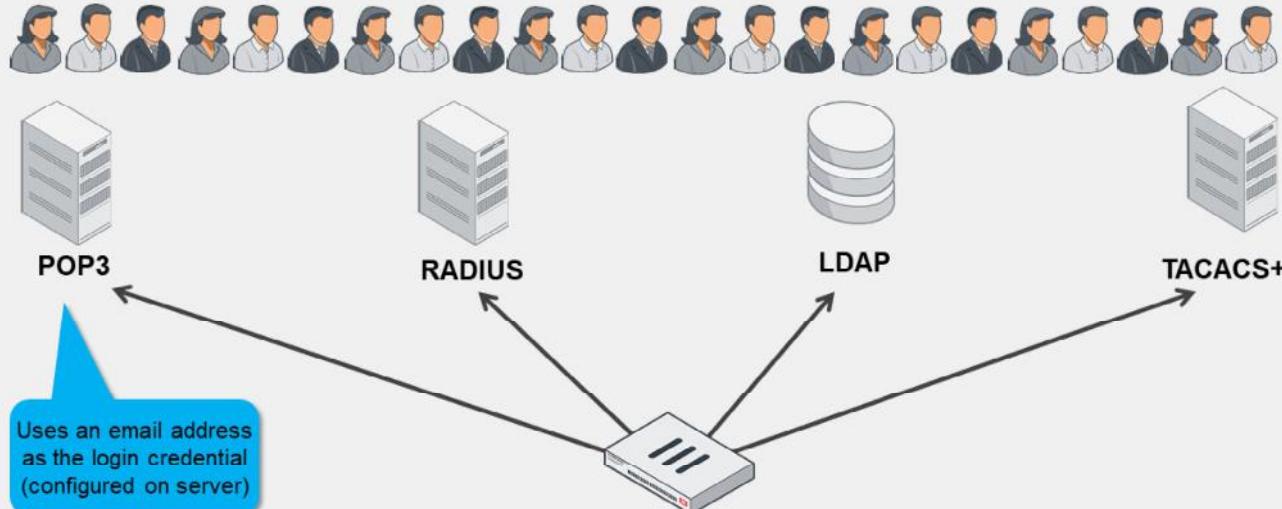
When server-based password authentication is used, a remote authentication server authenticates users. This method is desirable when multiple FortiGate devices need to authenticate the same users or user groups, or when adding FortiGate to a network that already contains an authentication server.

When you use a remote authentication server to authenticate users, FortiGate sends the user's entered credentials to the remote authentication server. The remote authentication server responds by indicating whether the credentials are valid or not. If valid, FortiGate consults its configuration to deal with the traffic. Note that it is the remote authentication server—not FortiGate—that evaluates the user credentials.

When the server-based password authentication method is used, FortiGate does not store all (or, in the case of some configurations, any) of the user information locally.

DO NOT REPRINT
© FORTINET

Remote Authentication Servers



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

8

FortiGate provides support for many remote authentication servers, including POP3, RADIUS, LDAP, and TACACS+.

POP3 is the only server that requires an email address as the login credential. All other remote authentication servers use the user name. Some POP3 servers require the full email with domain (user@example.com), others require the suffix only, while still others accept both formats. This requirement is determined by the configuration of the server and is not a setting on FortiGate. You can configure POP3 authentication only through the CLI. Note that you can configure LDAP to validate with email, rather than the user name.

DO NOT REPRINT
© FORTINET

Server-Based Password Authentication—Users

- Create user accounts on FortiGate
 - Select remote server type and point to preconfigured remote server
 - Add user to a group
- Add the remote authentication server to user groups

Must be preconfigured on FortiGate

User & Authentication > User Definition

FORTINET.
 Training Institute

© Fortinet Inc. All Rights Reserved.

9

You can configure FortiGate to use external authentication servers in the following two ways:

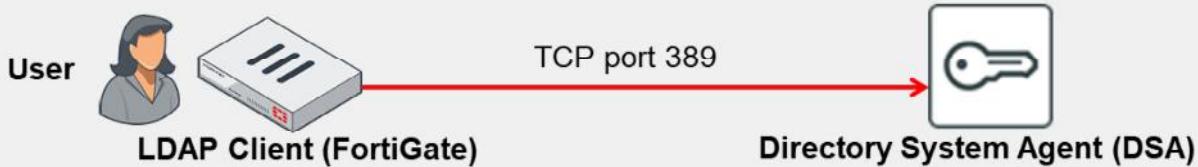
- Create user accounts on FortiGate. With this method, you must select the remote authentication server type (RADIUS, TACACS+, or LDAP), point FortiGate to your preconfigured remote authentication server, and add the user to an appropriate group. This is usually done when you want to add two-factor authentication to your remote users. Remember, POP3 is only configurable through the CLI.
- Add the remote authentication server to user groups. With this method, you must create a user group and add the preconfigured remote server to the group. Accordingly, any user who has an account on the remote authentication server can authenticate. If you are using other types of remote servers, such as an LDAP server, as the remote authentication server, you can control access to specific LDAP groups, as defined on the LDAP server.

Similar to local password authentication, you must then add the preconfigured user group (in which the user is a member) to a firewall policy in order to authenticate. You will learn about user groups and firewall policies later in this lesson.

DO NOT REPRINT**© FORTINET**

LDAP Overview

- LDAP is an application protocol for accessing and maintaining distributed directory information services



- LDAP maintains authentication data, including:
 - Departments, people (and groups of people), passwords, email addresses, and printers
- LDAP consists of a data-representation scheme, a set of defined operations, and a request-and-response network
- Binding is the operation in which the LDAP server authenticates the user

Lightweight Directory Access Protocol (LDAP) is an application protocol used for accessing and maintaining distributed directory information services.

The LDAP protocol is used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. LDAP consists of a data-representation scheme, a set of defined operations, and a request-and-response network.

The LDAP protocol includes a number of operations that a client can request, such as search, compare, and add or delete an entry. Binding is the operation in which the LDAP server authenticates the user. If the user is successfully authenticated, binding allows the user access to the LDAP server, based on that user's permissions.

DO NOT REPRINT
© FORTINET

Configuring an LDAP Server on FortiGate

Directory tree attribute that identifies users

Part of the hierarchy where user records exist

Credentials for an LDAP administrator

User & Authentication > LDAP Servers

Name	External_Server
Server IP/Name	10.0.1.150
Server Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training
Exchange server	<input checked="" type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	uid=adadmin,cn=Users,dc=trainingAD,dc=local
Password	*****
Secure Connection	<input checked="" type="checkbox"/>
Connection status	✓ Successful
<input type="button" value="Test Connectivity"/> Test User Credentials	

On the **LDAP Servers** page, you can configure FortiGate to point to an LDAP server for server-based password authentication. The configuration depends heavily on the server's schema and security settings. Windows Active Directory (AD) is very common.

The **Common Name Identifier** setting is the attribute name you use to find the user name. Some schemas allow you to use the attribute userid. AD most commonly uses `sAMAccountName` or `cn`, but can use others as well.

The **Distinguished Name** setting identifies the top of the tree where the users are located, which is generally the `dc` value; however, it can be a specific container or `ou`. You must use the correct X.500 or LDAP format.

The **Bind Type** setting depends on the security settings of the LDAP server. You must use the setting **Regular** (to specify a regular bind) if you are searching across multiple domains and require the credentials of a user that is authorized to perform LDAP queries (for example, an LDAP administrator).

If you want to have a secure connection between FortiGate and the remote LDAP server, enable **Secure Connection** and include the LDAP server protocol (LDAPS or STARTTLS) as well as the CA certificate that verifies the server certificate. LDAPS uses port 636 for communication.

The **Test Connectivity** button tests only whether the connection to the LDAP server is successful or not. To test whether a user's credentials can successfully authenticate, you can use the **Test User Credentials** button or use the CLI.

DO NOT REPRINT**© FORTINET**

RADIUS Overview

- RADIUS is a standard protocol that provides AAA services



RADIUS is much different from LDAP, because there is no directory tree structure to consider. RADIUS is a standard protocol that provides authentication, authorization, and accounting (AAA) services.

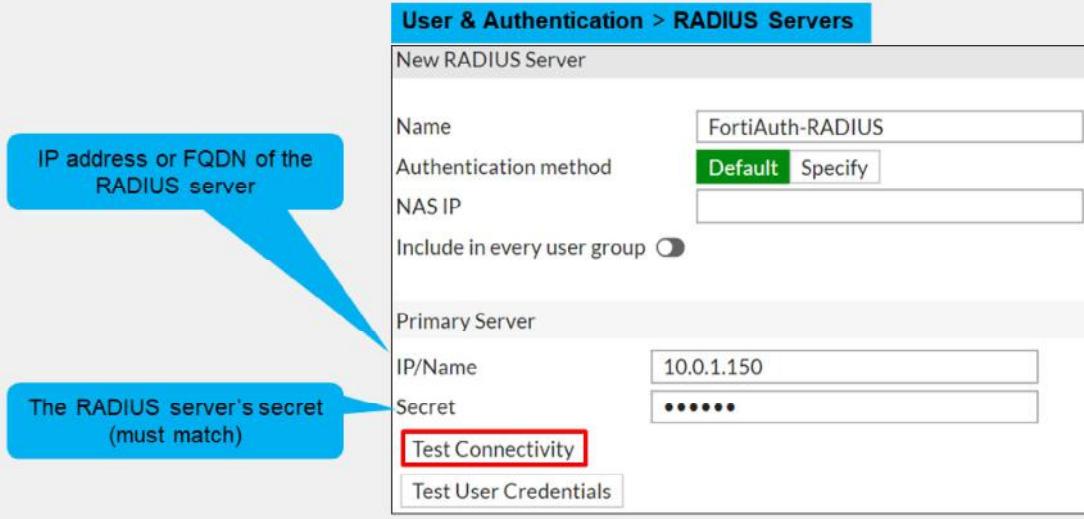
When a user is authenticating, the client (FortiGate) sends an ACCESS-REQUEST packet to the RADIUS server. The reply from the server is one of the following:

- ACCESS-ACCEPT, which means that the user credentials are ok
- ACCESS-REJECT, which means that the credentials are wrong
- ACCESS-CHALLENGE, which means that the server is requesting a secondary password ID, token, or certificate. This is typically the reply from the server when using two-factor authentication.

Not all RADIUS clients support the RADIUS challenge method.

DO NOT REPRINT
© FORTINET

Configuring a RADIUS Server on FortiGate



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

You can configure FortiGate to point to a RADIUS server for server-based password authentication through the **RADIUS Servers** page.

The **Primary Server IP/Name** setting is the IP address or FQDN of the RADIUS server.

The **Primary Server Secret** setting is the secret that was set up on the RADIUS server in order to allow remote queries from this client. Backup servers (with separate secrets) can be defined in case the primary server fails. Note that FortiGate must be listed on the RADIUS server as a client of that RADIUS server or else the server will not reply to queries done by FortiGate.

The **Authentication Method** setting refers to the authentication protocol that the RADIUS server supports. Options include chap, pap, mschap, and mschap2. If you select **Default**, FortiGate will use pap, mschap2, and chap (in that order).

Unlike LDAP configurations, the **Test Connectivity** button used in the example shown on this slide can test actual user credentials, but, like LDAP, you can also test this using the CLI.

The **Include in every User Group** option adds the RADIUS server and all users that can authenticate against it, to every user group created on FortiGate. So, you should enable this option only in very specific scenarios (for example, when only administrators can authenticate against the RADIUS server and policies are ordered from least restrictive to most restrictive).

DO NOT REPRINT
© FORTINET

Testing the LDAP and RADIUS Query on the CLI

- diagnose test authserver ldap <server_name> <username> <password>
- Example:

```
# diagnose test authserver ldap External_Server aduser1 Training!
authenticate 'aduser1' against 'External_Server' succeeded!
Group membership(s) - CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab
```

- diagnose test authserver radius <server_name> <scheme> <user> <password>
- Example:

```
# diagnose test authserver radius FortiAuth-RADIUS pap student fortinet
authenticate 'student' against 'pap' succeeded, server=primary
assigned_rad_session_id=810153440 session timeout=0 secs!
Group membership(s) - remote-RADIUS-admins
```

Group memberships are provided by vendor-specific attributes configured on the RADIUS server

Use the diagnose test authserver command on the CLI to test whether a user's credentials can successfully authenticate. You want to ensure that authentication is successful, before implementing it on any of your firewall policies.

The response from the server reports success, failure, and group membership details.

Testing RADIUS is much the same as testing LDAP. Use the diagnose test authserver command on the CLI to test whether a user's credentials can successfully authenticate. Again, you should do this to ensure authentication is successful before implementing it on any of your firewall policies.

Like LDAP, it reports success, failure, and group membership details, depending on the server's response. Deeper troubleshooting usually requires RADIUS server access.

Note that Fortinet has a vendor-specific attributes (VSA) dictionary to identify the Fortinet-proprietary RADIUS attributes. This capability allows you to extend the basic functionality of RADIUS. You can obtain the Fortinet VSA dictionary from the Fortinet Knowledge Base (kb.fortinet.com).

DO NOT REPRINT

© FORTINET

Two-Factor Authentication and One-Time Passwords

- Strong authentication that improves security by preventing attacks associated with the use of static passwords alone
- Requires two independent methods of identifying a user:
 - Something you know, such as a password or PIN
 - Something you have, such as a token or certificate
- One-time passwords (OTPs) can be used one time only
 - OTPs are more secure than static passwords
- Available on both user and administrator accounts
 - The user or user group is added to a firewall policy in order to authenticate
- Methods of OTP delivery include:
 - FortiToken 200 or FortiToken Mobile
 - Generates a six-digit code every 60 seconds based on a unique seed and GMT time
 - Email or SMS
 - An OTP is sent to the user's email or SMS
 - Email or SMS must be configured on the user's account
 - FortiToken mobile push
 - Supports two-factor authentication without requiring user to enter code
 - NTP server recommended!



© Fortinet Inc. All Rights Reserved.

15

Traditional user authentication requires your user name plus something you know, such as a password. The weakness in this traditional method of authentication is that if someone obtains your username, they need only your password to compromise your account. Furthermore, since people tend to use the same password across multiple accounts (some sites with more security vulnerabilities than others), accounts are vulnerable to attack, regardless of password strength.

Two-factor authentication, on the other hand, requires something you know, such as a password, and something you have, such as a token or certificate. Because this method places less importance on often vulnerable passwords, it makes compromising the account more complex for an attacker. You can use two-factor authentication on FortiGate with both user and administrator accounts. The user (or user group to which the user belongs) is added to a firewall policy in order to authenticate. Note that you cannot use two-factor authentication with explicit proxies.

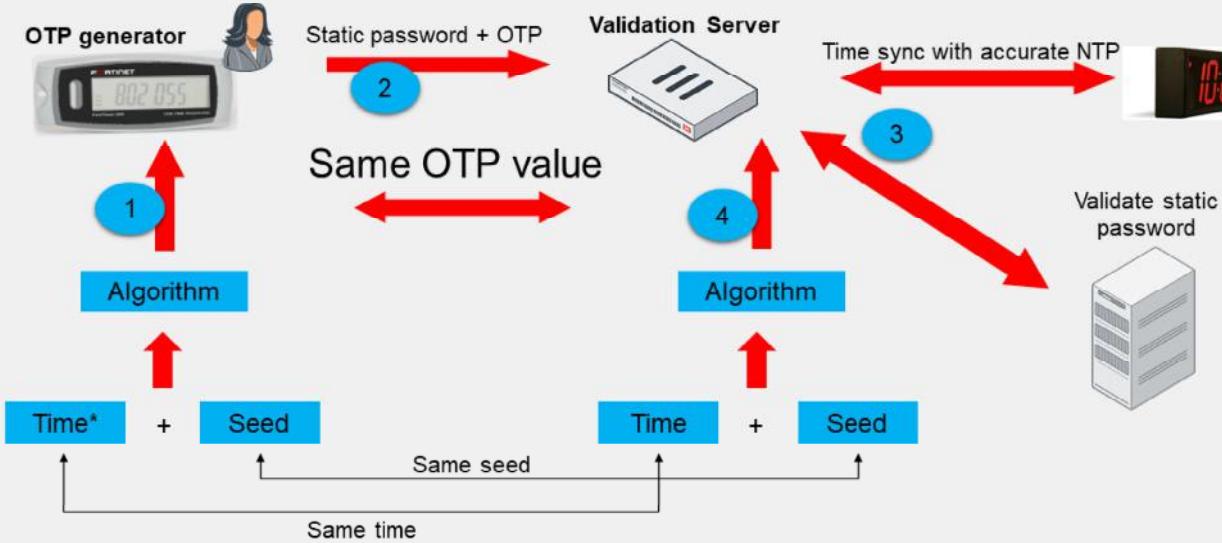
You can use one-time passwords (OTPs) as your second factor. OTPs are more secure than static passwords because the passcode changes at regular intervals and is valid for only a short amount of time. Once you use the OTP, you can't use it again. So, even if it is intercepted, it is useless. FortiGate can deliver OTPs through tokens, such as FortiToken 200 (hardware token) and FortiToken Mobile (software token), as well as through email or SMS. To deliver an OTP over email or SMS, the user account must contain user contact information.

FortiTokens and OTPs delivered through email and SMS are time based. FortiTokens, for example, generate a new, six-digit password every 60 seconds (by default). An NTP server is highly recommended to ensure the OTPs remain in sync. FortiToken Mobile Push allows users to accept the authorization request from their FortiToken mobile app, without the need to enter an additional code.

DO NOT REPRINT

© FORTINET

FortiTokens



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

16

Tokens use a specific algorithm to generate an OTP. The algorithm consists of:

- A seed: a unique, randomly-generated number that does not change over time
- The time: obtained from an accurate internal clock

Both seed and time go through an algorithm that generates an OTP (or passcode) on the token. The passcode has a short life span, usually measured in seconds (60 seconds for FortiToken 200, possibly more or less for other RSA key generators). Once the life span ends, a new passcode generates.

When using two-factor authentication using a token, the user must first log in with a static password followed by the passcode generated by the token. A validation server (FortiGate) receives the user's credentials and validates the static password first. The validation server then proceeds to validate the passcode. It does so by regenerating the same passcode using the seed and system time (which is synchronized with the one on the token) and comparing it with the one received from the user. If the static password is valid, and the OTP matches, the user is successfully authenticated. Again, both the token and the validation server must use the same seed and have synchronized system clocks. As such, it is crucial that you configure the date and time correctly on FortiGate, or link it to an NTP server (which is recommended).

DO NOT REPRINT

© FORTINET

Assigning a FortiToken to a User

The screenshot shows the FortiGate User & Authentication interface. On the left, the 'FortiTokens' page lists two tokens: 'Mobile Token' FTKMOB781E57E34F and 'Mobile Token' FTKMOB783867923E, both marked as 'Available'. A blue callout points to the 'Create New' button with the text 'Two free FortiToken Mobile activations'. Below this, a 'New FortiToken' dialog shows a 'Mobile Token' being created with activation code '0000-0000-0000-0000'. A blue callout points to the 'Mobile Token' radio button with the text 'Can add a user to a group and create a firewall policy based on the user group'. On the right, a 'New User' dialog shows a user 'student' being created with 'Two-factor Authentication' enabled, 'FortiToken' selected as the authentication type, and 'FTKMOB6B91B33BE5' assigned as the token. A blue callout points to the 'Two-factor Authentication' checkbox with the text 'Two free FortiToken Mobile activations'.

User & Authentication > FortiTokens

New FortiToken

New User

Two free FortiToken Mobile activations

- Enable **Two-factor Authentication** and select the registered FortiToken

Can add a user to a group and create a firewall policy based on the user group

© Fortinet Inc. All Rights Reserved. 17

You can add a FortiToken 200 or FortiToken Mobile to FortiGate on the **FortiTokens** page.

A hard token has a serial number that provides FortiGate with details on the initial seed value. If you have several hard tokens to add, you can import a text file, where one serial number is listed per line.

A soft token requires an activation code. Note that each FortiGate (and FortiGate VM) provides two free FortiToken Mobile activations. You must purchase any additional tokens from Fortinet.

You cannot register the same FortiToken on more than one FortiGate. If you want to use the same FortiToken for authentication on multiple FortiGate devices, you must use a central validation server, such as FortiAuthenticator. In that case, FortiTokens are registered and assigned to users on FortiAuthenticator, and FortiGate uses FortiAuthenticator as its validation server.

After you have registered the FortiToken devices with FortiGate, you can assign them to users to use as their second-factor authentication method. To assign a token, edit (or create) the user account and select **Enable Two-factor Authentication**. On the **Token** drop-down list, select the registered token you want to assign.

DO NOT REPRINT**© FORTINET**

Authentication Methods and Active Authentication

- Active
 - User receives a login prompt
 - Must manually enter credentials to authenticate
 - POP3, LDAP, RADIUS, Local, and TACACS+
- Passive
 - User does not receive a login prompt from FortiGate
 - Credentials are determined automatically
 - Method varies depending on type of authentication used
 - FSSO, RSSO, and NTLM



© Fortinet Inc. All Rights Reserved.

18

All the authentication methods you've learned about—local password authentication, server-based authentication, and two-factor authentication—use active authentication. Active authentication means that users are prompted to manually enter their login credentials before being granted access.

But not all users authenticate the same way. Some users can be granted access transparently, because user information is determined without asking the user to enter their login credentials. This is known as passive authentication. Passive authentication occurs with the single sign-on method for server-based password authentication: FSSO, RSSO, and NTLM.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which firewall authentication method does FortiGate support?
 A. Local password authentication
 B. Biometric authentication

2. A remote LDAP user is trying to authenticate with a username and password. How does FortiGate verify the login credentials?
 A. FortiGate queries its own database for user credentials.
 B. FortiGate sends the user-entered credentials to the remote server for verification.

3. When FortiGate uses a RADIUS server for remote authentication, which statement about RADIUS is true?
 A. FortiGate must query the remote RADIUS server using the distinguished name (dn).
 B. RADIUS group memberships are provided by vendor-specific attributes (VSAs) configured on the RADIUS server

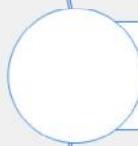
DO NOT REPRINT

© FORTINET

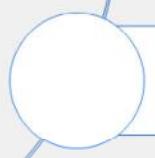
Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

Good job! You now understand the basics of firewall authentication.

Now, you will learn about user groups.

DO NOT REPRINT

© FORTINET

User Groups

Objectives

- Configure user groups

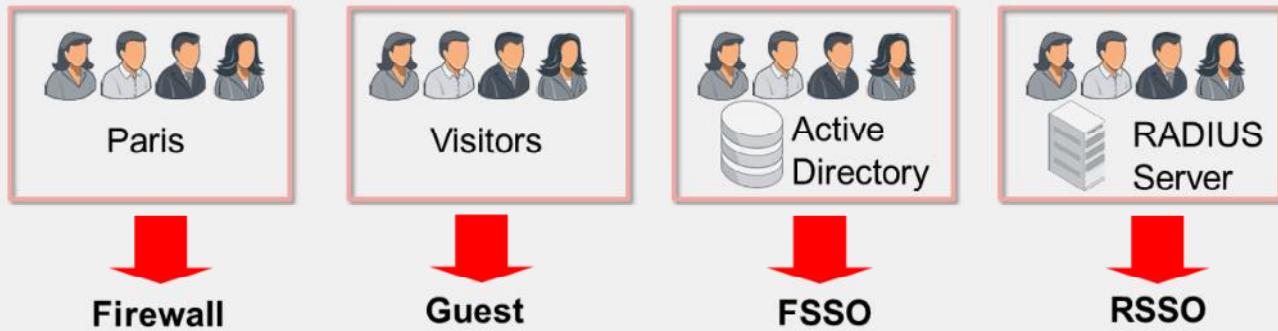
After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in user groups, you will be able to configure user groups to efficiently manage firewall policies.

DO NOT REPRINT

© FORTINET

Types of User Groups



- User groups types: firewall, Fortinet single sign-on (FSSO), guest, and RADIUS single sign-on (RSSO)
- Firewall user groups provide access to firewall policies that require authentication
- FSSO and RSSO are used for single sign-on authentication

FortiGate allows administrators to assign users to groups. Usually, groups are used to more effectively manage individuals that have some kind of shared relationship. You might want to group employees by business area, such as finance or HR, or by employee type, such as contractors or guests.

After you create user groups, you can add them to firewall policies. This allows you to control access to network resources because policy decisions are made on the group as a whole. You can define both local and remote user groups on a FortiGate device. There are four user group types:

- Firewall
- Guest
- Fortinet single sign-on (FSSO)
- RADIUS single sign-on (RSSO)

The firewall user groups on FortiGate do not need to match any type of group that may already exist on an external server, such as an LDAP server. The firewall user groups exist solely to make configuration of firewall policies easier.

Most authentication types have the option to make decisions based on the individual user, rather than just user groups.

DO NOT REPRINT
© FORTINET

Guest User Groups

- Most commonly used for guest access in wireless networks
- Guest groups contain temporary accounts

User & Authentication > User Groups

Name: Guests

Type: Guest (highlighted in red)

Batch Guest Account Creation:

User ID: Email Auto Generated Specify

Maximum Accounts:

Guest Details:

- Enable Name:**
- Enable Email:**
- Enable SMS:**
- Password:** Auto Generated Specify
- Sponsor:** Optional Required
- Company:** Optional Required

Expiration:

Start Countdown: On Account Creation After First Login

Time: Days: 0 Hours: 4 Minutes: 0 Seconds: 0

Account expiry

© Fortinet Inc. All Rights Reserved.

FORTINET
 Training Institute

23

Guest user groups are different from firewall user groups because they contain exclusively temporary guest user accounts (the whole account, not just the password). Guest user groups are most commonly used in wireless networks. Guest accounts expire after a predetermined amount of time.

Administrators can manually create guest accounts or create many guest accounts at once using randomly generated user IDs and passwords. This reduces administrator workload for large events. Once created, you can add accounts to the guest user group and associate the group with a firewall policy.

You can create guest management administrators who have access only to create and manage guest user accounts.

DO NOT REPRINT
© FORTINET

Configuring User Groups

User & Authentication > User Groups

Name: Training-users
 Type: Firewall
 Members: +
 Remote Groups:

Remote Server	Group Name
External_Server	cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=...

Add members to group (local or PKI peer)

Can add preconfigured remote servers to the group

Select Entries

USER (2)

Local (2)

guest

student

Can select specific LDAP groups as defined on the LDAP server

You can configure user groups on the **User Groups** page. You must specify the user group type and add users to the group. Depending on the group you create, you require different configurations. For the firewall user group, for example, members can consist of local users, PKI peer users, and users from one or more remote authentication servers. If your remote authentication server is an LDAP server, you can select specific LDAP groups to add to your user group, as defined on the LDAP server. Note that you can also select RADIUS groups, but this requires additional configuration on your RADIUS server and FortiGate (see the Fortinet Knowledge Base at kb.fortinet.com).

User groups simplify your configuration if you want to treat specific users in the same way, for example, if you want to provide the entire training department with access to the same network resources. If you want to treat all users differently, you need to add all users to firewall policies separately.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which statement about guest user groups is true?
 A. Guest user group accounts are temporary.
 B. Guest user group account passwords are temporary.

2. Guest accounts are most commonly used for which purposes?
 A. To provide temporary visitor access to corporate network resources
 B. To provide temporary visitor access to wireless networks

DO NOT REPRINT

© FORTINET

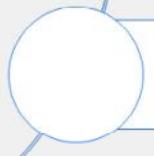
Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

Good job! You now understand the basics of user groups.

Now, you will learn about using firewall policies for authentication.

DO NOT REPRINT**© FORTINET**

Authentication Using Firewall Policies

Objectives

- Configure firewall policies
- Monitor firewall users

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

By demonstrating competence in firewall policies, you will be able to configure firewall policies to enforce authentication on specific users and user groups.

DO NOT REPRINT

© FORTINET

Firewall Policy—Source

- Firewall policies can use user and user group objects to define the source. The objects include:
 - Local firewall accounts
 - External (remote) server accounts
 - PKI (certificate) users
 - FSSO users
- Anyone who belongs to the group and provides correct information will have a successful authentication

Policies & Objects > Firewall Policy

Source	
Full_Access	port3
port1	
LOCAL_SUBNET	
External-Server-Users	
Destination	
all	
Schedule	
always	
Service	
ALL	
Action	
✓ ACCEPT	✗ DENY

Select Entries

Address User Internet Service

Q Search + Create

USER (2)

Local (2)

guest

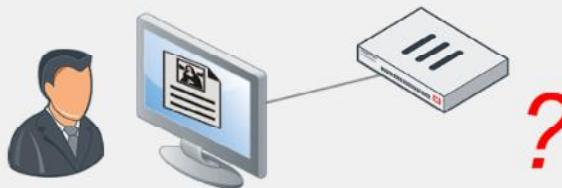
student

USER GROUP (3)

External-Server-Users

Guest-group

SSO_Guest_Users



A firewall policy consists of access and inspection rules (compartmentalized sets of instructions) that tell FortiGate how to handle traffic on the interface whose traffic they filter. After the user makes an initial connection attempt, FortiGate checks the firewall policies to determine whether to accept or deny the communication session. However, a firewall policy also includes a number of other instructions, such as those dealing with authentication. You can use the source of a firewall policy for this purpose. The source of a firewall policy must include the source address (IP address), but you can also include the user and user group. In this way, any user, or user group that is included in the source definition for the firewall policy can successfully authenticate.

User and user group objects can consist of local firewall accounts, external server accounts, PKI users, and FSSO users.

DO NOT REPRINT

© FORTINET

Firewall Policy—Service

- DNS traffic can be allowed if user has not authenticated yet
 - Hostname resolution is often required by the application layer protocol (HTTP/HTTPS/FTP/Telnet) that is used to authenticate
 - DNS service must be explicitly listed as a service in the policy

Policies & Objects > Firewall Policy

Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1	Full_Access	External-Server-Users LOCAL_SUBNET	all	always DNS HTTP	ACCEPT	Enabled

A firewall policy also checks the service in order to transport the named protocols or group of protocols. No service (with the exception of DNS) is allowed through the firewall policy before successful user authentication. DNS is usually used by HTTP so that people can use domain names for websites, instead of their IP address. DNS is allowed because it is a base protocol and will most likely be required to initially see proper authentication protocol traffic. Hostname resolution is almost always a requirement for any protocol. However, the DNS service must still be defined in the policy as allowed, in order for it to pass.

In the example shown on this slide, policy sequence 1 (Full_Access) allows users to use external DNS servers in order to resolve host names, before successful authentication. DNS is also allowed if authentication is unsuccessful because users need to be able to try to authenticate again. Any service that includes DNS would function the same way, like the default ALL service.

HTTP service is TCP port 80 and does not include DNS (UDP port 53).

DO NOT REPRINT

© FORTINET

Protocols

- A firewall policy must allow a protocol in order to show the authentication dialog that is used in active authentication:
 - HTTP
 - HTTPS
 - FTP
 - Telnet
- All other services are not allowed until the user has authenticated successfully through one of the protocols listed above

As well as the DNS service, the firewall policy must specify the allowed protocols, such as HTTP, HTTPS, FTP, and Telnet. If the firewall policy that has authentication enabled does not allow at least one of the supported protocols used for obtaining user credentials, the user will not be able to authenticate.

Protocols are required for all authentication methods that use active authentication (local password authentication, server-based password authentication, and two-factor authentication). Active authentication prompts the user for user credentials based on the following:

- The protocol of the traffic
- The firewall policy

Passive authentication, on the other hand, determines the user identity behind the scenes, and does not require any specific services to be allowed within the policy.

DO NOT REPRINT

© FORTINET

Mixing Policies

- Enabling authentication on a policy does not always force an active authentication prompt

port5 → port1								
Sequence	User	Source	Action	AV	SSL	Auth	Action	Enabled
17	Guest	LOCAL_SUBNET	all	Guest_AV	certificate-inspection	always	ALL	ACCEPT Enabled
18	Contractor	LOCAL_SUBNET	all	Contractor_AV	certificate-inspection	always	ALL	ACCEPT Enabled
19	Other	LOCAL_SUBNET	all	default	certificate-inspection	always	ALL	ACCEPT Enabled

- Three options:
 - Enable authentication on every policy that could match the traffic
 - Enforce authentication on demand option (CLI option only)
 - Enable a captive portal on the ingress interface for the traffic
- If login cannot be determined passively, then FortiGate uses active authentication
 - FortiGate does not prompt the user for login credentials when it can identify the user passively
 - By default, active authentication is intended to be used as a backup when passive authentication fails

In the example shown on this slide, assuming active authentication is used, any initial traffic from LOCAL_SUBNET will not match policy sequence 17 (Guest). Policy sequence 17 looks for both IP and user, and user group information (LOCAL_SUBNET and Guest-group respectively), and since the user has not yet authenticated, the user group aspect of the traffic does not match. Since the policy match is not complete, FortiGate continues its search down the sequence list, to see if there is a complete match.

Next, FortiGate evaluates policy sequence 18 to see if the traffic matches. It will not for the same reason it did not match 17.

Finally, FortiGate evaluates policy sequence 19 to see if the traffic matches. It matches all criteria, so traffic is allowed with no need to authenticate.

When you use only active authentication, if all possible policies that could match the source IP have authentication enabled, then the user will receive a login prompt (assuming they use an acceptable login protocol). In other words, if policy sequence 19 also had authentication enabled, the users would receive login prompts.

If you use passive authentication and it can successfully obtain user details, then traffic from LOCAL_SUBNET with users that belong to Guest-group will apply to policy sequence 17, even though policy sequence 19 does not have authentication enabled.

If you use both active and passive authentication, and FortiGate can identify a user's credentials through passive authentication, the user never receives a login prompt, regardless of the order of any firewall policies. This is because there is no need for FortiGate to prompt the user for login credentials when it can identify who the user is passively. When you combine active and passive authentication methods, active authentication is

DO NOT REPRINT

© FORTINET

intended to be used as a backup, to be used only when passive authentication fails.

DO NOT REPRINT
© FORTINET

Active Authentication Behavior

- Enable authentication on every policy that could match the traffic:
 - All firewall policies must have authentication enabled (active or passive)
- If there is a fall-through policy in place, unauthenticated users are not prompted for authentication
- Enforce authentication on demand option:
 - CLI option only

```
# config user setting
(setting) # set auth-on-demand
<always|implicit>
Implicit - default option. It will not
trigger authentication if there is a fall
through policy.
Always - Trigger authentication prompt for
policies that have active authentication
enabled regardless of a fall through policy
```

 - Provides more granular control
 - Authentication is enabled at a firewall policy level
 - You must place passive authentication policies on top of active authentication policy
- Enable a captive portal on the ingress interface for the traffic:
 - Authentication happens at an interface level
 - Traffic is not allowed without valid authentication unless it matches an exemption
 - All users are prompted for authentication before they can access any resource

As mentioned earlier, there are three different ways you can alter active authentication behavior. If you have an active authentication firewall policy followed by a fall-through policy that does not have authentication enabled on it, then all traffic will use the fall-through policy. This means that users are not asked to authenticate. By default, all traffic passes through the catch-all policy without being authenticated. You can alter this behavior by enabling authentication on all firewall policies. When you enable authentication, all the systems must authenticate before traffic is placed on the egress interface.

Alternatively, only on the CLI, you can change the auth-on-demand option to always. This instructs FortiGate to trigger an authentication request, if there is a firewall policy with active authentication enabled. In this case, the traffic is allowed until authentication is successful.

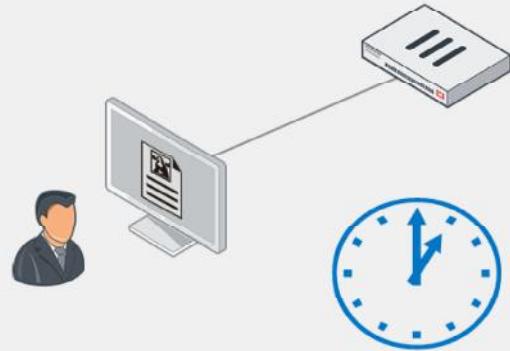
If you want to have all users connect to a specific interface, then it is better to enable captive portal authentication at the interface level. This way, all devices must authenticate before they are allowed to access any resources.

DO NOT REPRINT**© FORTINET**

Authentication Timeout

```
#config user setting
  set auth-timeout-type [idle-timeout|hard-timeout|new-session]
end
```

- Timeout specifies how long a user can remain idle before the user must authenticate again
 - Default is five minutes
- Three options for behavior:
 - Idle (default): no traffic for that amount of time
 - Hard: authentication expires after that amount of time, regardless of activity
 - New session: authentication expires if no new session is created in that amount of time



An authentication timeout is useful for security purposes. It minimizes the risk of someone using the IP of the legitimate authenticated user. It also ensures users do not authenticate and then stay in memory indefinitely. If users stayed in memory forever, it would eventually lead to memory exhaustion.

There are three options for timeout behavior:

- **Idle**: looks at the packets from the host IP. If there are no packets generated by the host device in the configured timeframe, then the user is logged out.
- **Hard**: time is an absolute value. Regardless of the user's behavior, the timer starts as soon as the user authenticates and expires after the configured value.
- **New session**: even if traffic is being generated on existing communications channels, the authentication expires if no new sessions are created through the firewall from the host device within the configured timeout value.

Choose the type of timeout that best suits the authentication needs of your environment.

DO NOT REPRINT

© FORTINET

Monitoring Users

Dashboard > User & Devices > Firewall Users

Method

1 Users

User Group

1 Users

Deauthenticate

Search

User Name	IP Address	User Group	Duration	Traffic Volume	Method
student	10.0.1.10	CP-group	1 minute(s) and 9 second(s)	10.43 kB	Firewall

Confirm

⚠ Are you sure you want to deauthenticate the selected user(s)?

OK Cancel

© Fortinet Inc. All Rights Reserved.

34

You can monitor users who authenticate through your firewall policies using the **Dashboard > User & Devices > Firewall Users** page. It displays the user, user group, duration, IP address, traffic volume, and authentication method.

It does not include administrators, because they are not authenticating through firewall policies that allow traffic. They are logging in directly on FortiGate.

This page also allows you to disconnect a user, or multiple users, at the same time.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Firewall policies dictate whether a user or device can or cannot authenticate on a network. Which statement about firewall authentication is true?
 A. Firewall policies can be configured to authenticate certificate users.
B. The order of the firewall policies always determines whether a user's credentials are determined actively or passively.
2. Which statement about active authentication is true?
A. Active authentication is always used before passive authentication.
 B. The firewall policy must allow the HTTP, HTTPS, FTP, and/or Telnet protocols in order for the user to be prompted for credentials.
3. Which statement best describes the authentication idle timeout feature on FortiGate?
A. The length of time FortiGate waits for the user to enter their authentication credentials
 B. The length of time an authenticated user is allowed to remain authenticated without any packets being generated by the host device

DO NOT REPRINT

© FORTINET

Lesson Progress



Methods of Firewall Authentication



User Groups



Authentication Using Firewall Policies

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

36

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Describe firewall authentication
- ✓ Identify the different methods of firewall authentication available on FortiGate devices
- ✓ Identify supported remote authentication servers
- ✓ Describe active and passive authentication and the order of operations
- ✓ Configure users for local password authentication, server-based password authentication, and two-factor authentication
- ✓ Configure a remote authentication server
- ✓ Configure user authentication and firewall policies
- ✓ Monitor firewall users



© Fortinet Inc. All Rights Reserved.

37

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

By mastering the objectives covered in this lesson, you learned how to use authentication on the firewall policies of FortiGate.

DO NOT REPRINT

© FORTINET

FORTINET
Training Institute



FortiGate Security

Logging and Monitoring

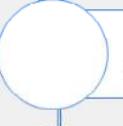
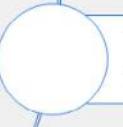
FortiOS 7.2

Last Modified: 13 June 2022

In this lesson, you will learn how to configure local and remote logging on FortiGate; view, search, and monitor logs; and protect your log data.

DO NOT REPRINT**© FORTINET**

Lesson Overview

**Log Basics****Local and Remote Logging****Log Settings and Log Search****Protect Log Data**

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

DO NOT REPRINT
© FORTINET

Log Basics

Objectives

- Describe the log workflow
- Identify log types and subtypes
- Describe log severity levels
- Describe the layout of a log message
- Describe the effect of logging on performance

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

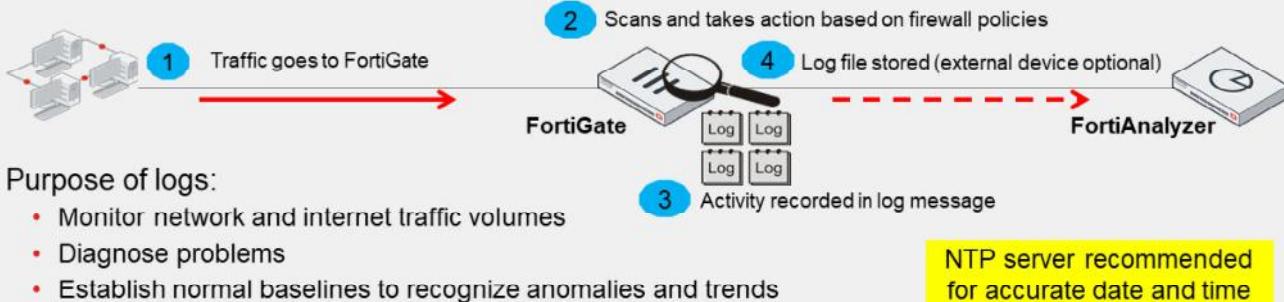
By demonstrating competence in log basics, you will be able to more effectively analyze log data from your database.

DO NOT REPRINT

© FORTINET

Logging Workflow

1. Traffic passes through FortiGate to your network
2. FortiGate scans the traffic and takes action based on configured firewall policies
3. Activity is recorded and the information is contained in a log message
4. Log message is stored in a log file and on a device capable of storing logs (local FortiGate device or an external device, such as FortiAnalyzer)



- Purpose of logs:
 - Monitor network and internet traffic volumes
 - Diagnose problems
 - Establish normal baselines to recognize anomalies and trends

NTP server recommended
for accurate date and time

When traffic passes through FortiGate to your network, FortiGate scans the traffic, and then takes action based on the firewall policies in place. This activity is recorded, and the information is contained in a log message. The log message is stored in a log file. The log file is then stored on a device capable of storing logs. FortiGate can store logs locally on its own disk space, or can send logs to an external storage device, such as FortiAnalyzer.

The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and more. Logs provide you with a greater perspective of your network, allowing you to adjust your network security settings if necessary.

Some organizations have legal requirements when it comes to logging, so it is important to be aware of your organization's policies during configuration.

For effective logging, your FortiGate system date and time should be accurate. You can either manually set the system date and time, or configure FortiGate to keep its time correct automatically by synchronizing with a Network Time Protocol (NTP) server. An NTP server is highly recommended.

DO NOT REPRINT**© FORTINET**

Log Types and Subtypes

- *Traffic* logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any)
- *Event* logs record system and administrative events, such as adding or modifying a setting, or daemon activities
- *Security* logs record security events, such as virus attacks and intrusion attempts, based on the security profile type (log type = utm)

Traffic	Event	Security
Forward	Endpoint	Application Control
Local	High Availability	Antivirus
Sniffer	General System	DNS Query
	User	File Filter
	Router	Web Filter
	VPN	Intrusion Prevention
	SD-WAN	Anomaly
	WiFi	SSL
	CIFS	SSH
	Security Ratings	
	SDN Connector	

To FortiGate, there are three different types of logs: traffic logs, event logs, and security logs. Each type is further divided into subtypes.

Traffic logs record traffic flow information, such as an HTTP/HTTPS request and its response, if any. It contains subtypes named forward, local, and sniffer.

- Forward traffic logs contain information about traffic that FortiGate either accepted or rejected according to a firewall policy.
- Local traffic logs contain information about traffic directly to and from the FortiGate management IP addresses. They also include connections to the GUI and FortiGuard queries.
- Sniffer logs contain information related to traffic seen by the one-arm sniffer.

Event logs record system and administrative events, such as adding or modifying a setting, or daemon activities. It contains the subtypes listed on the slide.

- System event logs contain information related to operations, such as automatic FortiGuard updates and GUI logins.
- User logs contain login and logout events for firewall policies with user authentication.
- Router, VPN, and wireless subtypes include logs for those features. For example, VPN contains IPsec and SSL VPN log entries.

Finally, security logs record security events, such as virus attacks and intrusion attempts. They contain log entries based on the security profile type (log type = utm), including the subtype listed on the slide.

DO NOT REPRINT**© FORTINET**

Log Severity Levels

- Each log entry includes a log level (also known as priority level) that ranges in order of importance
 - 0 = high importance / 6 = low importance

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality effected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information
7 – Debug	Diagnostic information for investigating issues

Rarely used, unless actively investigating an issue with Fortinet Support

Each log entry includes a log level (or priority level) that ranges in order of importance from emergency to information.

There is also a debug level that includes diagnostic information into the event log. The debug level is rarely used, unless you are actively investigating an issue with Fortinet Support. Generally, the lowest level you want to use is information, but even this level generates many logs and can cause premature hard disk failure. Depending on the type of log and the needs of your organization, you may want to log only notification levels or higher.

You and your organization's policies dictate what must be logged.

DO NOT REPRINT

© FORTINET

Log Message Layout

- Log header (similar in all logs)
 - Type and subtype = Name of log file

- Level = Severity level

```
date=2022-03-14 time=12:05:28 logid=0316013056 type=utm subtype=webfilter
eventtype=ftgd_blk level=warning vd=root
```

- Log body (varies by log type)

- policyid = Firewall policy applied to session
- hostname = URL or IP of host

- srcip and dstip = Source and destination IP
- action = Action taken by FortiGate
- msg = Reason for the action

```
policyid=1 sessionid=10879 user="" srcip=10.0.1.10 srcport=60952 srcintf="port3"
dstip=52.84.14.233 dstport=80 dstintf="port1" proto=6 service="HTTP"
hostname="miniclip.com" profile="default" action=blocked reqtype=direct
url="/lavicon.ico" sentbyte=297 rcvbyte=0 direction=outgoing
msg="URL belongs to a denied category in policy" method=domain cat=20 catdesc="Games"
crscore=30 crlevel=high
```

Every log message has a standard layout comprising two sections: a header and a body.

The header contains fields that are common to all log types, such as originating date and time, log identifier, log category, severity level, and virtual domain (VDOM). The value of each field, however, is specific to the log message. In the raw log entry example shown on this slide, the log type is UTM, the subtype is webfilter, and the level is warning. The type and subtype of logs determine what fields appear in the log body.

The body, therefore, describes the reason why the log was created, and the actions taken by FortiGate. These fields vary by log type. In the example shown on this slide, the fields are as follows:

- The `policyid` field indicates which firewall rule matched the traffic
- The `srcip` field indicates the source IP address
- The `dstip` field indicates the destination IP address
- The `hostname` field indicates the URL or IP of the host
- The `action` field indicates what FortiGate did when it found a policy that matched the traffic
- The `msg` field indicates the reason for the action taken. In this example, the action is `blocked`, which means that FortiGate prevented this IP packet from passing, and the reason is because it belonged to a denied category in the firewall policy.

If you log to a third-party device, such as a syslog server, knowing the log structure is crucial to integration. For information on log structures and associated meanings, visit <http://docs.fortinet.com>.

DO NOT REPRINT**© FORTINET**

Effect of Logging on Performance

- More logs = more CPU, memory, and disk space used
- Depending on the amount of traffic you have, and the logging settings that are enabled, your traffic logs can swell and impact the performance of your firewall
- Traffic logs record every session
 - Extra information for troubleshooting
 - Some UTM events
 - More system intensive

Enable performance statistic
logging for remote logging
devices on FortiGate

```
# config system global
    set sys-perf-log-interval <number from 0-15>
end
```

It is important to remember that the more logs that get generated, the heavier the toll on your CPU, memory, and disk resources. Storing logs for a period of time also requires disk space, as does accessing them. So, before configuring logging, make sure it is worth the extra resources and that your system can handle the influx.

Also important to note is the logging behavior with security profiles. Security profiles can, depending on the logging settings, create log events when a traffic matching the profile is detected. Depending on the amount of traffic you have, and the logging settings that are enabled, your traffic logs can swell and, ultimately, impact the performance of your firewall.

When using remote logging devices, such as FortiAnalyzer and syslog, you can enable performance statistic logging to occur every 1-15 minutes (0 to disable). This is not available for local disk logging or FortiCloud.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which type of logs are application control, web filter, and antivirus?
 A. Event
 B. Security

2. The log _____ contains fields that are common to all log types, such as originating date and time, log identifier, log category, and VDOM.
 A. header
 B. body

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Log Basics****Local and Remote Logging****Log Settings****View, Search, and Monitor Logs****Protect Log Data**

Good job! You now understand log basics.

Now, you will learn about local logging.

DO NOT REPRINT**© FORTINET**

Local and Remote Logging

Objectives

- Identify log storage options
- Enable local and remote logging
- Understand disk allocation and reserved space
- Understand how remote logging works with VDOMs
- Understand log transmission
- Enable reliable logging

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

By demonstrating competence in local logging, you will be able to successfully store logs to local disk and retain those logs, based on your requirements.

DO NOT REPRINT

© FORTINET

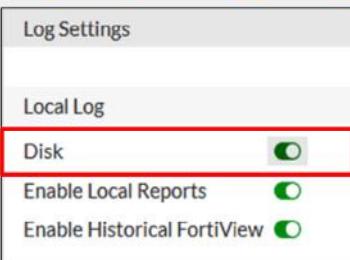
Log Storage—Local

- To store logs locally on FortiGate, you must enable disk logging


```
# config log disk setting
      set status enable
```
- If disk logging is enabled, the report daemon collects statistics used for historical FortiView from disk
 - If disk logging is disabled, FortiView logs are only available in real time
- By default, logs older than seven days are deleted from disk (configurable)


```
# config log disk setting
      set maximum-log-age <integer>
```

Log & Report > Log Settings



- FortiGate devices that have a hard drive store logs in an SQL database
- Data is extracted from the SQL database for reports



Hard drive

Performance may be impacted under heavy strain

Typically, mid-level to high-end FortiGate models have a hard drive. FortiGate can store logs on its hard drive. This operation is known as local logging or disk logging. Depending on the model series, disk logging may be enabled by default.

FortiGate can store all log types, including log archives and traffic logs, locally. Traffic logs and log archives are larger files, and need a lot of room when being logged by FortiGate.

Under heavy log usage, disk logging will result in a performance impact.

If you are using the local hard disk on a device for WAN optimization, you cannot also log to disk, unless your device has two separate disks. If your device has two separate disks, you can use one for WAN optimization and the other for logging. If you are using the local hard disk for WAN optimization, and only one disk is available, you can log to remote FortiAnalyzer devices or syslog servers.

If you want to store logs locally on FortiGate, you must enable disk logging on the **Log Settings** page. Only some FortiGate models support disk logging. If your FortiGate does not support disk logging, you can log to an external device instead.

You must enable disk logging in order for information to appear on the FortiView dashboards. If disabled, logs display in real-time only. You can also enable this setting using the CLI `config log disk setting` command.

By default, logs older than seven days are deleted from the disk. This value is configurable.

DO NOT REPRINT
© FORTINET

FortiGate Disk Allocation—Reserved Space

- The system reserves approximately 25% of its disk space for system usage and unexpected quota overflow
 - Only ~75% of disk space is available to store logs

```
FGT_A (global) # diagnose sys logdisk usage
Total HD usage: 208MB/118145MB
Total HD logging space: 88608MB
HD logging space usage for vdom "root": 0MB/9965MB
HD logging space usage for vdom "vdom1": 0MB/104857MB
```

Use this command to obtain the amount of reserved space on your FortiGate

- Formulas:
 - disk - logging = reserved (i.e. 118145MB - 88608MB = 29537MB reserved)
 - reserved/disk*100 = reserved % (i.e. 29537/118145*100 = 25%)

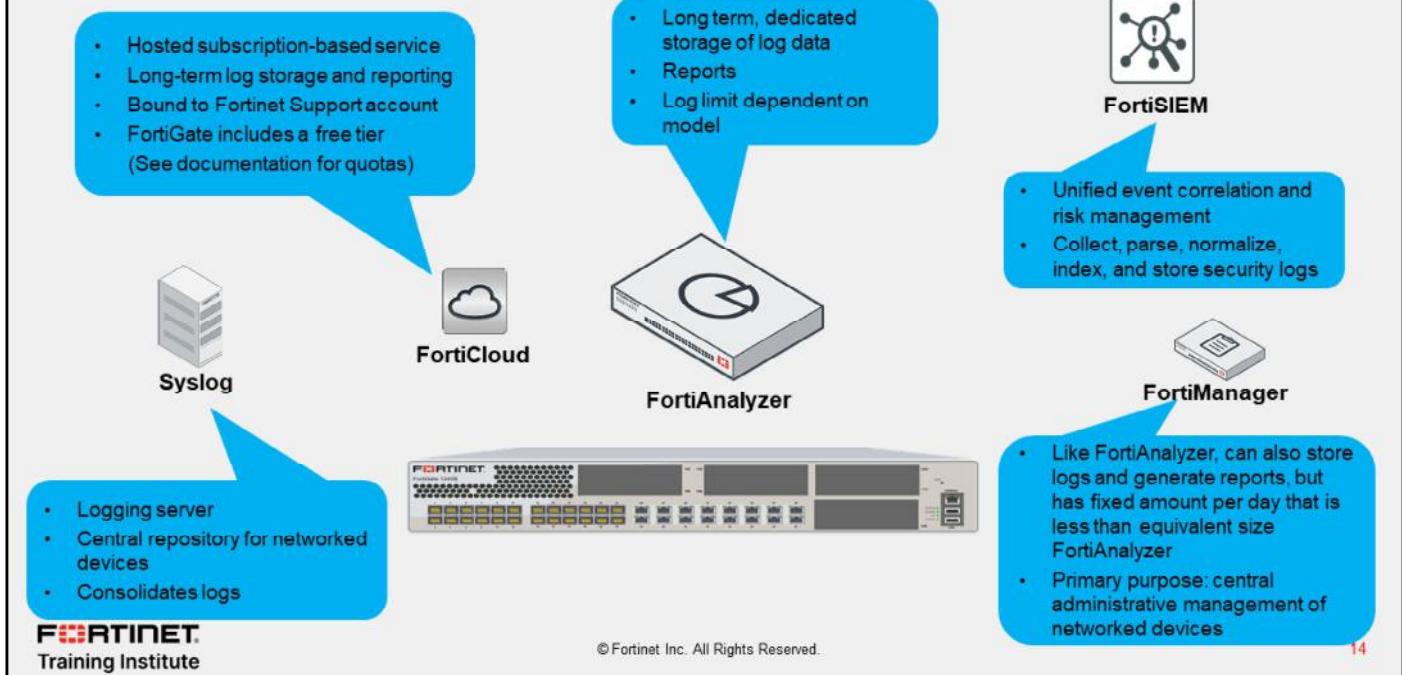
If you decide to log locally on FortiGate, be aware that the entire disk space is not available to store logs. The FortiGate system reserves approximately 25% of its disk space for system usage and unexpected quota overflow.

To determine the amount of reserved space on your FortiGate, use the CLI command `diagnose sys logdisk usage`. Subtract the total logging space from the total disk space to calculate the reserved space.

DO NOT REPRINT

© FORTINET

Log Storage—Remote



You can configure FortiGate to store logs on syslog servers, FortiCloud, FortiSIEM, FortiAnalyzer, or FortiManager. These logging devices can also be used as a backup solution. Whenever possible, it is preferred to store logs externally.

Syslog is a logging server that is used as a central repository for networked devices.

FortiCloud is a Fortinet subscription-based, hosted security management and log retention service that offers long-term storage of logs with reporting. If you have a smaller network, FortiCloud is usually more feasible than buying a dedicated logging device. Note that every FortiGate offers a free tier and will keep logs for seven days. You must upgrade to the paid service to retain logs for one year.

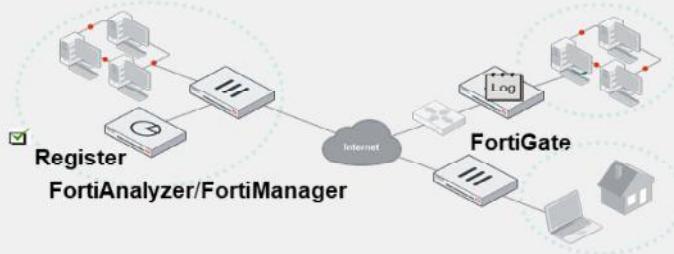
FortiSIEM provides unified event correlation and risk management that can collect, parse, normalize, index, and store security logs.

FortiAnalyzer and FortiManager are external logging devices with which FortiGate can communicate. You can place FortiAnalyzer or FortiManager in the same network as FortiGate, or outside of it. While FortiAnalyzer and FortiManager share a common hardware and software platform and can both take log entries, FortiAnalyzer and FortiManager actually have different capabilities that are worth noting. The primary purpose of FortiManager is to centrally manage multiple FortiGate devices. As such, log volumes are limited to a fixed amount per day, which are less than the equivalent size FortiAnalyzer. On the other hand, the primary purpose of FortiAnalyzer is to store and analyze logs, so the log limit is much higher (though the limit is model dependent). Note that local logging is not required for you to configure logging to FortiAnalyzer or FortiManager.

DO NOT REPRINT
© FORTINET

FortiAnalyzer and FortiManager Log Storage

- FortiGate can send logs to both FortiAnalyzer and FortiManager (FortiGate must be a registered device)



- Can configure up to three separate FortiAnalyzer and FortiManager devices or one cloud FortiAnalyzer instance using the CLI
 - Multiple devices may be needed for redundancy
 - Generating and sending logs requires resources—be aware!

Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager Disabled

IP address: 10.0.1.210

Connection status: Connected

Storage usage: 56.07 MiB / 1000.00 MiB

Analytics usage: 20.82 MiB / 700.00 MiB

Archive usage: 35.25 MiB / 300.00 MiB

Upload option: Real Time | Every Minute | Every 5 Minutes

Allow access to FortiGate REST API:

Verify FortiAnalyzer certificate: FAZ-VM0000065040

```
# config log [fortianalyzer | fortianalyzer-cloud|fortianalyzer2|fortianalyzer3] setting
  set status enable
  set server <server_IP>
end
```

Commands **not** cumulative

The process to configure FortiGate to send logs to FortiAnalyzer or FortiManager is identical. For FortiGate to send logs to either device, you must register FortiGate with FortiAnalyzer or FortiManager. After it is registered, FortiAnalyzer or FortiManager can begin to accept incoming logs from FortiGate.

You can configure remote logging to FortiAnalyzer or FortiManager using both the GUI and CLI.

Note that the **Test Connectivity** function on the GUI will report as failing until FortiGate is registered on FortiAnalyzer or FortiManager, because it is not yet authorized to send logs.

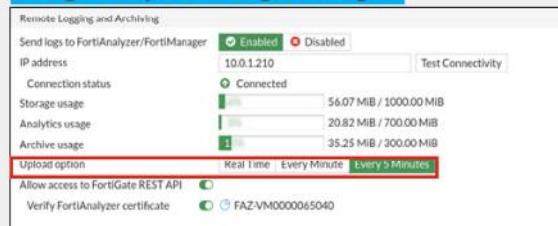
DO NOT REPRINT

© FORTINET

Upload Option

- Near real-time uploading and consistent high-speed compression and analysis
- Configure logging options:
 - store-and-upload (CLI configuration only)
 - **Real Time**
 - **Every Minute**
 - **Every 5 Minutes** (default)

Log & Report > Log Settings



```
# configure log fortianalyzer setting
  set upload-option [store-and-upload |realtime/1-minute/5-minute]
```

- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten; however, you can configure FortiAnalyzer to stop logging

FortiGate allows near real-time uploading and consistent high-speed compression and analysis to FortiAnalyzer and FortiManager.

On the GUI, upload options include **Real Time**, **Every Minute**, and **Every 5 Minutes** (default).

If your FortiGate model includes an internal hard drive, you also have the **store-and-upload** option. This allows you to store logs to disk and then upload to FortiAnalyzer or FortiManager at a scheduled time (usually a low bandwidth time). You can configure the **store-and-upload** option, as well as a schedule, on the CLI only.

DO NOT REPRINT

© FORTINET

FortiAnalyzer Temporarily Unavailable to FortiGate?

- The FortiGate *miglogd* process caches logs on FortiGate when FortiAnalyzer is not reachable
- When maximum cached value is reached, *miglogd* will drop cached logs (oldest first)
- When FortiAnalyzer connection is back, *miglogd* will send the cached logs
 - FortiGate buffer will keep logs long enough to sustain a reboot of FortiAnalyzer, but is not intended for lengthy outages
- FortiGate devices with an SSD have a configurable log buffer

```
Local-FortiGate # diagnose test application miglogd 6

mem=0, disk=0, alert=0, alarm=0, sys=0, faz=19, faz-cloud=0, webt=0, fds=0
interface-missed=0
Queues in all miglogds: cur:0 total-so-far:153
global log dev statistics:
faz 0: sent=15, failed=0, cached=0, dropped=0, relayed=0

Local-FortiGate # diagnose log kernel-stats

fgtlog: 1
fgtlog 0: total-log=32, failed-log=0 log-in-queue=0
```

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

17

If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the *miglogd* process will begin dropping cached logs (oldest first) once this value is reached. When the connection between the two devices is restored, the *miglogd* process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example), but it is not intended for a lengthy FortiAnalyzer outage.

On FortiGate, the CLI command `diagnose test application miglogd 6` displays statistics for the *miglogd* process, including the total cache size and current cache size.

The CLI command `diagnose log kernel-stats` will show an increase in `failed-log` if the cache is full and needs to drop logs.

FortiGate devices with an SSD disk have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, FortiGate can buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully after the connection to FortiAnalyzer is restored.

DO NOT REPRINT

© FORTINET

FortiCloud, Syslog, and FortiSIEM Log Storage

FortiCloud

- Must activate FortiCloud account (dashboard)

Log & Report > Log Settings

Cloud Logging Settings

Type: FortiGate Cloud

```
# config log fortiguard setting
set status enable
set source-ip <src IP used to connect FortiCloud>
set upload-option <realtime | 1-minute | 5-minute>
set enc-algorithm <high-medium | high | low>
end
```

Encryption algorithm setting not available to configure in the GUI

Syslog and FortiSIEM

Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager: Enabled

Send logs to syslog: Enabled

IP Address/FQDN

```
# config log [syslogd | syslogd2 | syslogd3 | syslogd4] setting
set status enable
set server <syslog_IP>
end
```

Can configure up to four remote syslog service or FortiSIEMs using the CLI

- FortiGate logs can be sent to syslog servers in default, CSV, or CEF format

```
# config log syslogd3 setting
set format [default | csv | cef]
end
```

Similar to FortiAnalyzer and FortiManager, you can configure remote logging to FortiCloud on the **Log Settings** page or the CLI. However, you must first activate your FortiCloud account, so FortiGate can communicate with your FortiCloud account. Once complete, you can enable FortiCloud logging and set the upload option. If you want to store your logs to disk first and then upload to FortiCloud, you must specify a schedule. When disk usage is set to WAN optimization (`wanopt`), the store and upload option for logging to FortiCloud is removed.

You can also configure remote logging to syslog and FortiSIEM on the **Log Settings** page or the CLI. You can configure FortiGate to send logs to up to four syslog servers or FortiSIEM devices using the `config log syslogd` CLI command.

FortiGate supports sending logs to syslog in CSV and CEF format, which is an open log management standard that provides interoperability of security-related information between different network devices and applications. CEF data can be collected and aggregated for analysis by enterprise management or Security Information and Event Management (SIEM) systems, such as FortiSIEM. You can configure each syslog server separately to send log messages in CEF or CSV format.

You can configure an individual syslog to use CSV and CEF format using the CLI. The example shown on this slide is for `syslogd3`. All other syslog settings can be configured as required independently of the log message format, including the server address and transport (UDP or TCP) protocol.

DO NOT REPRINT
© FORTINET

VDOMs and Remote Logging

- If you have a FortiGate with Virtual Domains (VDOMs) configured, you can globally add multiple FortiAnalyzer and syslog servers.
 - Up to three FortiAnalyzer devices
 - Up to four syslog servers

```
# config global
  config log fortianalyzer setting
    set status enable
    set server 10.0.1.1
  end
  config log fortianalyzer2 setting
    set status enable
    set server 10.0.2.1
  end
```

If override FAZ/Syslog
needed, must enable it
from VDOM level

```
# config vdom
  edit Training
    config log setting
      set faz-override enable
      set syslog-override enable
  end
```

If you have a FortiGate with virtual domains (VDOMs) configured, you can globally add multiple FortiAnalyzer and syslog servers. You can configure up to three FortiAnalyzer devices and up to four syslog servers under global settings.

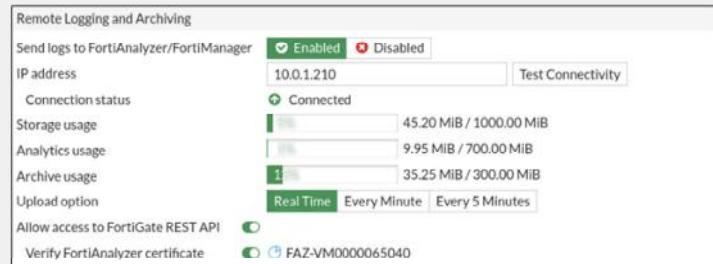
DO NOT REPRINT

© FORTINET

Log Transmission

- FortiGate uses UDP 514 for log transmission by default

```
config log fortianalyzer setting
  set status enable
  set server "10.0.1.210"
  set serial "FAZ-VM0000065040"
  set enc-algorithm high-medium
  set upload-option realtime
end
```



- Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format
 - Reduces disk log size and reduces log transmission time and bandwidth usage

FortiGate uses UDP port 514 for log transmission by default .

Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format. This reduces disk log size and reduces log transmission time and bandwidth usage.

Reliable Logging and OFTPS

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
- If you enable logging to FortiAnalyzer using the GUI, reliable logging is auto-enabled
 - If you enable logging to FortiAnalyzer using the CLI, reliable logging is not auto-enabled. You must manually enable it using the CLI command shown in the screenshot below
- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high)
- If using reliable logging, you can encrypt communications using SSL-secured OFTP (OFTPS)

```

# config log fortianalyzer setting
  set status enable
  set enc-algorithm [high medium | high | low]
  set reliable enable
end

```

When you enable reliable logging on FortiGate, the log transport delivery method changes from User Datagram Protocol (UDP) to Transmission Control Protocol (TCP). TCP provides reliable data transfer, guaranteeing that the transferred data remains intact and arrives in the same order in which it was sent.

If you enable logging to FortiAnalyzer or FortiManager using the GUI, reliable logging is automatically enabled. If you enable logging using the CLI, you must enable reliable logging using the CLI command shown on this slide.

Logging to FortiCloud uses TCP, and you can set the encryption algorithm using the CLI. The default encryption setting is high.

Optionally, if using reliable logging, you can encrypt communications using SSL-encrypted OFTP traffic, so when a log message is generated, it is safely transmitted across an unsecure network. You can choose the level of SSL protection used by configuring the `enc-algorithm` setting on the CLI.

When both FortiGate and FortiAnalyzer are running version 7.2 or later, and reliable logging is configured, FortiGate keeps logs in a *confirm queue* until it verifies those logs were received by FortiAnalyzer. This is achieved by using sequence numbers (`seq_no`) to track the logs received. FortiOS periodically queries FortiAnalyzer for the latest `seq_no` of the last log received, and clears logs from the *confirm queue* up to the `seq_no`.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. Which storage type is preferred for logging?
 A. Remote logging
 B. Hard drive

2. Which protocol does FortiGate use to send encrypted logs to FortiAnalyzer?
 A. OFTPS
 B. SSL

3. If you enable reliable logging, which transport protocol will FortiGate use?
 A. UDP
 B. TCP

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Log Basics****Local and Remote Logging****Log Settings and Log Search****Protect Log Data**

Good job! You now understand remote logging.

Now, you will learn about log settings.

DO NOT REPRINT**© FORTINET**

Log Settings and Log Search

Objectives

- Configure log settings
- Enable logging on firewall policies
- Hide user names in logs
- View and search for log messages
- Configure alert email
- Configure threat weight

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

By demonstrating competence in log settings, you will be able to successfully enable logging on your FortiGate, and ensure logs are generated on traffic caused by traffic passing through your firewall policies.

DO NOT REPRINT

© FORTINET

Logging Settings: If, Where, and How

Log & Report > Log Settings

Local Log

- Disk
- Enable Local Reports
- Enable Historical FortiView

Event Logging

Local Traffic Log

- All Customize
- All Customize
- Log Allowed Traffic
- Log Local Out Traffic
- Log Denied Unicast Traffic
- Log Denied Broadcast Traffic

GUI Preferences

- Resolve Hostnames
- Resolve Unknown Applications

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager Enabled Disabled

IP address: 10.0.1.210

Connection status: Connected

Storage usage: 45.20 MB / 1000.00 MB

Analytics usage: 9.95 MB / 700.00 MB

Archive usage: 35.25 MB / 300.00 MB

Upload option: Real Time | Every Minute | Every 5 Minutes

Allow access to FortiGate REST API

Verify FortiAnalyzer certificate FAZ-VM0000065040

- Log event logs and traffic logs?
- Local traffic logs = traffic directly to and from FortiGate (disabled by default)
- Event logs = system information generated by FortiGate
- Translate IPs to host names for convenience? (Can impact CPU usage and page responsiveness.)

The **Log Settings** page allows you to decide if, where, and how a log is stored.

As previously discussed, you must configure whether to store logs locally on your FortiGate disk, or remotely to an external device, such as FortiAnalyzer.

You must also configure what event logs and local traffic logs to capture. By default, this option is disabled because of the large number of logs they can generate.

Event logs provide all of the system information generated by FortiGate, such as administrator logins, configuration changes made by administrators, user activity, and daily operations of the device—they are not directly caused by traffic passing through firewall policies. The event logs you choose to enable depend on what features you are implementing and what information you need to get from the logs.

The **Resolve Hostnames** feature resolves IP addresses to host names. This requires FortiGate to perform reverse DNS lookups for all IP addresses. If your DNS server is not available, or is slow to reply, it can impact your ability to look through the logs, because the requests will time out.

DO NOT REPRINT

© FORTINET

Log Filtering

- Configure log filter settings to determine which logs are recorded
 - Configure up to four remote syslog or FortiSIEM logging servers:

```
# config log [syslogd | syslogd2 | syslogd3 | syslogd4] filter
```

- Configure up to three FortiAnalyzer or FortiManager devices or one cloud FortiAnalyzer instance:

```
# config log [fortianalyzer | fortianalyzer-cloud | fortianalyzer2 | fortianalyzer3] filter
```

- Filters include:

- Severity <level>
- Forward traffic [enable/disable]
- Local traffic [enable/disable]
- Multicast traffic [enable/disable]
- Sniffer traffic [enable/disable]
- Anomaly [enable/disable]
- VOIP [enable/disable]
- ZTNA-traffic [enable/disable]
- GTP [enable/disable]
- Filter [string]
- Filter type [include | exclude]



© Fortinet Inc. All Rights Reserved.

26

While you use the log settings on the GUI to configure which event logs and local traffic logs to capture, you can set more granular options using the CLI.

You can configure FortiGate to send logs to external servers. You can control which logs are sent to each of these devices separately, using the command `config log syslogd filter` for remote syslog or FortiSIEM, and the command `config log fortianalyzer filter` for FortiAnalyzer or FortiManager devices.

In this way, you can set devices to different logging levels and/or send only certain types of logs to one device and other types (or all logs) to others. For example, you can send all logs at information level and above to `fortianalyzer`, alert level and above to `fortianalyzer2`, and only traffic logs to `fortianalyzer3`.

For example, the following commands configure the log filter for the first syslog server to include only logs related to traffic directly to and from the FortiGate management IP addresses, with a severity level of *critical* or higher:

```
#config log syslogd filter
#(filter) set severity critical
#(filter) set local-traffic enable
```

DO NOT REPRINT

© FORTINET

Enabling Logging on Firewall Policies

- Firewall policy settings decide if a log message caused by traffic passing through a firewall policy is generated or not
- Hardware acceleration affects logging**
 - Traffic offloaded to NP6 and NP6Lite processors does not log traffic statistics.
 - Traffic offloaded to NP7 processors have improved logging of traffic statistics capabilities
 - Can disable hardware acceleration
 - Can enable NP packet logging (degrades NP performance)

Must enable one or more security profiles on your firewall policy to generate a log message for that profile

Policy & Objects > Firewall Policy

Must enable and set which traffic to log. If disabled, you will not receive logs of any kind—even if you have enabled a security profile on your firewall policy.

After you configure all logging settings, you can enable logging on your firewall policies. Only when enabled on a firewall policy can a log message—caused by traffic passing through that firewall policy—generate.

Generally, if you configure FortiGate to inspect traffic, you should also enable logging for that security feature to help you track and debug your traffic flow. Except for violations that you consider to be low in severity, you'll want to know if FortiGate is blocking attacks. Most attacks don't result in a security breach on the first try. A proactive approach, when you notice a persistent attacker whose methods seem to be evolving, can avoid a security breach. To get early warnings like this, enable logging for your security profiles.

To enable logging on traffic passing through a firewall policy, you must do the following:

- Enable the desired security profile(s) on your firewall policy.
- Enable **Log Allowed Traffic** on that firewall policy. This setting is vital. If disabled, you will not receive logs of any kind—even if you have enabled a security profile on your firewall policy. You can choose to log only security events, or log all sessions:
 - Security Events:** If enabled (along with one or more security profiles), security log events appear in the forward traffic log and security log. A forward traffic log generates for packets causing a security event.
 - All Sessions:** If enabled, a forward traffic log generates for every single session. If one or more security profiles are also enabled, security log events appear in the forward traffic log and security log.

DO NOT REPRINT**© FORTINET**

Hiding User Names in Logs

- Some laws require that usernames be anonymized
- Use the following command to hide usernames in traffic and UTM logs, so that the username appears as anonymous

```
# config log setting
  set user-anonymize enable
end
```

```
date=2021-03-16 time=14:45:16 logid=0317013312 type=utm subtype=webfilter
eventtype=ftgd_allow level=notice vd="root" policyid=2 identidx=1
sessionid=31232959 user="anonymous" group="ldap_users" srcip=192.168.1.24
srcport=63355 srcintf="port2" dstip=66.171.121.44 dstport=80 dstintf="port1"
service="http" hostname="www.fortinet.com" profiletype="Webfilter_Profile"
profile="default" status="passthrough" reqtype="direct" url="/" sentbyte=304
rcvdbyte=60135 msg="URL belongs to an allowed category in policy" method=domain
class=0 cat=140 catdesc="custom1"
```

On FortiGate, you can hide usernames in traffic logs and UTM logs, so that the username appears as anonymous. This is useful, because some countries do not permit non-anonymized logging.

To anonymize usernames, use the `set user-anonymize enable` CLI command.

It is assumed that logging is enabled in firewall policies and security profiles, and that identity-based policies are configured on FortiGate.

DO NOT REPRINT
© FORTINET

Viewing and Searching Log Messages—GUI

Log & Report

Forward Traffic

Date/Time % Source Device Destination

Local Traffic 2 minutes ago 10.0.1.20 94.102.51.124

Sniffer Traffic 2 minutes ago 10.0.1.20 139.99.113.97 (homeschoolingpena.com)

System Events 3 minutes ago 10.0.1.20 34.102.136.180 (taxtube.com)

Security Events 3 minutes ago 10.0.1.20 87.247.245.130 (www.oxtown.net)

Log Settings 3 minutes ago 10.0.1.20 35.208.12.102 (jowriter.com)

Threat Weight 3 minutes ago 10.0.1.20 31.170.1.86 (www.drvnlnclusmaykeh.com)

3 minutes ago 10.0.1.20 172.67.25.5 (cpanel.cow.stackit.net)

Set log filters to narrow search

Log location = disk

Application Name Disk Result

Log Details

Details Security

General

Absolute Date/Time 2022/01/04 11:55:52

Time 11:55:52

Duration 1s

Session ID 3524

Virtual Domain root

NAT Translation Source

Source

IP 10.0.1.20

NAT IP 10.200.1.1

Source Port 55362

Country/Region Reserved

Source Interface port3

User

Destination

IP 34.102.136.180

Port 80

Country/Region United States

Destination Interface port1

Application Control

© Fortinet Inc. All Rights Reserved.

29

You can access your logs on the GUI in the **Log & Report** menu.

Select the type of log you want to view, such as **Forward Traffic**. Logs on the GUI appear in a formatted table view. The formatted view is easier to read than the raw view, and it enables you to filter information when viewing log messages. To view the log details, select the log in the table. The log details then appear in the **Log Details** pane on the right side of the window.

If archiving is enabled on security profiles that support it (such as DLP), archived information appears in the **Log Details** pane in the **Archived Data** section. Archived logs are also recorded when using FortiAnalyzer or FortiCloud.

If you configure FortiGate to log to multiple locations, you can change the log display location in this section. In the example shown on this slide, the log location is set to **Disk**. If logging to a syslog, you must view logs on the syslog instead.

To navigate the logs more efficiently, you can set up log filters. The more information you specify in the filter, the easier it is to find the precise log entry. Filters are configurable for each column of log data on the display. Click **Add Filter** to select the filter in the drop-down list that appears. If you see data that you want to filter on in a log that is already in the table, you can right-click that data to select the quick filter option. For example, if you see an antivirus log in the table with a specific botnet name, right-click the botnet name in the table, and a quick filter option opens, allowing you to filter on all logs with that botnet name.

By default, the most common columns are shown and less common columns are hidden. To add columns, right-click any column field and, in the pop-up menu that opens, select the column in the **Available Columns** section.