



**FortiGate IPv6 support
FortiOS 3.0 MR5**



www.fortinet.com

FortiGate IPv6 support Technical Note

11 April 2007

01-30005-0081-20070411

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

IPv6 overview	5
Overview of IPv6 address space	5
Address notation	5
IP addresses	5
Netmasks	6
Address types	6
IPv6 neighbor discovery	7
Transition from IPv4 to IPv6	7
IPv4 addresses in IPv6 format	7
IPv6 tunneling	8
FortiGate IPv6 configuration	9
Configuring IPv6 interfaces	10
Adding an IPv6 address to an interface	10
Creating the prefix list for the interface	11
Configuring IPv6 routing	12
Configuring static routing	12
Configuring IPv6 router advertisements	12
Testing connections with ping6	14
Configuring IPv6 over IPv4 tunneling	14
Creating the IPv6 tunnel	14
Defining the firewall policies	15
Defining routing	15
Configuring IPv6 IPsec VPNs	16
Certificates	16
Phase 1 configuration	16
Phase 2 configuration	17
Firewall policies	17
Routing	17
Configuring IPv6 firewall policies	18

IPv6 overview

IPv6 is version 6 of the Internet Protocol. It can provide billions more unique IP addresses than the previous standard, IPv4.

This technical note describes IPv6 addressing support on all FortiGate units using firmware version 3.0 MR5 or later. This document has two chapters:

- [IPv6 overview](#), this chapter, provides some background information about IPv6 addressing and how networks are making the transition from IPv4 to IPv6 addressing.
- [FortiGate IPv6 configuration](#) provides information about the IPv6 features of FortiGate units and how to configure them.

Overview of IPv6 address space

IPv6 addresses are 128 bits long. IPv4 addresses are only 32 bits long.

IPv6 requires an MTU of at least 1280 bytes. An MTU of 1500 or more is recommended (RFC-2640) to allow for encapsulations such as tunneling.

Address notation

The IPv6 addressing standard is specified in detail in RFC 3513. The following is a quick overview.

IP addresses

IPv6 addresses are normally written as eight groups of 4 hexadecimal digits each. For example,

```
3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234
```

is a valid IPv6 address.

If a 4 digit group is 0000, it may be omitted. For example,

```
3f2e:6a8b:78a3:0000:1725:6a2f:0370:6234
```

is the same IPv6 address as

```
3f2e:6a8b:78a3::1725:6a2f:0370:6234
```

You can use the "::" notation to indicate multiple consecutive omitted zero groups. There must not be more than one use of "::" in an address, as this is ambiguous. Also, you can omit leading zeros in a group. Thus

```
19a4:0478:0000:0000:0000:0000:1a57:ac9e
```

```
19a4:0478:0000:0000:0000::1a57:ac9e
```

```
19a4:478:0:0:0:0:1a57:ac9e
```

```
19a4:478:0::0:1a57:ac9e
```

```
19a4:478::1a57:ac9e
```

are all valid and are the same address.

For IPv4-compatible or IPv4-mapped IPv6 addresses (see [Address types](#)), you can enter the IPv4 portion using either hexadecimal or dotted decimal, but the FortiGate CLI always shows the IPv4 portion in dotted decimal format. For all other IPv6 addresses, the CLI accepts and displays only hexadecimal.

Netmasks

As with IP addresses, hexadecimal notation replaces the dotted decimal notation of IPv4. CIDR notation can also be used. This notation appends a slash ("/") to the IP address, followed by the number of bits in the network portion of the address.

Table 1: IPv6 address notation

IP Address	3ffe:ffff:1011:f101:0210:a4ff:fee3:9566
Netmask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
Network	3ffe:ffff:1011:f101:0000:0000:0000:0000
CIDR IP/Netmask	3ffe:ffff:1011:f101:0210:a4ff:fee3:9566/64

Address types

There are more types of IPv6 addresses than IPv4 addresses. The types are identifiable by their prefix values.

Table 2: Types of IPv6 addresses

Address Type	Prefix/prefix length	Comments
Unspecified	::/128	Equivalent to 0.0.0.0 in IPv4.
Loopback	::1/128	Equivalent to 127.0.0.1 in IPv4.
IPv4-compatible	::/96	Lowest 32 bits can be in IPv6 hexadecimal or IPv4 dotted decimal format.
IPv4-mapped	::FFFF/96	Lowest 32 bits can be in IPv6 hexadecimal or IPv4 dotted decimal format.
Multicast	::FF00/8	
Anycast	all prefixes except those listed above	Multiple servers can have the same address with routing used to balance the traffic load. Unlike IPv4, IPv6 anycast addresses are indistinguishable from other unicast addresses.
Link-local	FE80::/10	Link-Local addresses are used for addressing on a single link for automatic address configuration, neighbor discovery, or when no routers are present. Routers must not forward packets with link-local source or destination addresses.
Site-local	FEC0::/10	Site-local addresses are used for addressing inside of a site without needing a global prefix. Routers must not forward packets with site-local source or destination addresses outside of the site.
Global	all others	

IPv6 neighbor discovery

The IPv6 Neighbor Discovery protocol replaces the combination of IPv4 protocols ARP, ICMPv4 Router Discovery and ICMP Redirect. This provides more efficient address resolution and enables autoconfiguration of network interfaces.

Hosts and routers use neighbor discovery

- to determine and detect changes in the link-layer (MAC) addresses of neighbors on attached links
- to keep track of which neighbors are reachable and which are not
- to determine which address prefixes are on-link
- to determine the next hop for routing packets
- to redirect packets when there is a better first hop to a particular destination

To facilitate neighbor discovery, routers periodically send messages advertising their availability. This communication includes lists of the address prefixes for destinations available on each router's interfaces. RFC 2461 specifies IPv6 Neighbor Discovery in detail.

Transition from IPv4 to IPv6

The Internet is in transition from IPv4 to IPv6 addressing. IPv6 hosts and routers maintain interoperability with the existing IPv4 infrastructure in two ways:

- implementing dual IP layers to support both IPv6 and IPv4
- using IPv6 over IPv4 tunneling to encapsulate IPv6 packets within IPv4 headers to carry them over IPv4 infrastructure

FortiGate units are dual IP layer IPv6/IPv4 nodes and they support IPv6 over IPv4 tunneling.

IPv4 addresses in IPv6 format

There are two ways that IPv4 addresses are represented in IPv6 format. You can distinguish them by the 16 bits that precede the IPv4 portion of the address:

Table 3: IPv6 formats for IPv4 addresses

IPv4-compatible IPv6 address	0000:0000:0000:0000:0000: or ::	0000:	874B:2B34 or 135.75.43.52
IPv4-mapped IPv6 address	0000:0000:0000:0000:0000: or ::	FFFF:	874B:2B34 or 135.75.43.52

IPv4-compatible addresses are used for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv4-mapped addresses are used for nodes that do not support IPv6.

IPv6 tunneling

Networks using IPv6 addressing can be linked through IPv4-addressed infrastructure using several tunneling techniques:

Table 4: Tunneling techniques

IPv6-over-IPv4	Encapsulates IPv6 packets within IPv4 so that they can be carried across IPv4 routing infrastructures.
Configured	The endpoint address is determined by configuration information on the encapsulating node.
Automatic	The IPv4 tunnel endpoint address is determined from the IPv4 address embedded in the IPv4-compatible destination address of the IPv6 packet being tunneled.
IPv4 multicast	IPv4 tunnel endpoint address is determined using Neighbor Discovery. No address configuration is required, but the IPv4 infrastructure must support IPv4 multicast.

FortiGate units support IPv6-over-IPv4 tunneling.

FortiGate IPv6 configuration

This chapter describes how to configure your FortiGate unit's IPv6 functionality. Currently, the FortiGate unit supports IPv6 routing, tunneling, firewall policies and IPsec VPN.

You must use the Command Line Interface (CLI) to configure your FortiGate unit for IPv6 operation. IPv6 configuration is not supported in the web-based manager. This technical note outlines the relevant CLI commands. For detailed information about the CLI, see the *FortiGate CLI Reference Guide*.

This technical note contains the following sections:

- [Configuring IPv6 interfaces](#)
- [Configuring IPv6 routing](#)
- [Configuring IPv6 over IPv4 tunneling](#)
- [Configuring IPv6 IPsec VPNs](#)
- [Configuring IPv6 firewall policies](#)

Configuring IPv6 interfaces

You can assign both an IPv4 and an IPv6 address to any interface on a FortiGate unit. Assigning an IPv6 address to the interface does not affect its IPv4 functionality. The IPv6 address you assign to the interface receives only IPv6-addressed packets. (Note: IPv6 is not supported over PPPoE or modem.)

Adding an IPv6 address to an interface

The following CLI commands are used to create an IPv6 address on an interface and to set administrative access to the interface:

```
config system interface
  edit <interface_name>
    config ipv6
      set ip6-address <if_ipv6mask>
      set ip6-allowaccess <access_types>
    end
  end
end
```

Variable	Description	Default
edit <interface_name>	Edit an existing interface or create a new VLAN interface.	None.
ip6-address <if_ipv6mask>	The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This is available in NAT/Route mode only.	::/0
ip6-allowaccess <access_types>	Enter the types of management access permitted on this IPv6 interface. Valid types are: http https ping snmp ssh telnet. Separate the types with spaces. If you want to add or remove an option from the list, retype the list as required.	Varies for each interface.

The `config ipv6` subcommand also contains keywords for defining the prefix list and configuring router advertisements. See [“Creating the prefix list for the interface”](#) next and [“Configuring IPv6 router advertisements”](#) on page 12.

The following example sets 3f30:0000:0000:0000:0000:0000:2348:9abc as the IPv6 address for the internal interface and enables HTTPS and SSH administrative access:

```
config system interface
  edit internal
    config ipv6
      set ip6-address 3f30::2348:9abc/60
      set ip6-allowaccess https ssh
    end
  end
end
```

Creating the prefix list for the interface

In IPv4-addressed networks the subnet mask alone determines which addresses are available on an interface. IPv6-addressing is more flexible. Routers exchange lists of address prefixes considered to be “on-link”, meaning that they are reachable on the interface. This is part of the IPv6 Neighbor Discovery process.

The following commands configure prefix lists:

```
config system interface
  edit <interface_name>
    config ipv6
      config ip6-prefix-list
        edit <ipv6_prefix>
          set autonomous-flag {enable | disable}
          set onlink-flag {enable | disable}
          set preferred-life-time <seconds>
          set valid-life-time <seconds>
        end
      end
    end
  end
```

Variable	Description	Default
edit <interface_name>	Edit an existing interface or create a new VLAN interface.	None.
edit <ipv6_prefix>	Edit an existing prefix or create a new one.	
autonomous-flag {enable disable}	Set the state of the autonomous flag for the IPv6 prefix.	disable
onlink-flag {enable disable}	Set the state of the on-link flag ("L-bit") in the IPv6 prefix.	disable
preferred-life-time <seconds>	Enter the preferred lifetime, in seconds, for this IPv6 prefix.	604800
valid-life-time <seconds>	Enter the valid lifetime, in seconds, for this IPv6 prefix.	2592000

Example

```
config system interface
  edit internal
    config ipv6
      config ip6-prefix-list
        edit 5f00::/64
          set autonomous-flag enable
          set preferred-life-time 432000
        end
      end
    end
  end
```

For more information on IPv6 routing, see the next section.

Configuring IPv6 routing

You can configure static routes and the router advertisements that the FortiGate unit sends on each interface.

Configuring static routing

FortiGate units support static routing for IPv6-addressed packets. The following command specifies static IPv6 routes:

```
config router static6
  edit <sequence_number>
    set device <interface_name>
    set dst <destination-address_ipv6mask>
    set gateway <gateway-address_ipv6>
  end
```

Keywords and variables	Description	Default
edit <sequence_number>	Enter a sequence number for the route.	No default.
device <interface_name>	The name of the FortiGate interface through which to route traffic.	Null.
dst <destination-address_ipv6mask>	The destination IPv6 address and netmask for this route. You can enter ::/0 to create a new static default route for IPv6 traffic.	::/0
gateway <gateway-address_ipv6>	The IPv6 address of the next-hop router to which traffic is forwarded.	::

Example

```
config router static6
  edit 2
    set dev internal
    set dst 12AB:0:0:CD30::/60
    set gateway 12AB:0:0:CD30:123:4567:89AB:CDEF
  end
```

Configuring IPv6 router advertisements

The FortiGate CLI provides the following commands to configure router advertisements for the interface.

```
config system interface
  edit <interface_name>
    config ipv6
      set ip6-address <if_ipv6mask>
      set ip6-allowaccess <access_types>
      set ip6-default-life <ipv6_life_seconds>
      set ip6-hop-limit <ipv6_hops_limit>
      set ip6-link-mtu <ipv6_mtu>
      set ip6-manage-flag {disable | enable}
      set ip6-max-interval <advert_max_seconds>
      set ip6-min-interval <advert_min_seconds>
      set ip6-other-flag {disable | enable}
      set ip6-reachable-time <reachable_msecs>
      set ip6-retrans-time <retrans_msecs>
      set ip6-send-adv {enable | disable}
```

```

config ip6-prefix-list
...
end
end
end
end

```

Keywords and variables	Description	Default
edit <interface_name>	Edit an existing interface or create a new VLAN interface.	None.
ip6-address ip6-allowaccess	See “Adding an IPv6 address to an interface” on page 10.	
ip6-default-life <ipv6_life_seconds>	Enter the number, in seconds, to add to the Router Lifetime field of router advertisements sent from the interface. The valid range is 0 to 9000.	1800
ip6-hop-limit <ipv6_hops_limit>	Enter the number to be added to the Cur Hop Limit field in the router advertisements sent out this interface. Entering 0 means no hop limit is specified. This is available in NAT/Route mode only.	0
ip6-link-mtu <ipv6_mtu>	Enter the MTU number to add to the router advertisements options field. Entering 0 means that no MTU options are sent.	0
ip6-manage-flag {disable enable}	Enable or disable the managed address configuration flag in router advertisements.	disable
ip6-max-interval <adverts_max_seconds>	Enter the maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800.	600
ip6-min-interval <adverts_min_seconds>	Enter the minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800.	198
ip6-other-flag {disable enable}	Enable or disable the other stateful configuration flag in router advertisements.	disable
ip6-reachable-time <reachable_msecs>	Enter the number to be added to the reachable time field in the router advertisements. The valid range is 0 to 3600. Entering 0 means no reachable time is specified.	0
ip6-retrans-time <retrans_msecs>	Enter the number to be added to the Retrans Timer field in the router advertisements. Entering 0 means that the Retrans Timer is not specified.	0
ip6-send-adv {enable disable}	Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations.	disable
config ip6-prefix-list	See “Creating the prefix list for the interface” on page 11.	

For information about configuring prefix lists, see [“Creating the prefix list for the interface” on page 11.](#)

Testing connections with ping6

The ping command is a much-used tool in networking. FortiGate units provide an IPv6-specific version of the ping command.

```
execute ping6 {<address_ipv6> | <host-name_str>}
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

Configuring IPv6 over IPv4 tunneling

FortiGate units support the transmission of IPv6-addressed traffic over an IPv4-addressed network. This technique is called IPv6 tunneling. You need to

- create the tunnel (a virtual interface)
- create firewall policies
- define at least one route

Creating the IPv6 tunnel

You configure a tunnel using the following FortiGate CLI command:

```
config system ipv6-tunnel
  edit <tunnel_name>
    set destination <tunnel_address>
    set interface <name>
    set ip6 <address_ipv6mask>
    set source <address_ipv4>
  end
```

Variables	Description	Default
edit <tunnel_name>	Enter a name for the IPv6 tunnel.	No default.
destination <tunnel_address>	The destination IPv4 address for this tunnel.	0.0.0.0
interface <name>	The interface used to send and receive traffic for this tunnel.	No default.
ip6 <address_ipv6mask>	The network prefix (IPv6 address and netmask) assigned to the interface to enable IPv6 processing on the interface.	::/0
source <address_ipv4>	The source IPv4 address for this tunnel.	0.0.0.0

Example

The following example creates a tunnel, 6tunnel, that uses port3 to send and receive traffic. 6tunnel is a virtual interface that you use in firewall policies and routes.

```
config system ipv6-tunnel
  edit 6tunnel
    set destination 10.10.10.1
    set interface port3
    set ip6 12AB:0:0:CD30::/60
    set source 192.168.50.1
  end
```

Defining the firewall policies

You need to define firewall policies to permit traffic to flow between the local subnet and the IPv6 tunnel interface. A policy is required for each direction.

```
config firewall policy6
  edit 1
    set srcintf port2
    set dstintf 6tunnel
    set action accept
    ...
  next
  edit 2
    set srcintf 6tunnel
    set dstintf port2
    set action accept
    ...
  next
end
```

For more information about IPv6 firewall policies, see [“Configuring IPv6 firewall policies” on page 18](#).

Defining routing

You need at least one route so that the IPv6 traffic is sent through the tunnel virtual interface. For example, 6tunnel, created in an earlier example, is the route to a particular IPv6 subnet:

```
config router static6
  edit 1
    set dst 1200:2345::3450/64
    set device 6tunnel
  next
end
```

Configuring IPv6 IPsec VPNs

The FortiGate unit supports interface-based IPv6 IPsec, but not policy-based. This section describes only how IPv6 IPsec support differs from IPv4 IPsec support.

FortiOS 3.0 supports IPv6 VPNs, but only in the CLI. The web-based manager does not display the configurations or status of any IPv6 VPN.

Where both the gateways and the protected networks use IPv6 addresses, sometimes called IPv6 over IPv6, you can create either an auto-keyed or manually-keyed VPN. You can combine IPv6 and IPv4 addressing in an auto-keyed VPN in the following ways:

- IPv4 over IPv6 The VPN gateways have IPv6 addresses.
The protected networks have IPv4 addresses. The phase 2 configurations at either end use IPv4 selectors.
- IPv6 over IPv4 The VPN gateways have IPv4 addresses.
The protected networks use IPv6 addresses. The phase 2 configurations at either end use IPv6 selectors.

Compared with IPv4 IPsec VPN functionality, there are some limitations:

- Except for IPv6 over IPv4, remote gateways with Dynamic DNS are not supported. This is because FortiOS 3.0 does not support IPv6 DNS.
- You cannot use RSA certificates in which the common name (cn) is a domain name that resolves to an IPv6 address. This is because FortiOS 3.0 does not support IPv6 DNS.
- DHCP over IPsec is not supported, because FortiOS 3.0 does not support IPv6 DHCP.
- Selectors cannot be firewall address names. Only IP address, address range and subnet are supported.
- Redundant IPv6 tunnels are not supported.

Certificates

On a VPN with IPv6 phase 1 configuration, you can authenticate using VPN certificates in which the common name (cn) is an IPv6 address. The `cn-type` keyword of the `user peer` command has a new option, `ipv6`, to support this.

Phase 1 configuration

You define an IPsec phase 1 configuration as IPv6 by setting `ip-version` to 6. Its default value is 4. Then, the `local-gw` and `remote-gw` keywords are hidden and the corresponding `local-gw6` and `remote-gw6` keywords are available. The values for `local-gw6` and `remote-gw6` must be IPv6 addresses.

To configure IPv6 IPsec VPN phase 1

```
config vpn ipsec phase1-interface
  edit tunnel6
    set ip-version 6
    set remote-gw6 0:123:4567::1234
    set interface port3
    set proposal 3des-md5
  end
```

Phase 2 configuration

An IPv6 IPsec phase 2 configuration has IPv6 address selectors. The `src-addr-type` and `dst-addr-type` options `ip6`, `range6` and `subnet6` require IPv6 addresses, but are otherwise the same as the similarly-named IPv4 options. The `name` option, referring to a firewall address or address group name, applies only to IPv4 configurations.

To configure IPv6 IPsec VPN phase 2

```
config vpn ipsec phase2-interface
edit tunnel6_p2
set src-addr-type subnet6
set dst-addr-type subnet6
set dst-subnet6 1200:2345::3456/64
set interface port3
set proposal 3des-md5
end
```

Firewall policies

To complete the VPN configuration, you need a firewall policy in each direction to permit traffic between the protected network's port and the IPsec interface. You need IPv6 policies unless the VPN is IPv4 over IPv6.

Routing

Appropriate routing is needed for both the IPsec packets and the encapsulated traffic within them. You need a route, which could be the default route, to the remote VPN gateway via the appropriate interface. You also need a route to the remote protected network via the IPsec interface. For example, where the remote network is `fec0:0000:0000:0004::/64` and the IPsec interface is `toB`:

```
config router static6
edit 1
set device port2
set dst 0::/0
next
edit 2
set device toB
set dst fec0:0000:0000:0004::/64
next
end
```

If the VPN is IPv4 over IPv6, the route to the remote protected network is an IPv4 route. If the VPN is IPv6 over IPv4, the route to the remote VPN gateway is an IPv4 route.

Configuring IPv6 firewall policies

The FortiGate unit supports IPv6 firewall policies.

Use the following CLI commands to create an IPv6 firewall policy. For details about other CLI commands, see the *FortiGate CLI Reference*.

To create an IPv6 firewall address:

```
config firewall address6
  edit <address_name>
    set ip6 <ipv6_address_prefix>
  end
```

Keywords and variables	Description	Default
<address_name>	The name of the address.	No default.
ip6 <ipv6_address_prefix>	Enter the IPv6 IP address.	No default.

To create an IPv6 firewall policy:

```
config firewall policy6
  edit <id_integer>
    set action {accept | deny}
    set comments <comment_str>
    set diffserv-forward {enable | disable}
    set diffserv-reverse {enable | disable}
    set diffservcode-forward <outbound_binary>
    set diffservcode-rev <reply_binary>
    set dstaddr <name_str>
    set dstintf <name_str>
    set fsae {enable | disable}
    set fixedport {enable | disable}
    set gbandwidth <bandwidth_integer>
    set groups <name_str>
    set logtraffic {enable | disable}
    set maxbandwidth <bandwidth_integer>
    set nat {enable | disable}
    set priority {high | low | medium}
    set profile <name_str>
    set profile-status {enable | disable}
    set schedule <name_str>
    set service <name_str>
    set srcaddr [all | <name_str>]
    set srcintf <name_str>
    set status {enable | disable}
    set trafficshaping {enable | disable}
  end
```

Keywords and variables	Description	Default
id_integer	The unique ID number of this policy.	No default
action {accept deny}	Enter accept to accept packets that match the firewall policy. Enter deny to deny packets that match the firewall policy.	deny

Keywords and variables	Description	Default
comments <comment_str>	Optionally add a description or other information about the policy. <code>comment_str</code> is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces.	No default.
diffserv-forward {enable disable}	Enable or disable forward (original) Differentiated Services traffic for this policy.	disable
diffserv-reverse {enable disable}	Enable or disable reverse (reply) Differentiated Services traffic for this policy.	disable
diffservcode-forward <outbound_binary>	Set the Differentiated Services Code Point (DSCP) value in the Diffserv field of outbound packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
diffservcode-rev <reply_binary>	Set the Differentiated Services Code Point (DSCP) value in the Diffserv field of reply packets. The value is 6 bits binary. The valid range is 000000-111111.	000000
dstaddr <name_str>	Enter the destination address for the policy. For a NAT policy a virtual IP can be added. <code>name_str</code> is case-sensitive.	null
dstintf <name_str>	Enter the destination interface for the policy. The interface can be a physical interface, a VLAN subinterface or a zone. If the interface or VLAN subinterface has been added to a zone, the interface or VLAN subinterface cannot be used for <code>dstintf</code> .	null
fsae {enable disable}	Enable or disable ActiveDirectory authentication.	disable
fixedport {enable disable}	When the action is set to accept, prevent a NAT policy from translating the source port. Some applications do not function correctly if the source port is changed. If <code>fixedport</code> is entered, also enable IP pools. Not enabling IP pools means a policy with <code>fixedport</code> can only allow one connection at a time for this port or service.	disable
gbandwidth <bandwidth_integer>	When traffic shaping is enabled, guarantee the amount of bandwidth available for traffic controlled by the policy. <code>bandwidth_integer</code> can be 0 to 100000 Kbytes/second.	0
groups <name_str>	When the action is set to accept and authentication is enabled, enter one or more user group names for users that authenticate through this policy. When user groups are created, they are paired with protection profiles. The user group name is case sensitive.	No Default.
logtraffic {enable disable}	Enable or disable recording traffic log messages for this policy.	disable
maxbandwidth <bandwidth_integer>	When traffic shaping is enabled, limit the maximum amount of bandwidth available for traffic controlled by the policy. <code>bandwidth_integer</code> can be 0 to 100000 Kbytes/second. If maximum bandwidth is set to 0 no traffic is allowed by the policy.	100

Keywords and variables	Description	Default
nat {enable disable}	When the action is set to accept, configure the policy for network address translation (NAT). NAT translates the source address and the source port of packets accepted by the policy. When NAT is enabled, <code>ippool</code> and <code>fixedport</code> can also be enabled or disabled.	disable
priority {high low medium}	When traffic shaping is enabled, set the priority for traffic controlled by the policy. The available settings are <code>high</code> for high priority traffic, <code>medium</code> for medium priority traffic, and <code>low</code> for low priority traffic.	high
profile <name_str>	When a protection profile is being used, enter the name of a profile to add the protection profile to the policy. The <code>name_str</code> variable is case-sensitive. This is automatically disabled if a user group with a protection profile has been selected for authentication.	No Default.
profile-status {enable disable}	Enable or disable using a protection profile for the policy. This is automatically disabled if a user group has been selected for authentication.	disable
schedule <name_str>	Enter the name of the one-time or recurring schedule to use for the policy. The <code>name_str</code> variable is case-sensitive.	No default.
service <name_str>	Enter the name of the service to use for the policy. The <code>name_str</code> variable is case-sensitive.	No default.
srcaddr [all <name_str>]	Enter the source address for the policy. The <code>name_str</code> variable is case-sensitive.	null
srcintf <name_str>	Enter the source interface for the policy. The interface can be a physical interface, a VLAN subinterface or a zone. If the interface or VLAN subinterface has been added to a zone, interface or VLAN subinterface cannot be used for <code>srcintf</code> .	null
status {enable disable}	Enable or disable the policy.	enable
trafficshaping {enable disable}	Enable or disable traffic shaping. Also set <code>gbandwidth</code> , <code>maxbandwidth</code> , and <code>priority</code> .	disable

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com