

# A Brief IPv6 Firewall Comparison

---

**Brian Meilak, Miju Systems**

# Firewalls Compared

---

## #1 Fortinet Fortigate

- v4.0MR3 Patch 10, VM  
Release date: 10 September 2012  
[www.fortinet.com/products/fortigate](http://www.fortinet.com/products/fortigate)
- Recommended reading: *FortiOS Handbook v3 for FortiOS 4.0 MR3, Chapter 2 Firewall, Internet Protocol version 6 (IPv6)*

# Firewalls Compared

---

## #2 McAfee Firewall Enterprise

- 8.3.0, VM Release date: 19 September 2012

[www.mcafee.com/us/products/firewall-er](http://www.mcafee.com/us/products/firewall-er)

- Recommended reading: *Product Guide, McAfee Firewall Enterprise 8.3.0, Chapter 21 IPv4 and IPv6 overview*

# What I looked at

---

- Firewall aspects from the viewpoint of an administrator, someone would install and administer these devices on a day-to-day basis.
- Touching on the IPv6 capability
- Administered Firewalls using the appropriate standalone firewall admin client GUI tool
- Comparison relates to VMs, appliances may or may not be different

# Firewall Platforms/OS

---

- Fortigate
  - FortiOS: proprietary OS
  - UTM, DLP, WAN opt
  - Subscription services
- McAfee
  - Linux underneath + Type Enforcement
  - UTM
  - Application firewall, “AppPrism”
  - Subscription services

# 1. Firewall Initial Install

---

- Both Firewalls are dual-stacked and enabled
- Fortigate with initial install:
  - Has no default IPv4/IPv6 addressing
  - Connect via IPv4 to enable IPv6 on GUI via **System->Admin->Settings**, select **IPv6 Support** , or enable via console
- McAfee with initial install:
  - Configure IPv4 at install time
  - IPv6 features enabled by default on GUI

# Fortigate Enable IPv6 on GUI

The screenshot displays the FortiGate VM web interface. The left sidebar shows the navigation menu with 'System' selected and 'Settings' highlighted. The main content area is titled 'Administrators Settings' and contains the following sections:

- Central Management**
  - Status: + Not Managed
  - FortiManager IP/Domain Name:
- Administration Settings**
  - HTTP Port:
  - HTTPS Port:
  - Telnet Port:
  - SSH Port:
  - Idle Timeout:  (1-480 mins)
- Enable Password Policy**
- View Settings**
  - Language:
  - Lines Per Page:  (20 - 1000)
- Display Options on GUI**
  - IPv6
  - Central NAT Table
  - Dynamic Profile
  - Object Tagging and Coloring
  - Load Balance
  - ICAP
  - VoIP
  - Implicit Firewall Policies
  - IPsec Manual Key
  - DNS Database

# Fortigate Interface Addressing

The screenshot shows the FortiGate VM web interface. The top navigation bar includes the FortiGate VM logo, a Help icon, a Logout icon, and the Fortinet logo. The left sidebar shows a navigation menu with categories like System, Network, Config, Admin, Certificates, and Monitor. The 'Network' category is expanded, and 'Interface' is selected. The main content area displays a table of network interfaces.

	Name	IP/Netmask	IPv6 Address	Access	Administrative Status	Link Status	IPv6 Access	Type	Ref.
<input type="checkbox"/>	port1	192.168.178.43 / 255.255.255.0	2001:db8::43:43:43/64	HTTP,HTTPS,PING,SSH	+	+	HTTP,HTTPS,PING,SSH	Physical	<a href="#">0</a>
<input type="checkbox"/>	port2	0.0.0.0 / 0.0.0.0	2001:db8::43/0		+	+	HTTPS,PING,SSH,TELNET	Physical	<a href="#">1</a>
<input type="checkbox"/>	port3	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port4	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port5	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port6	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port7	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port8	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port9	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>
<input type="checkbox"/>	port10	0.0.0.0 / 0.0.0.0	::/0		+	+		Physical	<a href="#">0</a>



# Fortigate Interface Addressing

FortiGate VM Help Lo

**System** Edit Interface

- Dashboard
  - Status
- Network
  - Interface**
  - DNS
  - DHCP Server
  - Explicit Proxy
- Config
- Admin
- Certificates
- Monitor

Name: port1 (00:0C:29:DE:D0:B8)  
Alias:   
Link Status: Up

Addressing mode:  Manual  DHCP  PPPoE  
IP/Netmask:   
IPv6 Address:

Dedicate this interface to FortiAP connection  
 Enable one-arm sniffer  
 Enable Explicit Web Proxy  
 Override Default MTU Value  (bytes)

Administrative Access:  HTTPS  PING  HTTP  FMG-Access  
 SSH  SNMP  TELNET

IPv6 Administrative Access:  HTTPS  PING  HTTP  FMG-Access  
 SSH  SNMP  TELNET

Weight:   
Spillover Threshold:  kbit/s

Secondary IP Address

Comments:  0/63

Administrative Status:  Up  Down

Router OK Cancel Apply

# McAfee Interface Addressing

The screenshot shows the McAfee Firewall Enterprise Admin Console. The left sidebar contains a tree view with categories like Firewalls, Network, and Maintenance. The main window displays the 'Interface Configuration' for 'NIC and NIC Group Configuration'. A table lists three interfaces: 'em2', 'external\_network', and 'internal\_network'. The 'internal\_network' interface is selected and highlighted in blue. Below the table, a scrollable area provides 'Additional interface information' for the selected interface.

Name	NIC Or NIC Group	Enabled	Zone	IP addresses
em2	em2			
external_network	em0	✓	external	192.168.1.83, 2001:db8::83
internal_network	em1	✓	internal	192.168.178.83, 2001:db8:178::83

Additional interface information:  
Name: internal\_network  
Interface Type: Standard  
NIC or NIC Group: em1  
Enabled: Yes  
Zone: internal  
IP addresses: 192.168.178.83, 2001:db8:178::83

• Click to edit Master text styles

– Second level

• Third level

– Fourth level

» Fifth level

# McAfee Interface Addressing

Interface Configuration: Interface Properties

Interface name: external\_network  Enable interface

Description: Default external network interface  Enable SPAN

NIC or NIC Group

em0

VLAN id: 2 (1 - 4094)

MTU Size (Bytes)

Standard (1500)

Jumbo (9000)

Custom (1280 - 9000)

Address Configuration

Zone: external

Enable IPv6 on this interface

IPv6 stateless auto address configuration

Static  Host mode  Router mode

Obtain an IPv4 address automatically via DHCP

IPv4 addresses:

Type	Address/Mask
primary	192.168.1.83/24

IPv6 addresses:

Type	Address/Mask
primary	2001:db8::83/64

Quality of Service Profile

<None>

QoS profiles only limit the bandwidth of traffic leaving an interface. QoS profiles are not supported on VLANs.

Interface id: 020c29ffe6e9e82

The interface id only applies to interfaces where IPv6 is enabled.

OK Cancel Help

# Modifying IPv6 Specific Settings

---

- Fortigate
  - Settings via CLI, refer *FortiOS CLI Reference FortiOS 4.0 MR3*
- McAfee
  - router advertisement daemon (rtadvd)  
/etc/rtadvd.conf
  - sysctl, used to get or set kernel state values  
/etc/sysctl.conf

# McAfee Network Defense Settings

The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The left-hand navigation pane shows a tree structure with 'Network Defenses' selected. The main content area is titled 'Server: mfe830.test.com Area: Network Defenses' and features a 'Restore Defaults' button. A tabbed interface at the top includes 'TCP', 'IP', 'UDP', 'ICMP', 'ARP', 'IPsec', and 'IPv6', with 'IPv6' currently active. An information icon and text state: 'Select the attacks and protocol compliance issues to audit. The McAfee Firewall Enterprise always defends against all attacks and compliance issues regardless of the audits you select.'

**IP Audits**

Audit the selected IPv6 attacks:

- address scope conflict
- header too small
- hop-by-hop header malformed
- hop-by-hop jumbo option malformed
- invalid address
- invalid version
- link layer broadcast
- loopback address spoofed
- malformed option
- netprobe
- option header length incorrect
- too many headers
- unknown hop-by-hop option

Audit the selected IPv6 compliance issues:

- Audit all IPv6 compliance issues
- Audit severe and moderate IPv6 compliance issues
- Audit severe IPv6 compliance issues
- Do not audit any IPv6 compliance issues

Select All    Deselect All

**IP Audit Frequency**

Limit auditing (recommended)

Audit the first  occurrence(s) every  seconds.

Always audit

Ticket: .....

## 2. Firewall Administration Methods

---

- Fortigate IPv4/IPv6:
  - HTTP/S (GUI), SNMP, SSH, Telnet, FortiManager
- McAfee IPv4 only:
  - Windows Admin Console (GUI), SSH, Telnet, Control Center

# Fortigate First Look

The screenshot displays the FortiGate VM web interface. The top navigation bar includes 'FortiGate VM', 'Help', 'Logout', and the Fortinet logo. A left sidebar contains a 'System' menu with options like Dashboard, Status, Network, Config, Admin, Certificates, and Monitor. Below this is a 'Router' section with various configuration options.

The main content area is divided into several sections:

- System Information:** A table showing details such as Host Name (Fortigate-VM), Serial Number (FGVMEV000000000), Operation Mode (NAT), HA Status (Standalone), System Time (Mon Oct 8 12:59:08 2012), Firmware Version (v4.0.build0639.120906), System Configuration (Last Backup: N/A), Current Administrator (admin), Uptime (0 day(s) 0 hour(s) 1 min(s)), and Virtual Domain (Disabled).
- License Information:** A table showing the VM License status (Valid), CPUs Detected (1/1), Evaluation License Expires (Sun Oct 14 15:39:40 2012), Support Contract (Unreachable), and FortiGuard Services (AntiVirus, IPS, Vulnerability Scan, Web Filtering, Email Filtering) all marked as Unreachable or Not Registered.
- Traffic History:** A line graph showing traffic volume in bits per second (bit/s) over a 1-hour period for interface port2. The y-axis ranges from 1500 to 4000 bit/s.
- System Resources:** Two gauges showing CPU Usage at 0% and Memory Usage at 13%.
- Top Sessions:** A horizontal bar chart showing the top sessions by source address as of 2012-10-08 12:59:08. The top session is from 192.168.178.54 with 9 sessions.
- Unit Operation:** A diagram showing the FortiGate VM connected to FortiAnalyzer and FortiManager, with FortiClient software installed on a laptop.
- Alert Message Console:** A log of recent alerts, including '2012-10-08 12:59:05 License status changed to VALID' and '2012-10-08 12:58:06 System restart'.

# McAfee First Look

The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The main window title is "McAfee Firewall Enterprise Admin Console". The server information is "Server: mfe830.test.com Area: mfe830.test.com Dashboard". The interface is divided into several sections:

- Left Navigation Panel:** Shows a tree view with "Firewalls" expanded, containing "mfe821p05.test.com" and "mfe830.test.com Dashboard". Under the dashboard, there are icons for "Monitor", "Policy", "Network", and "Maintenance".
- Top Right:** Includes "Maximize Usage Report Tabs", "Refresh Rate: 5 Minutes", and a "Disconnect" button.
- System Status (mfe830.test.com - 8.3.0 - Standalone Appliance):**
  - Licensing: Expires in 22 days
  - Interfaces: 2 of 3 enabled
  - Admins logged in: 2 administrators
  - Application sessions: 9
  - VPN Definitions: 0 (0 idle)
  - Blackholed IPs: 0
  - Uptime: 04:03:28
  - Global Threat: Not in use
- Messages from McAfee:** A message box stating "No messages are available".
- System Resources:** Displays usage bars for:
  - Virtual partition: 47% (1.4 of 3.0 GB used)
  - User partition: 29% (0.3 of 1.0 GB used)
  - Memory usage: 18%
  - CPU usage: 1%
- Download updates:** A table listing updates:

Name	Version	Last checked
A/V signatures	6854	10/04/12 10:03 PM
Application signatures	3.162	10/04/12 10:01 PM
Geo-Location	201210030520.232	10/04/12 10:02 PM
IPS signatures	201210031457.5111	10/04/12 10:02 PM
Messages from McAfee	144	10/06/12 11:31 PM

A "Perform update(s)" button is located below the table.
- Applications Audit:** A tabbed interface with "Applications" selected. It shows filters for "Threats", "Policy", "Geo-Location", "Users", "GTI", and "NIA". The display settings are "15 most frequently-audited Network-Applications over the past day". The audit data is shown in a table:

Name	Count	Bytes transferred	Risk
Admin Console	4	417.04 KB	LOW
SSH Server	1	0 bytes	LOW

"Export" and "View Audit..." buttons are at the bottom right of the table.



# 3. Firewall IPv6 Objects

---

Object Type	Fortigate	McAfee
Address	IPv6 Address	IP address
IP Range		
Subnet	IPv6 Address	Subnet
IP Pools / Netmap(NAT)		Netmap
FQDN / Domain	FQDN	Domain
Host	N/A	Host
Geo-Location		
Group	Group (IPv6 only)	Netgroup (mixed)
Wildcard		N/A

# Fortigate Adding Objects By GUI

The screenshot displays the FortiGate VM web interface. The top navigation bar includes the 'FortiGate VM' logo, a 'Help' button, a 'Logout' button, and the 'FORTINET' logo. On the left, a sidebar menu shows 'System', 'Router', 'Policy', and 'Firewall Objects'. Under 'Firewall Objects', the 'Address' category is expanded, showing sub-items 'Address' and 'Group'. The main content area features a table of existing objects and a 'Create New' dropdown menu. The dropdown menu is open, showing options: 'Address/FQDN', 'IPv6 Address', and 'Address Group'. The table below has columns for Name, Address/FQDN, Interface, Type, Tags, and Ref.

		Name	Address/FQDN	Interface	Type	Tags	Ref.
<input type="checkbox"/>			0.0.0.0/0.0.0.0	Any	Subnet		0
<input type="checkbox"/>		SSLVPN_TUNNEL_ADDR1	10.212.134.[200-210]	Any	IP Range		2
<input type="checkbox"/>		all	::/0		IPV6		0

# Fortigate Adding Objects By GUI

The screenshot displays the FortiGate VM web interface. The top navigation bar includes the 'FortiGate VM' logo, a 'Help' icon, a 'Logout' icon, and the 'FORTINET' logo. The left sidebar shows a tree view of configuration categories: System, Router, Policy, Firewall Objects, Service, Schedule, Traffic Shaper, Virtual IP, Load Balance, and Monitor. The 'Firewall Objects' category is expanded, and the 'Address' sub-category is selected. The main content area is titled 'New Address' and contains the following fields:

- Address Name:
- Color:  [Change]
- IPv6 Address:
- Tags: Applied tags (empty), Add tags  +

At the bottom of the form are 'OK' and 'Cancel' buttons. A mouse cursor is positioned over the 'OK' button.

# Fortigate Adding Objects By GUI

---

The screenshot displays the FortiGate VM web interface. The top navigation bar includes the 'FortiGate VM' logo, 'Help', 'Logout', and the 'FORTINET' brand name. The left sidebar is titled 'System' and contains a tree view of configuration categories: Router, Policy, Firewall Objects, Address, Group, Service, Schedule, Traffic Shaper, Virtual IP, Load Balance, and Monitor. The 'Firewall Objects' category is expanded, and the 'Address' sub-category is selected. The main content area is titled 'New Address' and contains the following configuration fields:

- Address Name:** subnetA\_gui
- Color:** [Change]
- IPv6 Address:** 2001:db8:1000:2000::56
- Tags:**
  - Applied tags: (empty)
  - Add tags: (empty) +

At the bottom of the configuration area, there are two buttons: 'OK' and 'Cancel'. A mouse cursor is positioned over the 'OK' button.

# Fortigate Adding Objects By CLI

---

```
Fortigate-UM # config firewall address6
Fortigate-UM (address6) # edit testA_cmd
new entry 'testA_cmd' added
Fortigate-UM (testA_cmd) # set ip6 2001:db8::a:b:c:d
Fortigate-UM (testA_cmd) # next
Fortigate-UM (address6) # edit subnetA_cmd
new entry 'subnetA_cmd' added
Fortigate-UM (subnetA_cmd) # set ip6 2001:db8:1000:2000::/56
Fortigate-UM (subnetA_cmd) # end
Fortigate-UM #
```

# Fortigate Adding Objects By CLI

---

```
Fortigate-UM #
Fortigate-UM # show firewall address6
config firewall address6
  edit "all"
  next
  edit "testA_gui"
    set ip6 2001:db8::a:b:c:d/128
  next
  edit "subnetA_gui"
    set ip6 2001:db8:1000:2000::/56
  next
  edit "testA_cmd"
    set ip6 2001:db8::a:b:c:d/128
  next
  edit "subnetA_cmd"
    set ip6 2001:db8:1000:2000::/56
  next
end
Fortigate-UM # _
```

# Fortigate Objects

FortiGate VM

Help Logout FORTINET

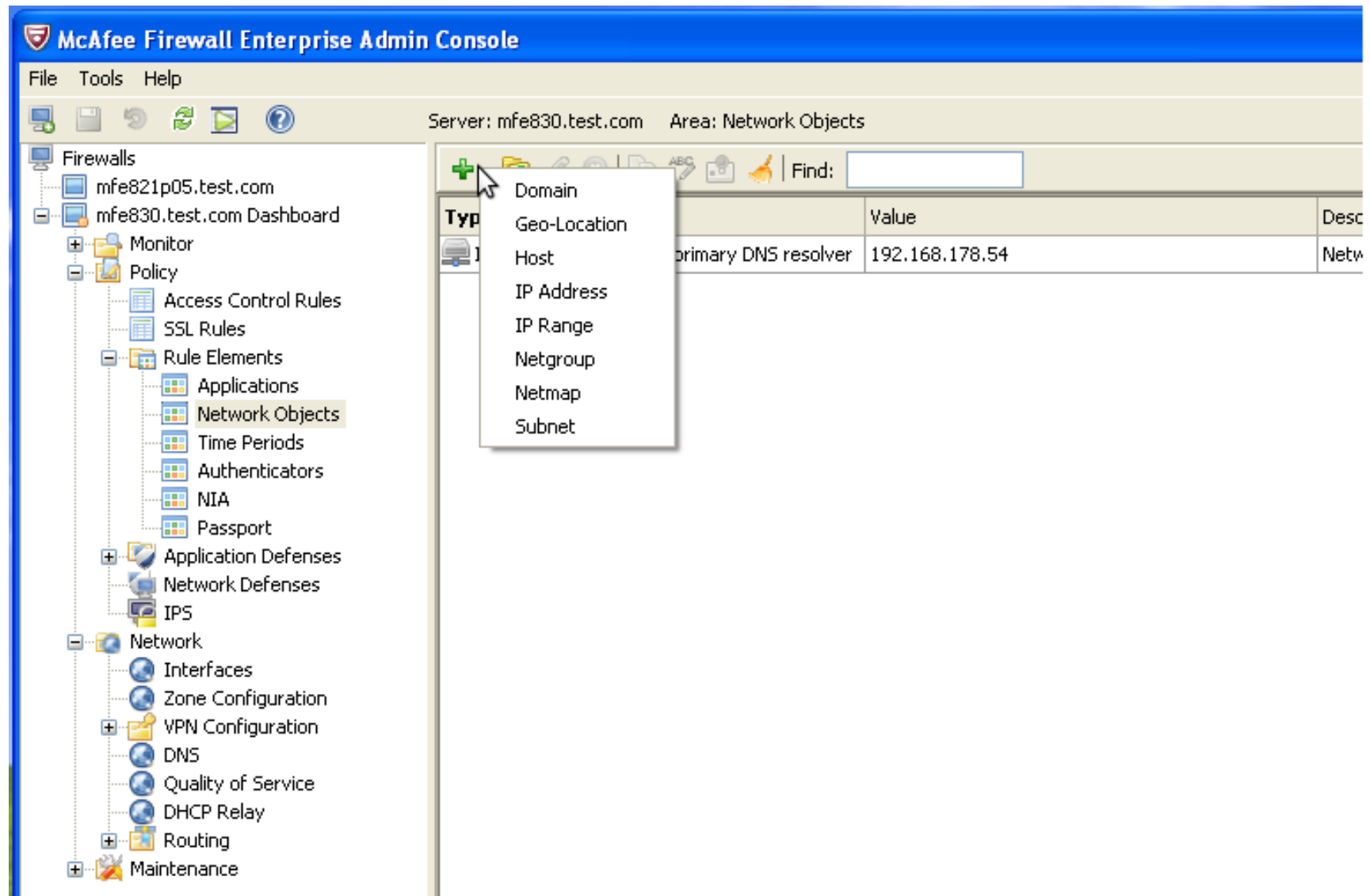
System  
Router  
Policy  
**Firewall Objects**

- Address
  - Address**
  - Group
- Service
- Schedule
- Traffic Shaper
- Virtual IP
- Load Balance
- Monitor

Create New Edit Delete

<input type="checkbox"/>	Name	Address/FQDN	Interface	Type	Tags	Ref.
<input type="checkbox"/>	all	0.0.0.0/0.0.0.0	Any	Subnet		0
<input type="checkbox"/>	SSLVPN_TUNNEL_ADDR1	10.212.134.[200-210]	Any	IP Range		2
<input type="checkbox"/>	all	:::0		IPV6		0
<input type="checkbox"/>	subnetA_cmd	2001:db8:1000:2000::/56		IPV6		0
<input type="checkbox"/>	subnetA_gui	2001:db8:1000:2000::/56		IPV6		0
<input type="checkbox"/>	testA_cmd	2001:db8::a:b:c:d/128		IPV6		0
<input type="checkbox"/>	testA_gui	2001:db8::a:b:c:d/128		IPV6		0

# Adding McAfee Objects by GUI



The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The title bar reads "McAfee Firewall Enterprise Admin Console". Below the title bar is a menu bar with "File", "Tools", and "Help". The status bar shows "Server: mfe830.test.com" and "Area: Network Objects".

The left sidebar shows a tree view of the console's structure. Under "Firewalls", there are two servers: "mfe821p05.test.com" and "mfe830.test.com". Under "mfe830.test.com", there is a "Dashboard" and a "Policy" folder. The "Policy" folder is expanded, showing "Access Control Rules", "SSL Rules", "Rule Elements", "Applications", "Network Objects" (highlighted), "Time Periods", "Authenticators", "NIA", and "Passport". Other folders include "Application Defenses", "Network Defenses", "IPS", "Network", "VPN Configuration", "DNS", "Quality of Service", "DHCP Relay", "Routing", and "Maintenance".

The main pane shows a "Network Objects" table. A context menu is open over the table, listing the following object types: Domain, Geo-Location, Host, IP Address, IP Range, Netgroup, Netmap, and Subnet. The table has columns for "Type", "Value", and "Desc". One row is visible with "Host" as the type, "primary DNS resolver" as the value, and "192.168.178.54" as the description.

Type	Value	Desc
Host	primary DNS resolver	192.168.178.54



# McAfee Adding Objects By GUI

The screenshot displays the McAfee Firewall Enterprise Admin Console. The main window title is "McAfee Firewall Enterprise Admin Console". The interface includes a menu bar (File, Tools, Help) and a toolbar with various icons. The status bar shows "Server: mfe830.test.com" and "Area: Network Objects".

The left-hand navigation pane shows a tree structure under "Firewalls". The selected path is "mfe830.test.com Dashboard" > "Policy" > "Network Objects".

The main content area displays a table of network objects:

Type	Name	Value	Desc
IP Address	internal primary DNS resolver	192.168.178.54	Netw

A modal dialog box titled "Network Objects: IP Address" is open in the foreground. It contains the following fields:

- Name: testA\_gui
- Description: (empty)
- IP Address: 2001:db8::a:b:c:d

At the bottom of the dialog, there are three buttons: "Add", "Close", and "Help". A mouse cursor is pointing at the "Add" button.

# McAfee Adding Objects By GUI

The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The main window shows the 'Network Objects' configuration area for the server 'mfe830.test.com'. A table lists existing objects:

Type	Name	Value	Description
IP Address	internal primary DNS resolver	192.168.178.54	Netw...
IP Address	testA_gui	2001:db8::a:b:c:d	

A dialog box titled 'Network Objects: Subnet' is open, showing the configuration for a new subnet object:

- Name: subnetA\_gui
- Description: (empty field)
- Subnet: 2001:db8:1000:2000:: (with a dropdown menu set to 56)

Buttons at the bottom of the dialog include 'Add', 'Close', and 'Help'.

# McAfee Adding Objects By CLI

---

```
mMcAfee:Admn {11} % cf ipaddr add name=testA_cmd
ipaddr=2001:db8::a:b:c:d
mMcAfee:Admn {12} % cf subnet add name=subnetA_cmd
bits=56 subnet=2001:db8:1000:2000::
mMcAfee:Admn {13} % cf ipaddr query
ipaddr add name=testA_gui ipaddr=2001:db8::a:b:c:d
description="" \
    last_changed_by='admin on Thu Oct 4 22:13:21 2012'
ipaddr add name=testA_cmd
ipaddr=2001:0db8:0000:0000:000a:000b:000c:000d \
    description="" last_changed_by='admin on Thu Oct 4
22:31:06 2012'
ipaddr add name='internal primary DNS resolver'
ipaddr=192.168.178.54 \
    description='Network object for internal zone primary DNS
resolver' \
    last_changed_by='system on Sat Sep 29 05:51:58 2012'
mMcAfee:Admn {14} % cf subnet query
subnet add name=subnetA_cmd bits=56 \
```

# McAfee Objects

The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The title bar reads "McAfee Firewall Enterprise Admin Console". The menu bar includes "File", "Tools", and "Help". The status bar shows "Server: mfe830.test.com" and "Area: Network Objects".

The left-hand navigation pane shows a tree structure under "Firewalls". The "mfe830.test.com" node is expanded to show a "Dashboard" and a "Policy" folder. The "Policy" folder is further expanded to show "Access Control Rules", "SSL Rules", "Rule Elements", "Applications", "Network Objects" (which is highlighted in blue), "Time Periods", "Authenticators", "NIA", and "Passport". Other folders include "Application Defenses", "Network Defenses", "IPS", "Network", "Interfaces", "Zone Configuration", "VPN Configuration", "DNS", "Quality of Service", "DHCP Relay", "Routing", and "Maintenance".

The main content area displays a table of Network Objects. The table has four columns: "Type", "Name", "Value", and "Desc". The data is as follows:

Type	Name	Value	Desc
IP Address	internal primary DNS resolver	192.168.178.54	Netw
IP Address	testA_cmd	2001:0db8:0000:0000:000a:000b:000c:000d	
IP Address	testA_gui	2001:db8::a:b:c:d	
Subnet	subnetA_cmd	2001:0db8:1000:2000:0000:0000:0000/56	
Subnet	subnetA_gui	2001:db8:1000:2000::/56	

# 4. Applications vs Services

---

- Fortigate has *Services*
  - TCP/UDP/SCTP
  - Icmp
  - Icmp6
  - IP
- McAfee has *Applications*
  - UDP/TCP
  - HTTP
  - Other ( predefined application is a parent)

# Fortigate Services

FortiGate VM

System

Router

Policy

Firewall Objects

- Address
  - Address
  - Group
- Service
  - Predefined
  - Custom
  - Group
  - Web Proxy Service
  - Web Proxy Service Group
- Schedule
- Traffic Shaper
- Virtual IP
- Load Balance
- Monitor

Name	Detail
AFS3	TCP/7000-7009 UDP/7000-7009
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
CVSPSERVER	TCP/2401 UDP/2401
DCE-RPC	TCP/135 UDP/135
DHCP	UDP/67-68
DHCP6	UDP/546,547
DNS	TCP/53 UDP/53
ESP	IP/50
FINGER	TCP/79
FTP	TCP/21
FTP_GET	TCP/21
FTP_PUT	TCP/21
GOPHER	TCP/70
GRE	IP/47
H323	TCP/1720,1503 UDP/1719
HTTP	TCP/80
HTTPS	TCP/443
ICMP_ANY	ICMP/ANY
IKE	UDP/500,4500
IMAP	TCP/143
IMAPS	TCP/993
INFO_ADDRESS	ICMP/17
INFO_REQUEST	ICMP/15
IRC	TCP/6660-6669

# Fortigate Services

FortiGate VM

System

Router

Policy

**Firewall Objects**

- Address
  - Address
  - Group
- Service
  - Predefined
  - Custom**
  - Group
  - Web Proxy Service
  - Web Proxy Service Group
- Schedule
- Traffic Shaper
- Virtual IP
- Load Balance
- Monitor

Name: Custom-SSSH

Color: [Change]

Protocol Type: TCP/UDP/SCTP

Protocol	Source Port		Destination Port	
	Low	High	Low	High
TCP	1	65535	22	22
TCP	1	65535		

Add

OK Cancel

# McAfee Applications

McAfee Firewall Enterprise Admin Console

Server: mfe830.test.com Area: Applications

Manage: Applications

Filter by risk: LOW MEDIUM HIGH

Filter by categories: To filter applications by category, click on one or more categories from the list below.

- Anonymizers/Proxies
- Authentication Services
- Business Web Applications
- Collaboration/Content Management
- Commercial Monitoring
- Database
- Directory Services
- ERP/CRM
- Email
- Email Harvesters
- Embedded Web Applications
- Feed Readers
- File Sharing
- Gaming
- IT Utilities
- Infrastructure Services
- Instant Messaging
- Mobile Software
- Offline Crawlers
- Peer to Peer (P2P)
- Photo/Video Sharing
- Remote Administration
- Remote Desktop/Terminal Services
- Search/Indexing Engine Spiders and Crawlers
- Social Networking
- Software/System Updates
- Storage
- Streaming Media

1448 Matching Application(s)

Risk	Name	Filtered Categories	Other Categories
HIGH	100bao		Peer to Peer (P2P)
LOW	123spider		Search/Indexing Engine Spiders and Crawlers
LOW	126 Mail		Web Mail
LOW	1fichier		Storage
LOW	1und1 Mail		Web Mail
LOW	2Bone		Offline Crawlers
HIGH	2channel		Social Networking
LOW	2DPlay		Gaming
HIGH	4FileHosting		File Sharing
LOW	4RemoteSupport		Remote Administration
HIGH	4shared		File Sharing
HIGH	51.com		Gaming, Social Networking, Storage, Streaming ...
LOW	9cast.net		Streaming Media
HIGH	<Any>		Infrastructure Services

Name: 100bao Risk: HIGH

Application discovery (last 180 days): No stats available at this time.

Categories: Peer to Peer (P2P)

Associated rules:

Action	Name
--------	------

Description: **100bao**: A peer-to-peer file-sharing application  
Ports: TCP/80,443,1234 SSL/443  
[McAfee](#) [Audit](#) [Google](#) [Bing](#)

Ticket:



# McAfee Applications

McAfee Firewall Enterprise Admin Console

Server: mfe830.test.com Area: Applications

Manage: Applications

Filter by risk: LOW MEDIUM HIGH

Filter by categories: To filter applications by category, click on one or more categories from the list below.

1448 Matching Application(s)

Risk	Name	Filtered Categories	Other Categories
HIGH	Filemail.com		File Sharing
LOW	Gawab		Web Mail
HIGH	Gmail		Web Mail
LOW	GMX Mail		Web Mail

Applications: View Application

Name: Gmail Risk: HIGH

Application discovery (last 180 days): No stats available at this time.

Categories: Web Mail

Associated rules:

Action	Name
--------	------

Description:

**Gmail:** Web based mail provided by Google Inc.

Ports: TCP/80 SSL/443

[McAfee](#) [Source](#) [Audit](#) [Google](#) [Bing](#)

provided by Google Inc.

[Google](#) [Bing](#)

Close Help

# McAfee Applications

McAfee Firewall Enterprise Admin Console

Server: mfe830.test.com Area: Applications

Manage: Applications

Filter by risk: LOW MEDIUM HIGH

Filter by categories: To filter applications by category, click on one or more categories from the list below.

1448 Matching Application(s) Search: telnet

Risk	Name	Filtered Categories	Other Categories
HIGH	Telnet		Remote Administration
LOW	Telnet Server		

**Applications: New Application**

Name: Custom-SSH-IPv6

Description:

Parent application:

- TCP/UDP
- HTTP
- Other ...

TCP ports: 22

SSL ports:

UDP ports:

A custom application pairs the signature of a parent application with a new set of ports.

OK Cancel Help

Risk: HIGH

Remote Desktop/Terminal Services

Search/Indexing Engine Spiders and Craw

Social Networking

Software/System Updates

Storage

Streaming Media

Toolbars/PC Utilities

Tunnels

Voice over IP (VoIP)

Web Browsing

Web Conferencing

Web Mail

Application discovery (last 100 days): No stats available at this time.

Associated rules:

Action	Name
--------	------

Description: **Telnet (teletype network):** A network protocol for remote administration

Ports: TCP/23

[McAfee](#) [Source](#) [Audit](#) [Google](#) [Bing](#)

Ticket:

# McAfee Applications

Rules: Rule Properties

Overview Interactions

Name: TestIPv6 rule  Enable rule Action: Deny

Browse: Applications

Applications: SSH

Source: Endpoints <Any V6>

Destination: Endpoints <Any V6>

Capabilities:

Default ports: TCP/22

Application defense group: <Default group>

Zone: internal

Zone: external

GTI Host Reputation: None

Advanced

Always active NAT: <None> Redirect: <None>

Preserve source port Redirect port: 0

Audit: Verbose Authenticator: <None/Passport>

IPS Signatures: <None>

IPS Responses: <None>

Describe your rule here

Last modified by admin on 10/12/12 08:57:48 PM EST

OK Cancel Help

**Error**

Error encountered while modifying rule data: rule:TestIPv6 rule: The combination of source, dest, nat, redir and application:SSH will not pass traffic: The application must support IPv6.

OK

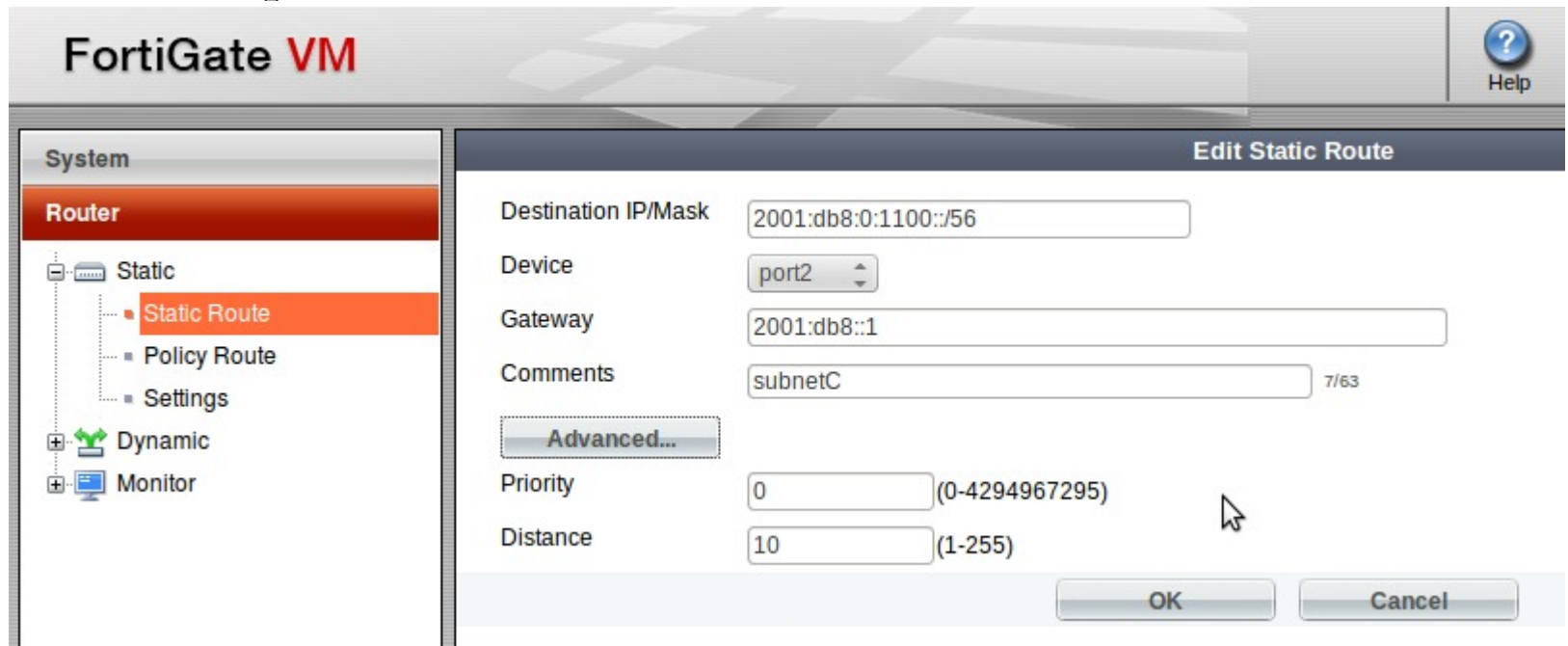
Name	Categories
<input type="checkbox"/> Custom-SSH-IPv6	Infrastructure Servi
<input checked="" type="checkbox"/> SSH	Remote Administrati
<input type="checkbox"/> SSH Server	

# 5. Routing

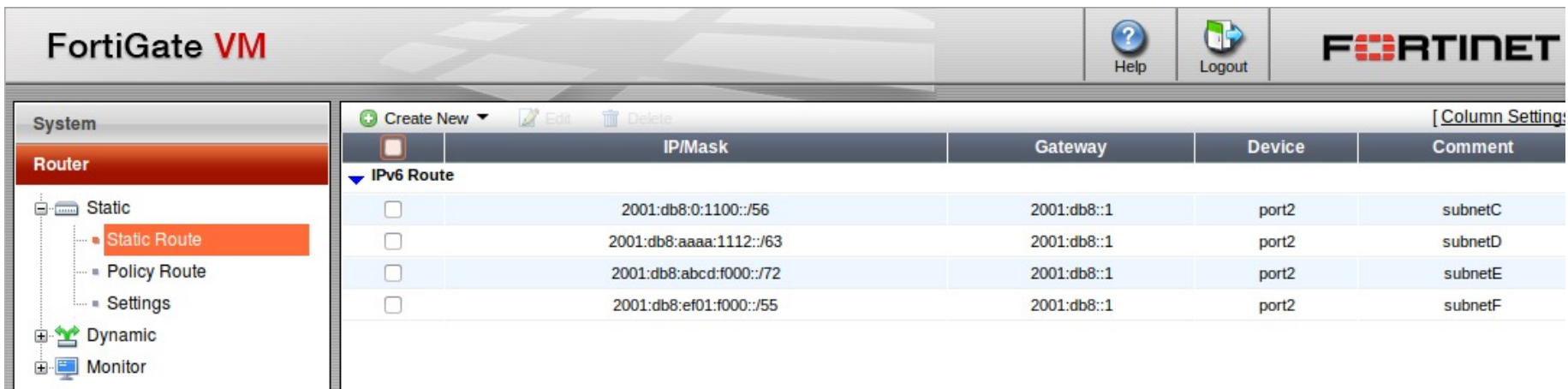
---

- Fortigate
  - Static, Dynamic: RIPng, BGP4+, OSPFv4
  - IPv6 dynamic routing must be configured using CLI
- McAfee
  - Static, Dynamic: BGP4+, OSPFv4
  - Configured using CLI/GUI. GUI invokes a file editor
  - Uses Quagga 0.99.21 for all route management  
[www.quagga.net](http://www.quagga.net) , FW:/secureos/etc/quagga

# Fortigate Add Static Routes By GUI



# Fortigate Add Static Routes By CLI



FortiGate VM

Help Logout FORTINET

System

Router

- Static
  - Static Route
  - Policy Route
  - Settings
- Dynamic
- Monitor

Create New Edit Delete [Column Setting]

	IP/Mask	Gateway	Device	Comment
<input type="checkbox"/>	2001:db8:0:1100::/56	2001:db8::1	port2	subnetC
<input type="checkbox"/>	2001:db8:aaaa:1112::/63	2001:db8::1	port2	subnetD
<input type="checkbox"/>	2001:db8:abcd:f000::/72	2001:db8::1	port2	subnetE
<input type="checkbox"/>	2001:db8:ef01:f000::/55	2001:db8::1	port2	subnetF

```
Fortigate-UM #
Fortigate-UM # config router static6

Fortigate-UM (static6) # edit 5
new entry '5' added

Fortigate-UM (5) # set comment "subnetG"

Fortigate-UM (5) # set device "port2"

Fortigate-UM (5) # set dst 2001:db8:1234:5678::/83

Fortigate-UM (5) # set gateway 2001:db8::1

Fortigate-UM (5) # next

Fortigate-UM (static6) # end

Fortigate-UM # _
```

# McAfee Add Static Routes By GUI

McAfee Firewall Enterprise Admin Console

Server: mfe830.test.com Area: Static Routing

Firewalls

- mfe821p05.test.com
- mfe830.test.com Dashboard
  - Monitor
  - Policy
    - Access Control Rules
    - SSL Rules
    - Rule Elements
      - Applications
      - Network Objects
      - Time Periods
      - Authenticators
      - NIA
      - Passport
    - Application Defenses
    - Network Defenses
    - IPS
  - Network
    - Interfaces
    - Zone Configuration
  - VPN Configuration
  - DNS
  - Quality of Service
  - DHCP Relay
  - Routing
    - Static Routing
    - Dynamic Routing
  - Maintenance

Route Type	Destination	Prefix	Gateway	Distance	Description
Primary Default	default		192.168.1.1		
Alternate Default	backup		192.168.178.1		
IPv6 Default	v6_default				

Static Routes: Host/Network Route Properties

Route type:  Host  Network

Description:

Destination:  Prefix:

Gateway:  Distance:

OK Cancel Help

# McAfee Add Static Routes By GUI

The screenshot displays the McAfee Firewall Enterprise Admin Console interface. The main window is titled "McAfee Firewall Enterprise Admin Console" and shows the "Static Routing" configuration area for the server "mfe830.test.com". The left sidebar contains a tree view of configuration objects, with "Static Routing" selected under the "Routing" category.

The main content area shows a table of static routes:

Route Type	Destination	Prefix	Gateway	Distance	Description
Primary Default	default		192.168.1.1		
Alternate Default	backup		192.168.178.1		
IPv6 Default	v6_default				
Network	2001:db8:0:1100::	56	2001:db8::1	1	subnetC
Network	2001:db8:aaaa:1112::	63	2001:db8::1	1	subnetD

An "Error" dialog box is overlaid on the configuration window, displaying the following message:

**Error**  
Error encountered while trying to add a static route: mask 72 is a non-contiguous subnet mask

The configuration window shows the following fields:

- Route type:  Host  Network
- Description: subnetE
- Destination: 2001:db8:abcd:f000::
- Prefix: 72
- Gateway: 2001:db8::1
- Distance: 1

Buttons for "OK", "Cancel", and "Help" are visible at the bottom of the configuration window.



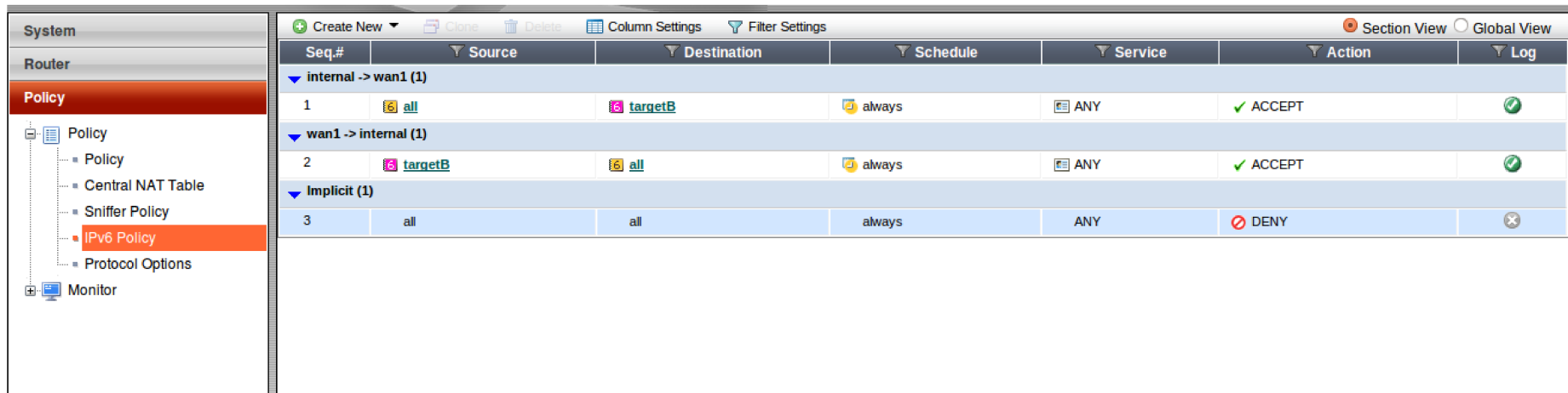
# McAfee Add Static Routes By CLI

---

```
mMcAfee:Admn {3} % cf route add route=2001:db8:ef01:f000::/72
gateway=2001:db8::1 distance=1
route add error: ParameterError: mask 72 is a non-contiguous
subnet mask
mMcAfee:Admn {4} % cf route add route=2001:db8:ef01:f000::/78
gateway=2001:db8::1 distance=1
route add error: ParameterError: mask 78 is a non-contiguous
subnet mask
mMcAfee:Admn {5} % cf route add route=2001:db8:ef01:f000::/55
gateway=2001:db8::1 distance=1
route add error: ParameterError: mask 55 is a non-contiguous
subnet mask
mMcAfee:Admn {6} % cf route add
route=2001:db8:ef01:f000::/56 gateway=2001:db8::1
distance=1
mMcAfee:Admn {7} % echo "obase=2;72;78;55;56" | bc
1001000
1001110
110111
```

# 6. FW IPv6 Policies

## Fortigate policy listing



The screenshot displays the Fortigate web interface for configuring IPv6 policies. The left sidebar shows a tree view with 'Policy' selected, and 'IPv6 Policy' highlighted. The main area shows a table of policies with columns for Seq.#, Source, Destination, Schedule, Service, Action, and Log. The table lists three policies: two explicit policies (1 and 2) and one implicit policy (3).

Seq.#	Source	Destination	Schedule	Service	Action	Log
internal -> wan1 (1)						
1	all	targetB	always	ANY	ACCEPT	✓
wan1 -> internal (1)						
2	targetB	all	always	ANY	ACCEPT	✓
Implicit (1)						
3	all	all	always	ANY	DENY	✗

# Fortigate IPv6 Rule

System

Router

**Policy**

- Policy
- Central NAT Table
- Sniffer Policy
- IPv6 Policy**
- Protocol Options

Monitor

### Edit Policy

Source Interface/Zone	internal
Source Address	all
Destination Interface/Zone	wan1
Destination Address	targetB
Schedule	always
Service	ANY
Action	ACCEPT

Log Allowed Traffic

---

Enable Identity Based Policy

---

UTM

- Enable AntiVirus default
- Enable Web Filter default
- Enable Email Filter default
- Enable DLP Sensor default

Protocol Options default

Traffic Shaping

- Shared Traffic Shaper [Please Select]
- Shared Traffic Shaper Reverse Direction [Please Select]

Tags

Applied tags

Add tags

Comments  0/63



# McAfee Rule

The screenshot shows the 'Rules: Rule Properties' dialog box for a rule named 'IPv6 general access'. The rule is enabled and set to 'Allow' action. The rule is configured with the following settings:

- Name:** IPv6 general access
- Enable rule:**
- Action:** Allow
- Applications:** <Any>
- Source Endpoints:** subnet\_pri2\_v6 (Subnet)
- Destination Endpoints:** subnet\_priv6 (Subnet)
- Zone:** external
- GTI Host Reputation:** None
- Advanced:** Always active, NAT: <None>, Redirect: <None>, Audit: Verbose, Authenticator: <None/Passport>, IPS Signatures: <None>, IPS Responses: <None>

The 'Browse' pane on the right shows a list of destination endpoints. The selected endpoint is 'subnet\_priv6 (Subnet)' with properties '2001:::a:::64'. Other endpoints include '<Any V4>', '<Any V6>', '<Any>', '<CommandCenter servers>', '<ePO server> (IP)', '<Firewall> (IP)', '<localhost> (Host)', '<SmartFilter server> (IP)', 'internal primary DNS resolv', 'subnet\_pri (Subnet)', 'subnet\_pri2 (Subnet)', and 'subnet\_pri2\_v6 (Subnet)'.

At the bottom of the dialog, it states: 'Last modified by admin on 10/11/12 12:01:49 PM EDT'. Buttons for 'OK', 'Cancel', and 'Help' are visible at the bottom right.

# Fortigate Logging

System

Router

Policy

Firewall Objects

UTM Profiles

VPN

User

WiFi Controller

Log&Report

- Log & Archive Access
  - Event Log
  - AntiVirus Log
  - Web Filter Log
  - Application Control Log
  - Attack Log
  - Email Filter Log
  - DLP Log
  - Traffic Log
  - Vulnerability Scan Log
- FAMS
- Log Config
- Monitor

Refresh Download Raw Log Column Settings Filter Settings Detailed Information

#	Date	Time	Src	Dst	Service	Sent	Received	Status
1	2012-10-11	23:51:55	2001:44b8:1117:1600:e931:3c67:c0f2:69ec	2001:db8:a:b:c:d:e:2	other	11.6 KB	1.3 KB	✓
2	2012-10-11	23:50:55	2001:44b8:1117:1600:e931:3c67:c0f2:69ec	2001:db8:a:b:c:d:e:2	1236/tcp	80 B	0 B	✓
3	2012-10-11	23:50:55	2001:44b8:1117:1600:e931:3c67:c0f2:69ec	2001:db8:a:b:c:d:e:2	32777/tcp	80 B	0 B	✓
4	2012-10-11	23:50:55	2001:44b8:1117:1600:e931:3c67:c0f2:69ec	2001:db8:a:b:c:d:e:2	2135/tcp	80 B	0 B	✓

Log location: Disk 1 / 207

Date Time	2012-10-11 23:51:55	Date	2012-10-11
Time	23:51:55	Level	notice
Sub Type	allowed	ID	2
Virtual Domain	root	Dir Display	org
Tran Display	noop	Src	2001:44b8:1117:1600:e931:3c67:c0f2:69ec
Src Name	2001:44b8:1117:1600:e931:3c67:c0f2:69ec	Src Port	0
Dst	2001:db8:a:b:c:d:e:2	Dst Name	2001:db8:a:b:c:d:e:2
Dst Port	0	Dst NAT IP	N/A
Dst NAT Port	0	Service	other
Protocol	58	IM and P2P Application	N/A
Duration	173	Rule	2
Policy ID	2	Sent	11.6 KB
Received	1.3 KB	Sent Packets	114
Received Packets	13	VPN	N/A
Src Interface	internal	Dst Interface	wan1
Serial Number	5092	Status	✓
User	N/A	Group	N/A
Carrier End Point	N/A	Application Name	N/A
Application Category	N/A	Sent Shaper Bytes Dropped	0
Received Shaper Bytes Dropped	0	Per-IP Shaper Bytes Dropped	0
Sent Shaper Name	N/A	Received Shaper Name	N/A
Per-IP Shaper Name	N/A	Identity Index	0
Src NAT IP	N/A	Src NAT Port	0
Destination Country	N/A	VPN Type	N/A
VPN Tunnel	N/A	Profile Group Name	N/A
Sub Application Category	N/A	Sub Application Name	N/A
Source Country	N/A		









# 7. Other IPv6 Bits

---

## Fortigate

DHCP Server

DNS Server

High Availability, 3 types:

- FGCP 2 to 4 units, Active
- TCP session synchronization
- VRRP: Active/Standby

Identity-based security policies

IPv6 tunnel over IPv4

IPv4 tunnel over IPv6

IPsec VPN

Logging

SNMP

SSL VPN

UTM Protection

## McAfee

Applications - not all support IPv6

DNS Server

High Availability:

Active/Standby

IPv6 NAT/Redirect

UTM - IPS + limited

Applications protection

VPN - Gateway to Gateway