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
- 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

- 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

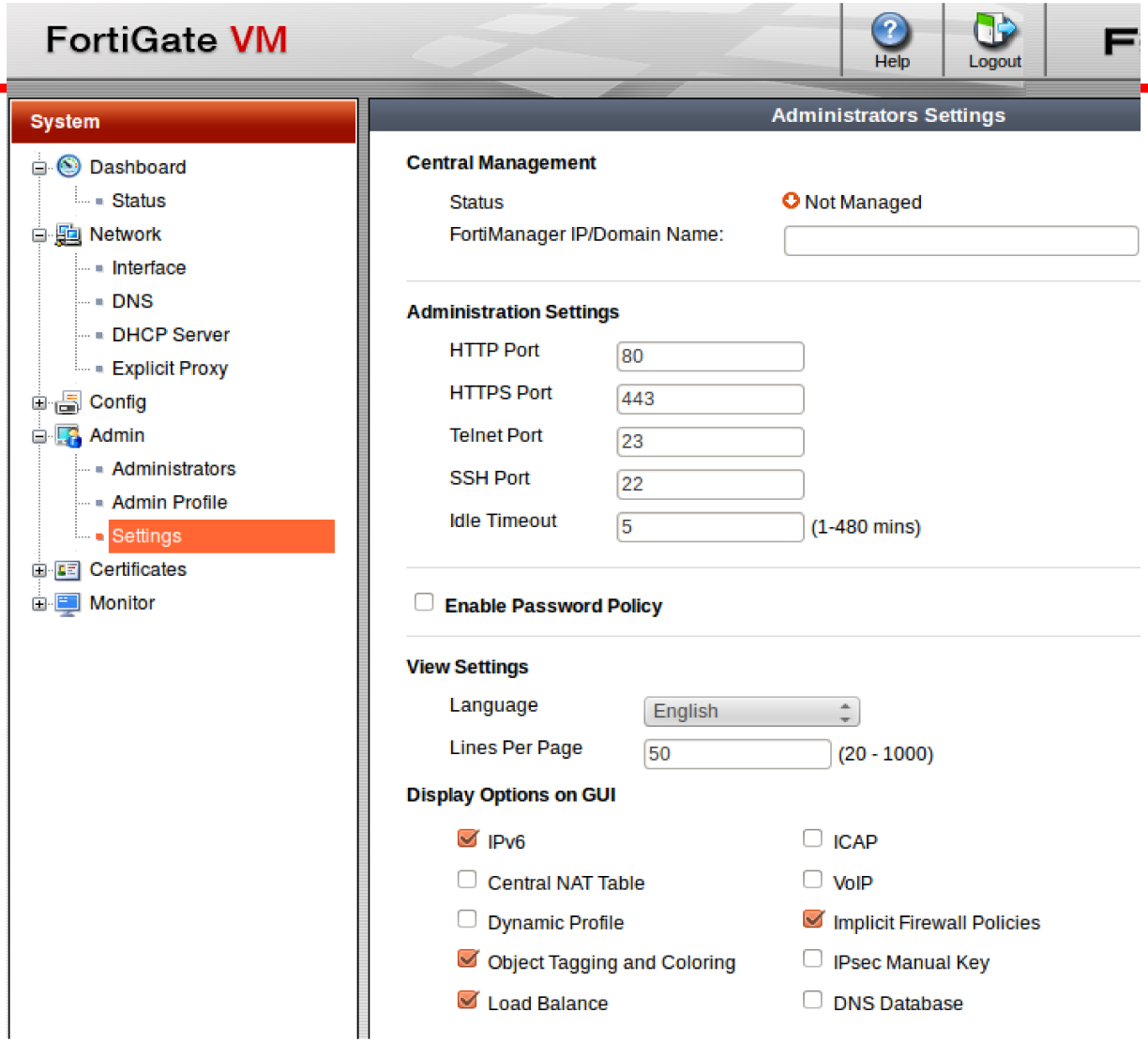
Firewall Platforms/OS

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

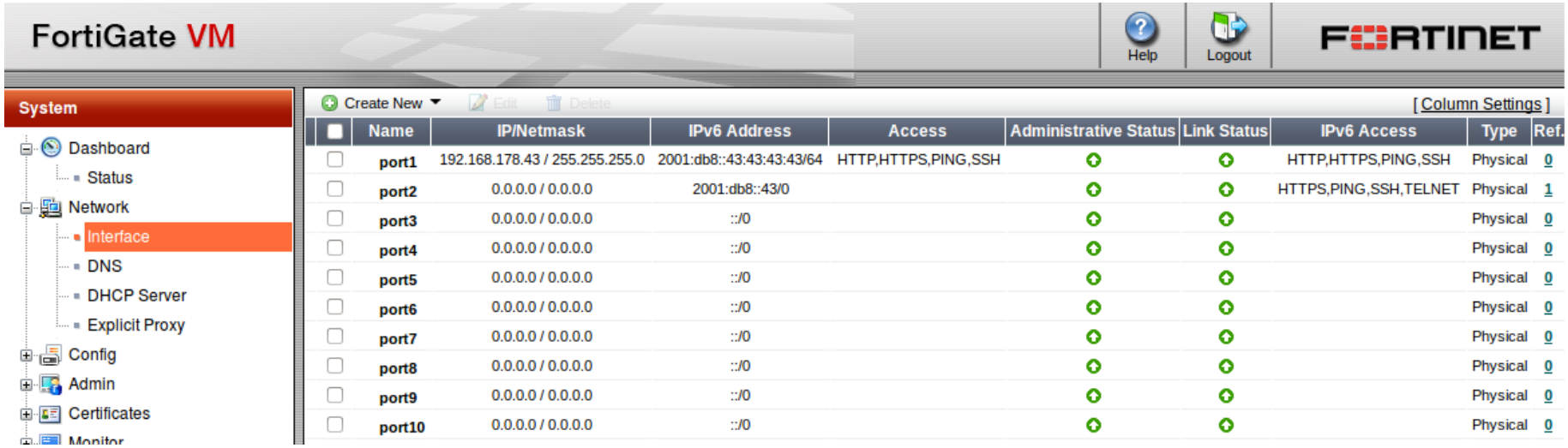
1. Firewall Initial Install

- 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

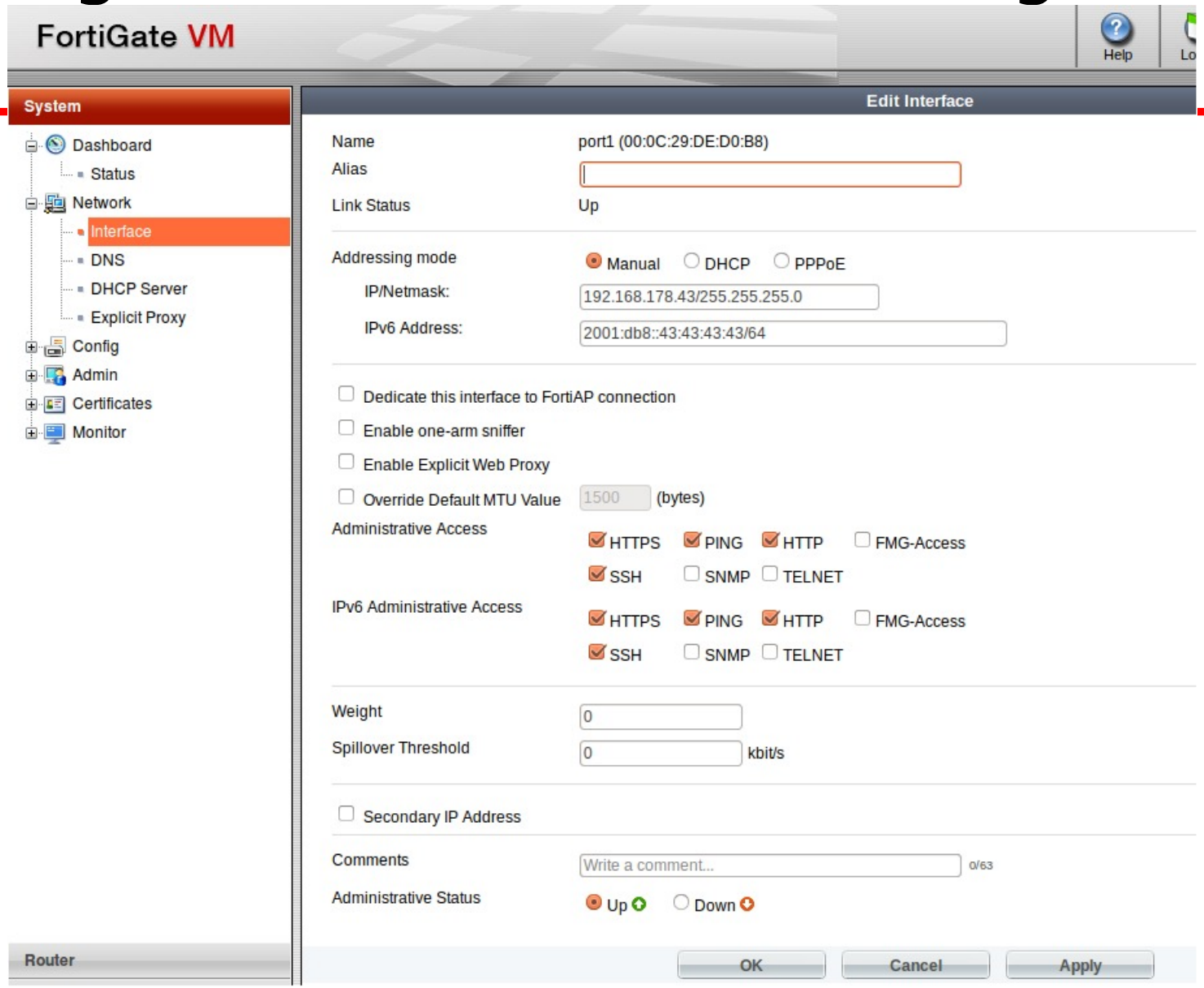
Fortigate Enable IPv6 on GUI



Fortigate Interface Addressing



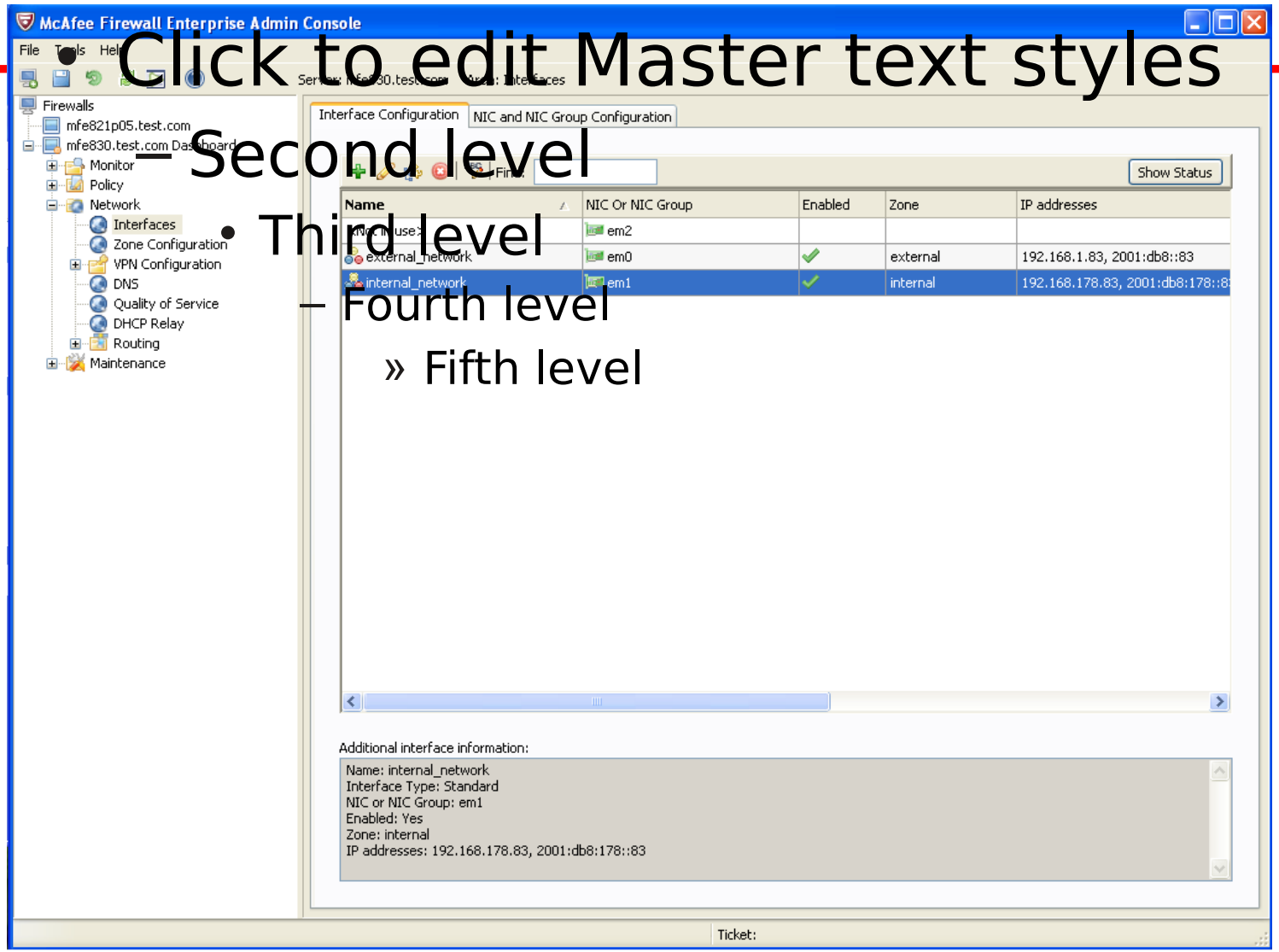
Fortigate Interface Addressing



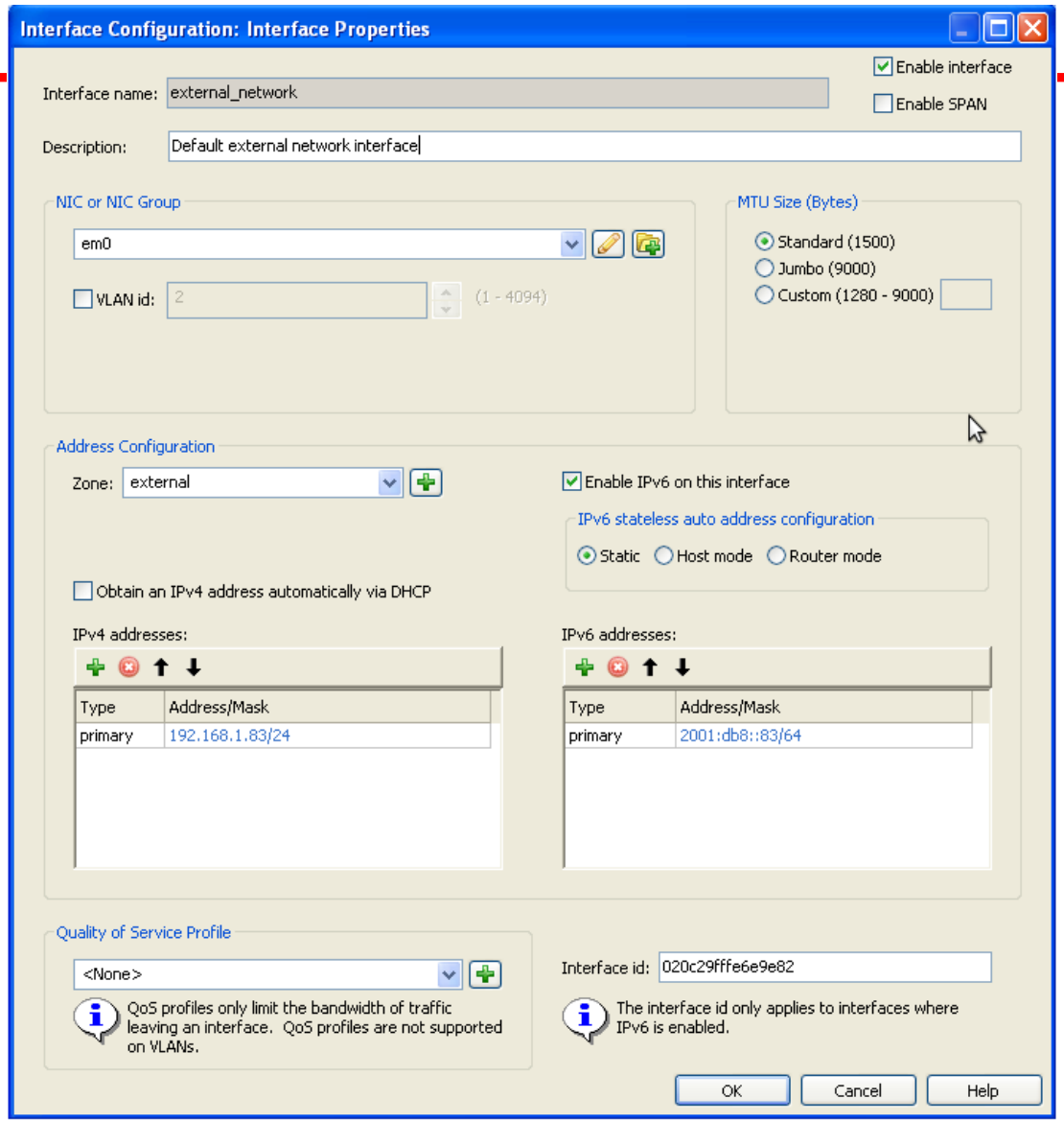
McAfee Interface Addressing

Click to edit Master text styles

- Second level
  - Third level
    - Fourth level
      - Fifth level



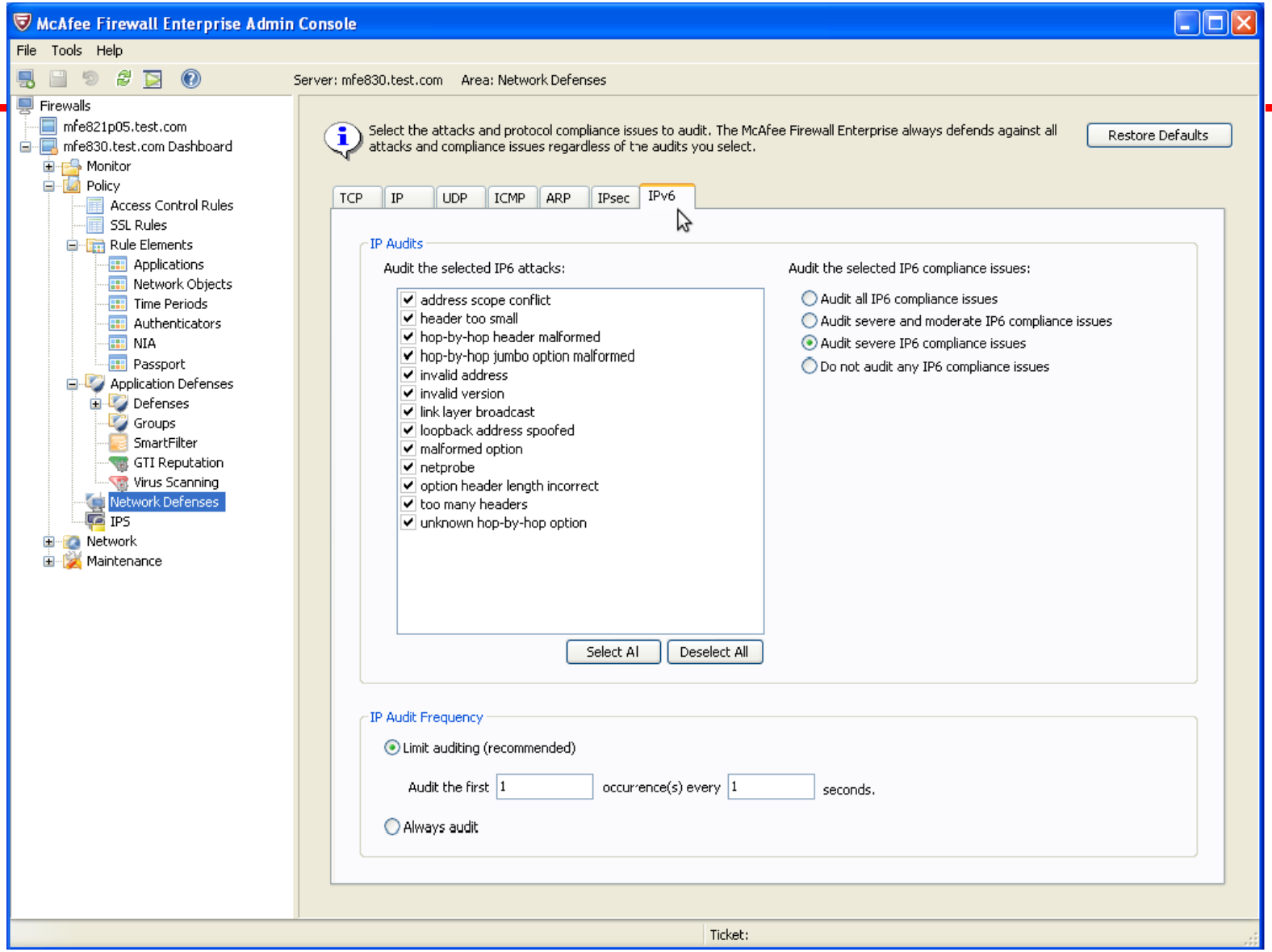
McAfee Interface Addressing



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

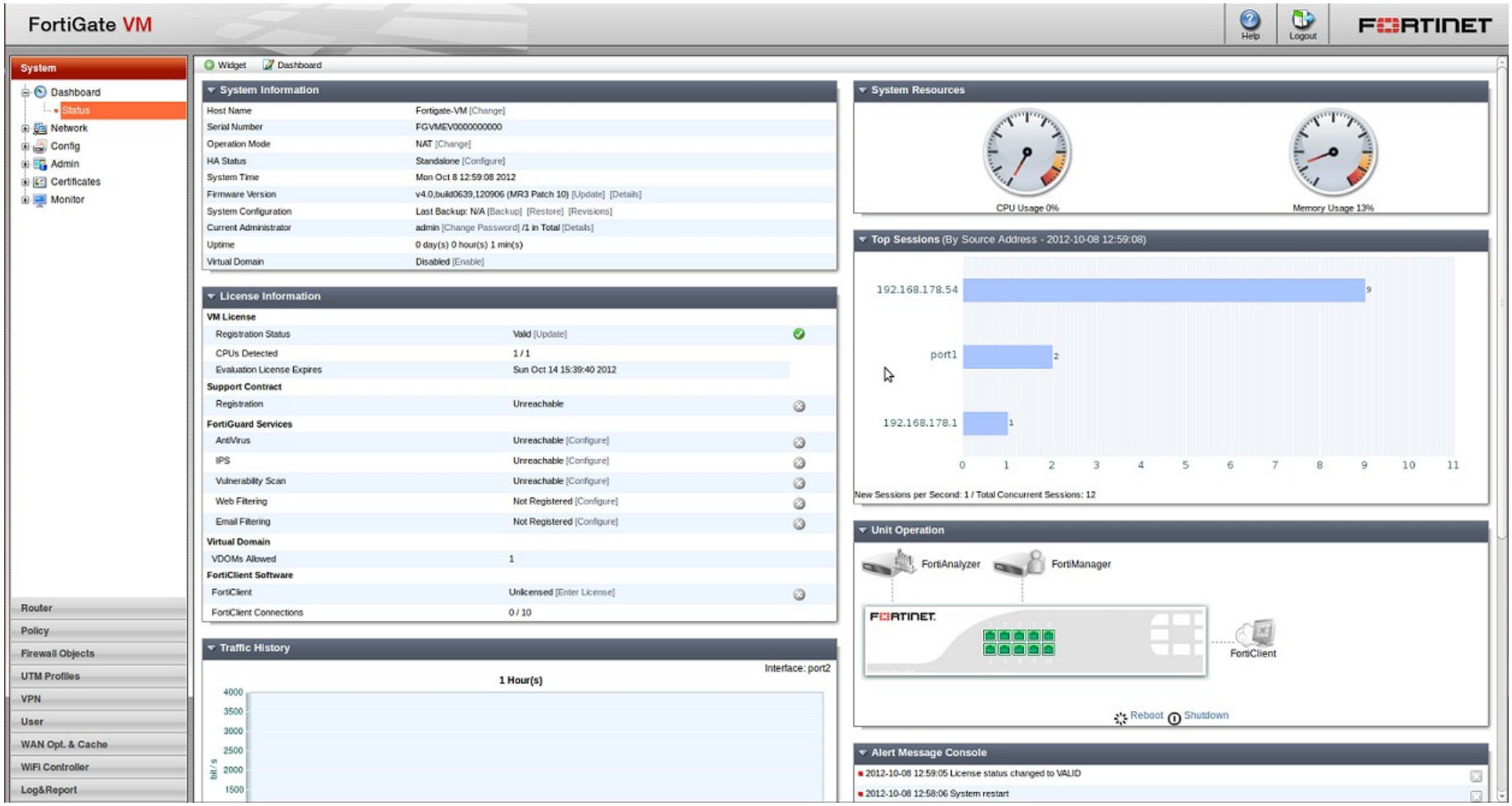
McAfee Network Defense Settings



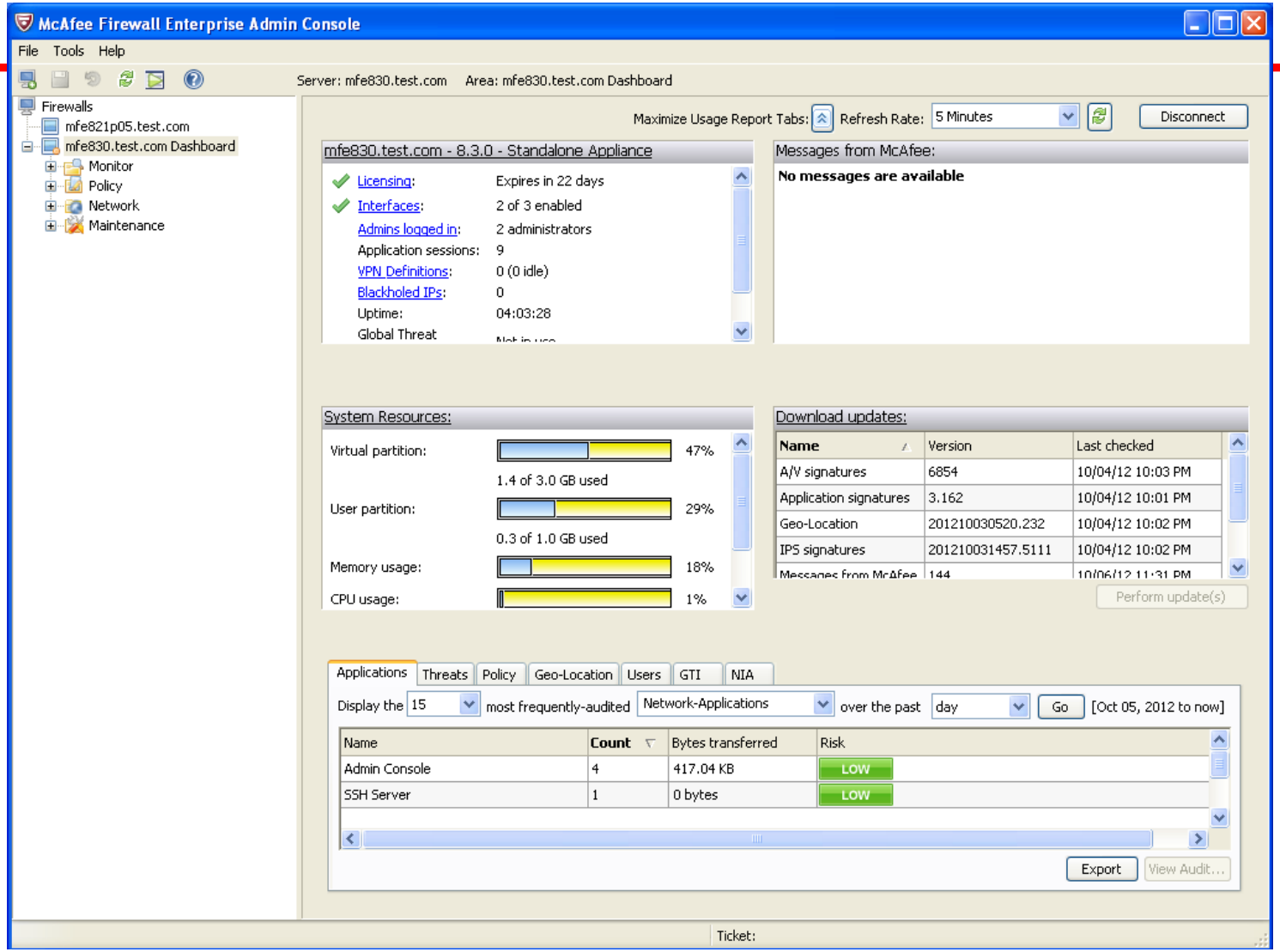
2. Firewall Administration Methods

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

Fortigate First Look



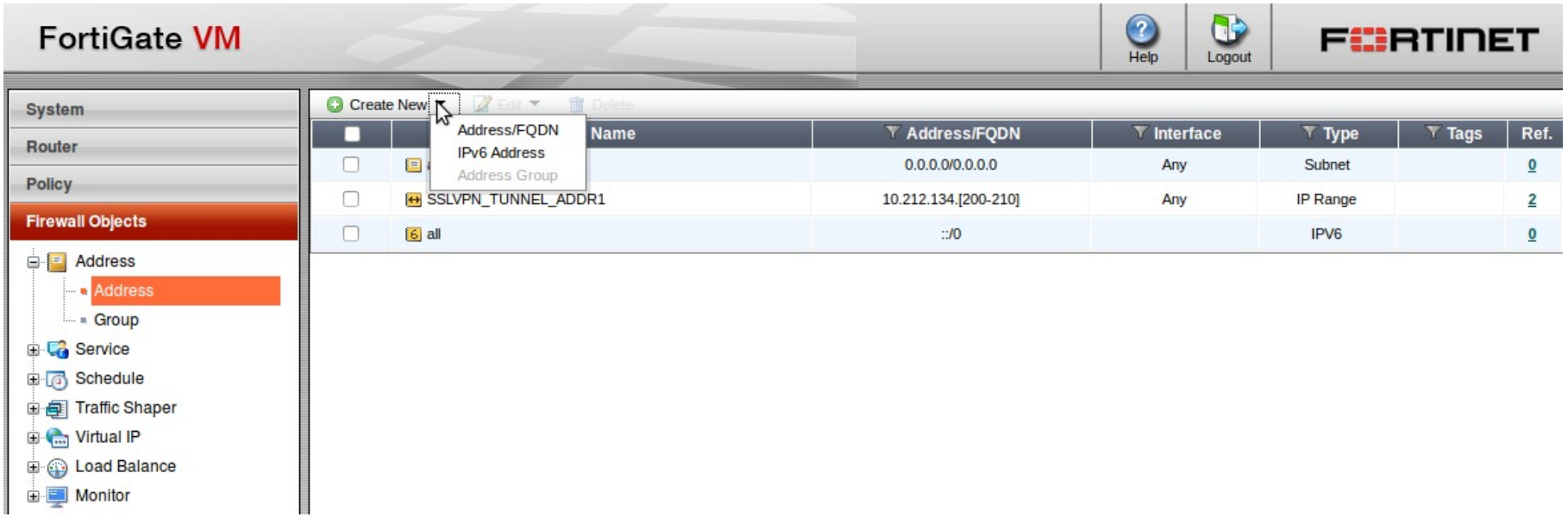
McAfee First Look



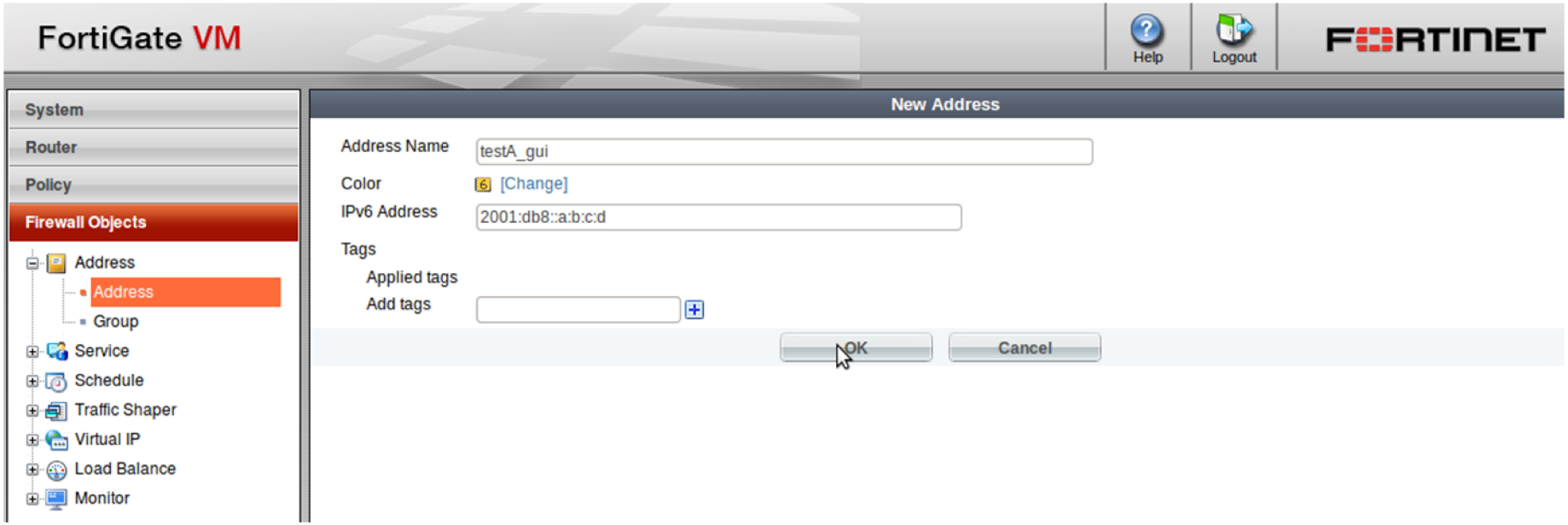
3. Firewall IPv6 Objects

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

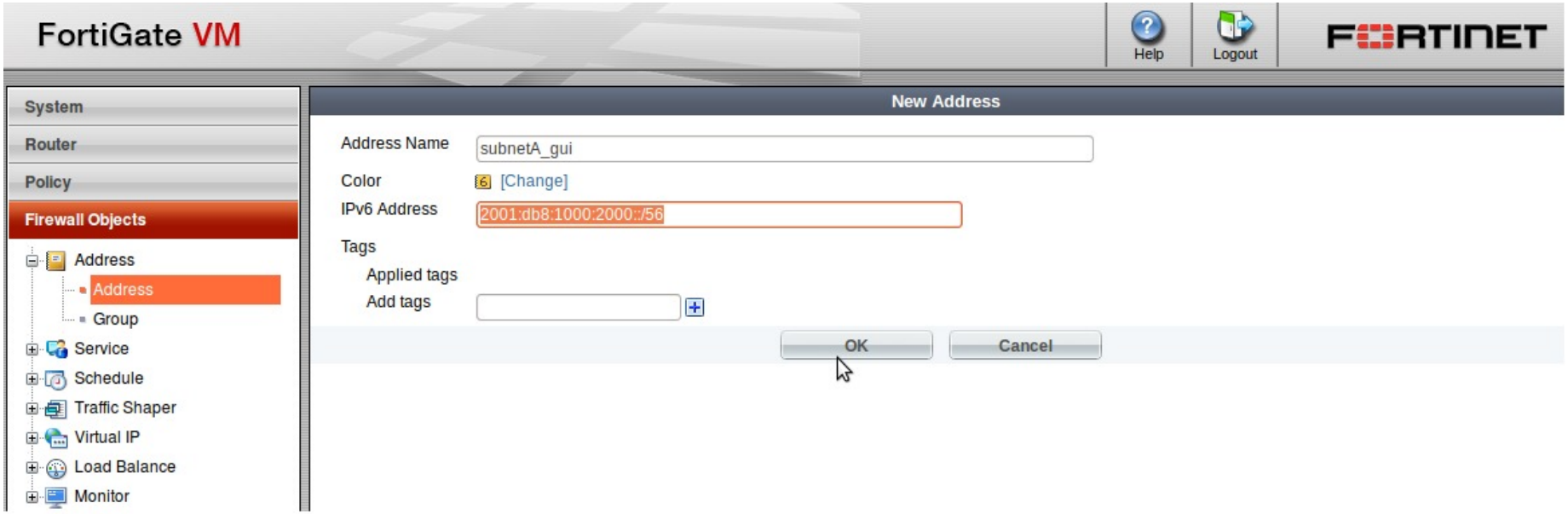
Fortigate Adding Objects By GUI



Fortigate Adding Objects By GUI



Fortigate Adding Objects By GUI



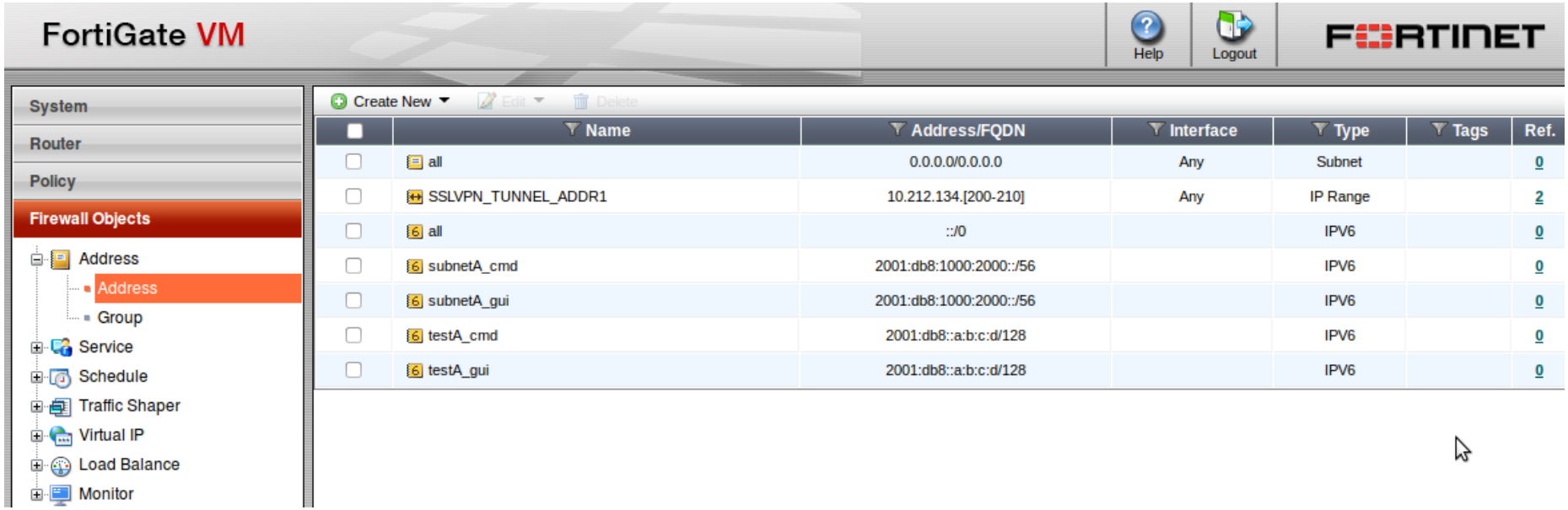
Fortigate Adding Objects By CLI

```
Fortigate-VM # config firewall address6

Fortigate-VM (address6) # edit testA_cmd
new entry 'testA_cmd' added

Fortigate-VM (testA_cmd) # set ip6 2001:db8::a:b:c:d

Fortigate-VM (testA_cmd) # next

Fortigate-VM (address6) # edit subnetA_cmd
new entry 'subnetA_cmd' added

Fortigate-VM (subnetA_cmd) # set ip6 2001:db8:1000:2000::/56

Fortigate-VM (subnetA_cmd) # end

Fortigate-VM #
```

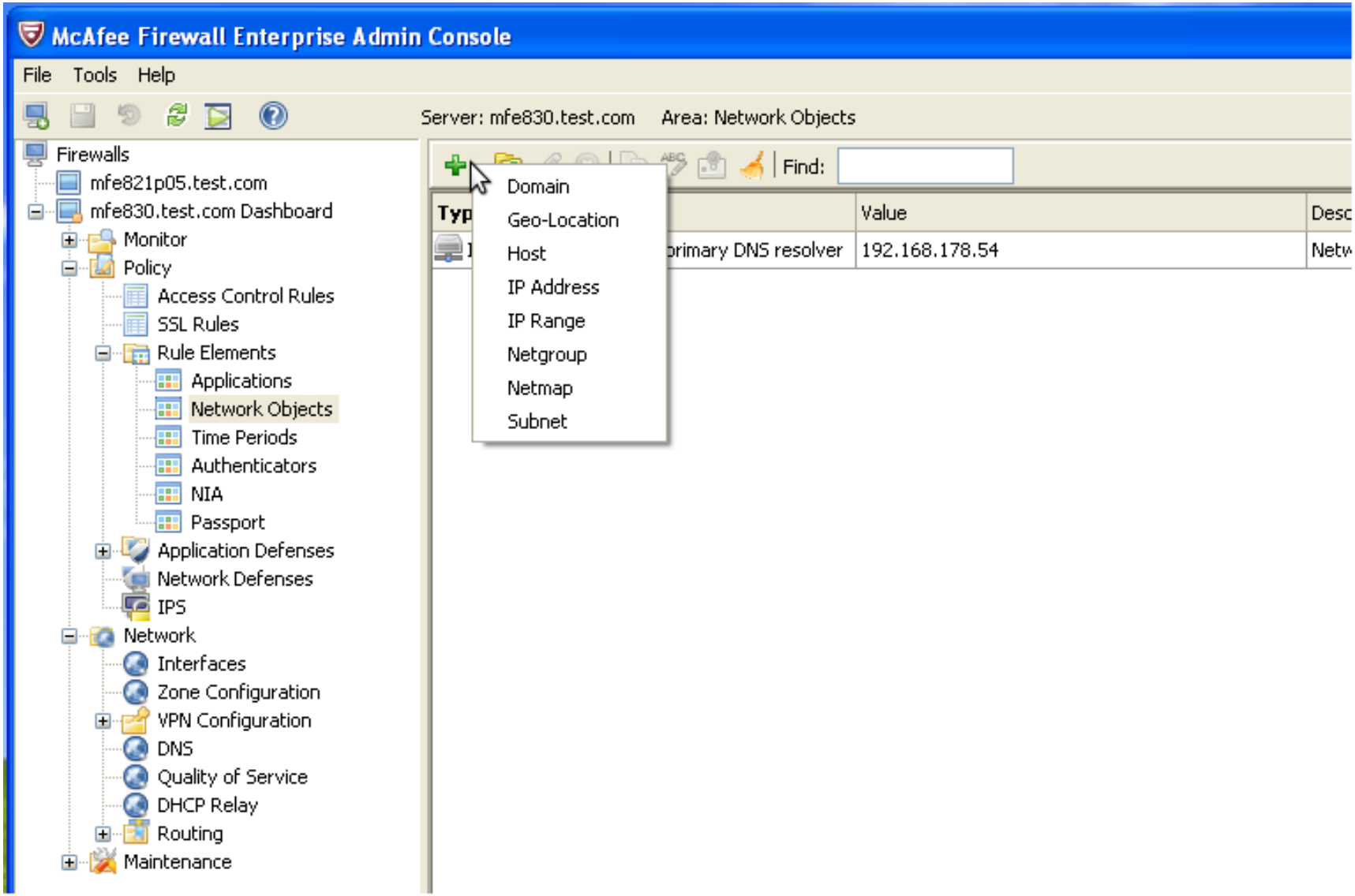
Fortigate Adding Objects By CLI

```
Fortigate-VM #
Fortigate-VM # 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-VM # _
```

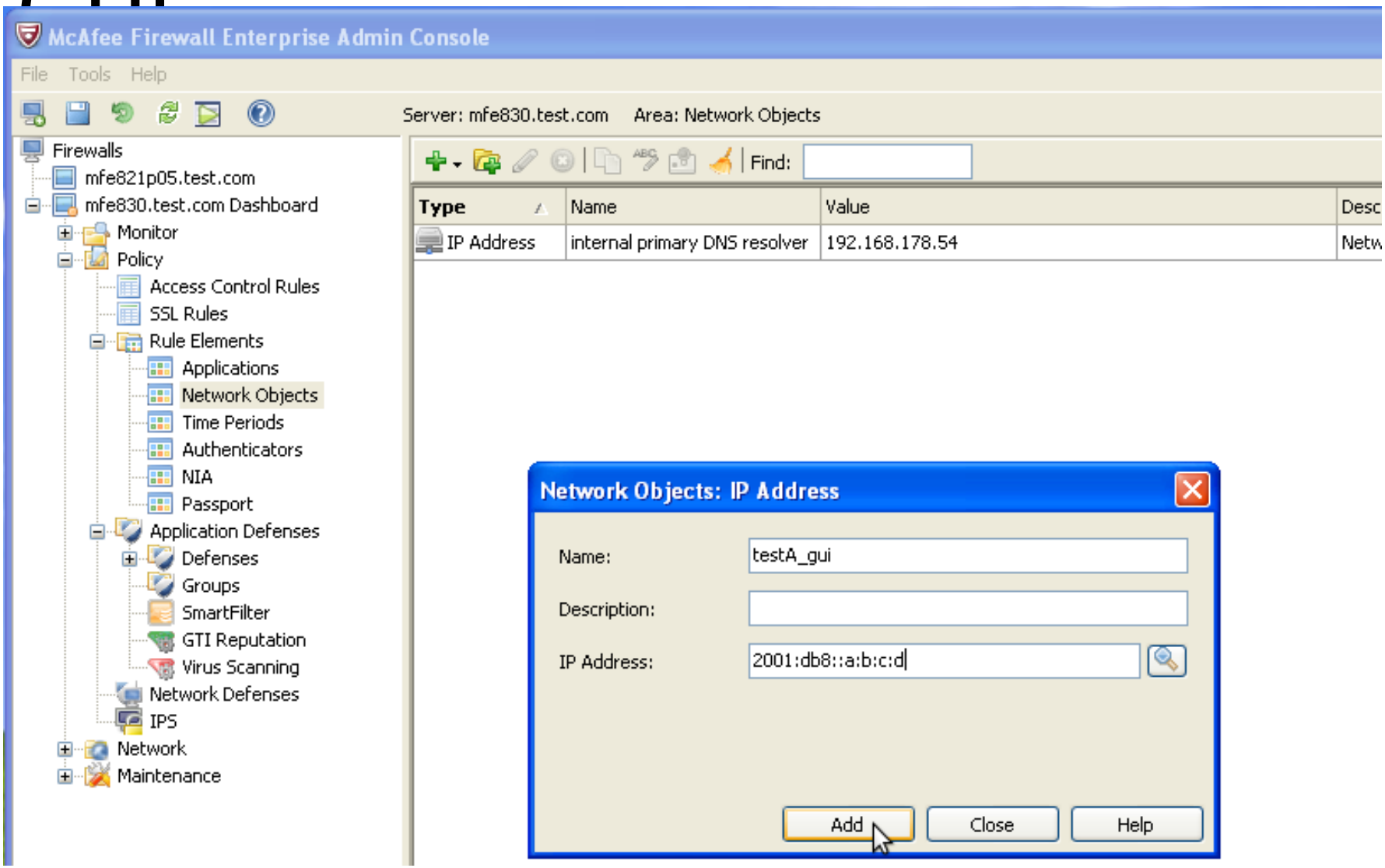
Fortigate Objects



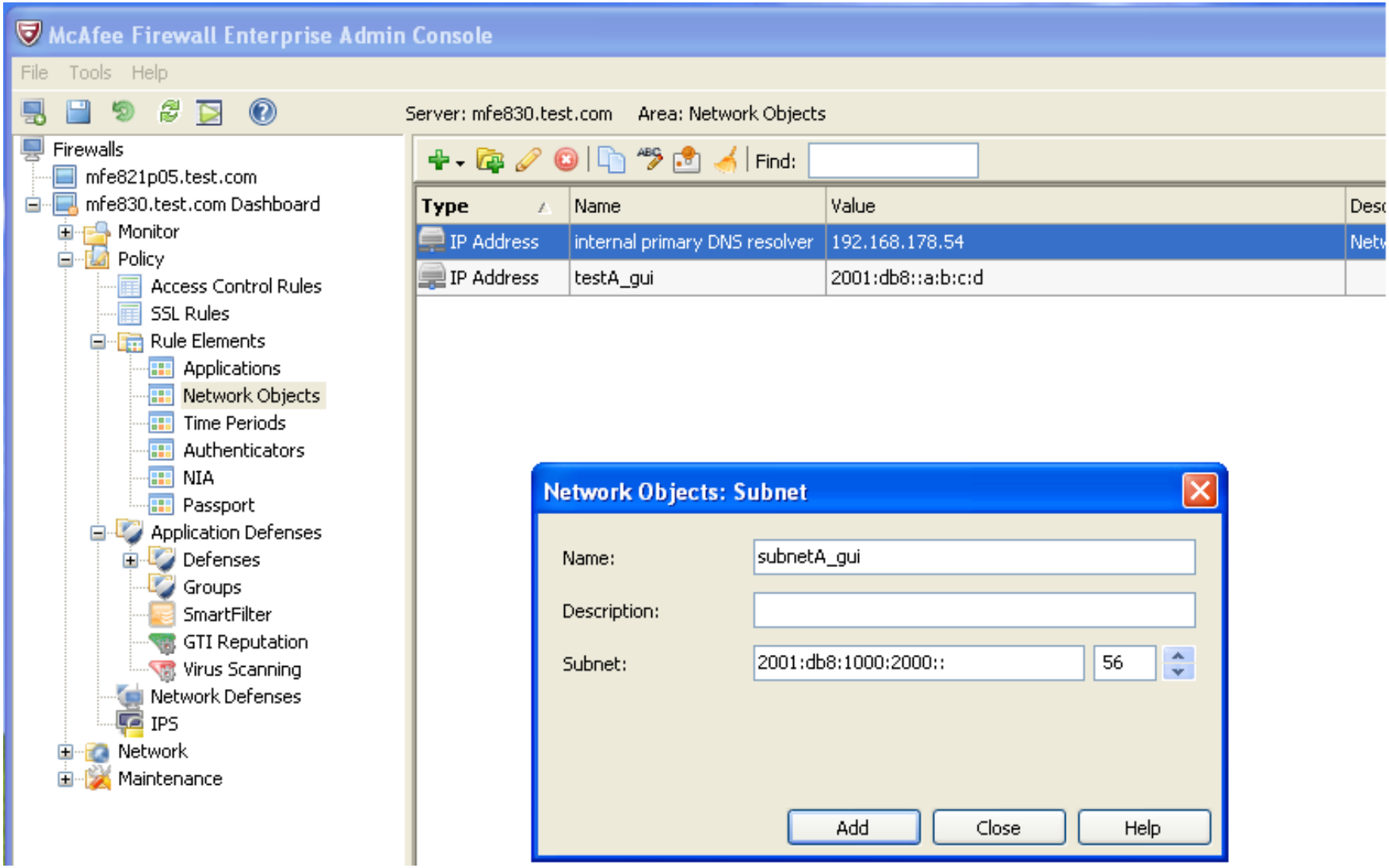
Adding McAfee Objects by GUI



McAfee Adding Objects By GUI



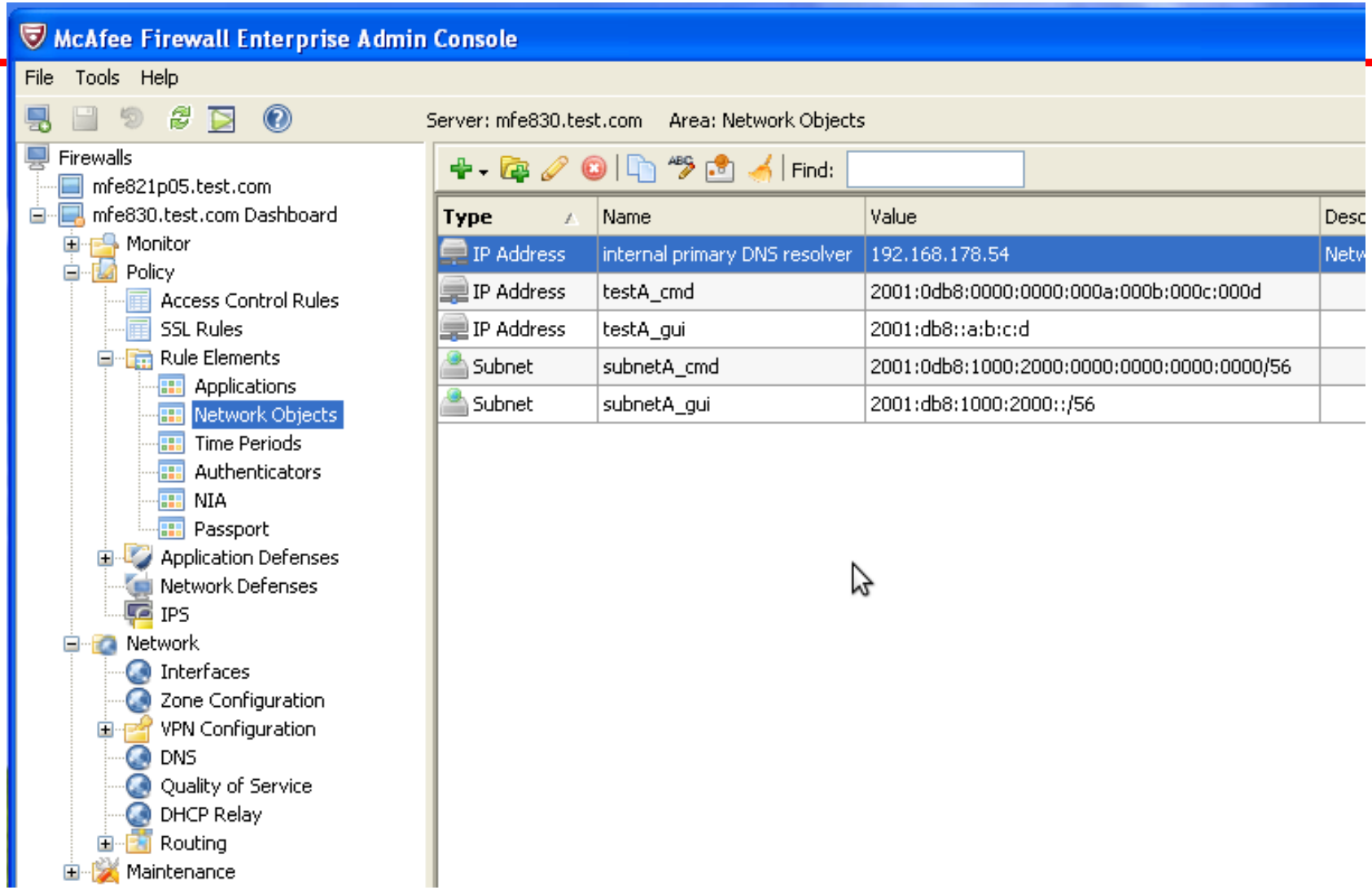
McAfee Adding Objects By GUI



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



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)

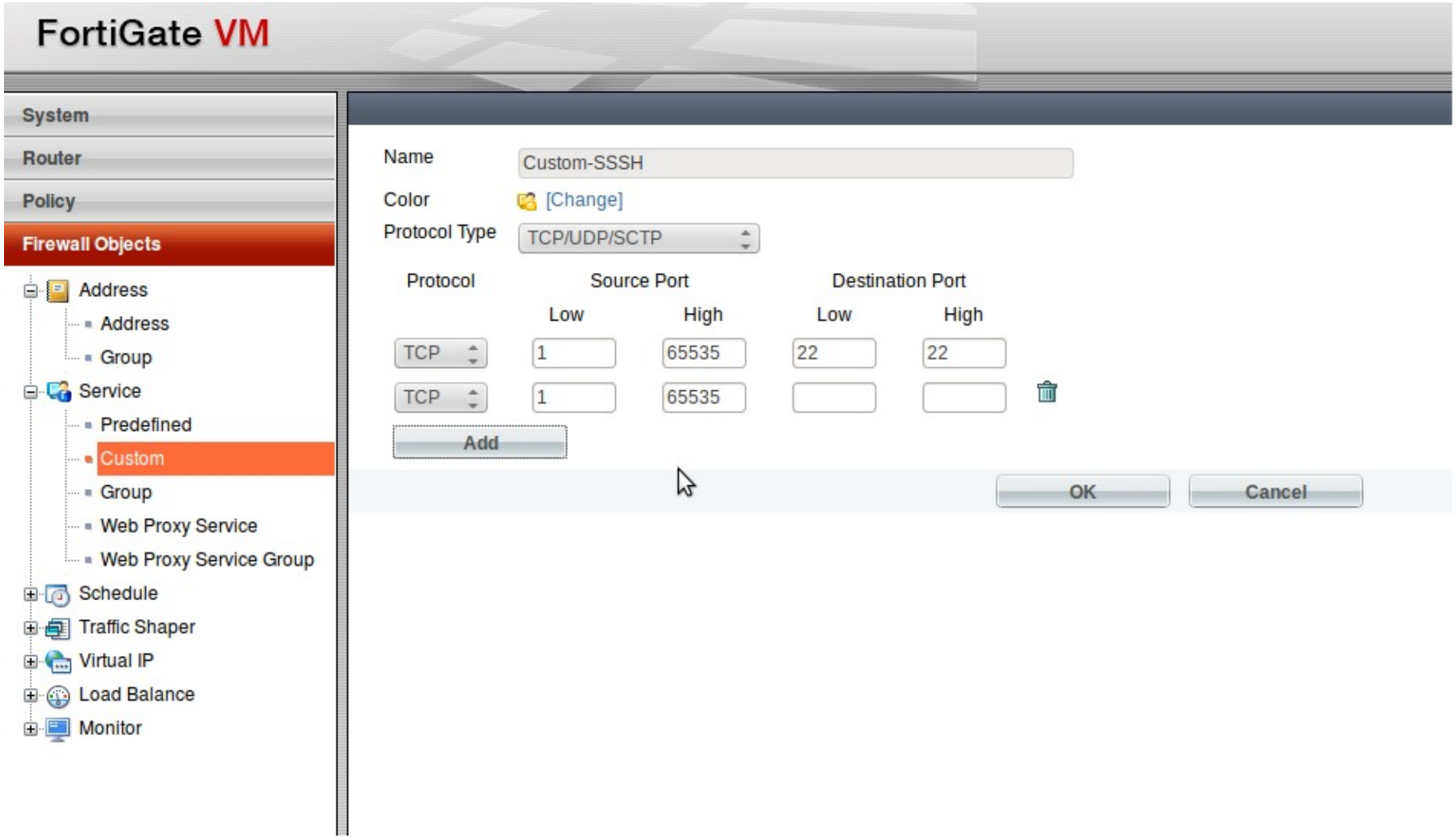
Fortigate Services

FortiGate VM

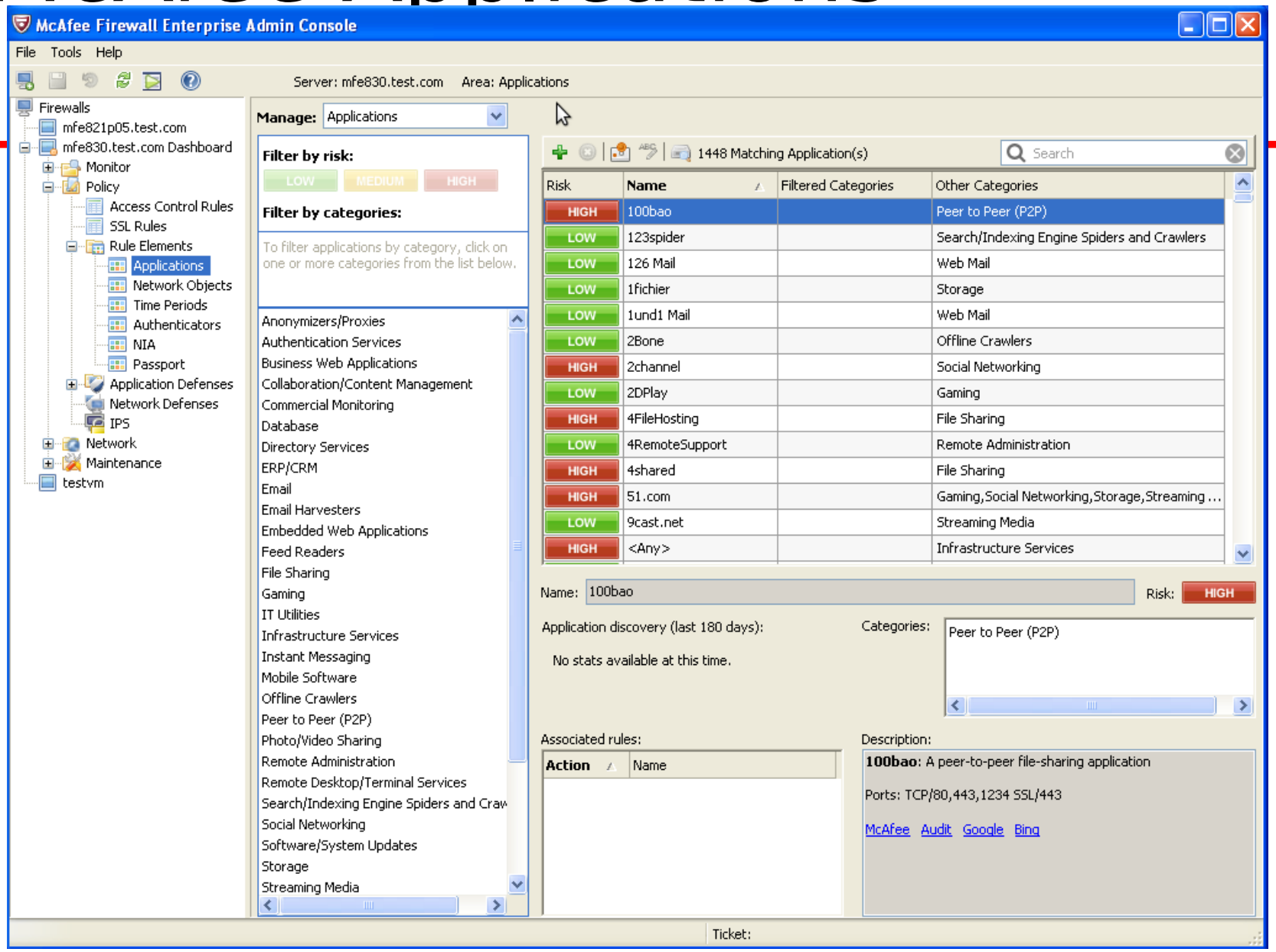
- System
- Router
- Policy
- Firewall Objects
  - Address
    - Address
    - Group
  - Service
    - Predefined
    - Custom
    - Group
    - Web Proxy Service
    - Web Proxy Service Group
  - Schedule
  - Traffic Shaper
  - Virtual IP
  - Load Balance
  - Monitor

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

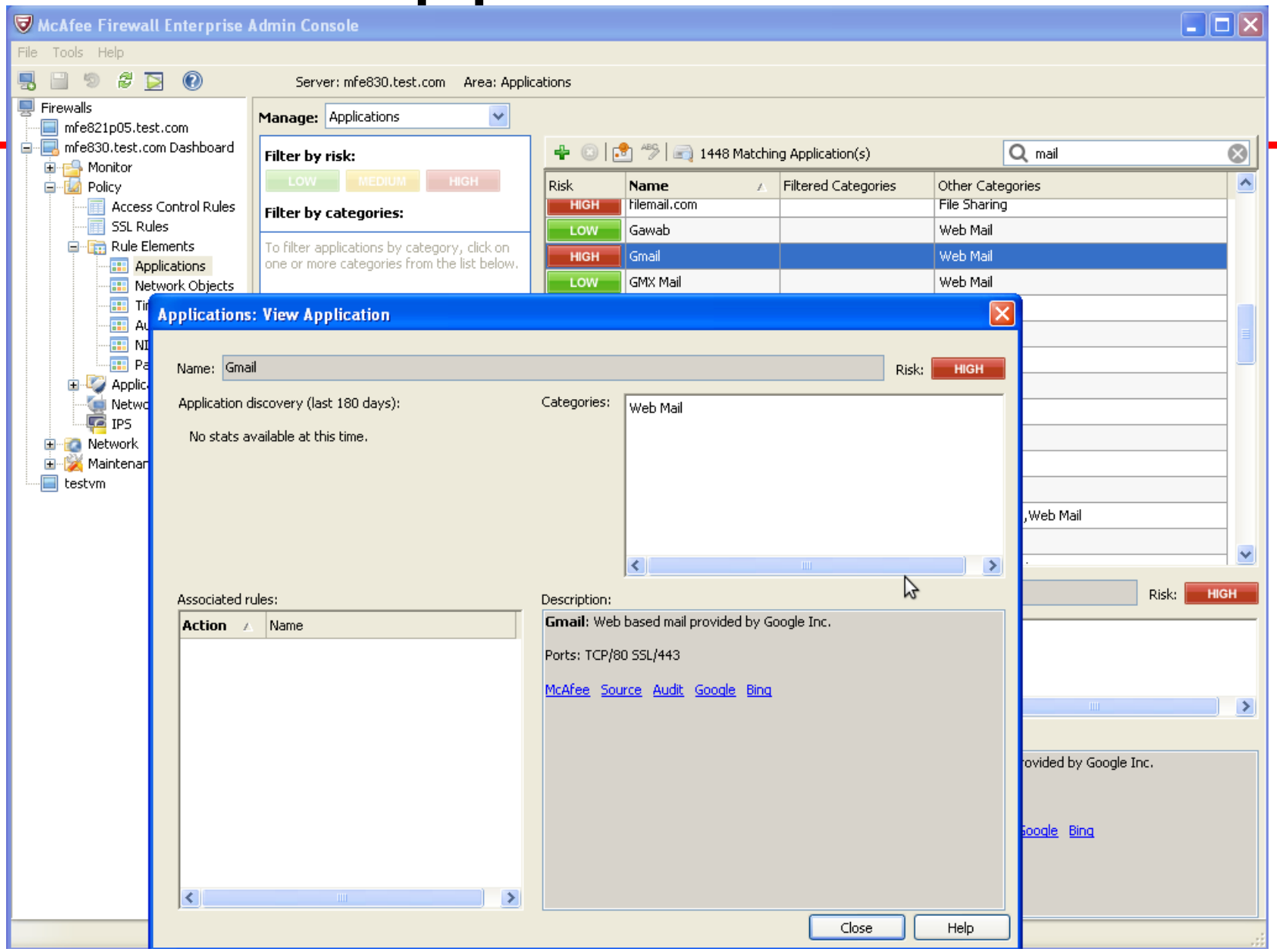
Fortigate Services



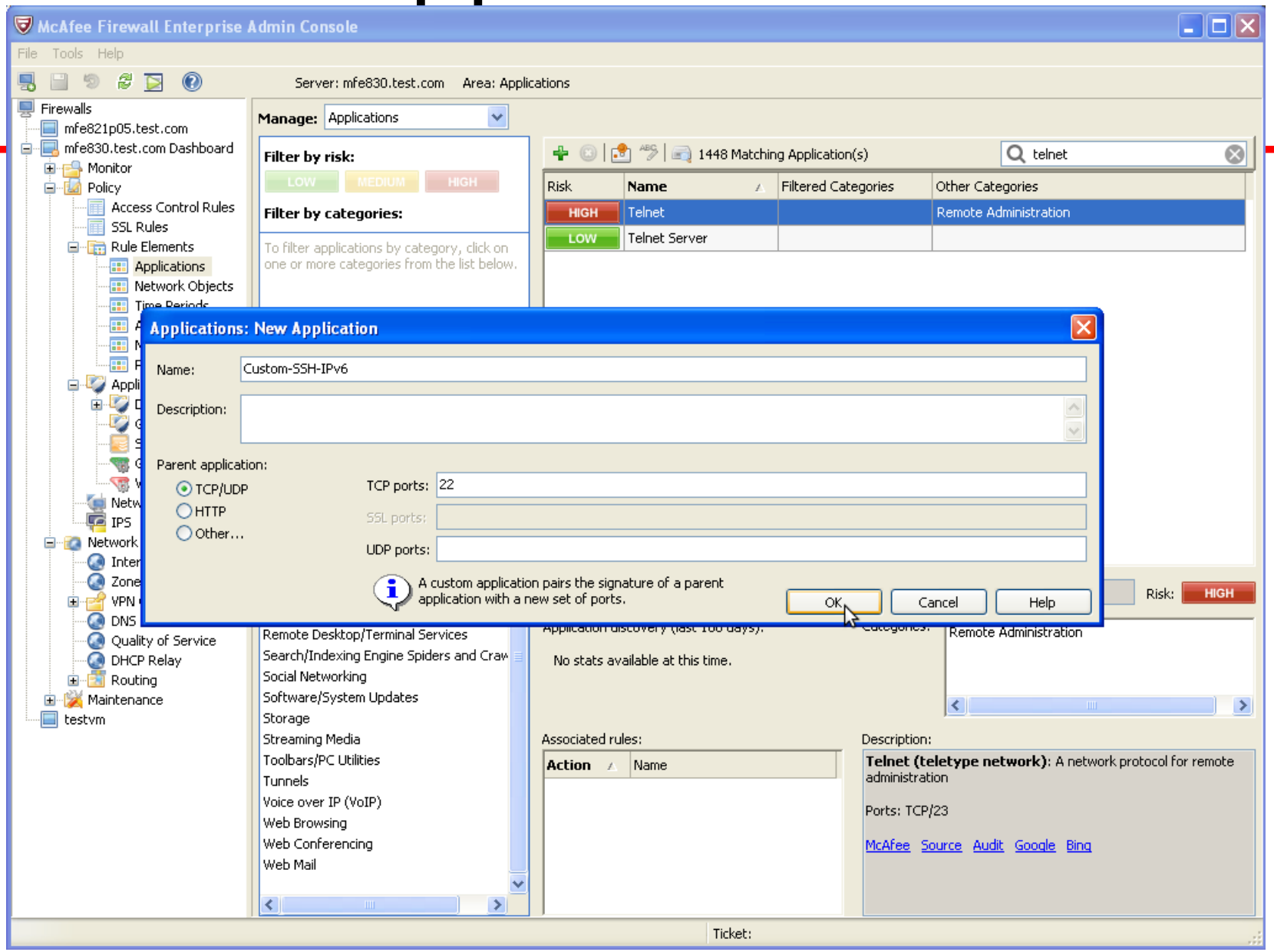
McAfee Applications



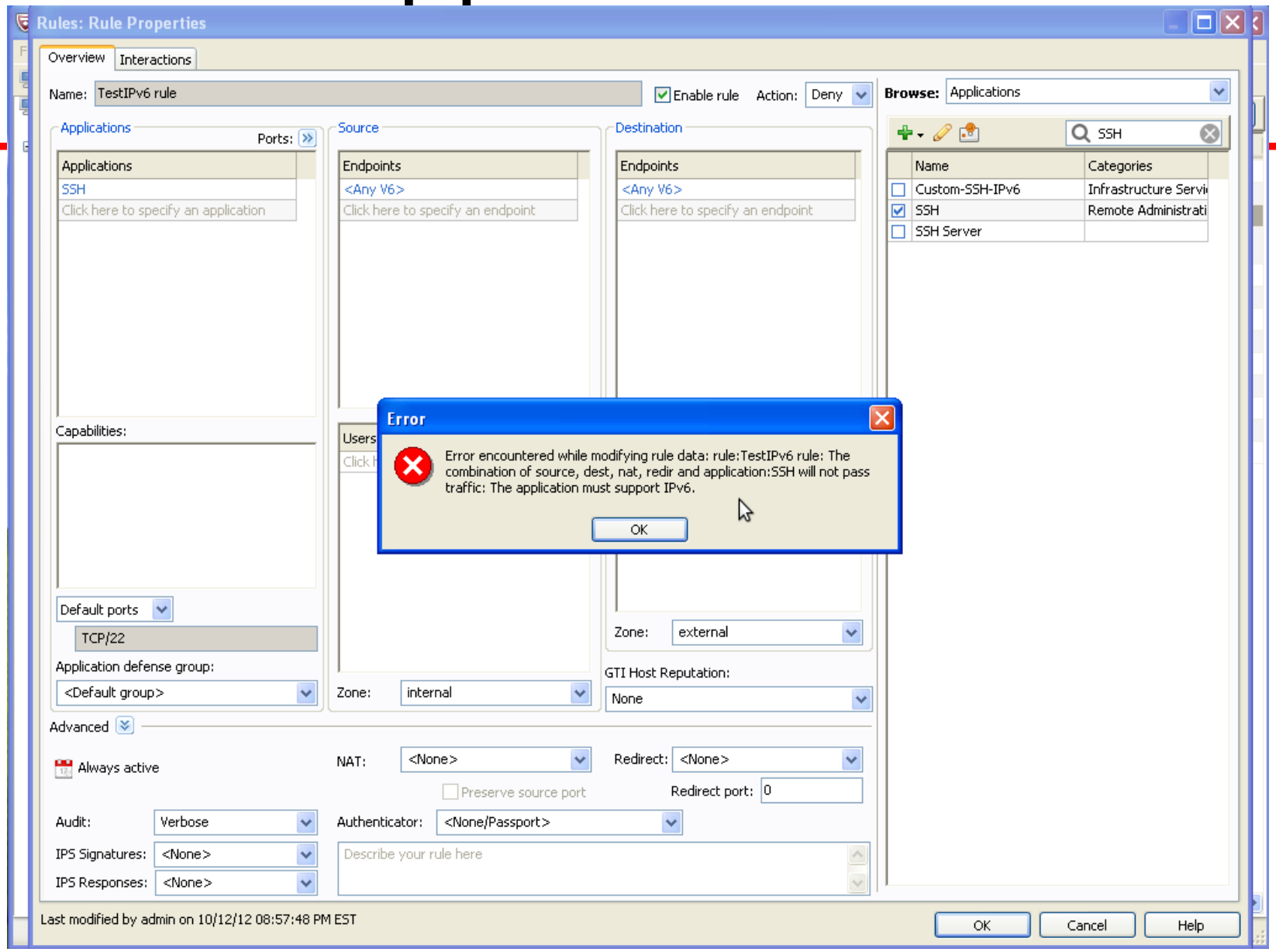
McAfee Applications



McAfee Applications



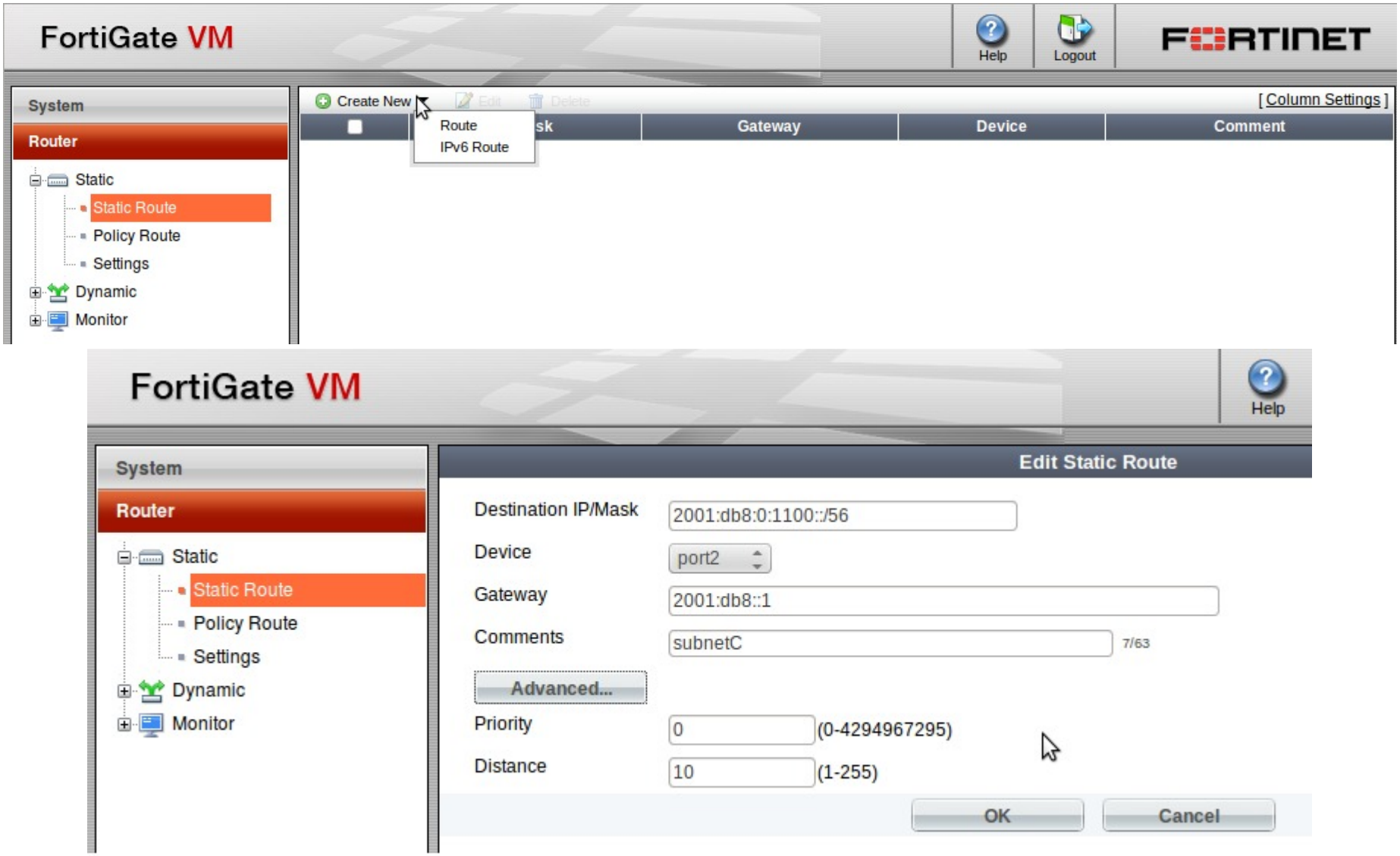
McAfee Applications



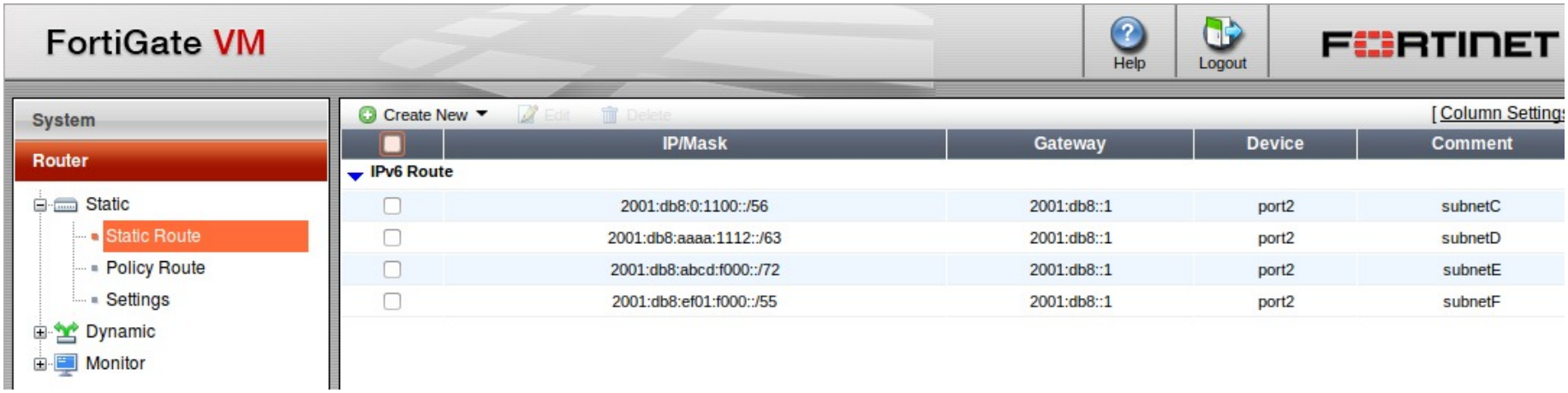
5.Routing

- 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 , FW:/secureos/etc/quagga

Fortigate Add Static Routes By GUI

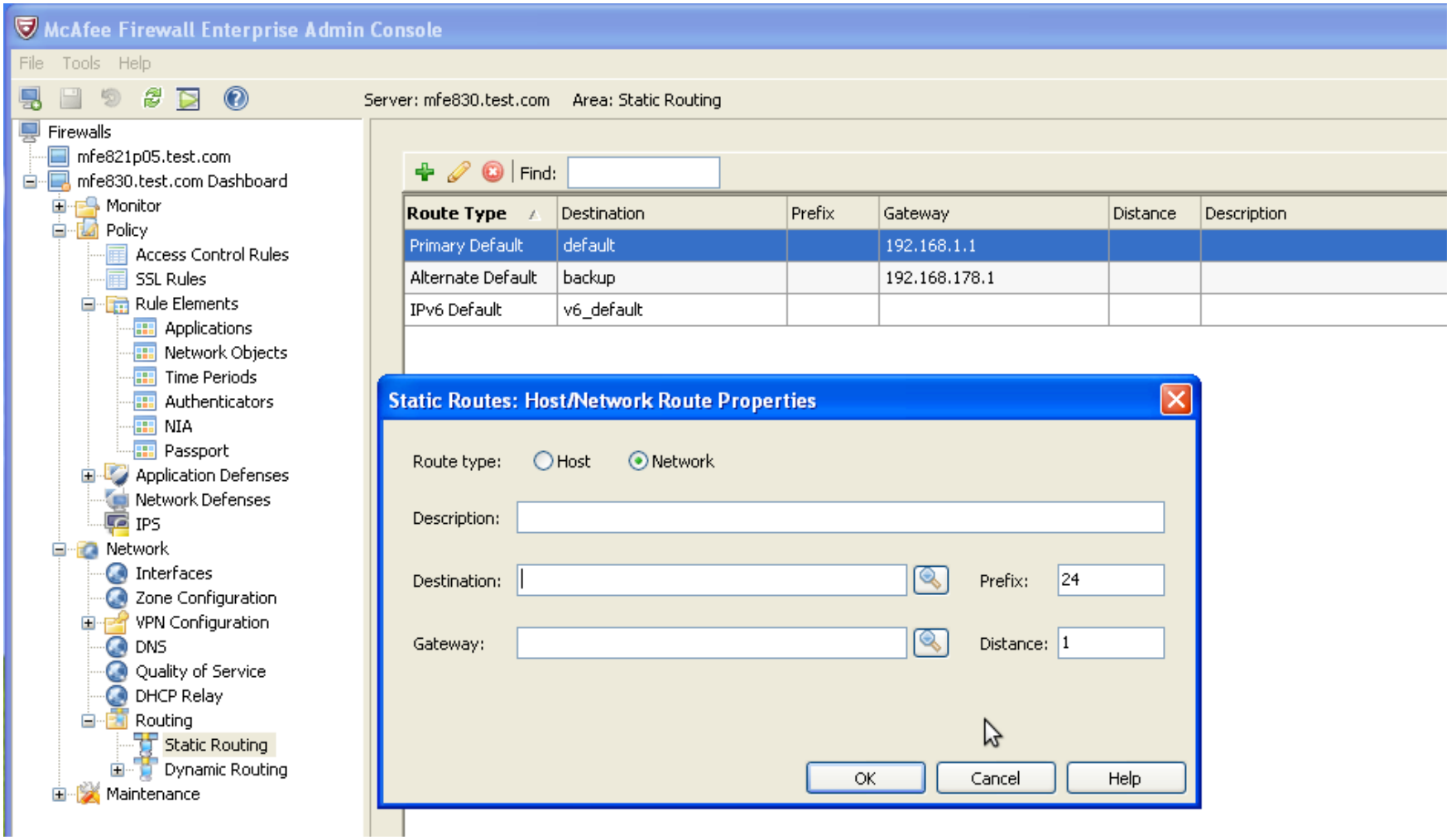


Fortigate Add Static Routes By CLI

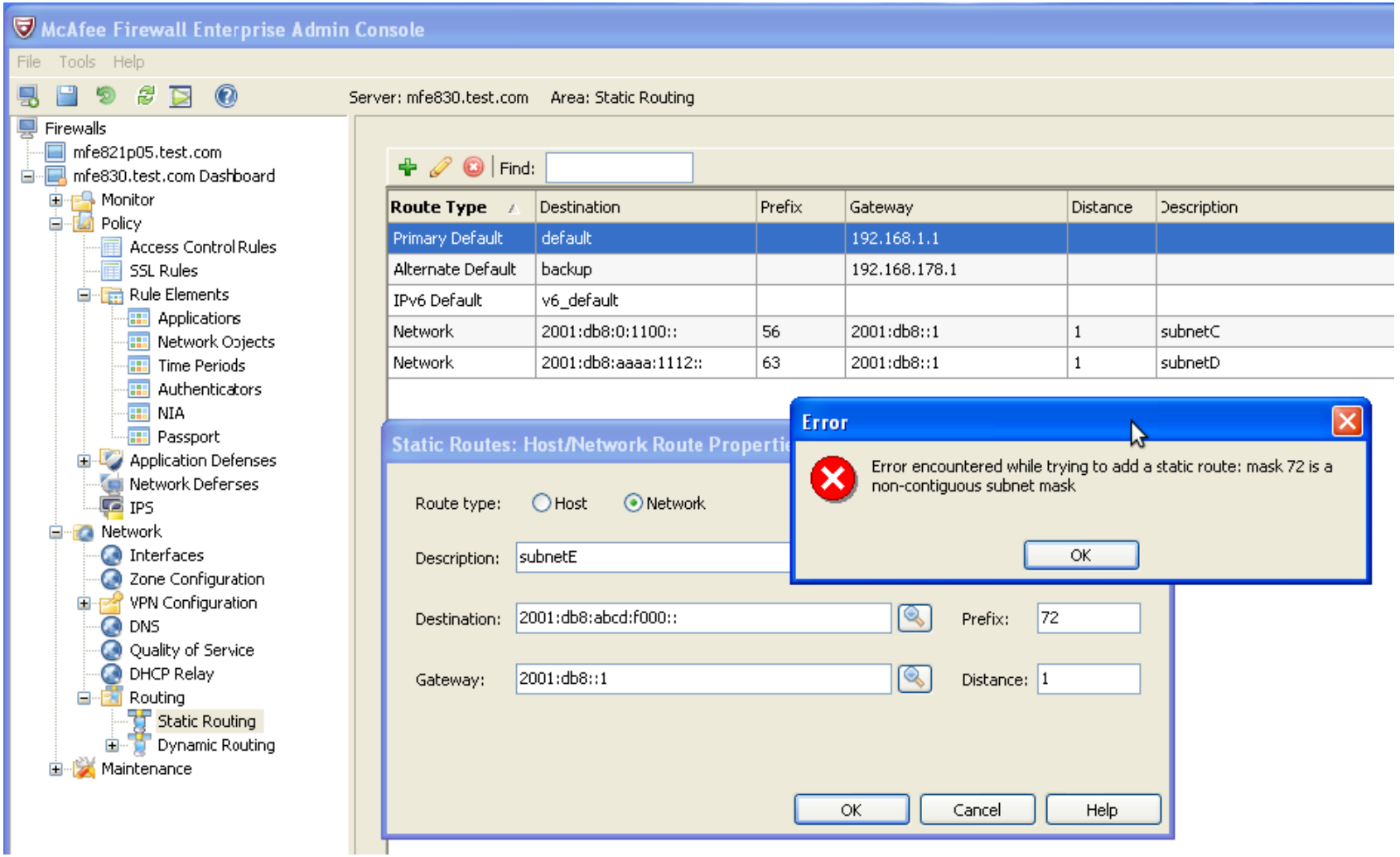



```
Fortigate-VM #
Fortigate-VM # config router static6

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

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

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

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

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

Fortigate-VM (5) # next

Fortigate-VM (static6) # end

Fortigate-VM # _
```

McAfee Add Static Routes By GUI



McAfee Add Static Routes By GUI

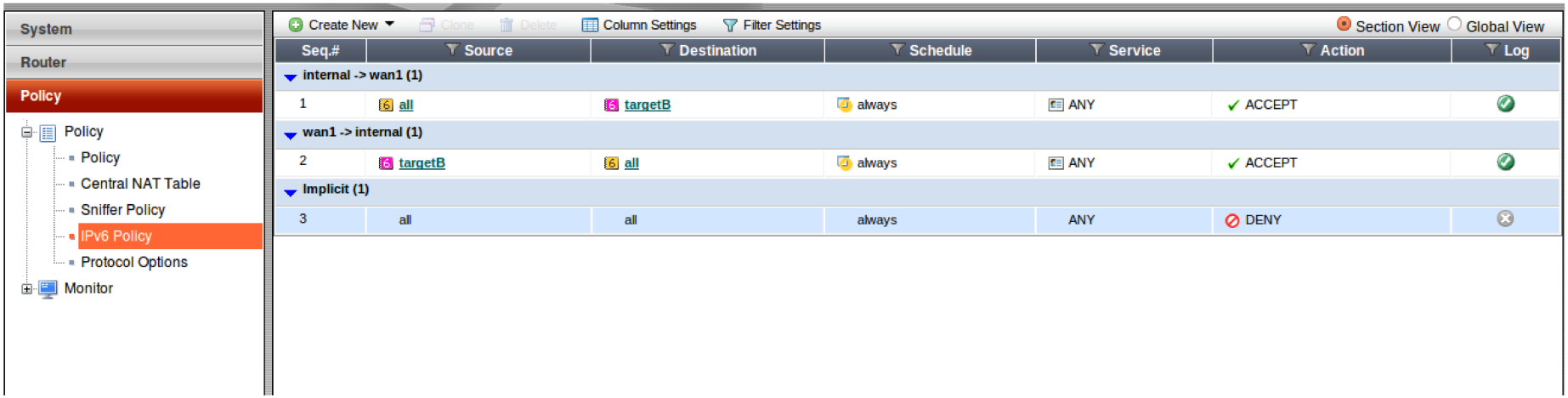


McAfee Add Static Routes By CLI

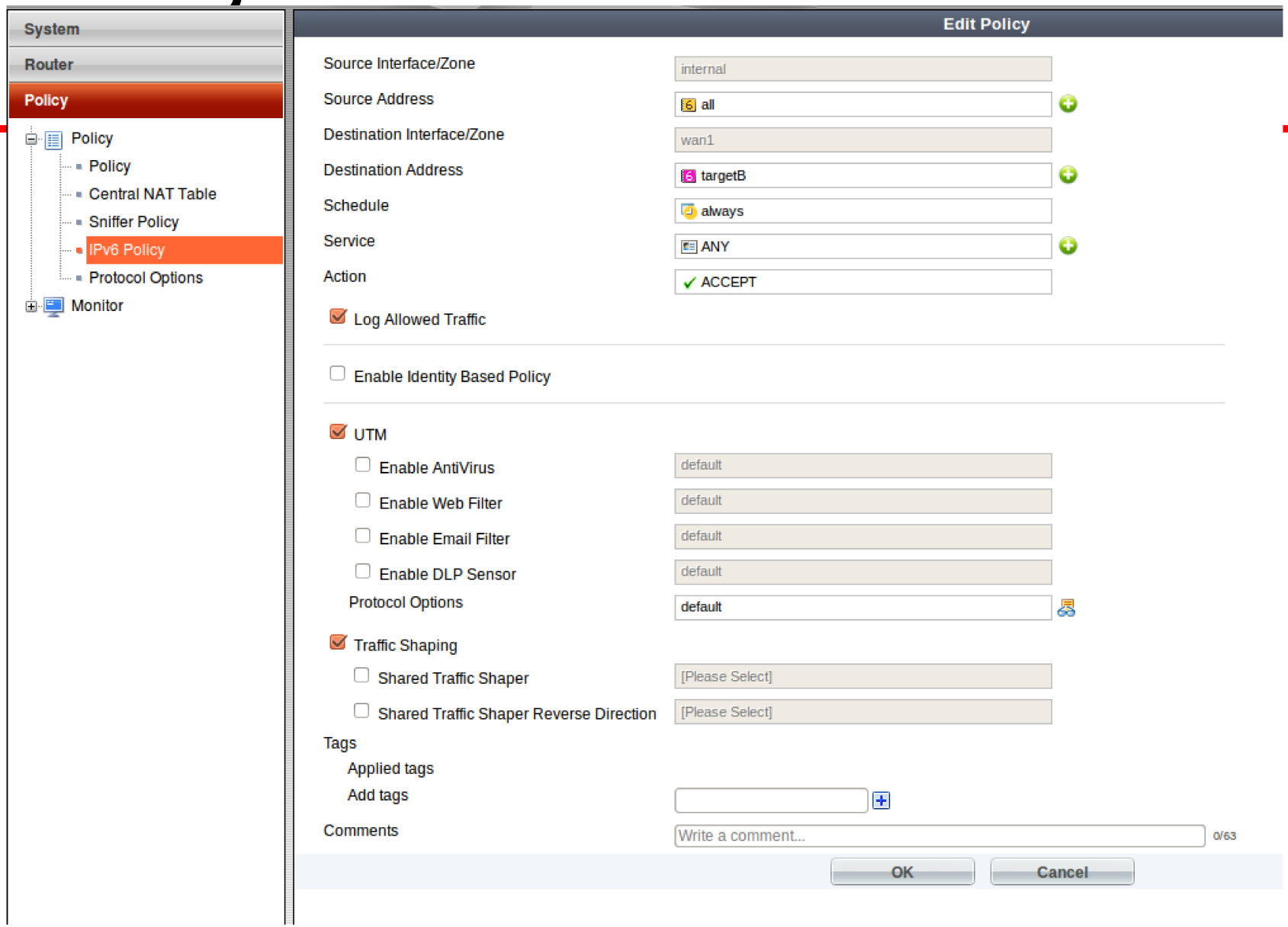
mMcAfee:Admn {3} % cf route add route=2001:db8:ef01:f000::/72 gateway=2001:db8::1 distance=1
route add error: ParameterError: mask 72 is a non-contiguous subnet mask
mMcAfee:Admn {4} % cf route add route=2001:db8:ef01:f000::/78 gateway=2001:db8::1 distance=1
route add error: ParameterError: mask 78 is 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
100**1**000
100**111**0
110**111**

6. FW IPv6 Policies

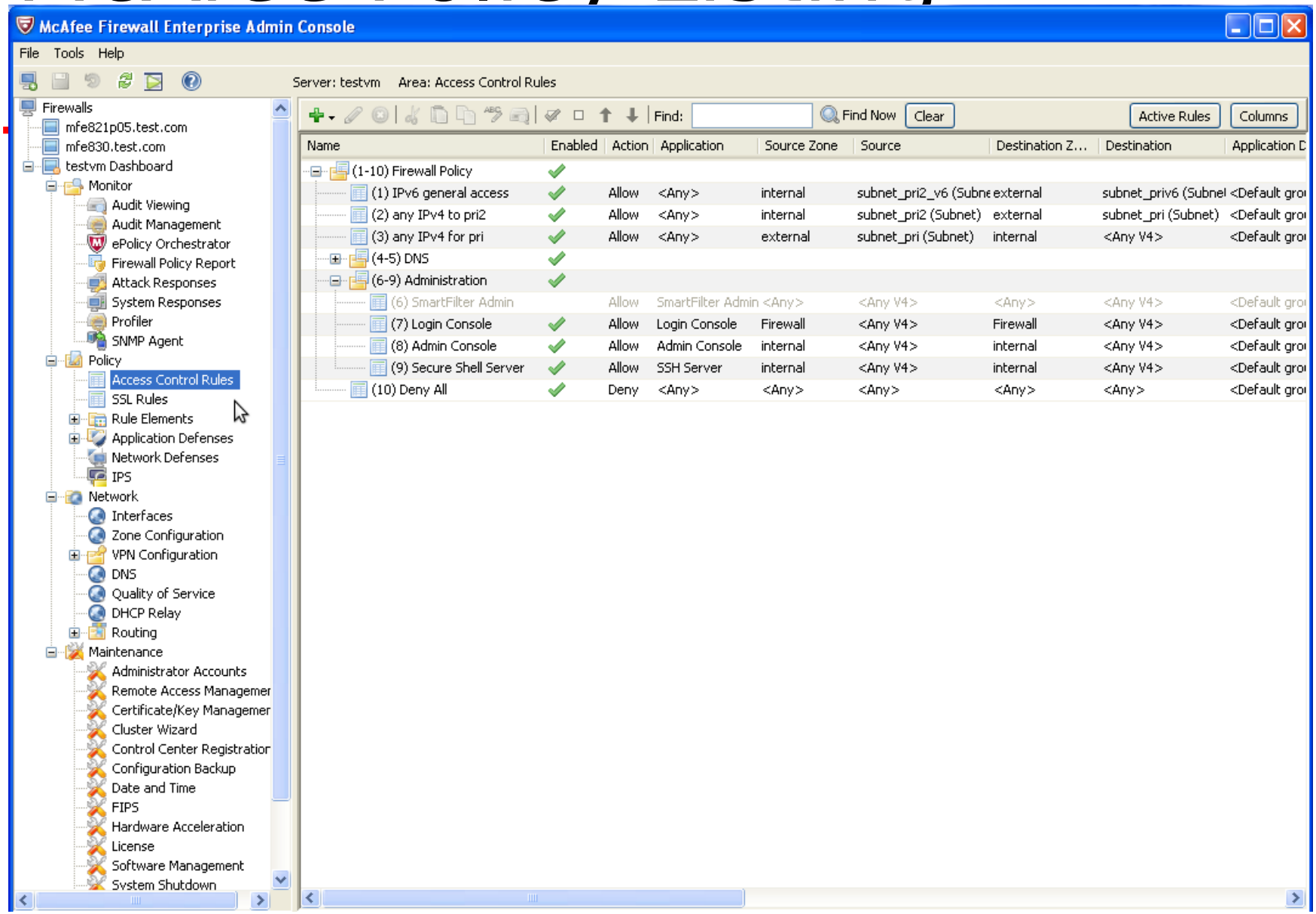
Fortigate policy listing



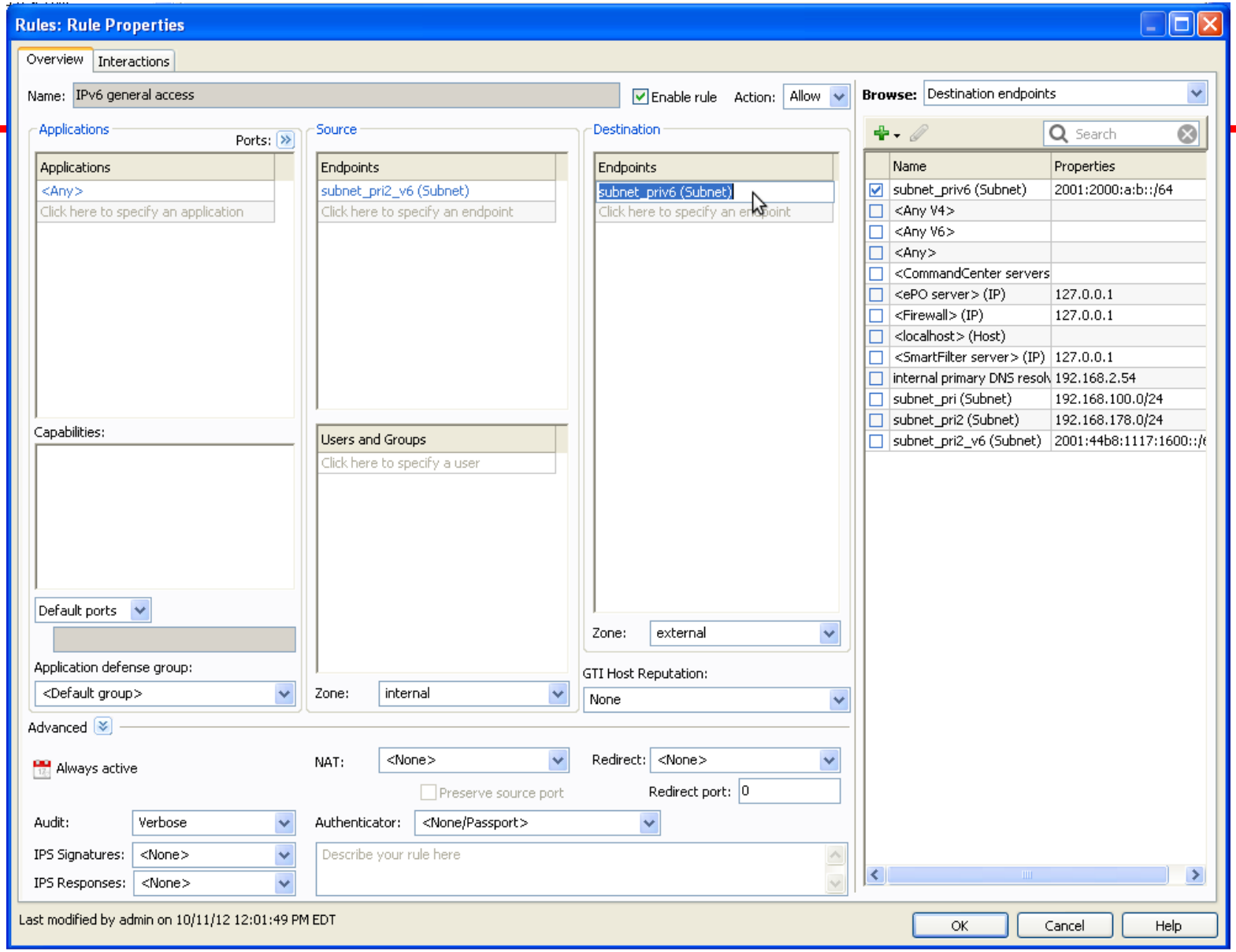
Fortigate IPv6 Rule



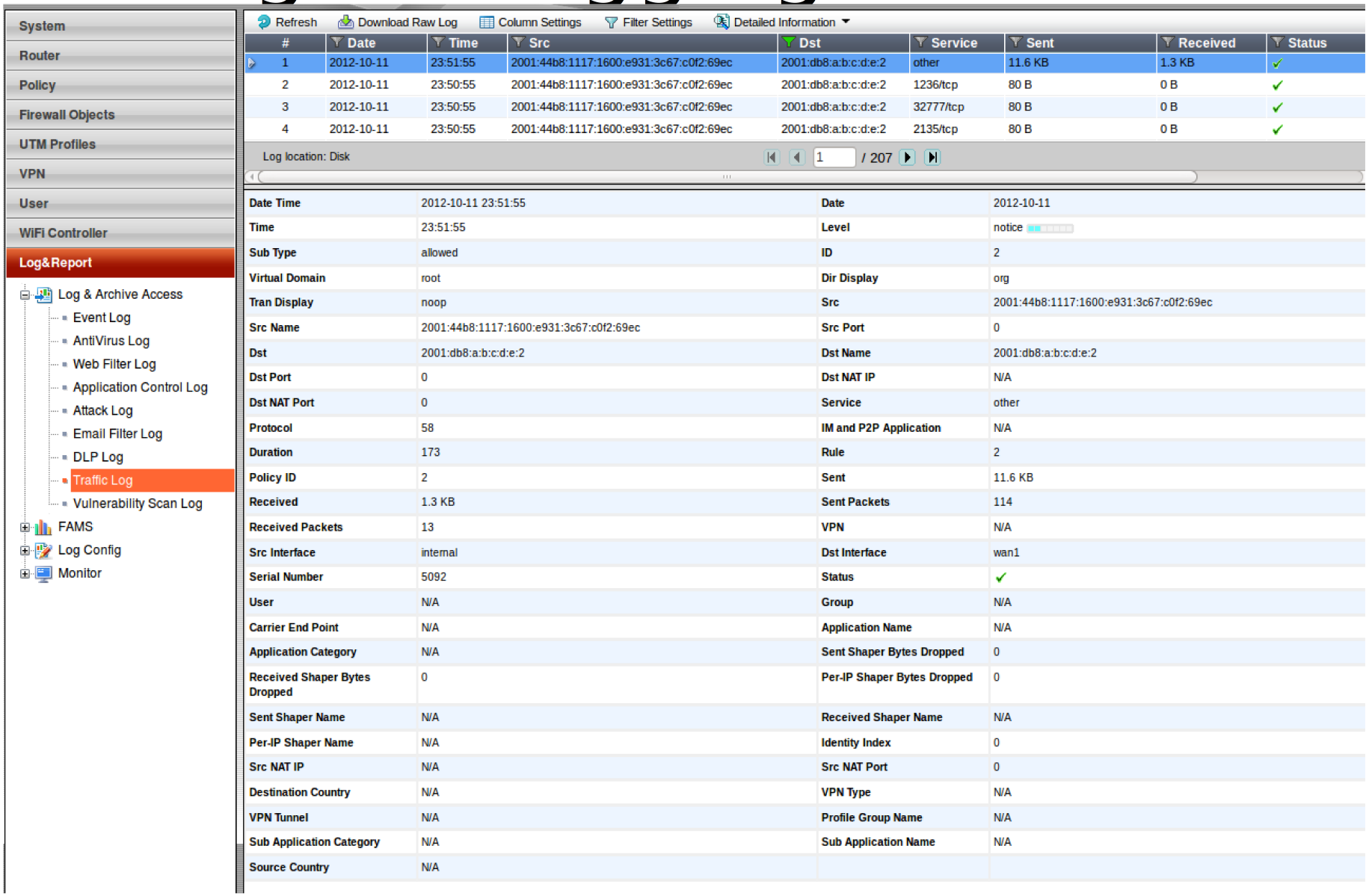
McAfee Policy Listing



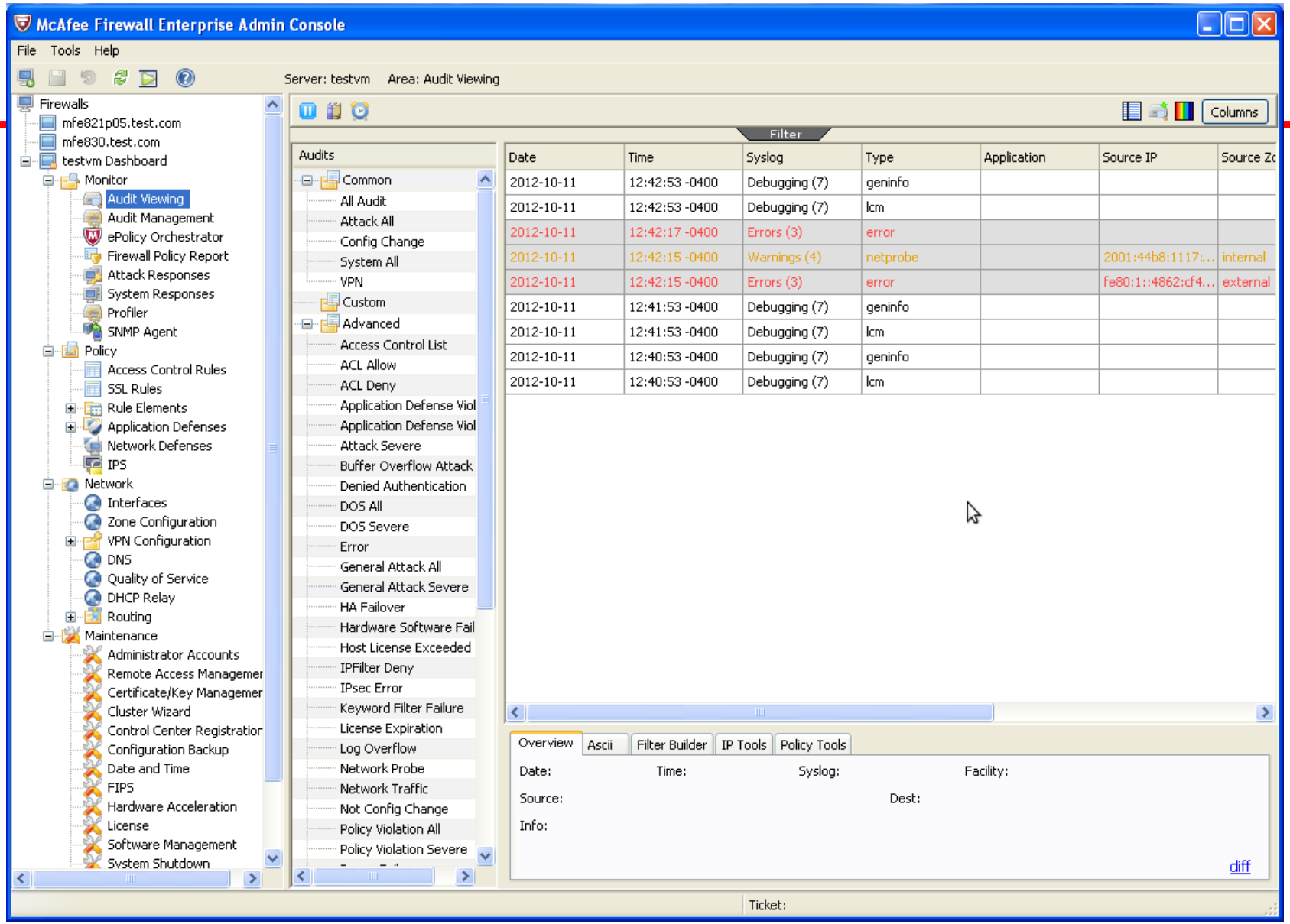
McAfee Rule


Rules: Rule Properties
Overview
Interactions
Name: IPv6 general access
Enable rule
Action: Allow
Browse: Destination endpoints
Applications
Ports:
Applications
<Any>
Click here to specify an application
Capabilities:
Default ports
Application defense group:
<Default group>
Source
Endpoints
subnet_pri2_v6 (Subnet)
Click here to specify an endpoint
Users and Groups
Click here to specify a user
Zone: internal
Destination
Endpoints
subnet_priv6 (Subnet)
Click here to specify an endpoint
Zone: external
GTI Host Reputation:
None
Search
Name
Properties
subnet_priv6 (Subnet) 2001:2000:a:b::/64
<Any V4>
<Any V6>
<Any>
<CommandCenter servers
<ePO server> (IP) 127.0.0.1
<Firewall> (IP) 127.0.0.1
<localhost> (Host)
<SmartFilter server> (IP) 127.0.0.1
internal primary DNS resol 192.168.2.54
subnet_pri (Subnet) 192.168.100.0/24
subnet_pri2 (Subnet) 192.168.178.0/24
subnet_pri2_v6 (Subnet) 2001:44b8:1117:1600::/
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 10/11/12 12:01:49 PM EDT
OK
Cancel
Help

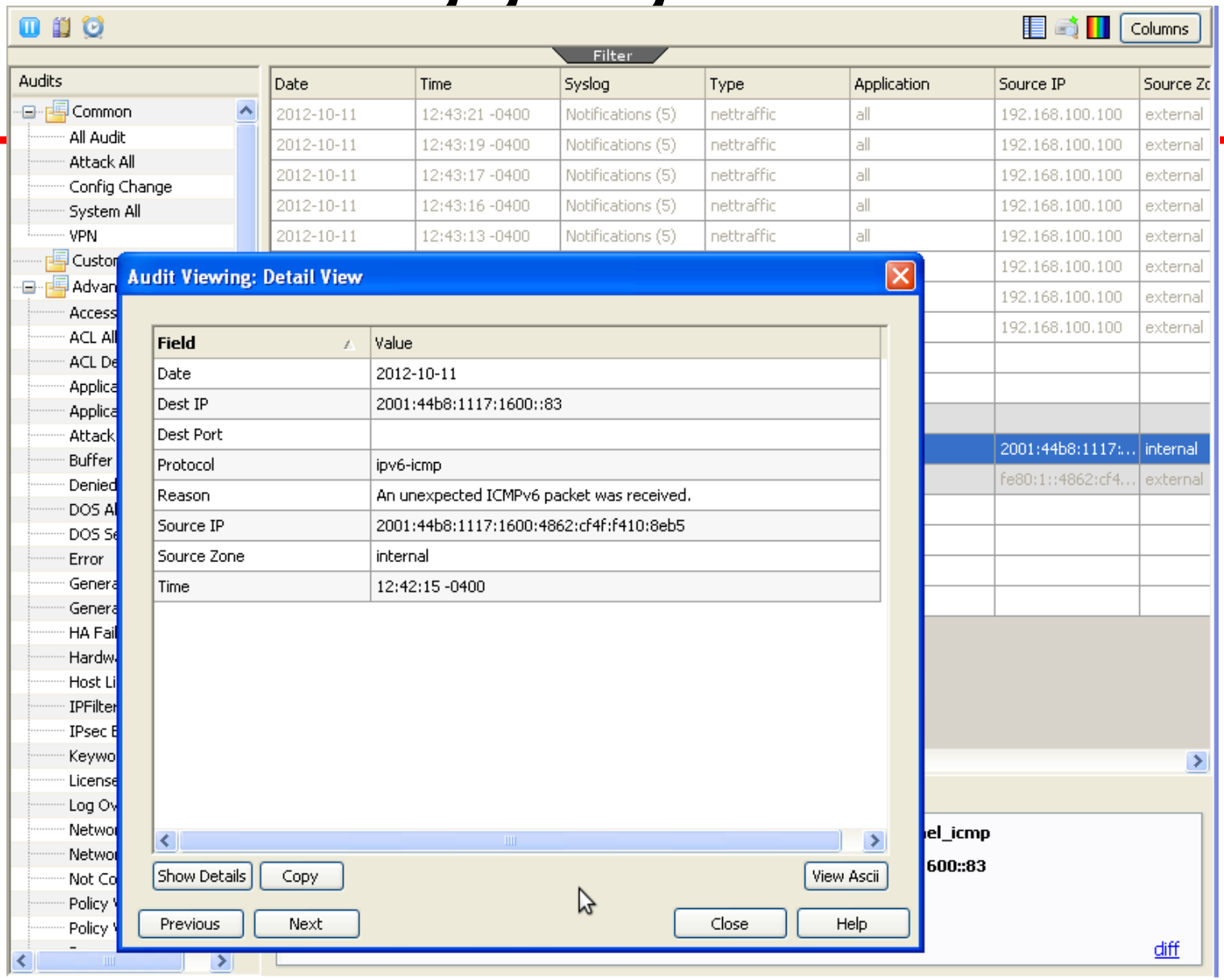
Fortigate Logging



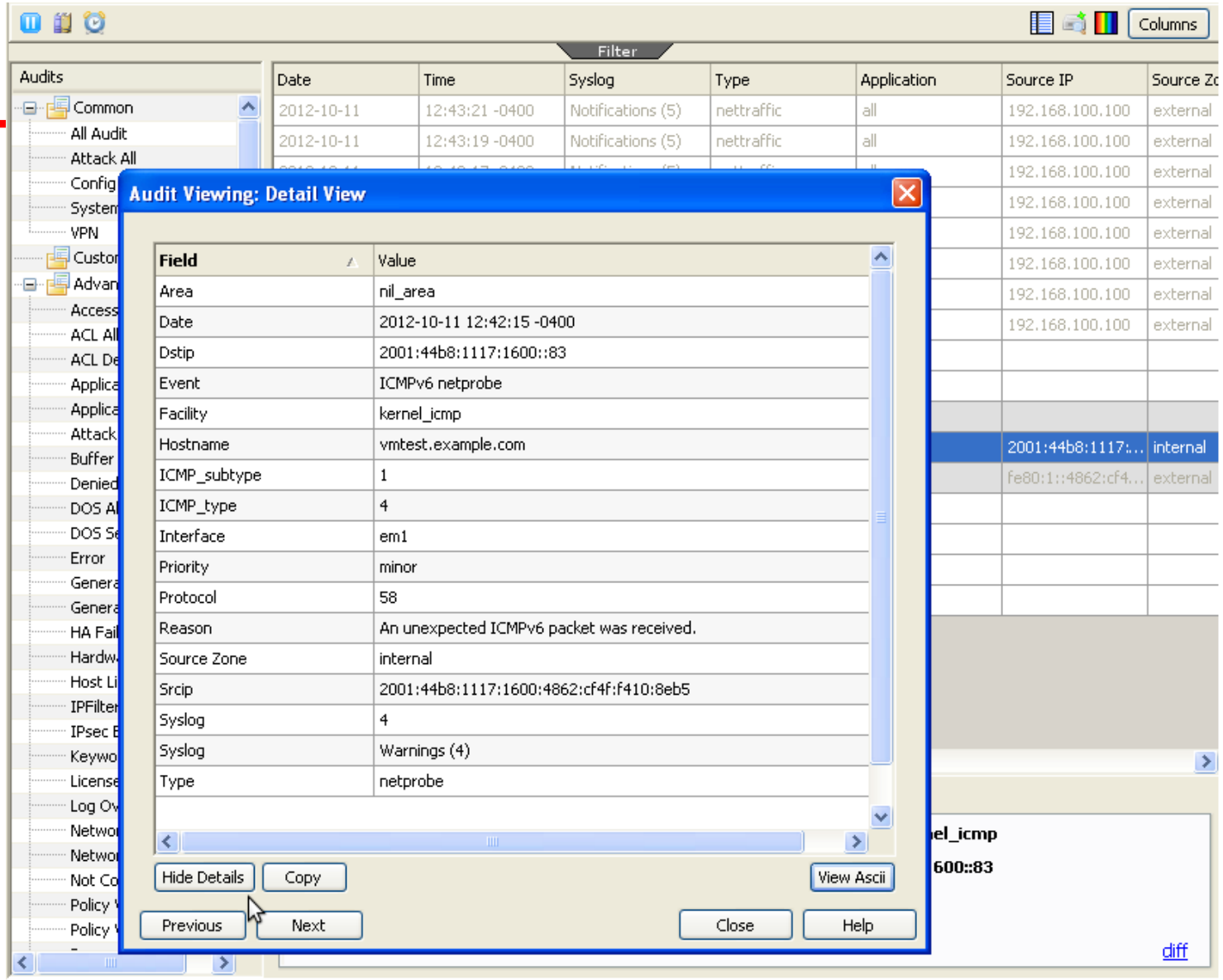
McAfee Logging



McAfee Logging



McAfee Logging



7. Other IPv6 Bits

Fortigate	McAfee
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	Applications - not all support IPv6 DNS Server High Availability: Active/Standby IPv6 NAT/Redirect UTM – IPS + limited Applications protection VPN – Gateway to Gateway