IPv6 on Check Point Security Gateways

Tobias Lachmann

- 34 years old
- Consultant at akquinet system integration GmbH in Hamburg (www.akquinet.de)
- akquinet is an Outsourcing Service Provider / MSP with data centers in Hamburg and nearby
- Main focus on SME customers, mostly in data center environments
- Main platform SPLAT on OpenServer and UTM-1 / Power-1 appliances
- Check Point experience since 2001, certified CCSE/CCSE+ since 2004
- Maybe you have read my Check Point blog on http://blog.lachmann.org?

„IPv6 is supported by Check Point on all versions starting with NGX R60 (except NGX R65 HFA30).“

Source: IPv6 Support FAQ in sk39374

This means Check Point has IPv6 support since 2005.
Let‘s have a look at 6 years of experience….

Denial of Service in combination with IPv6

Important note in sk44718:

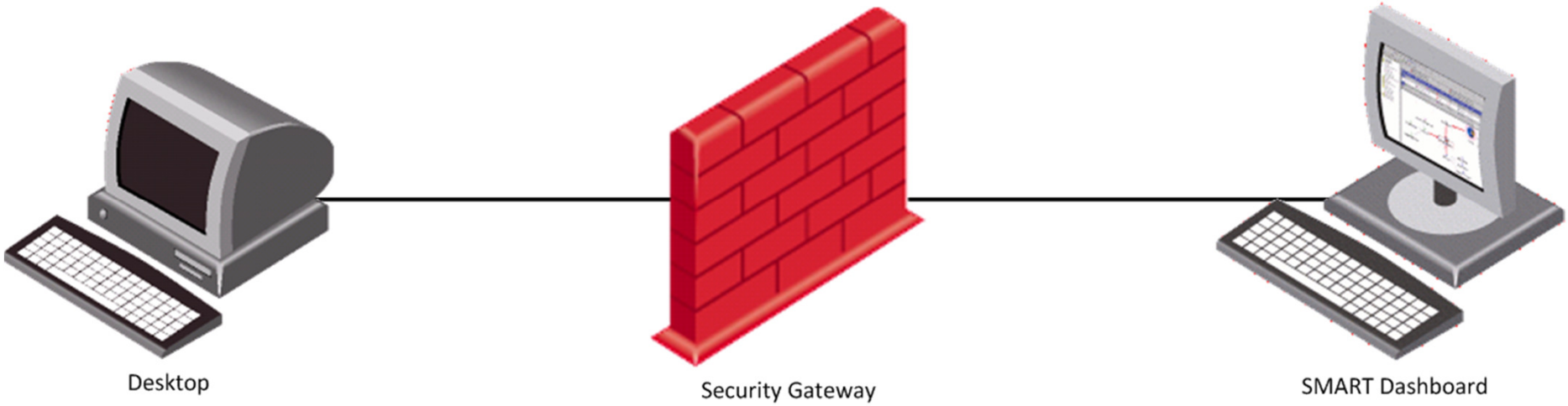
„(…)

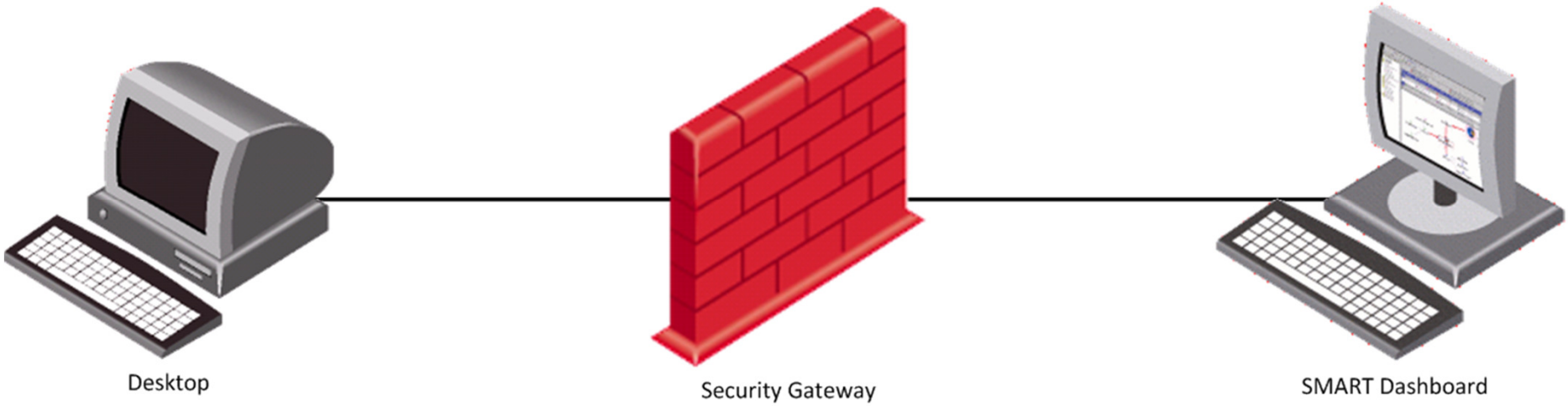
- Linux kernel 2.6 (before 2.6.20) with IPv6 support is vulnerable to Denial of Service attack (kernel panic).
- This vulnerability is relevant to these SecurePlatform based releases: NGX R65 SecurePlatform 2.6, R70.x, and R71.

(…)“

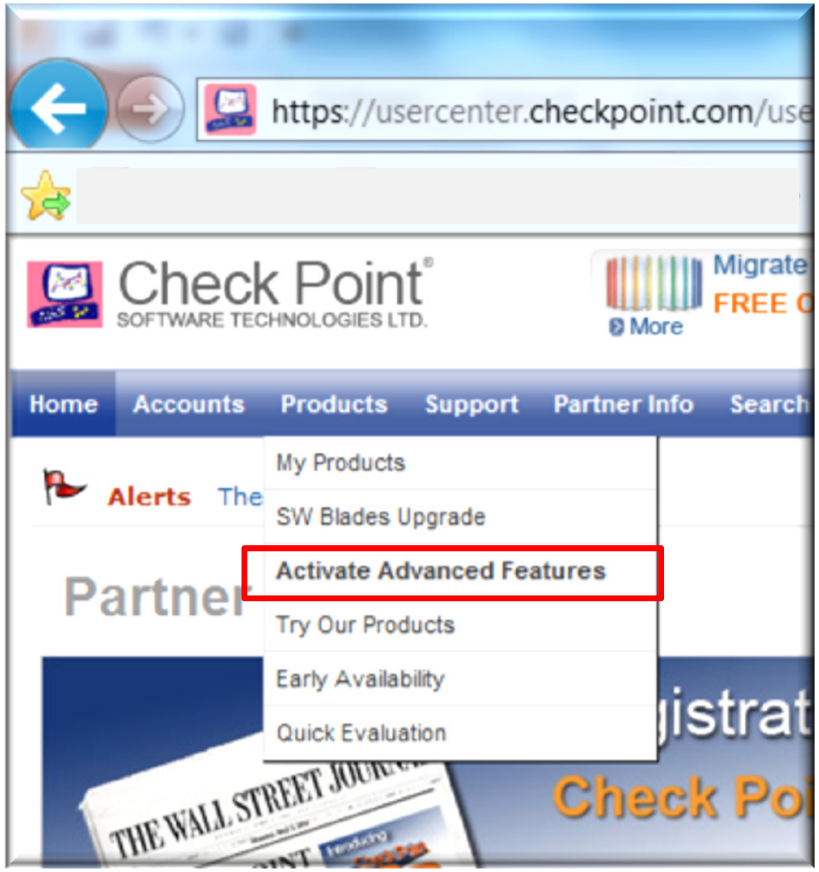
See http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1188 for the description of the vulnerability.

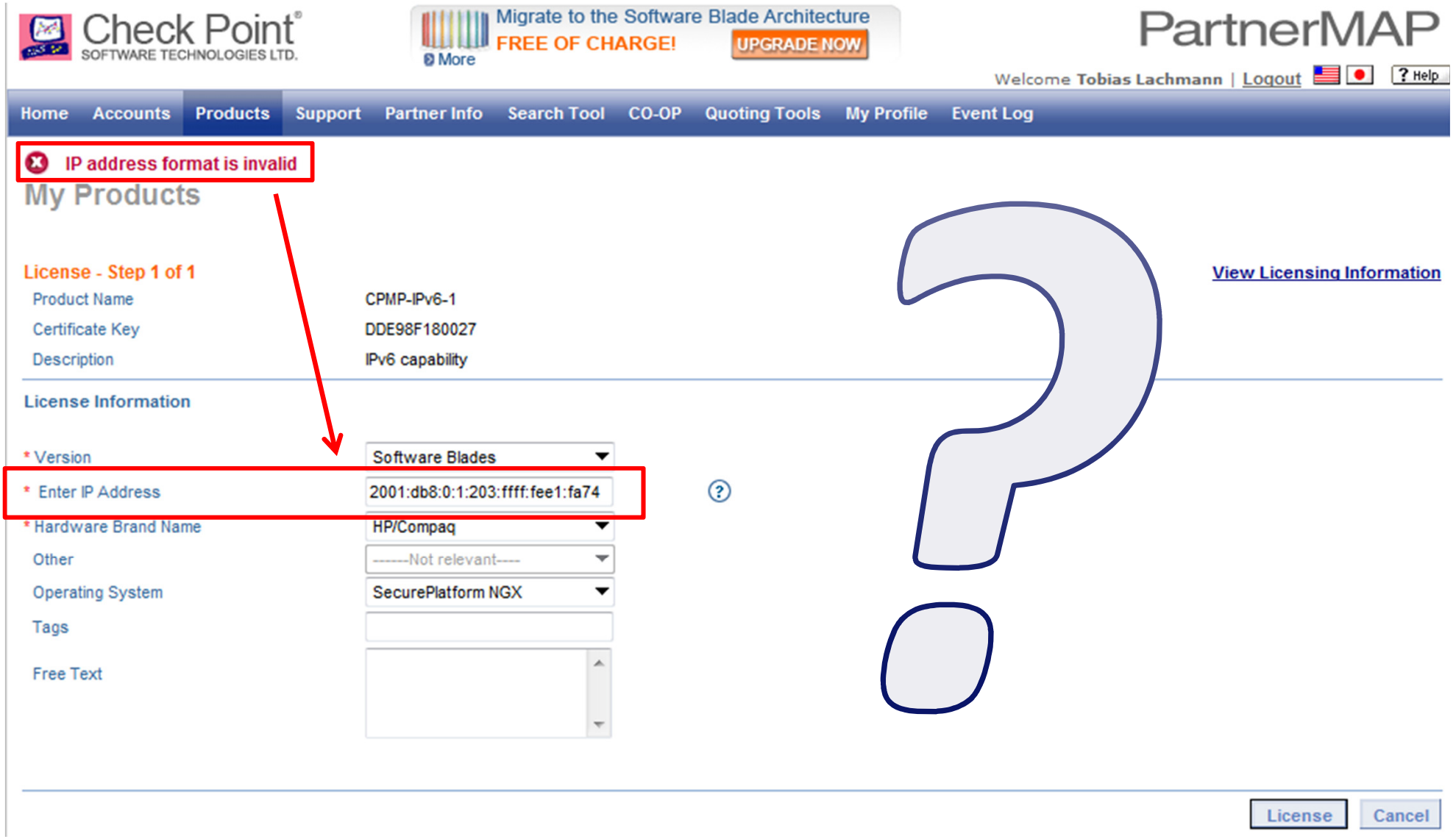
You have to contact Check Point support to get a fix for your version before starting with IPv6.


Desktop
Security Gateway
SMART Dashboard


Desktop
Security Gateway
SMART Dashboard
VMnet2
VMnet5
2001:DB8:0:1::/64
2001:DB8:0:2::/64

- You need IPv6 licenses for Security Management and Security Gateway(s)
- Can be obtained from UserCenter free of charge
- IPv6 license is a local license

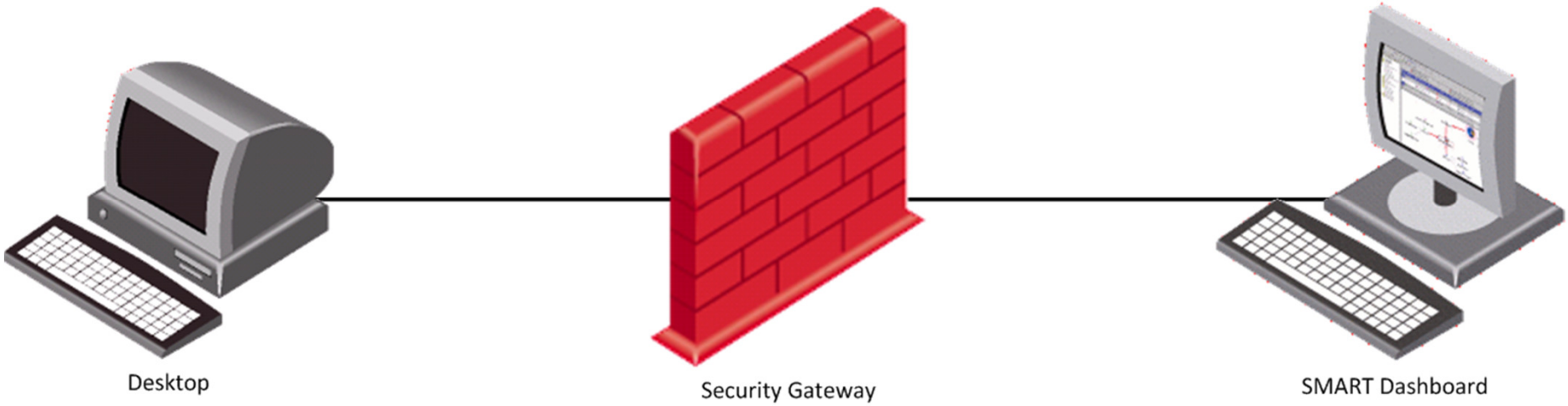



Check Point
SOFTWARE TECHNOLOGIES LTD.
Migrate to the Software Blade Architecture
FREE OF CHARGE!
UPGRADE NOW
More
PartnerMAP
Welcome Tobias Lachmann | Logout
Help
Home
Accounts
Products
Support
Partner Info
Search Tool
CO-OP
Quoting Tools
My Profile
Event Log
IP address format is invalid
My Products
License - Step 1 of 1
View Licensing Information
Product Name
CPMP-IPv6-1
Certificate Key
DDE98F180027
Description
IPv6 capability
License Information
* Version
Software Blades
* Enter IP Address
2001:db8:0:1:203:ffff:fee1:fa74
* Hardware Brand Name
HP/Compaq
Other
------Not relevant-----
Operating System
SecurePlatform NGX
Tags
Free Text
License
Cancel

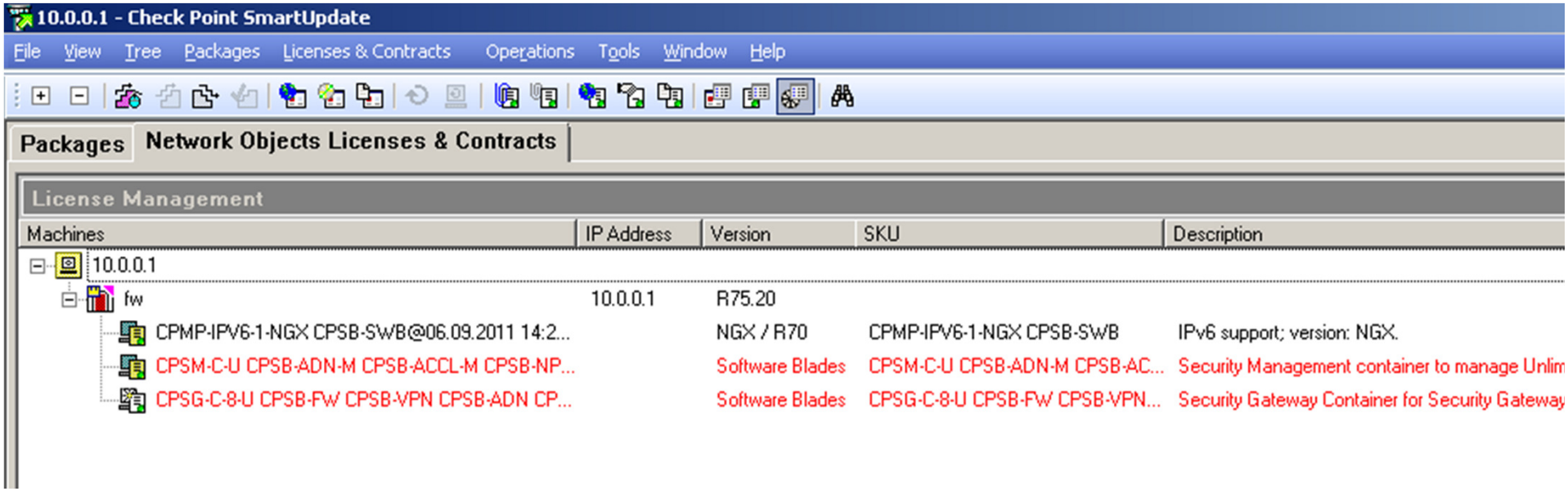
“IPv6 enabled modules must have interfaces configured with valid IPv4 addresses, since all firewall internal communication is IPv4 based.”

Source: R75.20 Firewall Administration Guide, Page 184

- Secure Internal Communication (SIC) is IPv4-based!
- No IPv6-only Gateway possible!

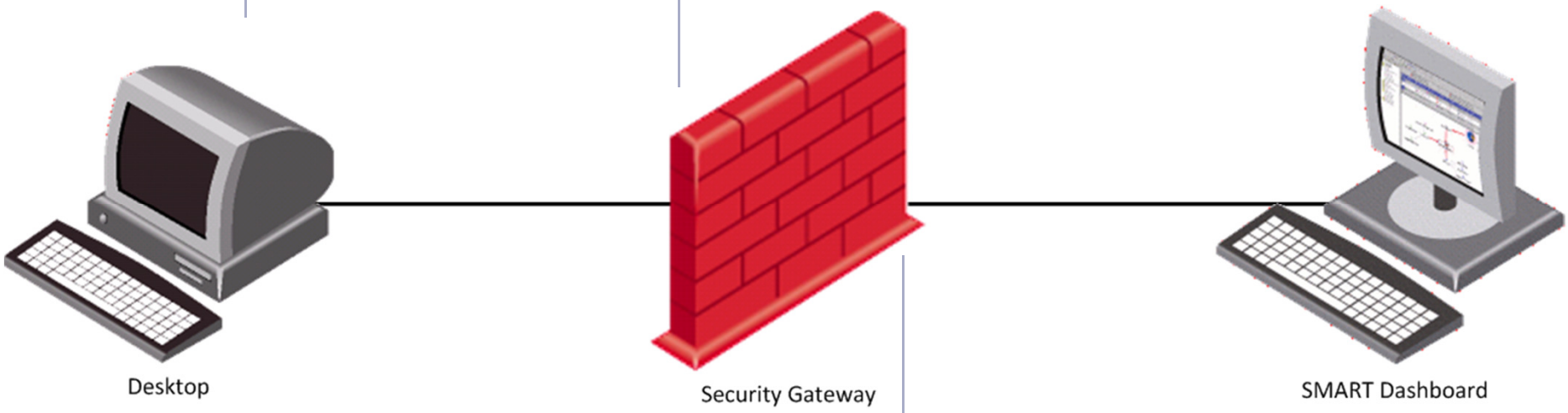

Desktop
Security Gateway
SMART Dashboard
.250
.1
.1
.250
VMnet2
VMnet5
131.107.0.0/24
10.0.0.0/24

- Install Security Gateway and Security Management
- Configure IPv4 addresses
- Connect with SmartUpdate
- Attach licenses



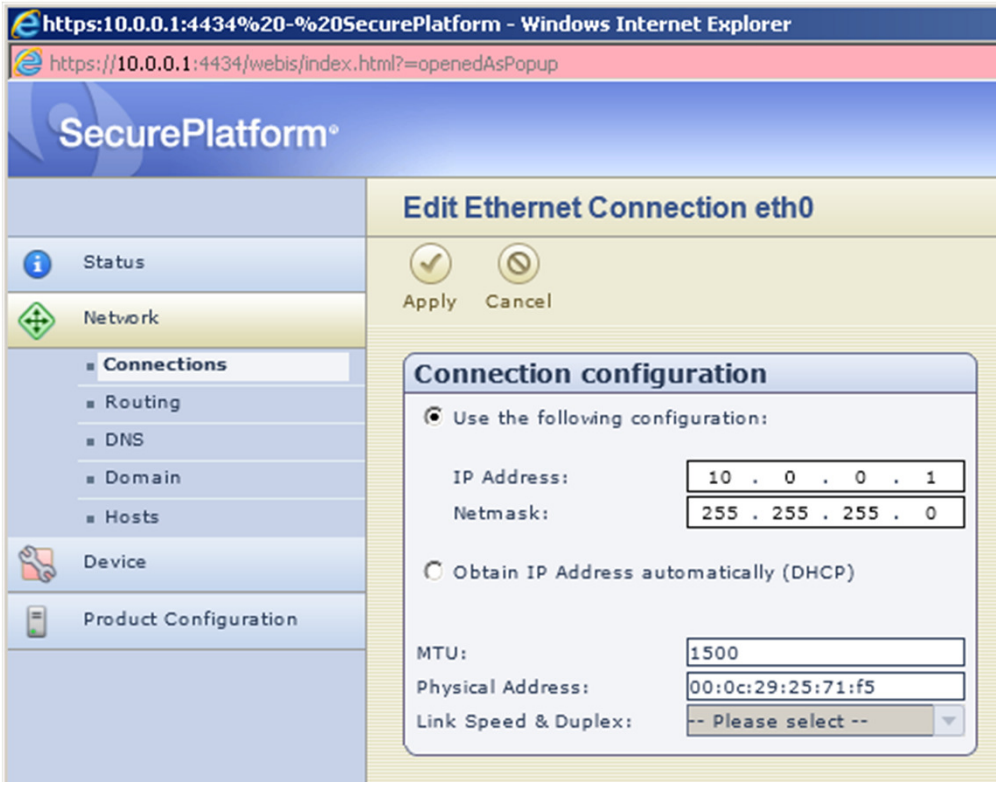
2001:DB8:0:1:203:ffff:fee1:2222

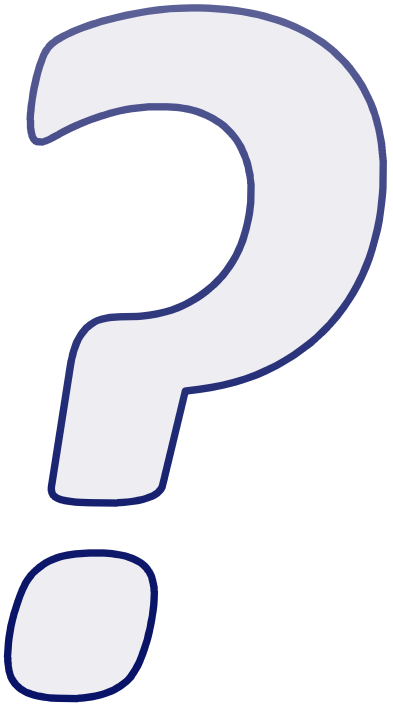
2001:DB8:0:1:203:ffff:fee1:4444



2001:DB8:0:2:203:abcd:fee1:3333

2001:DB8:0:2:203:abcd:fee1:5555





Where can I configure IPv6 addresses?

“The sysconfig utility does not support IPv6 configurations, neither using the CLI nor using the SecurePlatform Web UI. Instead, use Linux commands. For example, to add routes use "ip -6 route" or "route -A inet6". To preserve the configuration after reboot, add the commands to the S11IPv6 file located at /etc/rc.d/rc3.”

Source: R70 IPv6Pack Release Notes, Page 23, Known Limitations - ID 00504964

Please note:

All configuration made for IPv6 is not automatically backuped by the Check Point build-in backup utility! You have to make a backup by your own.

This applies for interface configuration as well as routing information.

Enabling IPv6 on the Gateway

- `touch /etc/rc.d/rc3.d/S11ipv6`
- `vi /etc/rc.d/rc3.d/S11ipv6`
- Add these commands to the file:

```
#!/bin/sh
modprobe ipv6
/sbin/ifconfig eth0 inet6 add 2001:DB8:0:2:203:abcd:fee1:3333/64
/sbin/ifconfig eth1 inet6 add 2001:DB8:0:1:203:ffff:fee1:4444/64
```

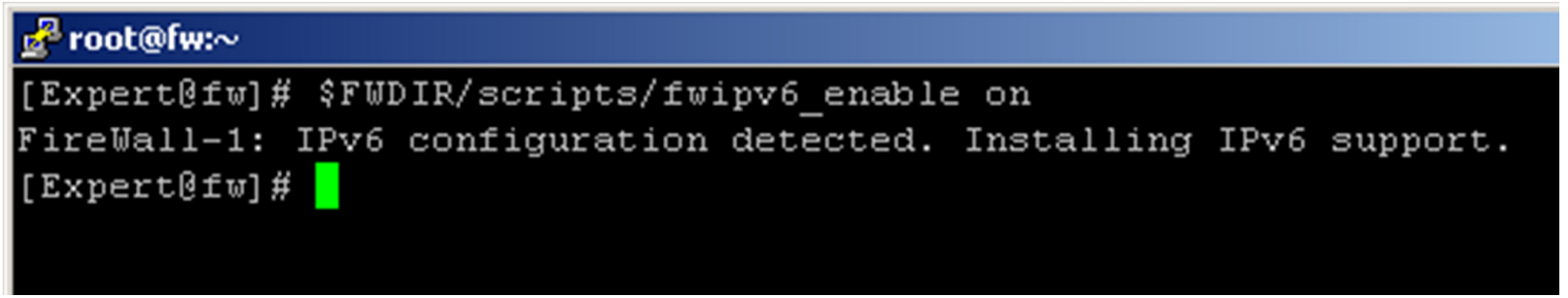
- `chmod +x /etc/rc.d/rc3.d/S11ipv6`

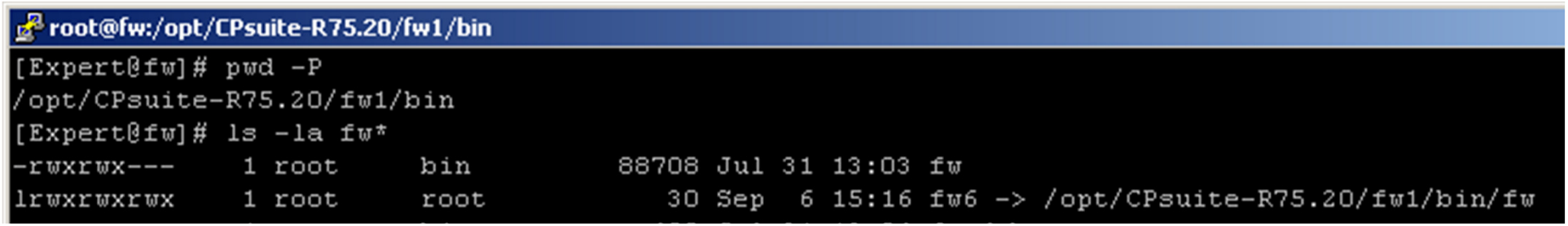
Setting IPv6 default route

- Add the following to **`/etc/rc.d/rc3.d/S11ipv6`**

```
ip -6 route add 2000::/3 via <gateway IPv6 address> metric 1
```

- Run **`/etc/rc.d/rc3.d/S11ipv6`**
- Enable IPv6 by running the command
  `$FWDIR/scripts/fwipv6_enable on`





- Reboot

Source: R75.20 Firewall Administration Guide, Page 185

```
[Expert@fw]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:25:71:F5
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: 2001:DB8:0:2:203:abcd:fee1:3333/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe25:71f5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1539 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1388 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:163291 (159.4 Kb)  TX bytes:181289 (177.0 Kb)
          Interrupt:67 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0C:29:25:71:FF
          inet addr:131.107.0.1  Bcast:131.107.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe25:71ff/64 Scope:Link
          inet6 addr: 2001:DB8:0:1:203:ffff:fee1:4444/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1676 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1479 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:173801 (169.7 Kb)  TX bytes:197364 (192.7 Kb)
          Interrupt:75 Base address:0x2080
```

Do you like auto-configuration of IPv6 addresses?

Sure!

But I don‘t like my Security Systems to be configured that way!!!

Secure Platform is reacting on Router Advertisement (RA) messages and configures IPv6 addresses with EUI-64 and no Privacy Extension. It also configures the Default Route.

While this behaviour changes on the Security Gateway when IPv6 forwarding is turned on, it‘s still active on Security Management if IPv6 is enabled.

„To disable Stateless Address Auto Configuration on the Security Gateway:

1. In **`/etc/rc.d/rc3.d/S10network`**, before the comment:

   ```
   #Disable sending gratuitous arp upon bond failover in CXL configuration
   ```

   Add:

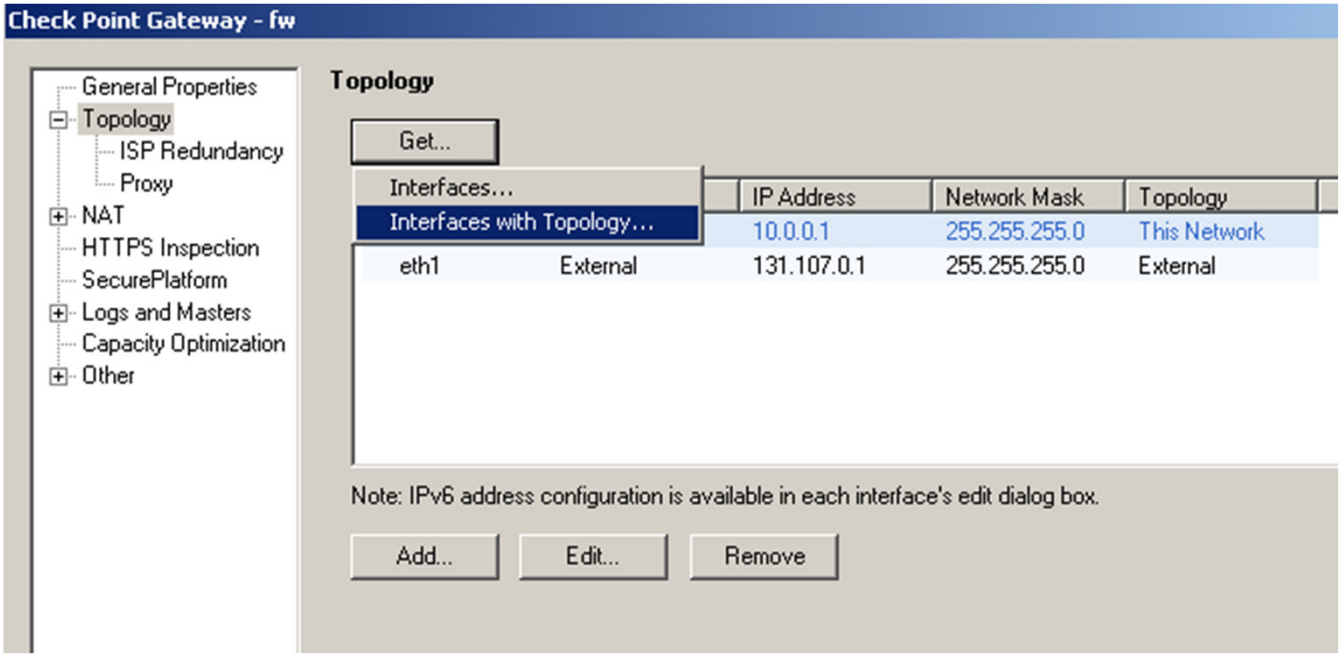
   ```
   echo "0"> /proc/sys/net/ipv6/conf/all/autoconf
   echo "0"> /proc/sys/net/ipv6/conf/default/autoconf
   ```

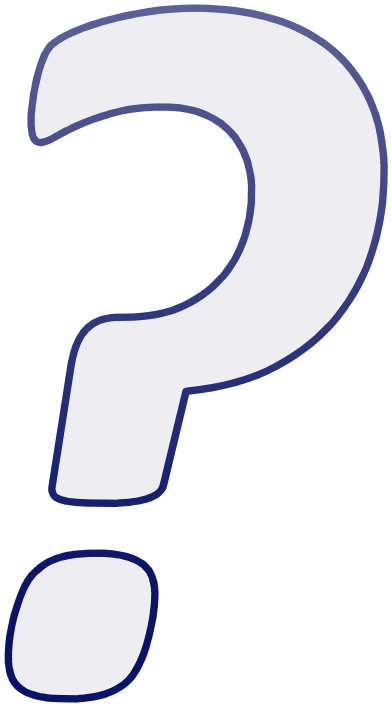
2. Also, add the following lines, one for each interface:

   ```
   echo "0"> /proc/sys/net/ipv6/conf/eth0/autoconf
   echo "0"> /proc/sys/net/ipv6/conf/eth1/autoconf
   ...
   echo "0"> /proc/sys/net/ipv6/conf/ethX/autoconf
   ```

3. Reboot.“

Source: R70 IPv6Pack Release Notes, Page 19

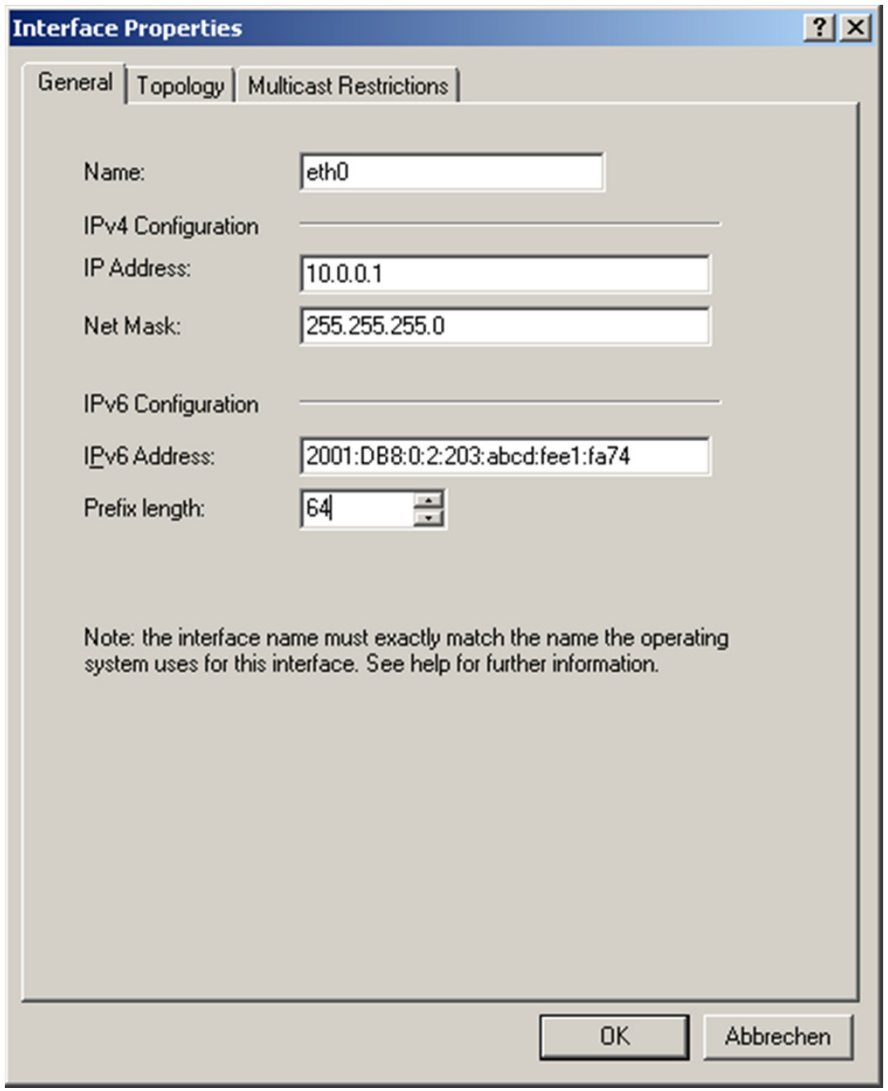


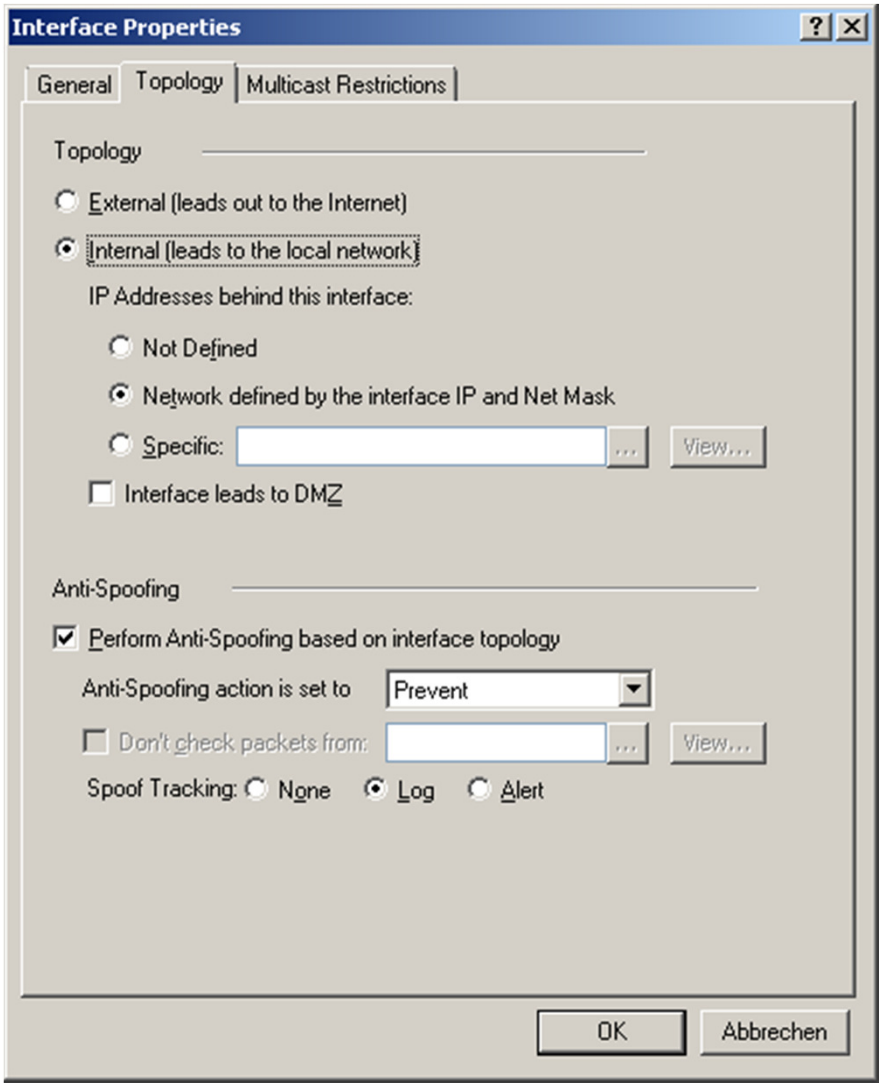


Why are there no IPv6 addresses?

“In SmartDashboard, automatic configuration of IPv6 topology (the "Get Topology" option) is not supported. You must manually configure the IPv6 interfaces.”

Source: R70 IPv6Pack Release Notes, Page 25, Known Limitations - ID **00504542**


Interface Properties
General
Topology
Multicast Restrictions
Name:
eth0
IPv4 Configuration
IP Address:
10.0.0.1
Net Mask:
255.255.255.0
IPv6 Configuration
IPv6 Address:
2001:DB8:0:2:203:abcd:fee1:fa74
Prefix length:
64
Note: the interface name must exactly match the name the operating system uses for this interface. See help for further information.
OK
Abbrechen


Interface Properties
General
Topology
Multicast Restrictions
Topology
External (leads out to the Internet)
Internal (leads to the local network)
IP Addresses behind this interface:
Not Defined
Network defined by the interface IP and Net Mask
Specific:
View...
Interface leads to DMZ
Anti-Spoofing
Perform Anti-Spoofing based on interface topology
Anti-Spoofing action is set to
Prevent
Don't check packets from:
View...
Spoof Tracking:
None
Log
Alert
OK
Abbrechen

“These features are not supported for IPv6 traffic:

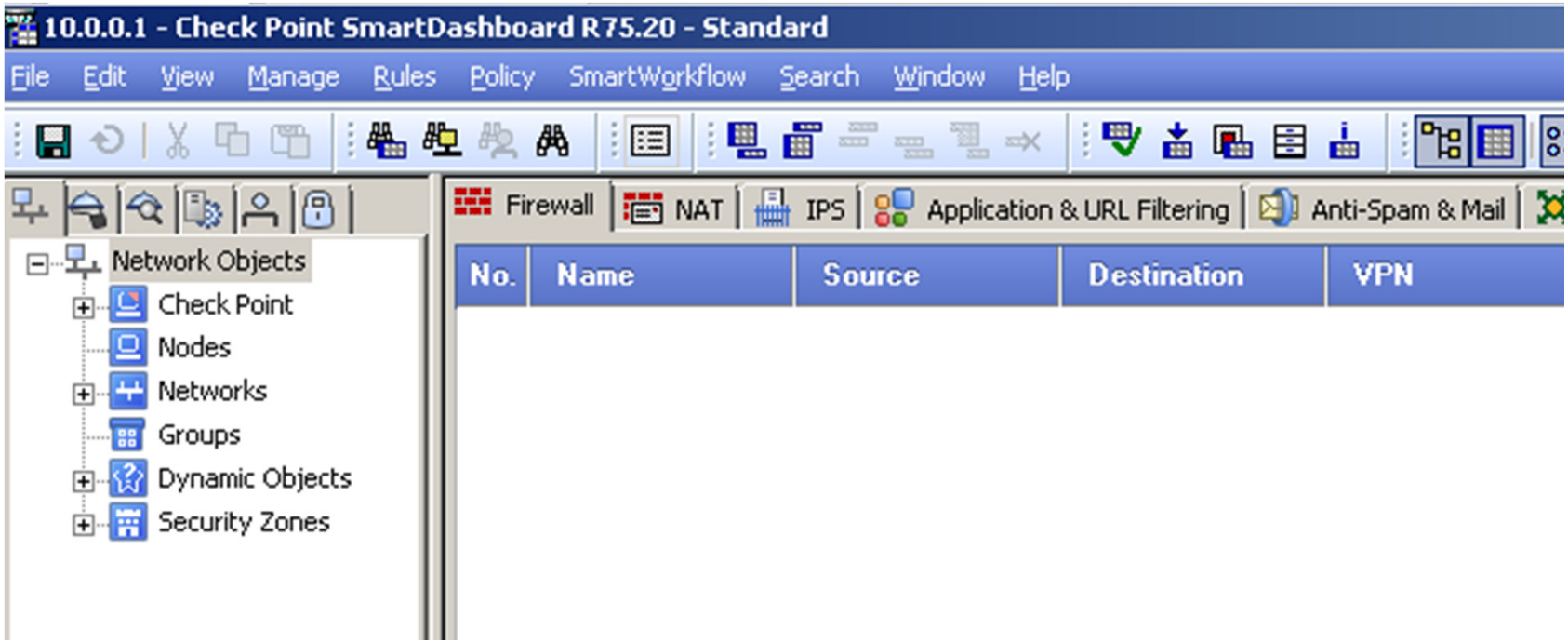
- **(…)**
- **Anti-spoofing**
- **(…)”**

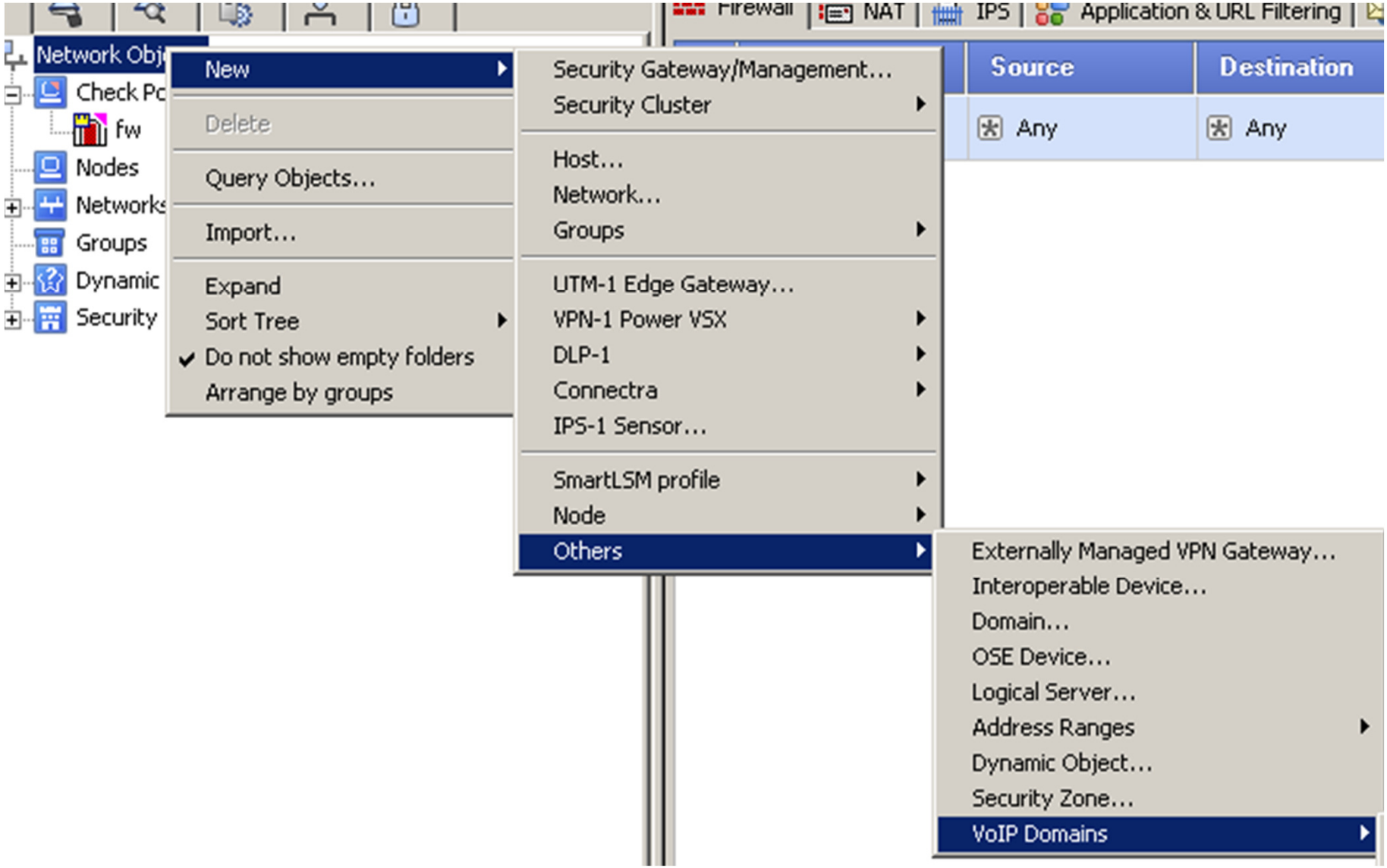
Source: R75.20 Firewall Administration Guide, Page 184

„SmartDashboard has no option to create IPv6 or IPv6 group“

Source: sk35201

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk35201

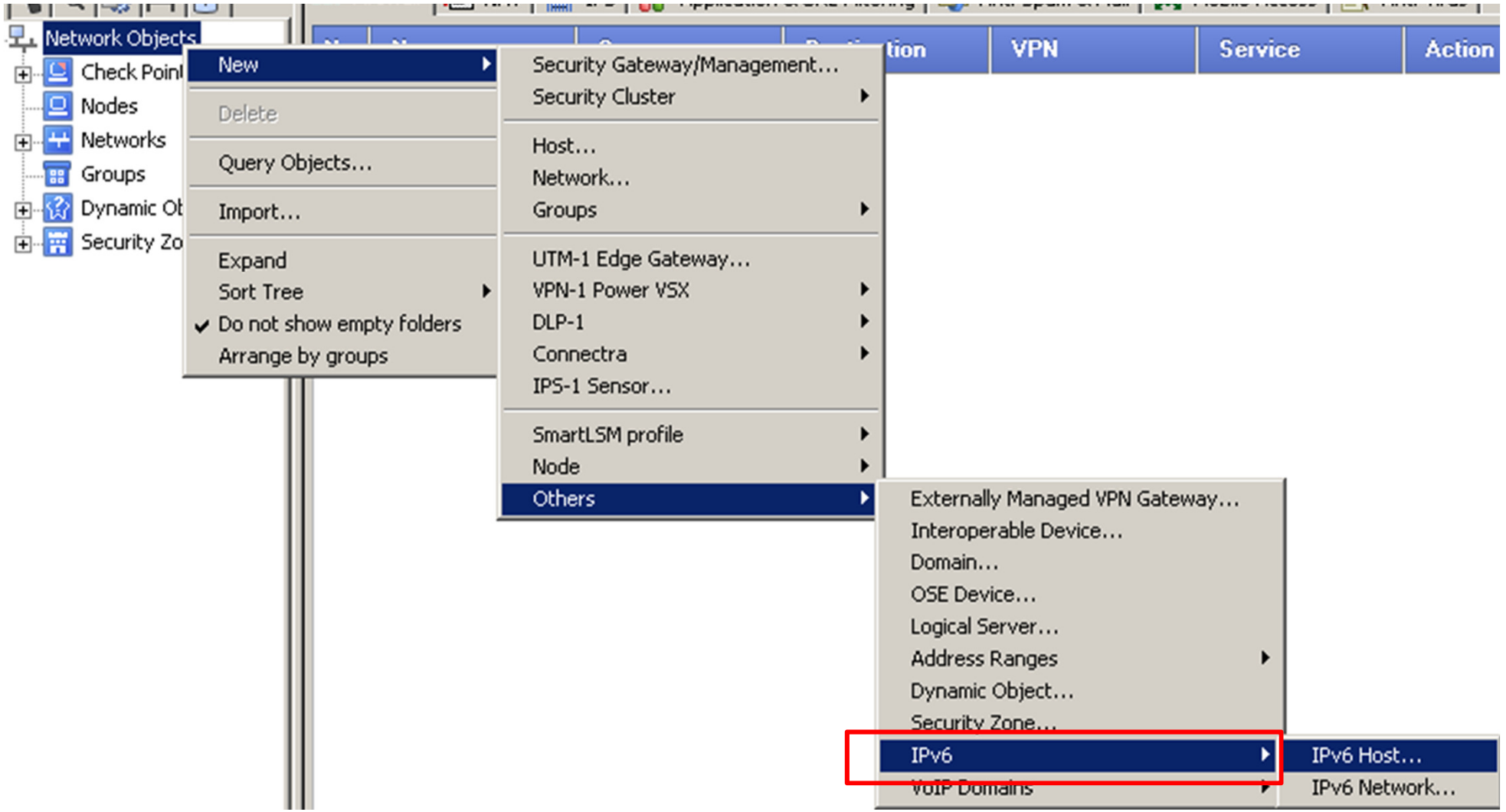


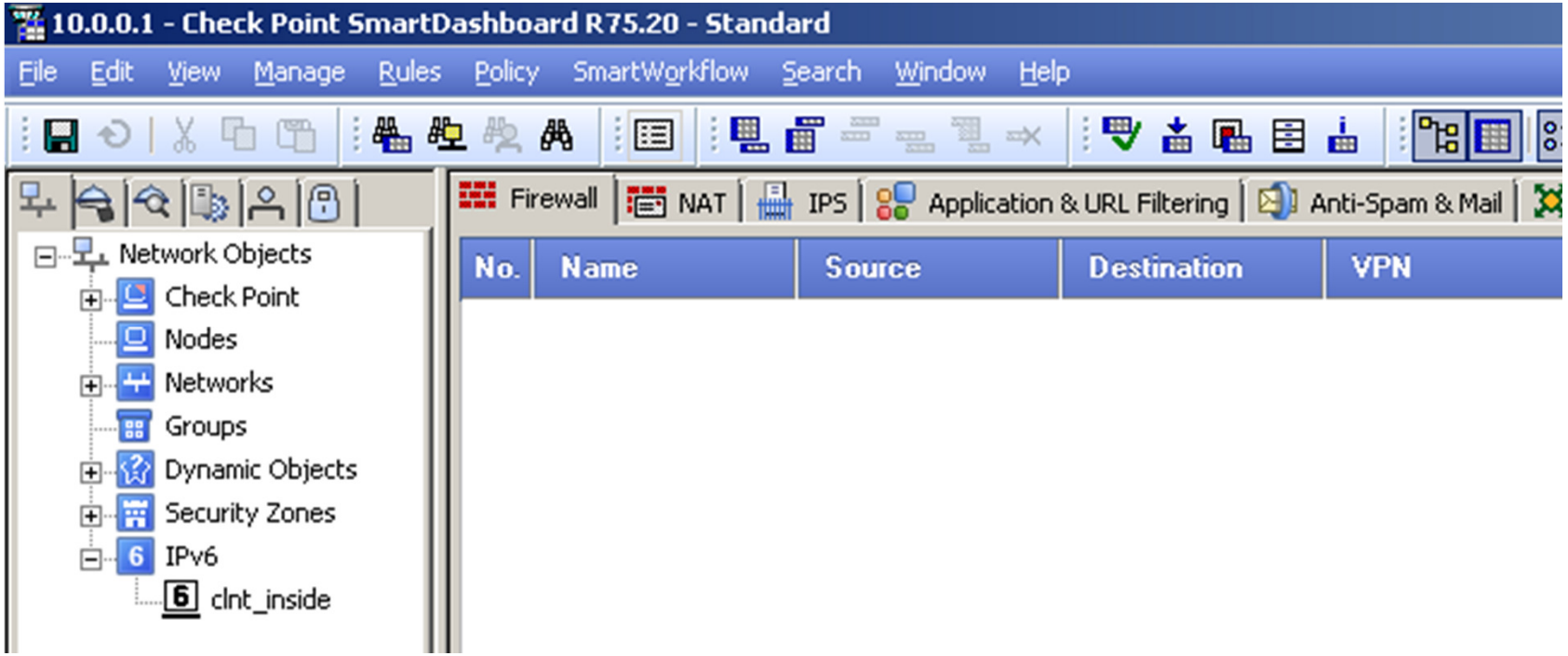

Firewall
NAT
IPS
Application & URL Filtering
Network Obj
Check Pc
fw
Nodes
Networks
Groups
Dynamic
Security
Source
Destination
Any
Any
New
Delete
Query Objects...
Import...
Expand
Sort Tree
Do not show empty folders
Arrange by groups
Security Gateway/Management...
Security Cluster
Host...
Network...
Groups
UTM-1 Edge Gateway...
VPN-1 Power VSX
DLP-1
Connectra
IPS-1 Sensor...
SmartLSM profile
Node
Others
Externally Managed VPN Gateway...
Interoperable Device...
Domain...
OSE Device...
Logical Server...
Address Ranges
Dynamic Object...
Security Zone...
VoIP Domains

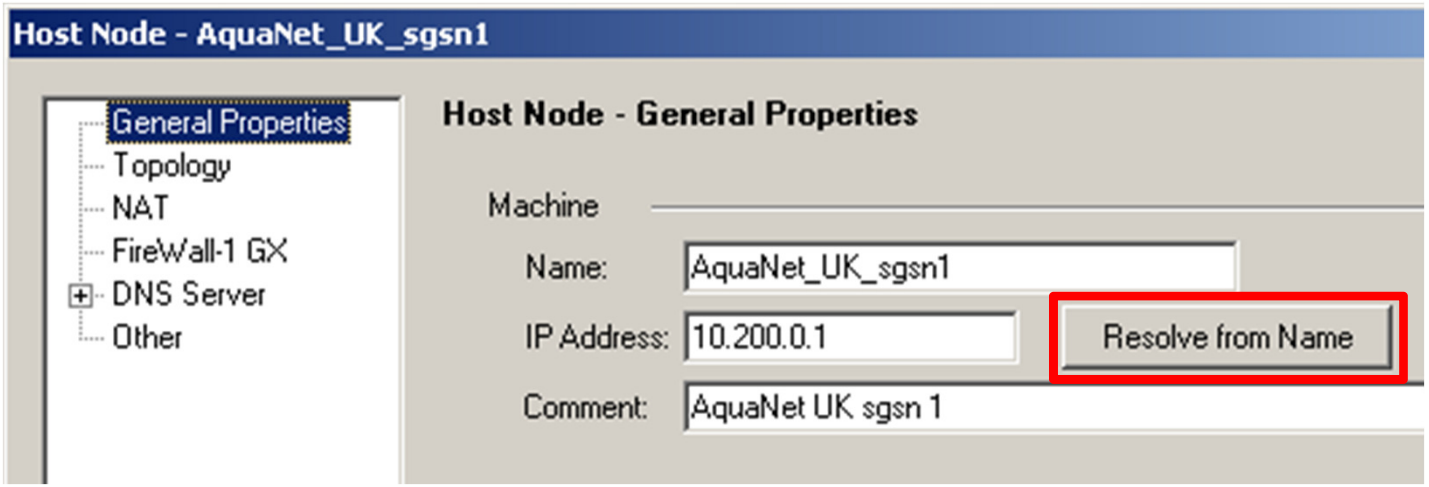
„(…) After the first object is created, the group will show up and other objects may be added from there. To create the first object right-click Network Objects > New> Others > IPv6. A new category should be created titled IPv6 and the new object should be shown. “

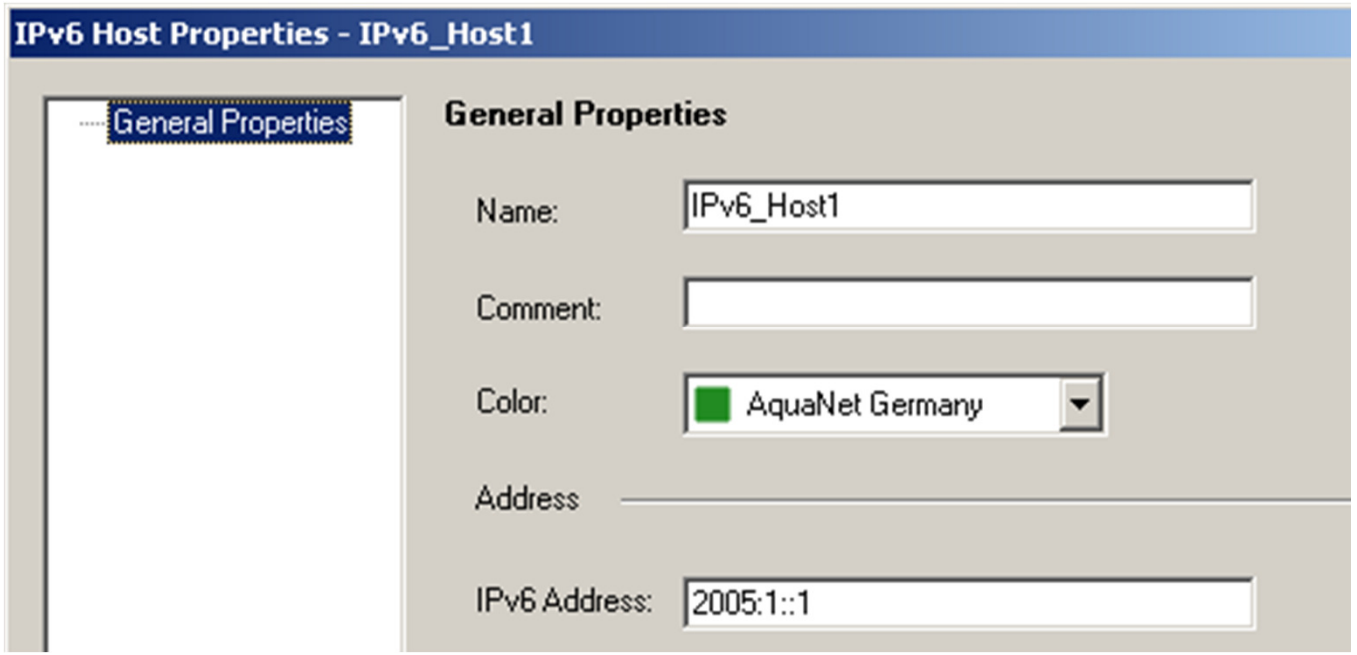
Source: sk35201

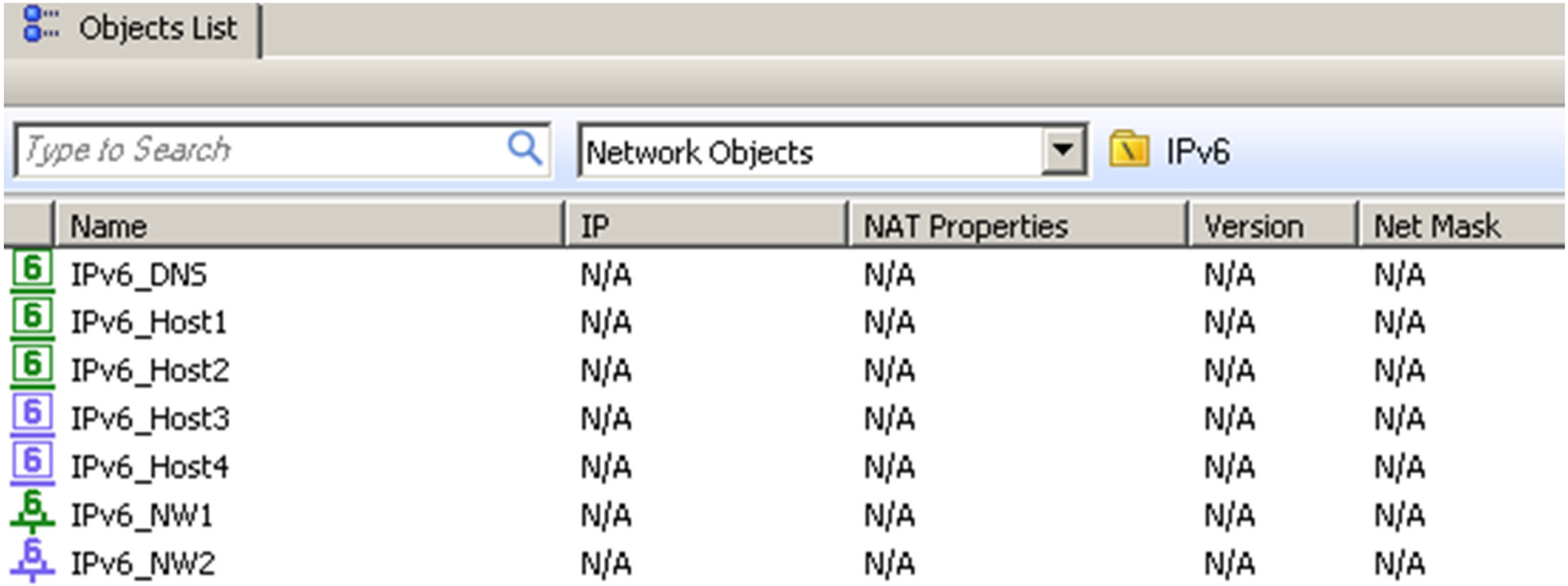
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk35201


Network Objects
Check Point
Nodes
Networks
Groups
Dynamic Ob
Security Zo
VPN
Service
Action
New
Delete
Query Objects...
Import...
Expand
Sort Tree
Do not show empty folders
Arrange by groups
Security Gateway/Management...
Security Cluster
Host...
Network...
Groups
UTM-1 Edge Gateway...
VPN-1 Power VSX
DLP-1
Connectra
IPS-1 Sensor...
SmartLSM profile
Node
Others
Externally Managed VPN Gateway...
Interoperable Device...
Domain...
OSE Device...
Logical Server...
Address Ranges
Dynamic Object...
Security Zone...
IPv6
VoIP Domains
IPv6 Host...
IPv6 Network...

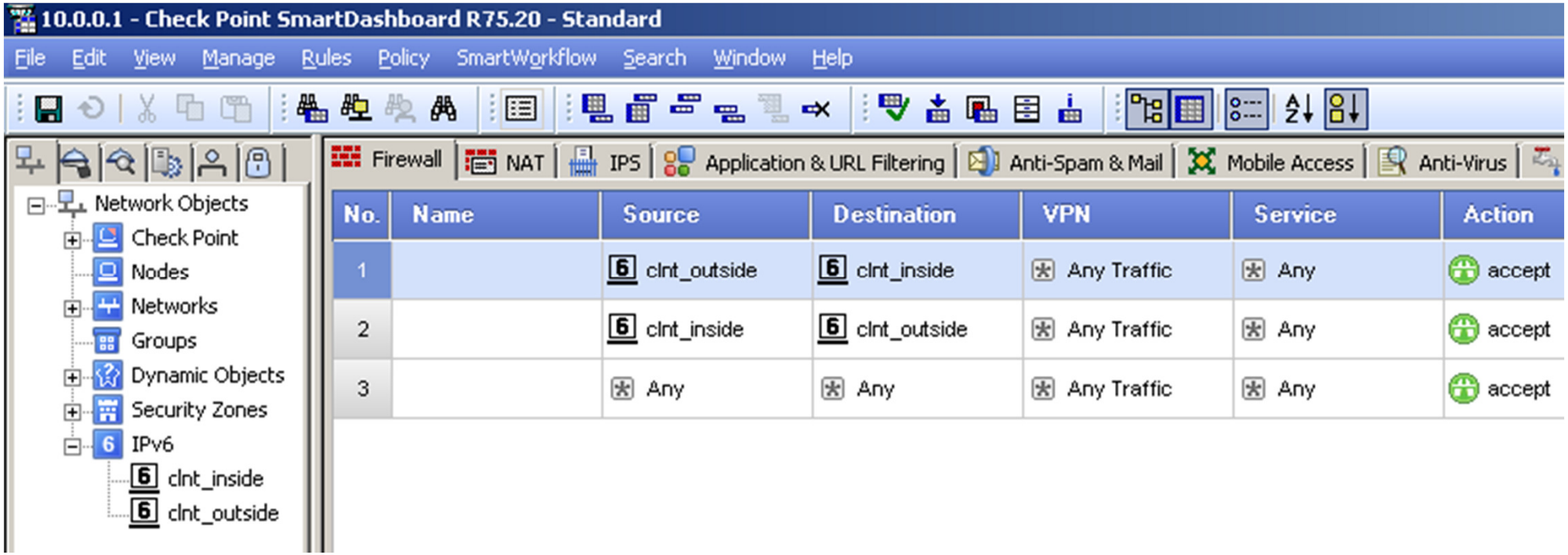

10.0.0.1 - Check Point SmartDashboard R75.20 - Standard
File Edit View Manage Rules Policy SmartWorkflow Search Window Help
Firewall NAT IPS Application & URL Filtering Anti-Spam & Mail
Network Objects
Check Point
Nodes
Networks
Groups
Dynamic Objects
Security Zones
IPv6
clnt_inside
No. Name Source Destination VPN

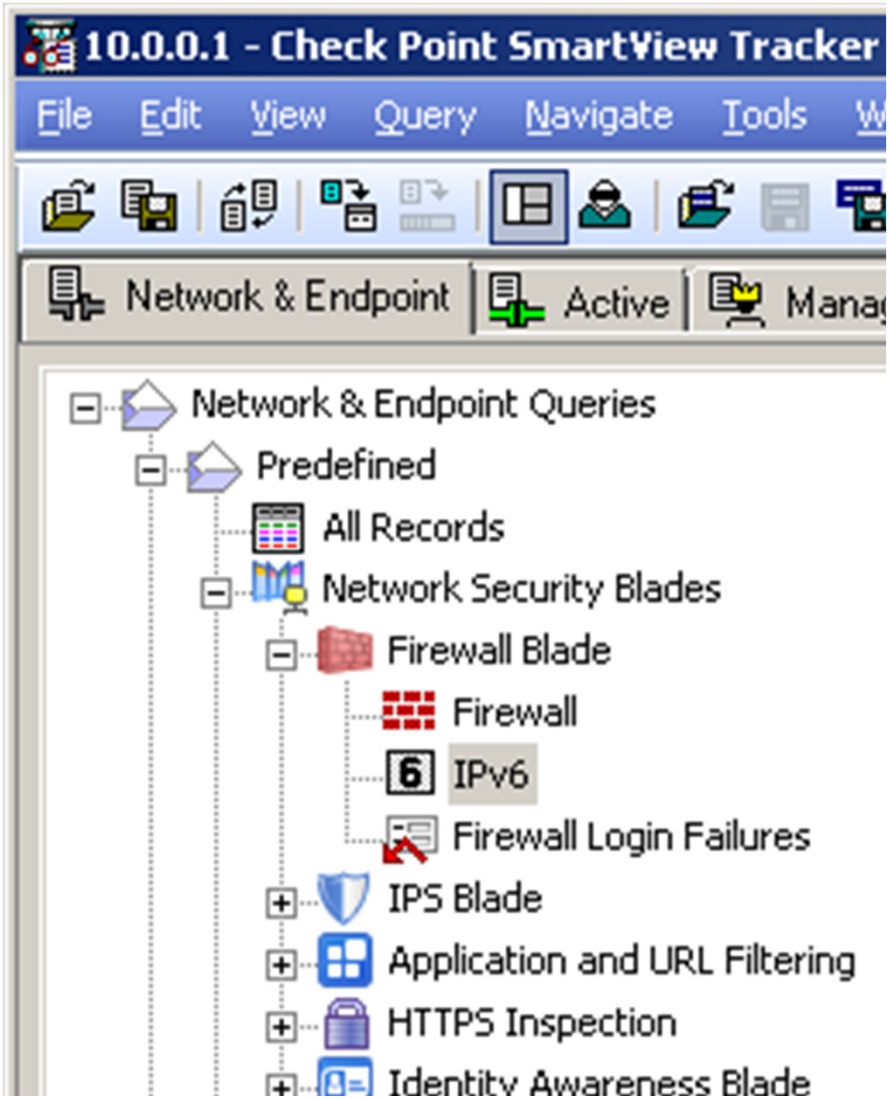

Host Node - AquaNet_UK_sgsn1
General Properties
Topology
NAT
FireWall-1 GX
DNS Server
Other
Host Node - General Properties
Machine
Name:
AquaNet_UK_sgsn1
IP Address:
10.200.0.1
Resolve from Name
Comment:
AquaNet UK sgsn 1

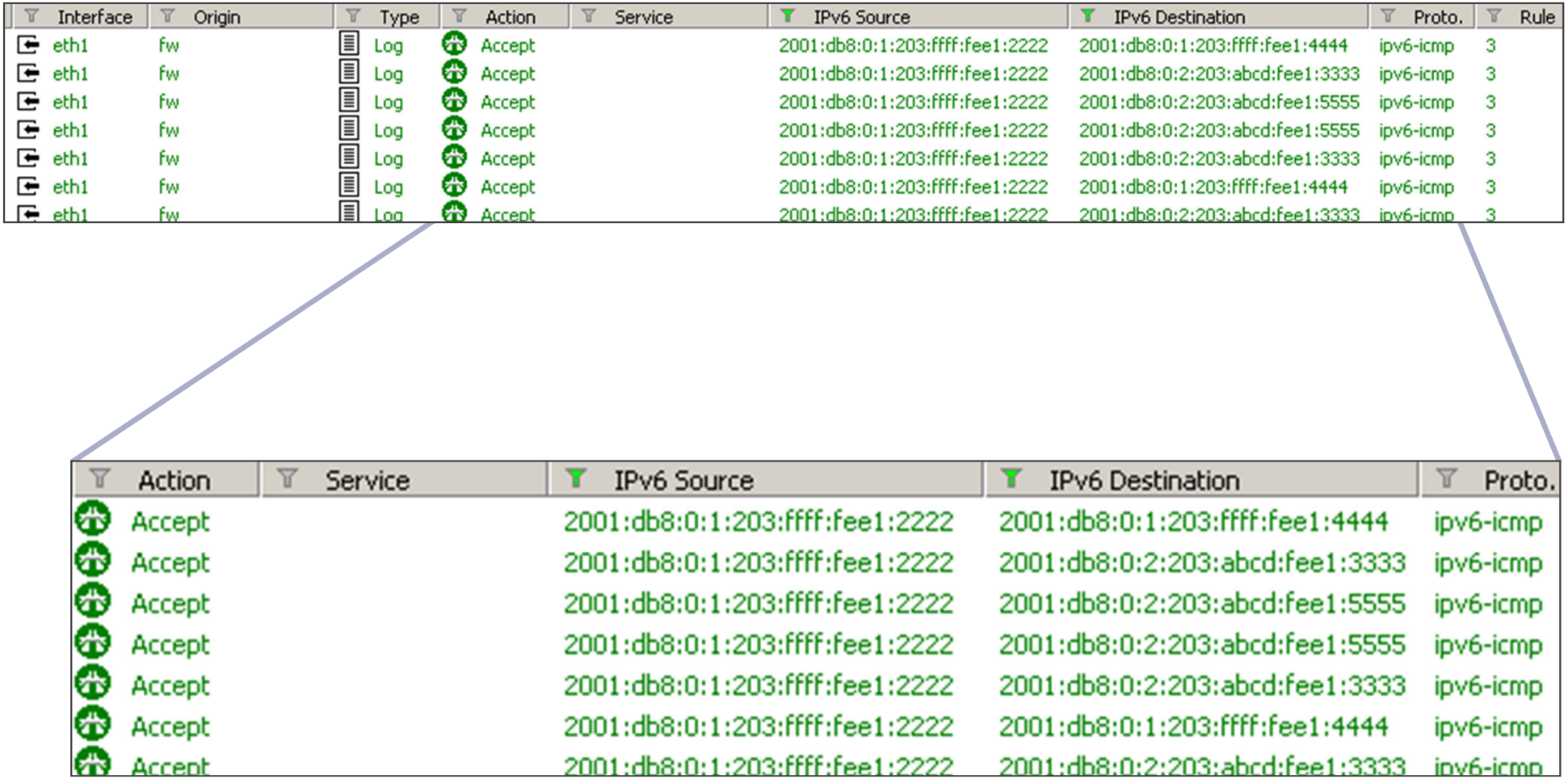

IPv6 Host Properties - IPv6_Host1
General Properties
General Properties
Name:
IPv6_Host1
Comment:
Color:
AquaNet Germany
Address
IPv6 Address:
2005:1::1



Name	IP	NAT Properties	Version	Net Mask
IPv6_DNS	N/A	N/A	N/A	N/A
IPv6_Host1	N/A	N/A	N/A	N/A
IPv6_Host2	N/A	N/A	N/A	N/A
IPv6_Host3	N/A	N/A	N/A	N/A
IPv6_Host4	N/A	N/A	N/A	N/A
IPv6_NW1	N/A	N/A	N/A	N/A
IPv6_NW2	N/A	N/A	N/A	N/A


10.0.0.1 - Check Point SmartDashboard R75.20 - Standard
File Edit View Manage Rules Policy SmartWorkflow Search Window Help
Firewall NAT IPS Application & URL Filtering Anti-Spam & Mail Mobile Access Anti-Virus
Network Objects
Check Point
Nodes
Networks
Groups
Dynamic Objects
Security Zones
IPv6
clnt_inside
clnt_outside
No. Name Source Destination VPN Service Action
1 clnt_outside clnt_inside Any Traffic Any accept
2 clnt_inside clnt_outside Any Traffic Any accept
3 Any Any Any Traffic Any accept


10.0.0.1 - Check Point SmartView Tracker
File
Edit
View
Query
Navigate
Tools
Network & Endpoint
Active
Network & Endpoint Queries
Predefined
All Records
Network Security Blades
Firewall Blade
Firewall
IPv6
Firewall Login Failures
IPS Blade
Application and URL Filtering
HTTPS Inspection
Identity Awareness Blade



Interface	Origin	Type	Action	Service	IPv6 Source	IPv6 Destination	Proto.	Rule
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:1:203:ffff:fee1:4444	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:5555	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:5555	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:1:203:ffff:fee1:4444	ipv6-icmp	3
eth1	fw	Log	Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp	3

Action	Service	IPv6 Source	IPv6 Destination	Proto.
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:1:203:ffff:fee1:4444	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:5555	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:5555	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:1:203:ffff:fee1:4444	ipv6-icmp
Accept		2001:db8:0:1:203:ffff:fee1:2222	2001:db8:0:2:203:abcd:fee1:3333	ipv6-icmp

„These features are supported with IPv6 traffic:

- Dual IP Stack IPv4 and IPv6 Firewall
- IPv6 Licensing
- IPv6 and IPv4 policy based access control
- Dynamically updated defenses
- Logging
- FTP Active and FTP Passive services
- Regular TCP and UDP services (like HTTP, SMTP, Telnet, etc.)
- DNS
- ICMPv6 service
- Traceroute6
- IPv6 'Other' services
- IPv6 fragments
- IPv6 extension headers
- IPv6 in IPv4 tunnels
- fw6 command, for interfacing with the IPv6 kernel“

Source: R75.20 Firewall Administration Guide, Page 183-184

We have (some) new commands

- fw6
- vpn6
- fwaccell6

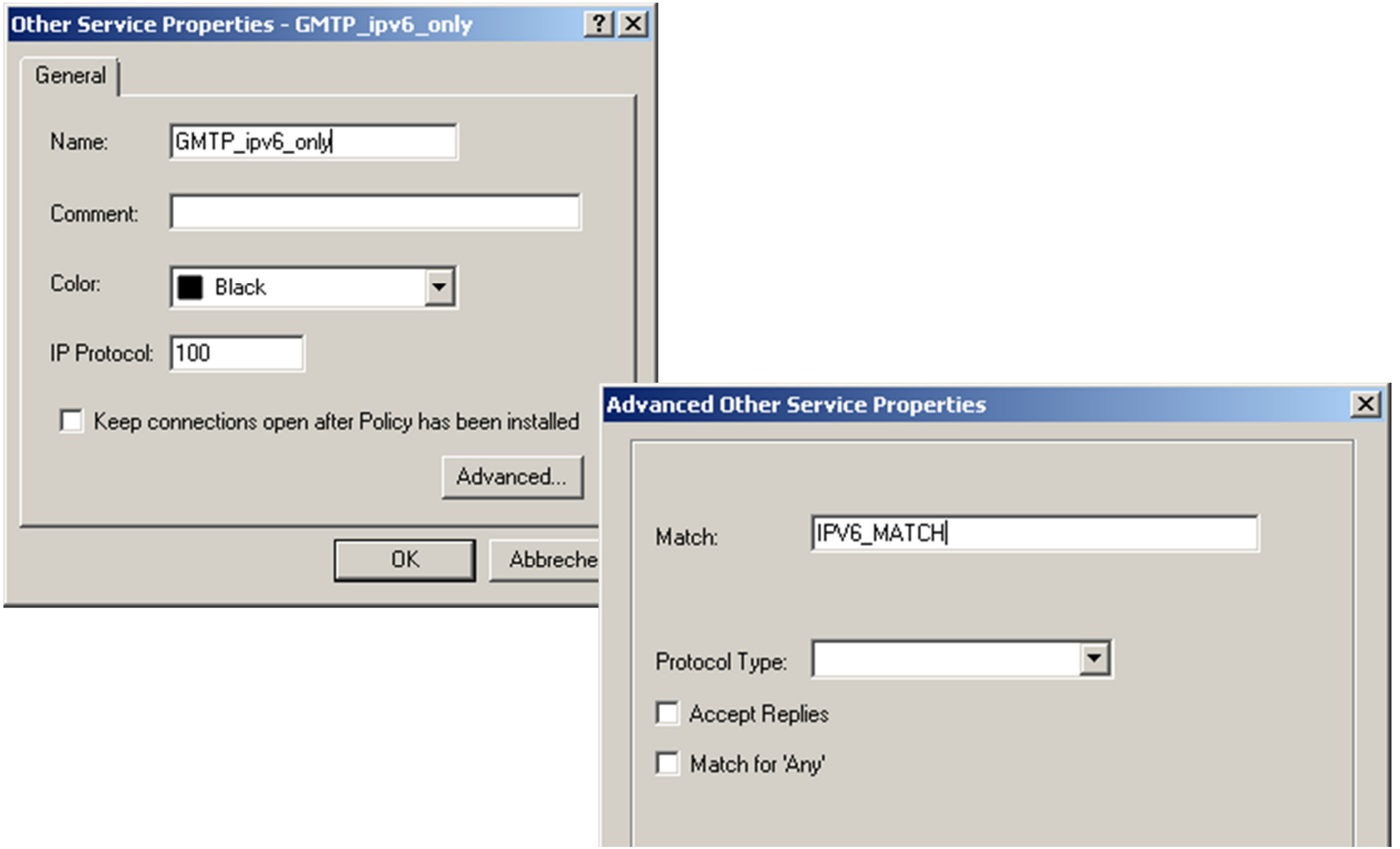
Not all commands work IPv6 specific, check out the Firewall Admin Guide of the version in use.

IPv6 extension headers

"Only fragmentation headers are allowed. It is possible to allow the following extension headers, but no content inspection is done on the extension headers themselves. Inspection is done on the next protocol as usual.

- EXTHDR_ROUTING 43
- EXTHDR_HOPOPTS 0
- EXTHDR_DSTOPTS 60
- EXTHDR_AH 51
- EXTHDR_MOBILE 135"

Source: R75.20 Firewall Administration Guide, Page 189


Other Service Properties - GMTP_ipv6_only
General
Name:
GMTP_ipv6_only
Comment:
Color:
Black
IP Protocol:
100
Keep connections open after Policy has been installed
Advanced...
OK
Abbreche
Advanced Other Service Properties
Match:
IPV6_MATCH
Protocol Type:
Accept Replies
Match for 'Any'

These features are not supported for IPv6 traffic:

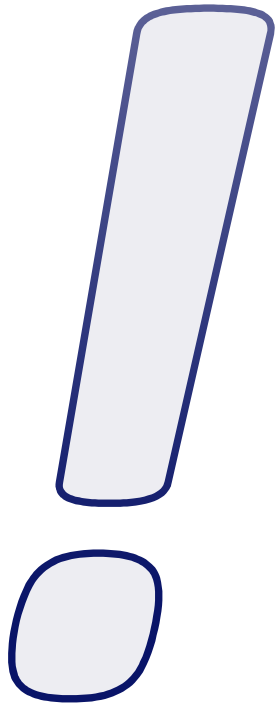
- IPS
- VPN
- NAT
- Anti-spoofing
- Application control, Anti- Spam & Mail, URL Filtering
- SAM
- ClusterXL High Availability, Load Sharing, State Synchronization
- CoreXL - you cannot activate CoreXL when IPv6 is enabled
- SecureXL only accelerates IPv4 traffic / Accept templates issue
- Dynamic Routing for SPLAT based Platforms
- Features not explicitly mentioned (…) are not supported.

Source: R75.20 Firewall Administration Guide, Page 184

We need to use one of the unsupported features, for example ClusterXL.

What can we do??

Get the IPv6Pack!



IPv6Pack is available for the following releases:

- R70.1 (End of Support in 18 month - March 2013)
- NGX R60 (Already Out Of Support)

No IPv6Pack for R75.x, but for a „future version“.

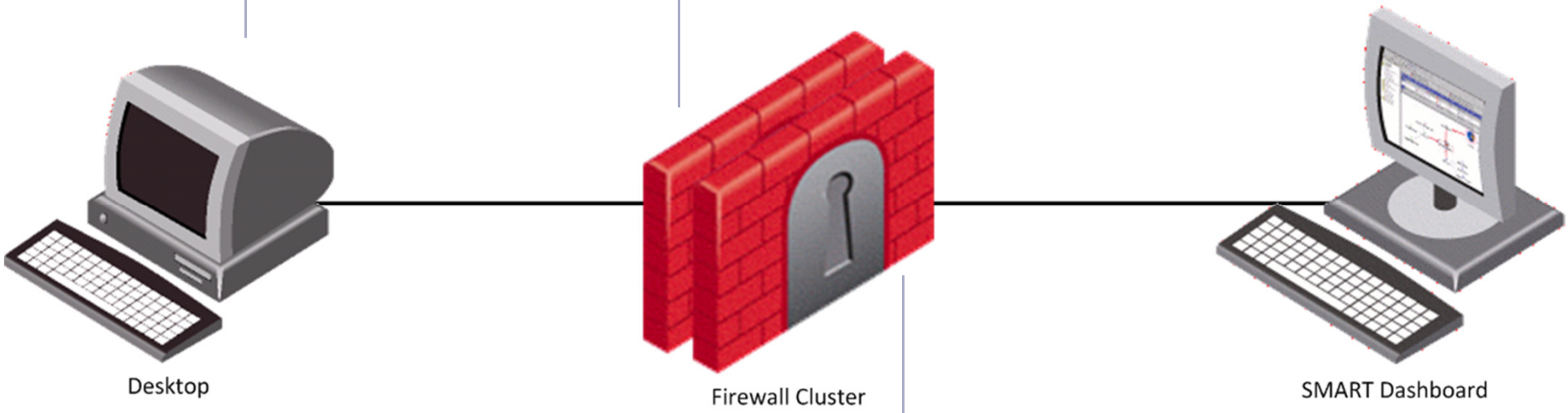
Supported features with IPv6Pack:

- High Availability clustering
- SecureXL
- CoreXL
- VPN (Site-2-Site, Domain-based, Simplified Mode VPN)
- IPv6 Layer 2 Support
- TCP Sequence
- Anti Spoofing
- Port Scan
- Aggressive Aging
- IPv6 in IPv4 Intra Tunnel Inspection
- IPS
  - Max ping size limit
  - Protection against Small PMTU bandwidth attack
- ICMPv6 Services

Source: R70 IPv6Pack Release Notes, Page 5-6

2001:DB8:0:1:203:ffff:fee1:2222

2001:DB8:0:1:203:ffff:fee1:4444 (Cluster)



2001:DB8:0:2:203:abcd:fee1:3333 (Cluster)

2001:DB8:0:2:203:abcd:fee1:5555

IPv6 on Check Point Security Gateways

Firewall Cluster

2001:DB8:0:1:203:ffff:fee1:1002
131.107.0.2

2001:DB8:0:2:203:abcd:fee1:1002
10.0.0.2

Firewall

172.17.100.2
172.17.100.3

2001:DB8:0:1:203:ffff:fee1:1003
131.107.0.3

2001:DB8:0:2:203:abcd:fee1:1002
10.0.0.3

Firewall

We need a distributed installation with a separate Security Management.

Let‘s install R75 management!

STOP!

Security Gateway has to be version R70.1 for IPv6Pack.

Security Management can only be version R70.1 when using a stand-alone installation.

When using a distributed installation you have to use R70.30 or R71.

No IPv6Pack management hotfix for R75 available!

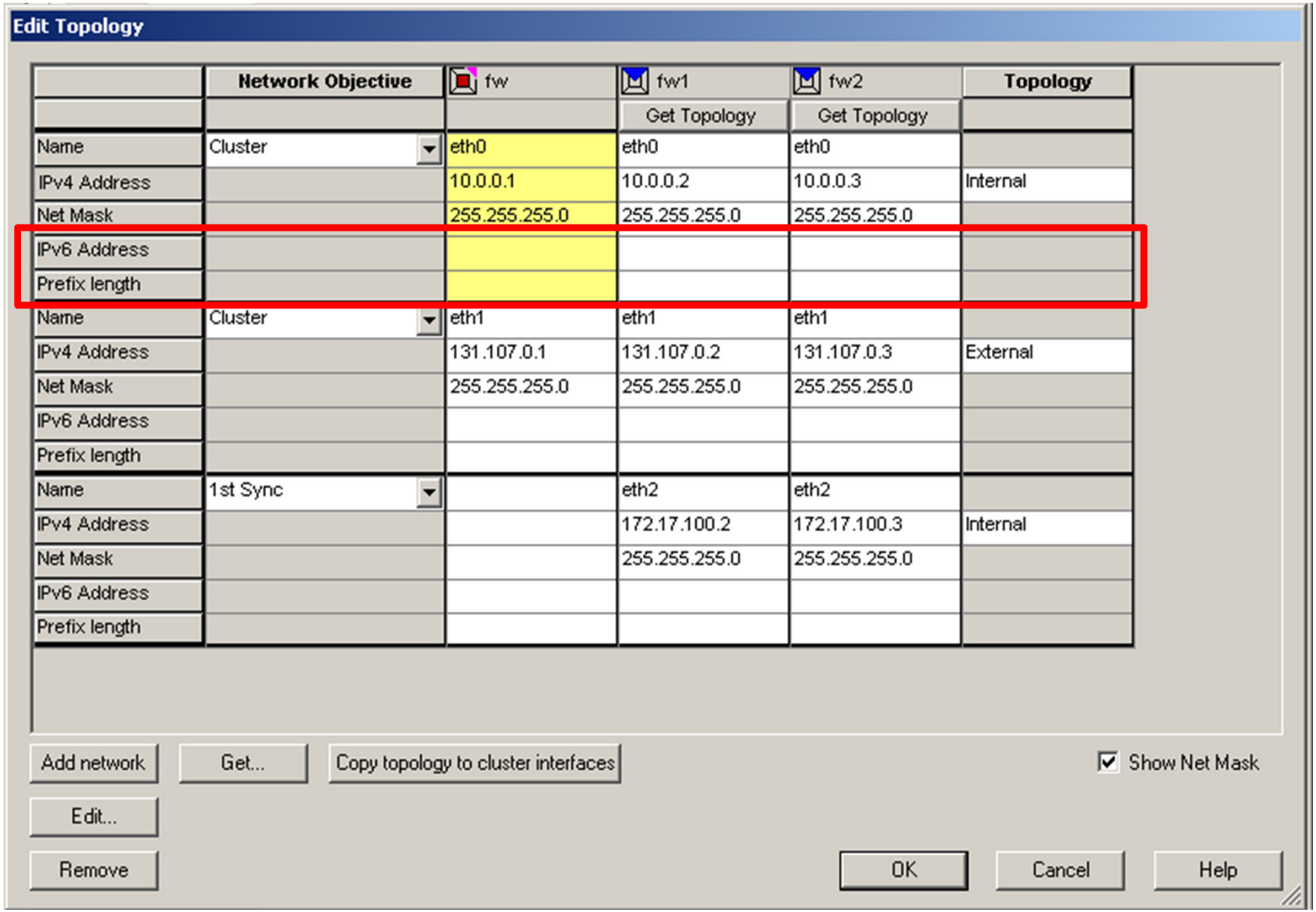
Source: R70 IPv6Pack Release Notes, Page 7

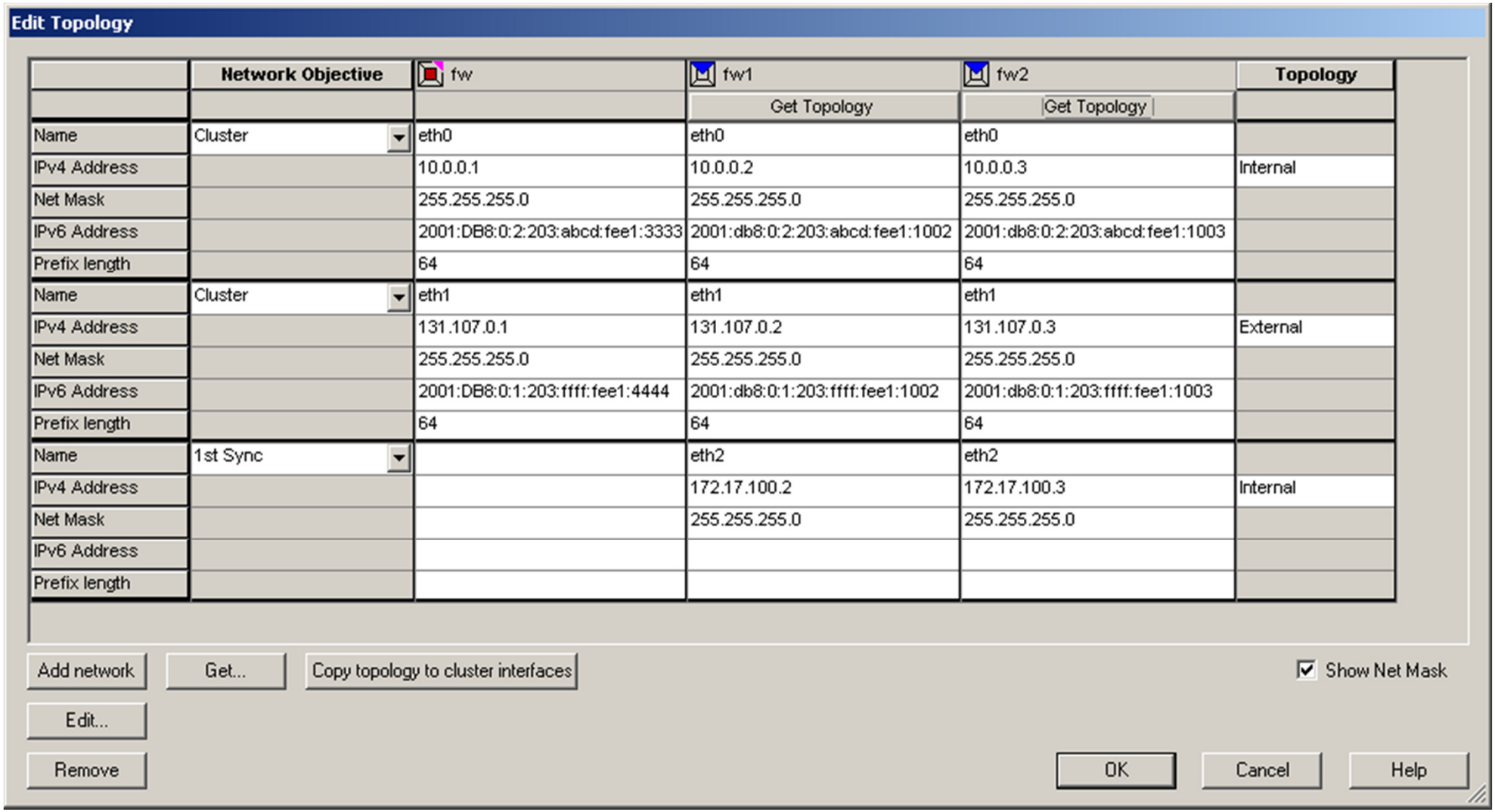
Building a cluster

- Install Security Management R71
- Install Security Gateway R70.1
- Configure IPv4 addresses
- Connect with SmartUpdate
- Attach licenses
- Install IPv6Pack on Security Gateway
- Install IPv6Pack Management Hotfix on Security Management
- Configure IPv6 addresses
- Activate IPv6 support
- Configure Cluster in SmartDashboard

```
************************************************************
Welcome to Check Point R70 IPv6Pack Installation
************************************************************
Installation Application is about to stop all Check Point Processes.
Do you wish to continue (y/n) [y] ? y
stopping Check Point Processes...
Installing SecurePlatform R70 IPv6Pack...Done!

Installing VPN-1 R70 IPv6Pack...Done!

Installing Performance Pack R70 IPv6Pack...Done!

To activate IPv6 support, you must run the command $FWDIR/scripts/fwipv6_enable and reboot

************************************************************************
Package Name                                                  Status
------------                                                  ------
SecurePlatform R70 IPv6Pack                                   Succeeded

VPN-1 R70 IPv6Pack                                            Succeeded

Performance Pack R70 IPv6Pack                                 Succeeded


************************************************************************

Installation Program Completed Successfully.
Do you wish to reboot your machine (y/n) ?
```

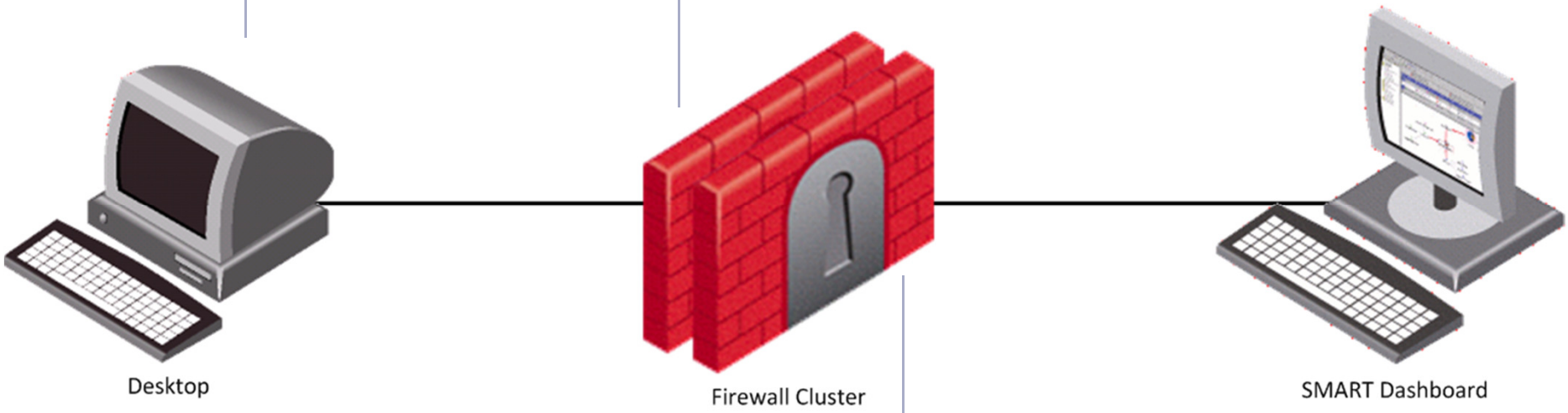
```
Do you want to proceed with installation of Check Point fw1 R71 Support FLIN
 R71 on this computer?
If you choose to proceed, installation will perform CPSTOP.
(y-yes, else no):y
evstop: Unable to find CpWatchDog - run cpstart
SmartView Monitor: Management stopped
VPN-1/FW-1 stopped
SVN Foundation: cpd is not running
SVN Foundation: cpWatchDog is not running
SVN Foundation: Stopping PostgreSQL Database
SVN Foundation stopped

**********************************************************************
Check Point Security Gateway Power/UTM R71
Check Point fw1 R71 Support FLINT_FLAMINGO
Installation completed successfully.
**********************************************************************

Installation was successful.
```


Edit Topology
Network Objective
fw
fw1
fw2
Topology
Get Topology
Get Topology
Name
Cluster
eth0
eth0
eth0
IPv4 Address
10.0.0.1
10.0.0.2
10.0.0.3
Internal
Net Mask
255.255.255.0
255.255.255.0
255.255.255.0
IPv6 Address
Prefix length
Name
Cluster
eth1
eth1
eth1
IPv4 Address
131.107.0.1
131.107.0.2
131.107.0.3
External
Net Mask
255.255.255.0
255.255.255.0
255.255.255.0
IPv6 Address
Prefix length
Name
1st Sync
eth2
eth2
IPv4 Address
172.17.100.2
172.17.100.3
Internal
Net Mask
255.255.255.0
255.255.255.0
IPv6 Address
Prefix length
Add network
Get...
Copy topology to cluster interfaces
Show Net Mask
Edit...
Remove
OK
Cancel
Help


Edit Topology
Network Objective
fw
fw1
fw2
Topology
Get Topology
Get Topology
Name
Cluster
eth0
eth0
eth0
IPv4 Address
10.0.0.1
10.0.0.2
10.0.0.3
Internal
Net Mask
255.255.255.0
255.255.255.0
255.255.255.0
IPv6 Address
2001:DB8:0:2:203:abcd:fee1:3333
2001:db8:0:2:203:abcd:fee1:1002
2001:db8:0:2:203:abcd:fee1:1003
Prefix length
64
64
64
Name
Cluster
eth1
eth1
eth1
IPv4 Address
131.107.0.1
131.107.0.2
131.107.0.3
External
Net Mask
255.255.255.0
255.255.255.0
255.255.255.0
IPv6 Address
2001:DB8:0:1:203:ffff:fee1:4444
2001:db8:0:1:203:ffff:fee1:1002
2001:db8:0:1:203:ffff:fee1:1003
Prefix length
64
64
64
Name
1st Sync
eth2
eth2
IPv4 Address
172.17.100.2
172.17.100.3
Internal
Net Mask
255.255.255.0
255.255.255.0
IPv6 Address
Prefix length
Add network
Get...
Copy topology to cluster interfaces
Show Net Mask
Edit...
Remove
OK
Cancel
Help

2001:DB8:0:1:203:ffff:fee1:2222

2001:DB8:0:1:203:ffff:fee1:4444 (Cluster)



2001:DB8:0:2:203:abcd:fee1:3333 (Cluster)

2001:DB8:0:2:203:abcd:fee1:5555

Known Limitations (examples):

- The fw6 monitor command cannot be filtered with expressions
- Console output is not useable, is just displays part of the IPv6 address that are converted from hexadecimal to decimal
- Writing the output into a file works and can be viewed in Wireshark like normal capture files

Known Limitations (examples):

- IPv6 Rule Base verification is less strict than for IPv4
- `fw_allow_simultaneous_ping` set might cause SecureXL to drop all ICMPv6 echo requests
- Not all types of VPN supported
- „Accept all encrypted traffic“ not supported
- `fw(6) unloadlocal` turns off ip-forwarding for IPv4 and IPv6

Known Limitations (examples):

- Groups with exclusions don‘t work with IPv6 objects
- Dynamic objects are not supported with IPv6
- IPv6 addresses for Externally Managed VPN Gateways objects only through GuiDBedit
- IPv6 address resolving is not supported by SmartView Tracker
- ClusterXL Load Sharing is not supported
- cphaprob does not support IPv6
- Ping6 on ClusterXL Virtual IP address is not supported and will fail

Source: R70 IPv6Pack Release Notes, Page 22-27

What else?

- radvd is available to enable IPv6 stateless auto configuration on the Security Gateway

Source: R70 IPv6Pack Release Notes, Page 19

"ClusterXL uses ICMPv6 Neighbor Advertisements to announce the cluster interfaces, not ICMPv6 Router Advertisements. As such it's not possible to use IPv6 Stateless Address Autoconfiguration for the hosts connected to the firewall"

@checkpointsw
Check Point Software

Check Point is participating in IPv6 Day!
worldipv6day.org/participants/i...

6 Jun via Twitter for Mac

http://twitter.com/#!/checkpointsw/status/77731727375745024

Just wondering… are they using their own products?

PARTICIPATING WEBSITES

The following websites successfully participated in World IPv6 Day on June 8th, 2011. Many remain IPv6-enabled today.

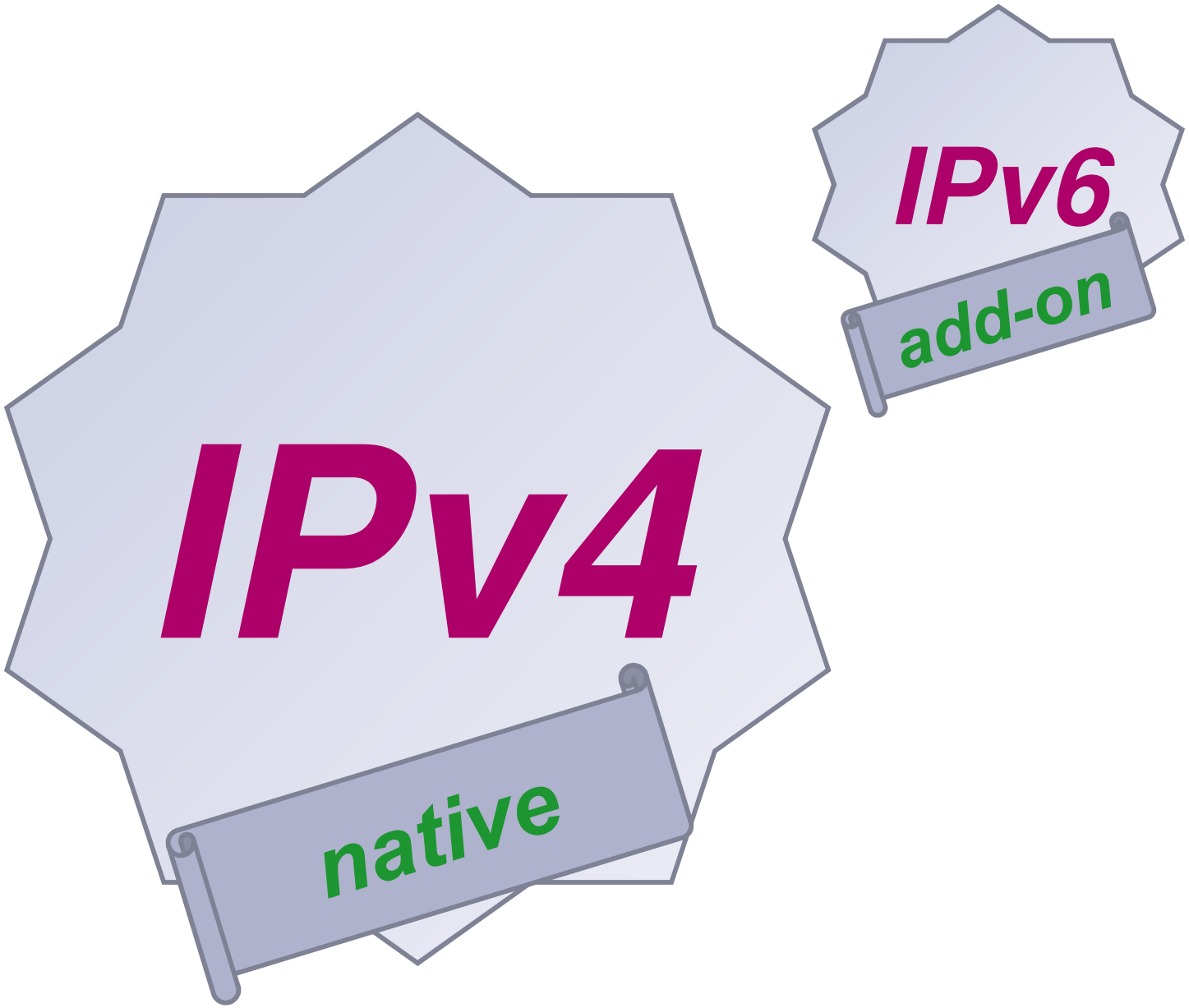
See below for other participating organisations

Show 100 entries Search: Check

Join Order	Participants	IPv6 Page	Participating Websites
338	Check Point Software Technologies Ltd.		www.checkpoint.com

Showing 1 to 1 of 1 entries (filtered from 415 total entries)

http://www.worldipv6day.org/participants/index.html


IPv6
add-on
IPv4
native

IPv6 interface information (Linux)

```
[Expert@fw1]# /sbin/ip -6 addr

1: lo: <LOOPBACK,UP,10000> mtu 16436
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qlen 1000
    inet6 2001:db8:0:2:203:abcd:fee1:1002/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0b:171a/64 scope link
       valid_lft forever preferred_lft forever

3: eth1: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qlen 1000
    inet6 2001:db8:0:1:203:ffff:fee1:1002/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe0b:1724/64 scope link
       valid_lft forever preferred_lft forever

4: eth2: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qlen 1000
    inet6 fe80::20c:29ff:fe0b:172e/64 scope link
       valid_lft forever preferred_lft forever
```

IPv6 interface information (Windows)

```
C:\Windows\system32>netsh interface ipv6 show address

Schnittstelle 11: LAN-Verbindung

Adresstyp  DAD-Status  Gültigkeit Bevorzugt Adresse
---------  ----------- ---------- ---------- ------------------------
Manuell    Bevorzugt     infinite   infinite 2001:db8:0:1:203:ffff:fee1:2222
Andere     Bevorzugt     infinite   infinite fe80::447d:a0d0:4952:5b3d%11
```

IPv6 routing information (Linux)

```
[Expert@fw]# /sbin/ip -6 route show
2001:db8:0:1::/64 dev eth1  metric 256  expires 2133213sec mtu 1500 advmss 1440
2001:db8:0:2::/64 dev eth0  metric 256  expires 2133213sec mtu 1500 advmss 1440
fe80::/64 dev eth0  metric 256  expires 2133213sec mtu 1500 advmss 1440
fe80::/64 dev eth1  metric 256  expires 2133213sec mtu 1500 advmss 1440
unreachable default dev lo  proto none  metric -1  error -101
ff00::/8 dev eth0  metric 256  expires 2133213sec mtu 1500 advmss 1440
ff00::/8 dev eth1  metric 256  expires 2133213sec mtu 1500 advmss 1440
unreachable default dev lo  proto none  metric -1  error -101
```

IPv6 routing information (Windows)

```
C:\Windows\system32>netsh interface ipv6 show route

Veröff.  Typ       Met   Präfix                    Idx  Gateway/Schnittstelle
-------  --------  ----  ------------------------  ---  --------------------
Nein     Manuell   256  ::/0                       11  2001:db8:0:1:203:ffff:fee1:4444
Nein     Manuell   256  ::1/128                     1  Loopback Pseudo-Interface 1
Nein     Manuell   256  2001:db8:0:1::/64          11  LAN-Verbindung
Nein     Manuell   256  2001:db8:0:1:203:ffff:fee1:2222/128   11  LAN-Verbindung
Nein     Manuell   256  fe80::/64                  13  LAN-Verbindung* 2
Nein     Manuell   256  fe80::/64                  11  LAN-Verbindung
Nein     Manuell   256  fe80::100:7f:fffe/128      13  LAN-Verbindung* 2
Nein     Manuell   256  fe80::447d:a0d0:4952:5b3d/128   11  LAN-Verbindung
Nein     Manuell   256  ff00::/8                    1  Loopback Pseudo-Interface 1
Nein     Manuell   256  ff00::/8                   13  LAN-Verbindung* 2
Nein     Manuell   256  ff00::/8                   11  LAN-Verbindung
```

IPv6 routing information (Windows)

```
C:\Windows\system32>netsh interface ipv6 show destinationcache

Schnittstelle 11: LAN-Verbindung


PMTU Zieladresse                                 Adresse des n. Hops
---- ------------------------------------------- ------------------------
   --
1500 2001:db8:0:1:203:ffff:fee1:2222             2001:db8:0:1:203:ffff:fee1:2222
1500 2001:db8:0:1:203:ffff:fee1:4444             2001:db8:0:1:203:ffff:fee1:4444
1500 2001:db8:0:2:203:abcd:fee1:3333             2001:db8:0:1:203:ffff:fee1:4444
1500 2001:db8:0:2:203:abcd:fee1:5555             2001:db8:0:1:203:ffff:fee1:4444
```

IPv6 neighbor information (Linux)

```
[Expert@fw]# /sbin/ip -6 neigh show
fe80::447d:a0d0:4952:5b3d dev eth1 lladdr 00:0c:29:69:5e:62 nud reachable
2001:db8:0:1:203:ffff:fee1:2222 dev eth1 lladdr 00:0c:29:69:5e:62 nud stale
fe80::3cd5:1c49:cbc6:5e7a dev eth0 lladdr 00:0c:29:fc:42:9d nud reachable
2001:db8:0:2:203:abcd:fee1:5555 dev eth0 lladdr 00:0c:29:fc:42:9d nud reachable
```

IPv6 neighbor information (Windows)

```
C:\Users\Tobias Lachmann>netsh interface ipv6 show neighbors

Schnittstelle 11: LAN-Verbindung

Internetadresse                                Physische Adresse   Typ
---------------------------------------------  ------------------  -----------
2001:db8:0:1:203:ffff:fee1:4444                00-0c-29-25-71-ff   Abgelaufen (Router)
fe80::20c:29ff:fe25:71ff                       00-0c-29-25-71-ff   Abgelaufen (Router)
ff02::2                                        33-33-00-00-00-02   Permanent
ff02::16                                       33-33-00-00-00-16   Permanent
ff02::1:2                                      33-33-00-01-00-02   Permanent
ff02::1:3                                      33-33-00-01-00-03   Permanent
ff02::1:ff25:71ff                              33-33-ff-25-71-ff   Permanent
ff02::1:ff52:5b3d                              33-33-ff-52-5b-3d   Permanent
ff02::1:ffe1:2222                              33-33-ff-e1-22-22   Permanent
ff02::1:ffe1:4444                              33-33-ff-e1-44-44   Permanent
```

IPv6 delete neighbor information (Linux)

```
[Expert@fw1]# /sbin/ip -6 neigh show

2001:db8:0:2:203:abcd:fee1:5555 dev eth0 lladdr 00:0c:29:fc:42:9d nud reachable
fe80::3cd5:1c49:cbc6:5e7a dev eth0 lladdr 00:0c:29:fc:42:9d nud reachable


[Expert@fw1]# /sbin/ip -6 neigh flush dev eth0


[Expert@fw1]# /sbin/ip -6 neigh show

2001:db8:0:2:203:abcd:fee1:5555 dev eth0  nud failed
fe80::3cd5:1c49:cbc6:5e7a dev eth0  nud failed
```

IPv6 delete neighbor information (Windows)

```
C:\Windows\system32>netsh interface ipv6 delete neighbors
OK.

C:\Windows\system32>netsh interface ipv6 show neighbors

Schnittstelle 11: LAN-Verbindung


Internetadresse                                Physische Adresse   Typ
---------------------------------------------  ------------------  -----------
2001:db8:0:1:203:ffff:fee1:4444                00-00-00-00-00-00   Nicht erreichbar
```

IPv6 Ressources

- R7x Firewall Administration Guide
- R70 IPv6Pack Release Notes

  http://downloads.checkpoint.com/dc/download.htm?ID=10908
- R70 IPv6Pack Administration Guide

  http://downloads.checkpoint.com/dc/download.htm?ID=10907
- sk39374: IPv6 Support FAQ

  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39374
- sk34552: How to set up IPv6 on SecurePlatform

  https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk34552

IPv6 Ressources

- Jens Roesen - Internet Protocol Version 6 Cheat Sheet

  http://www.roesen.org/files/ipv6_cheat_sheet.pdf

- Microsoft Test Lab Guide: Demonstrate IPv6

  http://www.microsoft.com/download/en/details.aspx?id=10564

- Step-by-Step Guide for Setting Up IPv6 in a Test Lab

  http://www.microsoft.com/download/en/details.aspx?DisplayLang=en&id=1736

Questions?

Tobias Lachmann

tobias@lachmann.org

http://blog.lachmann.org