



# NETWORK SECURITY FIREWALL CLI REFERENCE GUIDE

DFL-210/ 800/1600/ 2500  
DFL-260/ 860

VER. 1.02



NETWORK SECURITY SOLUTION <http://www.dlink.com>



---

# CLI Reference Guide

***DFL-210/260/800/860/1600/2500***  
***NetDefendOS version 2.20***

D-Link NetDefend Security  
<http://security.dlink.com.tw>

Published 2007-12-24  
Copyright © 2007

---

---

# **CLI Reference Guide**

## **DFL-210/260/800/860/1600/2500**

### **NetDefendOS version 2.20**

Published 2007-12-24

Copyright © 2007

#### **Copyright Notice**

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

#### **Disclaimer**

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

#### **Limitations of Liability**

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

---

## Table of Contents

Preface .....	9
1. Introduction .....	11
1.1. Running a command .....	11
1.2. Help .....	12
1.2.1. Help for commands .....	12
1.2.2. Help for object types .....	12
1.3. Function keys .....	13
1.4. Command line history .....	14
1.5. Tab completion .....	15
1.5.1. Inline help .....	15
1.5.2. Autocompleting current value and default value .....	15
1.5.3. Configuration object type categories .....	16
1.6. User roles .....	17
2. Command Reference .....	19
2.1. Configuration .....	19
2.1.1. activate .....	19
2.1.2. add .....	19
2.1.3. cancel .....	20
2.1.4. cc .....	20
2.1.5. commit .....	21
2.1.6. copy .....	22
2.1.7. delete .....	22
2.1.8. psongen .....	23
2.1.9. reject .....	24
2.1.10. reset .....	25
2.1.11. set .....	25
2.1.12. show .....	26
2.1.13. undelete .....	28
2.2. Runtime .....	30
2.2.1. about .....	30
2.2.2. alarm .....	30
2.2.3. arp .....	30
2.2.4. arpsnoop .....	31
2.2.5. ats .....	32
2.2.6. bigpond .....	32
2.2.7. blacklist .....	33
2.2.8. buffers .....	34
2.2.9. cam .....	34
2.2.10. certcache .....	35
2.2.11. cfglog .....	35
2.2.12. connections .....	35
2.2.13. cpuid .....	36
2.2.14. crashdump .....	37
2.2.15. customlog .....	37
2.2.16. dconsole .....	37
2.2.17. dhcp .....	38
2.2.18. dhcprelay .....	38
2.2.19. dhcpserver .....	39
2.2.20. dns .....	40
2.2.21. dnsbl .....	40
2.2.22. dynroute .....	41
2.2.23. frags .....	41
2.2.24. ha .....	42
2.2.25. httpposter .....	42
2.2.26. hwaccel .....	43
2.2.27. ifstat .....	43
2.2.28. igmp .....	44

2.2.29. ikesnoop .....	44
2.2.30. ippool .....	45
2.2.31. ipsecglobalstats .....	46
2.2.32. ipseckeepalive .....	46
2.2.33. ipsecstats .....	46
2.2.34. killsa .....	47
2.2.35. license .....	47
2.2.36. linkmon .....	48
2.2.37. lockdown .....	48
2.2.38. logout .....	49
2.2.39. memory .....	49
2.2.40. natpool .....	49
2.2.41. ospf .....	50
2.2.42. pipes .....	51
2.2.43. reconfigure .....	52
2.2.44. routemon .....	52
2.2.45. routes .....	52
2.2.46. rules .....	53
2.2.47. sessionmanager .....	54
2.2.48. shutdown .....	55
2.2.49. sipalg .....	56
2.2.50. sshserver .....	57
2.2.51. stats .....	58
2.2.52. time .....	58
2.2.53. updatecenter .....	59
2.2.54. urlcache .....	59
2.2.55. userauth .....	60
2.2.56. vlan .....	61
2.2.57. vpnstats .....	61
2.2.58. zonedefense .....	61
2.3. Utility .....	62
2.3.1. ping .....	62
2.4. Misc .....	63
2.4.1. help .....	63
2.4.2. history .....	63
3. Configuration Reference .....	65
3.1. Access .....	66
3.2. Address .....	68
3.2.1. AddressFolder .....	68
3.2.2. EthernetAddress .....	70
3.2.3. EthernetAddressGroup .....	70
3.2.4. IP4Address .....	70
3.2.5. IP4Group .....	70
3.2.6. IP4HAddress .....	70
3.3. AdvancedScheduleProfile .....	71
3.3.1. AdvancedScheduleOccurrence .....	71
3.4. ALG .....	72
3.4.1. ALG_FTP .....	72
3.4.2. ALG_H323 .....	73
3.4.3. ALG_HTTP .....	73
3.4.4. ALG_POP3 .....	74
3.4.5. ALG_SIP .....	75
3.4.6. ALG_TFTP .....	75
3.5. ARP .....	77
3.6. BlacklistWhiteHost .....	78
3.7. Certificate .....	79
3.8. Client .....	80
3.8.1. DynDnsClientCjbNet .....	80
3.8.2. DynDnsClientDLink .....	80
3.8.3. DynDnsClientDLinkChina .....	80
3.8.4. DynDnsClientDyndnsOrg .....	81
3.8.5. DynDnsClientDynsCx .....	81
3.8.6. DynDnsClientPeanutHull .....	82

3.8.7. LoginClientBigPond .....	82
3.9. COMPortDevice .....	83
3.10. ConfigModePool .....	84
3.11. DateTime .....	85
3.12. Device .....	86
3.13. DHCPRelay .....	87
3.14. DHCPServer .....	88
3.14.1. DHCPServerPoolStaticHost .....	88
3.14.2. DHCPServerCustomOption .....	89
3.15. DNS .....	90
3.16. Driver .....	91
3.16.1. IXP4NP EthernetDriver .....	91
3.16.2. MarvellEthernetPCIDriver .....	91
3.16.3. R8139EthernetPCIDriver .....	91
3.17. DynamicRoutingRule .....	92
3.17.1. DynamicRoutingRuleExportOSPF .....	92
3.17.2. DynamicRoutingRuleAddRoute .....	93
3.18. EthernetDevice .....	95
3.19. HighAvailability .....	96
3.20. HTTPPoster .....	97
3.21. IDList .....	98
3.21.1. ID .....	98
3.22. IDPRule .....	99
3.22.1. IDPRuleAction .....	99
3.23. IKEAlgorithms .....	101
3.24. Interface .....	102
3.24.1. DefaultInterface .....	102
3.24.2. Ethernet .....	102
3.24.3. GRE Tunnel .....	103
3.24.4. InterfaceGroup .....	103
3.24.5. IPSecTunnel .....	104
3.24.6. L2TPClient .....	106
3.24.7. L2TPServer .....	107
3.24.8. PPPoETunnel .....	108
3.24.9. VLAN .....	109
3.25. IPPool .....	111
3.26. IPRule .....	112
3.27. IPRuleFolder .....	114
3.27.1. IPRule .....	114
3.28. IPSecAlgorithms .....	115
3.29. LDAPServer .....	116
3.30. LocalUserDatabase .....	117
3.30.1. User .....	117
3.31. LogReceiver .....	118
3.31.1. EventReceiverSNMP2c .....	118
3.31.2. LogReceiverMemory .....	118
3.31.3. LogReceiverSMTP .....	119
3.31.4. LogReceiverSyslog .....	119
3.32. NATPool .....	121
3.33. OSPFProcess .....	122
3.33.1. OSPFArea .....	123
3.34. Pipe .....	126
3.35. PipeRule .....	129
3.36. PSK .....	130
3.37. RadiusServer .....	131
3.38. RemoteManagement .....	132
3.38.1. RemoteMgmtHTTP .....	132
3.38.2. RemoteMgmtSNMP .....	132
3.38.3. RemoteMgmtSSH .....	132
3.39. RoutingRule .....	134
3.40. RoutingTable .....	135
3.40.1. Route .....	135
3.40.2. SwitchRoute .....	136

---

3.41. ScheduleProfile .....	137
3.42. Service .....	138
3.42.1. ServiceGroup .....	138
3.42.2. ServiceICMP .....	138
3.42.3. ServiceIPProto .....	139
3.42.4. ServiceTCPUDP .....	139
3.43. Settings .....	141
3.43.1. ARPTableSettings .....	141
3.43.2. ConnTimeoutSettings .....	141
3.43.3. DHCPRelaySettings .....	142
3.43.4. DHCPServerSettings .....	143
3.43.5. FragSettings .....	143
3.43.6. ICMPSettings .....	144
3.43.7. IPSecTunnelSettings .....	144
3.43.8. IPSettings .....	145
3.43.9. L2TPServerSettings .....	146
3.43.10. LengthLimSettings .....	147
3.43.11. LocalReassSettings .....	147
3.43.12. LogSettings .....	148
3.43.13. MiscSettings .....	148
3.43.14. RemoteMgmtSettings .....	148
3.43.15. RoutingSettings .....	149
3.43.16. SSLSettings .....	150
3.43.17. StateSettings .....	151
3.43.18. TCPSettings .....	152
3.43.19. VLANSettings .....	153
3.44. SSHClientKey .....	154
3.45. ThresholdRule .....	155
3.45.1. ThresholdAction .....	155
3.46. UpdateCenter .....	157
3.47. UserAuthRule .....	158
3.48. ZoneDefenseBlock .....	160
3.49. ZoneDefenseExcludeList .....	161
3.50. ZoneDefenseSwitch .....	162
Index .....	164

---

## List of Examples

1. Command option notation .....	9
1.1. Help for commands .....	12
1.2. Help for object types .....	12
1.3. Command line history .....	14
1.4. Tab completion .....	15
1.5. Inline help .....	15
1.6. Edit an existing property value .....	16
1.7. Using categories with tab completion .....	16
2.1. Create a new object .....	19
2.2. Change context .....	21
2.3. Delete an object .....	23
2.4. Reject changes .....	24
2.5. Set property values .....	26
2.6. Show objects .....	27
2.7. Undelete an object .....	28
2.8. Block hosts .....	33
2.9. frags .....	42
2.10. Show a range of rules .....	54



---

# Preface

## Audience

The target audience for this reference guide is:

- Administrators that are responsible for configuring and managing the D-Link Firewall.
- Administrators that are responsible for troubleshooting the D-Link Firewall.

This guide assumes that the reader is familiar with the D-Link Firewall, and has the necessary basic knowledge in network security.

## Notation

The following notation is used throughout this reference guide when specifying the options of a command:

<b>Angle brackets</b> <code>&lt;name&gt;</code> or <b>-option=</b> <code>&lt;description&gt;</code>	Used for specifying the <i>name</i> of an option or a description of a value.
<b>Square brackets</b> <code>[option]</code> or <b>-option[=value]</b>	Used for specifying that an option or a value for an option is <i>optional</i> and can be omitted.
<b>Curly brackets</b> <code>{value1   value2   value3}</code>	Used for specifying the <i>available values</i> for an option.
<b>Ellipsis</b> ...	Used for specifying that <i>more than one</i> value can be specified for the option.

### Example 1. Command option notation

One of the usages for the **help** command looks like this:

```
help -category={COMMANDS | TYPES} [<Topic>]
```

This means that **help** has an option called `category` which has two possible values which are `COMMANDS` and `TYPES`. There is also an optional option called `Topic` which in this case is a search string used to specify what help topic to display. Since the topic is optional, it is possible to exclude it when running the command.

Both of the following examples are valid for the usage described above:

```
gw-world:/> help -category=COMMANDS
gw-world:/> help -category=COMMANDS activate
```

The usage for the **routes** command is:

```
routes [-all] [-switched] [-flushl3cache[=<percent>]] [-num=<n>]
        [-nonhost] [-tables] [-lookup=<ip address>] [-verbose]
        [-setmtu=<mtu>] [-cacheinfo] [<table name>]...
```

None of the options of this command are mandatory. The `flushl3cache` option also has an optional value. This is because that option has a default value, `100`, which will be used if no value is specified.

The following two examples will yield the same result:

```
gw-world:/> routes -flushl3cache=100
gw-world:/> routes -flushl3cache
```

Because the `table name` option is followed by ellipses it is possible to specify more than one routing table. Since `table name` is optional as well, the user can specify zero or more policy-based routing tables.

```
gw-world:/> routes Virroute Virroute2
```

---

# Chapter 1. Introduction

- Running a command, page 11
- Help, page 12
- Function keys, page 13
- Command line history, page 14
- Tab completion, page 15
- User roles, page 17

This guide is a reference for all commands and configuration object types that are available in the command line interface for NetDefendOS.

## 1.1. Running a command

The commands described in this guide can be run by typing the command name and then pressing the return key. Many commands require options to be set to run. If a required option is missing a brief syntax help will be displayed.

## 1.2. Help

### 1.2.1. Help for commands

There are two ways of getting help about a command. A brief help is displayed if the command name is typed followed by `-?` or `-h`. This applies to all commands and is therefore not listed in the option list for each command in this guide. Using the **help** command gives a more detailed help corresponding to the information found in this guide. In most cases it is possible to simply type **help** followed by the command name to get the full help. See Section 2.4.1, “help” for a more detailed description. To list the available commands, just type **help** and press return.

#### Example 1.1. Help for commands

Brief help for the **activate** command:

```
gw-world:/> activate -?  
gw-world:/> activate -h
```

Full help for **activate**:

```
gw-world:/> help activate
```

Help for the **arp** command. Arp is also the name of a configuration object type, so it is necessary to specify that the help text for the command should be displayed:

```
gw-world:/> help -category=COMMANDS arp
```

List all available commands:

```
gw-world:/> help
```

### 1.2.2. Help for object types

To get help about configuration object types, use the **help** command. It is also possible to get information about each property in an object type, such as data type, default value, etc. by entering the `?` character when entering the value of a property and pressing tab. More on this in Section 1.5.1, “Inline help”.

#### Example 1.2. Help for object types

Full help for **IP4Address**:

```
gw-world:/> help IP4Address
```

Help for the **ARP** configuration object type, which collides with the **arp** command:

```
gw-world:/> help -category=TYPES ARP
```

## 1.3. Function keys

In addition to the return key there are a number of function keys that are used in the CLI.

<b>Backspace</b>	Delete the character to the left of the cursor.
<b>Tab</b>	Complete current word.
<b>Ctrl-A or Home</b>	Move the cursor to the beginning of the line.
<b>Ctrl-B or Left Arrow</b>	Move the cursor one character to the left.
<b>Ctrl-C</b>	Clear line or cancel page view if more than one page of information is shown.
<b>Ctrl-D or Delete</b>	Delete the character to the right of the cursor.
<b>Ctrl-E or End</b>	Move the cursor to the end of the line.
<b>Ctrl-F or Right Arrow</b>	Move the cursor one character to the right.
<b>Ctrl-K</b>	Delete from the cursor to the end of the line.
<b>Ctrl-N or Down Arrow</b>	Show the next entry in the command history.
<b>Ctrl-P or Up Arrow</b>	Show the previous entry in the command history.
<b>Ctrl-T</b>	Transpose the current and the previous character.
<b>Ctrl-U</b>	Delete from the cursor to the beginning of line.
<b>Ctrl-W</b>	Delete word backwards.

## 1.4. Command line history

Every time a command is run, the command line is added to a history list. The up and down arrow keys are used to access previous command lines (up arrow for older command lines and down arrow to move back to a newer command line). See also Section 2.4.2, “history”.

### Example 1.3. Command line history

Using the command line history via the arrow keys:

```
gw-world:/> show Address
gw-world:/> (up arrow)
gw-world:/> show Address (the previous commandline is displayed)
```

## 1.5. Tab completion

By using the tab function key in the CLI the names of commands, options, objects and object properties can be automatically completed. If the text entered before pressing tab only matches one possible item, e.g. "activate" is the only match for "acti" if a command is expected, the name will be autocompleted. Should there be more than one match the part common to all matches will be completed. At this point the user can either enter more characters or press tab again, which will display a list of the possible completions. This can also be done without entering any characters, but the resulting list might be long if there are many possible completions, e.g. all commands.

### Example 1.4. Tab completion

An example of tab completion when using the **add** command:

```
gw-world:/> add Add (tab)
gw-world:/> add Address ("ress" was autocompleted)
gw-world:/> add Address i (tab)
gw-world:/> add Address IP4 ("IP4" was autocompleted)
gw-world:/> add Address IP4 (tab, or double tab if IP4 were entered manually)
A list of all types starting with IP4 is listed.
gw-world:/> add Address IP4a (tab)
gw-world:/> add Address IP4Address ("Address" was autocompleted)
gw-world:/> add Address IP4Address example_ip a (tab)
gw-world:/> add Address IP4Address example_ip Address= ("Address=" was autocompleted)
gw-world:/> add Address IP4Address example_ip Address=1.2.3.4
```

Tab completion of references:

```
gw-world:/> set Address IP4Group examplegroup Members= (tab, tab)
A list of valid objects is displayed.
gw-world:/> set Address IP4Group examplegroup Members=e (tab)
gw-world:/> set Address IP4Group examplegroup Members=example_ip
("xample_ip" was autocompleted)
```

### 1.5.1. Inline help

It is possible to get help about available properties of configuration objects while a command line is being typed by using the **?** character. Write **?** instead of a property name and press tab and a help text for the available properties is shown. If **?** is typed in stead of a property value and tab is pressed a help text for that property which contains more information such as data type, default value, etc. is displayed.

### Example 1.5. Inline help

Get inline help for all properties of an IP4Address:

```
gw-world:/> set IP4Address example_ip ? (tab)
A help text describing all available properties is displayed.
```

Getting inline help for the Address property:

```
gw-world:/> set IP4Address example_ip Address=? (tab)
A more detailed help text about Address is displayed.
```

### 1.5.2. Autocompleting current value and default value

Another special character that can be used together with tab completion is **<**. If **<** is entered instead of a property value and tab is pressed it will be replaced by the current value of that property. This is

useful when editing an existing list of items or a long text value. If no value has been set yet for the property in question the default value, if one exists, will be used. Some values, such as binary data, cannot be autocompleted in this way.

**Example 1.6. Edit an existing property value**

Edit the current value:

```
gw-world:/> add IP4Address example_ip Address=1.2.3.4
gw-world:/> set IP4Address example_ip Address=< (tab)
gw-world:/> set IP4Address example_ip Address=1.2.3.4 (the value was inserted)
The value can now be edited by using the arrow keys or backspace.

gw-world:/> set IP4Group examplegroup Members=ip1,ip2,ip3,ip5
gw-world:/> set IP4Group examplegroup Members=< (tab)
gw-world:/> set IP4Group examplegroup Members=ip1,ip2,ip3,ip5
(the value was inserted)
It is now possible to add or remove a member to the list without having to enter all
the other members again.
```

Edit the default value:

```
gw-world:/> add LogReceiverSyslog example Address=example_ip LogSeverity=< (tab)
gw-world:/> add LogReceiverSyslog example Address=example_ip LogSeverity=Emergency,
Alert,Critical>Error,Warning,Notice,Info (the default value was inserted)
Now it is easy to remove a log severity.
```

## 1.5.3. Configuration object type categories

Some object types are grouped together in a category in the CLI. This only matters when using tab completion as they are used to limit the number of possible completions when tab completing object types. The category can always be omitted when running commands if the type name is entered manually.

**Example 1.7. Using categories with tab completion**

Accessing an IP4Address object with the use of categories:

```
gw-world:/> show ad (tab)
gw-world:/> show Address (the category is autocompleted)
gw-world:/> show Address ip4a (tab)
gw-world:/> show Address IP4Address (the type is autocompleted)
gw-world:/> show Address IP4Address example_ip
```

Accessing an IP4Address object without the use of categories:

```
gw-world:/> show IP4Address example_ip
```



## 1.6. User roles

Some commands and options cannot be used unless the logged in user has administrator privilege. This is indicated in this guide by a note following the command or "Admin only" written next to an option.



---

# Chapter 2. Command Reference

- Configuration, page 19
- Runtime, page 30
- Utility, page 62
- Misc, page 63

## 2.1. Configuration

### 2.1.1. activate

Activate changes.

#### Description

Activate the latest changes.

This will issue a reconfiguration, using the new configuration. If the reconfiguration is successful a **commit** command must be issued within the configured timeout interval in order to save the changes to media. If not, the system will revert to using the previous version of the configuration.

#### Usage

```
activate
```



#### *Note*

*Requires Administrator privilege.*

### 2.1.2. add

Create a new object.

#### Description

Create a new object and add it to the configuration.

Specify the type of object you want to create and the identifier, if the type has one, unless the object is identified by an index. Set the properties of the object by writing the propertyname equals (=) and then the value. An optional category can be specified for some object types when using tab completion.

If a mandatory property isn't specified a list of errors will be shown after the object is created. If an invalid property or value type is specified or if the identifier is missing the command will fail and not create an object.

Adjustments can be made after the object is created by using the **set** command.

**Example 2.1. Create a new object**

```
Add objects with an identifier property (not index):
gw-world:/> add Address IP4Address example_ip Address=1.2.3.4
Comments="This is an example"
gw-world:/> add IP4Address example_ip2 Address=2.3.4.5

Add an object with an index:
gw-world:/main> add Route Interface=lan

Add an object without identifier:
gw-world:/> add DynDnsClientDynDnsOrg DNSName=example Username=example
```

## Usage

```
add [<Category>] <Type> [<Identifier>] [<key-value pair>]...
```

## Options

<Category>	Category that groups object types.
<Identifier>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<key-value pair>	One or more property-value pairs, i.e. <property name>=<value> or <property name>="<value>".
<Type>	Type of configuration object to perform operation on.



### Note

*Requires Administrator privilege.*

## 2.1.3. cancel

Cancel ongoing commit.

### Description

Cancel commit operation immediately, without waiting for the timeout.

### Usage

```
cancel
```



### Note

*Requires Administrator privilege.*

## 2.1.4. cc

Change the current context.

### Description

Change the current configuration context.

A context is a group of objects that are dependent on and grouped by a parent object. Many objects lie in the "root" context and do not have a specific parent. Other objects, e.g. User objects lie in a sub-context (or child context) of the root - in this case in a LocalUserDatabase. In order to add or modify users you have to be in the correct context, e.g. a LocalUserDatabase called "exampledb". Only objects in the current context can be accessed.

### Example 2.2. Change context

```
Change to a sub/child context:
gw-world:/> cc LocalUserDatabase exampledb
gw-world:/exampledb>

Go back to the parent context:
gw-world:/ospf1/areal> cc ..
gw-world:/ospf1> cc ..
gw-world:/>

Go back to the root context:
gw-world:/ospf1/areal> cc
gw-world:/>

or
gw-world:/ospf1/areal> cc /
gw-world:/>
```

## Usage

```
cc [<Category>] <Type> <Identifier>
```

Change the current context.

```
cc -print
```

Print the current context.

```
cc
```

Change to root context (same as "cc /").

## Options

<b>-print</b>	Print the current context.
<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

## 2.1.5. commit

Save new configuration to media.

### Description

Save the new configuration to media. This command can only be issued after a successful activate

command.

### Usage

```
commit
```



#### **Note**

*Requires Administrator privilege.*

## 2.1.6. copy

Copy object.

### Description

Make a copy of a configuration object. The created copy will have identical values for all properties, except for the identifier, which is modified to be unique for the new object.

Some objects can't be copied. It is not possible to copy an object that has child objects. Also it is not possible to copy for example "DNS" and "DateTime", as there can only be a single instance of these object types.

### Usage

```
copy [<Category>] <Type> [<Identifier>] [<Parent>]
```

### Options

<Category>	Category that groups object types.
<Identifier>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<Parent>	Parent of new object.
<Type>	Type of configuration object to perform operation on.

## 2.1.7. delete

Delete specified objects.

### Description

Delete the specified object, removing it from the configuration.

Add the force flag to delete the object even if it is referenced by other objects or if it is a context that has child objects that aren't deleted. This may cause objects referring to the specified object or one of its children to get errors that must be corrected before the configuration can be activated.

See also: **undelete**

**Example 2.3. Delete an object**

```

Delete an unreferenced object:
gw-world:/> delete Address IP4Address example_ip

Delete a referenced object:
(will cause error in exemplerule)
gw-world:/> set IPRule exemplerule SourceNetwork=examplenet
gw-world:/> delete Address IP4Address examplenet -force

```

**Usage**

```
delete [<Category>] <Type> [<Identifier>] [-force]
```

**Options**

<b>-force</b>	Force object to be deleted even if it's used by other objects or has children.
<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

**Note**

*Requires Administrator privilege.*

**2.1.8. psongen**

Generate random pre-shared key.

**Description**

Generate a pre-shared key of specified size, containing randomized key data. If a key with the specified name exists, the existing key is modified. Otherwise a new key object is created.

**Usage**

```
psongen <Name> [-comments=<String>] [-size={64 | 128 | 256 | 512 | 1024 | 2048 | 4096}]
```

**Options**

<b>-comments=&lt;String&gt;</b>	Comments for this key.
<b>-size={64   128   256   512   1024   2048   4096}</b>	Number of bits of data in the generated key. (Default: 64)
<b>&lt;Name&gt;</b>	Name of key.

**Note**

*Requires Administrator privilege.*

## 2.1.9. reject

Reject changes.

### Description

Reject the changes made to the specified object by reverting to the values of the last committed configuration.

All changes made to the object will be lost. If the object is added after the last commit, it will be removed.

To reject the changes in more than one object, use either the `-recursive` flag to delete a context and all its children recursively or the `-all` flag to reject the changes in *all* objects in the configuration.

See also: **activate**, **commit**

### Example 2.4. Reject changes

```
Reject changes in individual objects:
gw-world:/> set Address IP4Address example_ip
Comments="This comment will be rejected"
gw-world:/> reject Address IP4Address example_ip
gw-world:/> add Address IP4Address example_ip2 Address=1.2.3.4
Comments="This whole object will be removed"
gw-world:/> reject Address IP4Address example_ip2

Reject changes recursively:
(will reject changes in the user database and all users)
gw-world:/exampleddb> set User user1 Comments="Something"
gw-world:/exampleddb> set User user2 Comments="that will be"
gw-world:/exampleddb> set User user3 Comments="rejected"
gw-world:/exampleddb> cc ..
gw-world:/> reject LocalUserDatabase exampleddb -recursive

Reject all changes:
gw-world:/anycontext> reject -all

All changes since the last commit will be rejected:
(example_ip will be removed since it is newly added)
gw-world:/> add IP4Address example_ip Address=1.2.3.4
gw-world:/> delete IP4Address example_ip
gw-world:/> reject IP4Address example_ip
```

### Usage

```
reject [<Category>] <Type> [<Identifier>] [-recursive]
```

Reject changes made to the specified object.

```
reject -all
```

Reject all changes in the configuration.

### Options



<b>-all</b>	Reject all changes in the configuration.
<b>-recursive</b>	Recursively reject changes.
<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

**Note***Requires Administrator privilege.*

## 2.1.10. reset

Reset unit configuration and/or binaries.

### Description

Reset configuration or binaries to factory defaults.

### Usage

```
reset [-configuration] [-unit]
```

### Options

<b>-configuration</b>	Reset configuration to factory default.
<b>-unit</b>	Reset unit to factory defaults.

**Note***Requires Administrator privilege.*

## 2.1.11. set

Set property values.

### Description

Set property values of configuration objects.

Specify the type of object you want to modify and the identifier, if the type has one. Set the properties of the object by writing the propertyname equals (=) and then the value. An optional category can be specified for some object types when using tab completion.

If a mandatory property hasn't been specified or if a property has an error a list of errors will be shown after the specified properties have been set. If an invalid property or value type is specified the command will fail and not modify the object.

See also: **add**

**Example 2.5. Set property values**

```

Set properties for objects that have an identifier property:
gw-world:/> set Address IP4Address example_ip Address=1.2.3.4
Comments="This is an example"
gw-world:/> set IP4Address example_ip2 Address=2.3.4.5
Comments=comment_without_whitespace
gw-world:/main> set Route 1 Comment="A route"
gw-world:/> set IPRule 12 Index=1

Set properties for an object without identifier:
gw-world:/> set DynDnsClientDynDnsOrg Username=example

```

**Usage**

```

set [<Category>] <Type> [<Identifier>] [-disable] [-enable]
  [<key-value pair>]...

```

**Options**

<b>-disable</b>	Disable object. This option is not available if the object is already disabled.
<b>-enable</b>	Enable object. This option is not available if the object is already enabled.
<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;key-value pair&gt;</b>	One or more property-value pairs, i.e. <property name>=<value> or <property name>="<value>".
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

**Note**

*Requires Administrator privilege.*

**2.1.12. show**

Show objects.

**Description**

Show objects.

Show the properties of a specified object. There are a number of flags that can be specified to show otherwise hidden properties. To show a list of object types and categories available in the current context, just type **show**. Show a table of all objects of a type by specifying a type or a category. Use the **-errors** or **-changes** flags to show what objects have been changed or have errors in the configuration.

When showing a table of all objects of a certain type, the status of each object since the last time the

configuration was committed is indicated by a flag. The flags used are:

- The object is deleted.
- o The object is disabled.
- ! The object has errors.
- + The object is newly created.
- \* The object is modified.

Unchanged objects are not indicated by a flag.

When listing categories and object types, categories are indicated by [] and types where objects may be contexts by /.

### Example 2.6. Show objects

```
Show the properties of an individual object:
gw-world:/> show Address IP4Address example_ip
gw-world:/main> show Route 1
gw-world:/> show Client DynDnsClientDynDnsOrg

Show a table of all objects of a type and a selection of their
properties as well as their status:
gw-world:/> show Address IP4Address
gw-world:/> show IP4Address

Show a table of all objects for each type in a category:
gw-world:/> show Address

Show objects with changes and errors:
gw-world:/> show -changes
gw-world:/> show -errors

Show what objects use (refer to) a certain object:
gw-world:/> show Address IP4Address example_ip -references
```

## Usage

```
show
```

Show the types and categories available in the current context.

```
show [<Category>] [<Type> [<Identifier>]] [-disabled] [-references]
```

Show an object or list a type or category.

```
show -errors [-verbose]
```

Show all errors.

```
show -changes
```

Show all changes.

## Options

<b>-changes</b>	Show all changes in the current configuration.
<b>-disabled</b>	Show disabled properties.
<b>-errors</b>	Show all errors in the current configuration.
<b>-references</b>	Show all references to this object from other objects.
<b>-verbose</b>	Show error details.
<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

## 2.1.13. undelete

Restore previously deleted objects.

### Description

Restore a previously deleted object.

This is possible as long as the **activate** command has not been called.

See also: **delete**

#### Example 2.7. Undelete an object

```
Undelete an unreferenced object:
gw-world:/> delete Address IP4Address example_ip
gw-world:/> undelete Address IP4Address example_ip

Undelete a referenced object:
(will remove the error in exemplerule)
gw-world:/> set IPRule exemplerule SourceNetwork=examplenet
gw-world:/> delete Address IP4Address examplenet -force
gw-world:/> undelete Address IP4Address examplenet
```

### Usage

```
undelete [<Category>] <Type> [<Identifier>]
```

### Options

<b>&lt;Category&gt;</b>	Category that groups object types.
<b>&lt;Identifier&gt;</b>	The property that identifies the configuration object. May not be applicable depending on the specified <Type>.
<b>&lt;Type&gt;</b>	Type of configuration object to perform operation on.

***Note***

*Requires Administrator privilege.*

## 2.2. Runtime

### 2.2.1. about

Show copyright/build information.

#### Description

Show copyright and build information.

#### Usage

```
about
```

### 2.2.2. alarm

Show alarm information.

#### Description

Show list of currently active alarms.

#### Usage

```
alarm [-history] [-active]
```

#### Options

- active**        Show the currently active alarms.
- history**      Show the 20 latest alarms.

### 2.2.3. arp

Show ARP entries for given interface.

#### Description

List the ARP cache entries of specified interfaces.

If no interface is given the ARP cache entries of all interfaces will be presented.

The presented list can be filtered using the *ip* and *hw* options.

#### Usage

```
arp
```

Show all ARP entries.

```
arp -show [<Interface>] [-ip=<pattern>] [-hw=<pattern>] [-num=<n>]
```

Show ARP entries.

```
arp -hashinfo [<Interface>]
```

Show information on hash table health.

```
arp -flush [<Interface>]
```

Flush ARP cache of all specified interfaces.

```
arp -notify=<ip> [<Interface>] [-hwsender=<Ethernet address>]
```

Send gratuitous ARP for IP.

## Options

<b>-flush</b>	Flush ARP cache of all specified interfaces.
<b>-hashinfo</b>	Show information on hash table health.
<b>-hw=&lt;pattern&gt;</b>	Show only hardware addresses matching pattern.
<b>-hwsender=&lt;Ethernet address&gt;</b>	Sender ethernet address.
<b>-ip=&lt;pattern&gt;</b>	Show only IP addresses matching pattern.
<b>-notify=&lt;ip&gt;</b>	Send gratuitous ARP for <ip>.
<b>-num=&lt;n&gt;</b>	Show only the first <n> entries per interface. (Default: 20)
<b>-show</b>	Show ARP entries for given interface(s).
<b>&lt;Interface&gt;</b>	Interface name.

## 2.2.4. arpsnoop

Toggle snooping and displaying of ARP requests.

### Description

Toggle snooping and displaying of ARP queries and responses on-screen.

The snooped messages are displayed before the access section validates the sender IP addresses in the ARP data.

### Usage

```
arpsnoop
```

Show snooped interfaces.

```
arpsnoop -all [-verbose]
```

Snoop all interfaces.

```
arpsnoop <interface> [-verbose]
```

Snoop specified interface.

```
arpsnoop -disable
```

Disable all snooping.

### Options

<b>-all</b>	Snoop all interfaces.
<b>-disable</b>	Disable all snooping.
<b>-verbose</b>	Verbose.
<b>&lt;interface&gt;</b>	Interface name.

## 2.2.5. ats

Show active ARP Transaction States.

### Description

Show active ARP Transaction States.

### Usage

```
ats [-num=<n>]
```

### Options

**-num=<n>** Limit list to <n> entries. (Default: 20)

## 2.2.6. bigpond

Show BigPond information.

### Description

Show the BigPond information about specified interface.

### Usage

```
bigpond [<interface>]
```

### Options



<interface> Interface to show BigPond information.

## 2.2.7. blacklist

Blacklist.

### Description

Block and unblock hosts on the black and white list.

Note: Static blacklist hosts cannot be unblocked.

If *-force* is not specified, only the exact host with the service, protocol/port and destiny specified is unblocked.

#### Example 2.8. Block hosts

```
blacklist -show -black -listtime -info
blacklist -block 100.100.100.0/24 -serv=FTP -dest=50.50.50.1 -time=6000
```

### Usage

```
blacklist -show [-creationtime] [-dynamic] [-listtime] [-info]
           [-black] [-white] [-all]
```

Show information about the blacklisted hosts.

```
blacklist -block <host> [-serv=<service>] [-prot={TCP | UDP | ICMP
           | OTHER | TCPUDP | ALL}] [-port=<port number>] [-dest=<ip
           address>] [-time=<seconds>]
```

Block specified netobject.

```
blacklist -unblock <host> [-serv=<service>] [-prot={TCP | UDP |
           ICMP | OTHER | TCPUDP | ALL}] [-port=<port number>]
           [-dest=<ip address>] [-time=<seconds>] [-force]
```

Unblock specified netobject.

### Options

<b>-all</b>	Show all the information.
<b>-black</b>	Show blacklist hosts only.
<b>-block</b>	Block specified netobject. (Admin only)
<b>-creationtime</b>	Show creation time.
<b>-dest=&lt;ip address&gt;</b>	Destination address to block/unblock (ExceptEstablished flag is set on).
<b>-dynamic</b>	Show dynamic hosts only.

<b>-force</b>	Unblock all services for the host that matches to options.
<b>-info</b>	Show detailed information.
<b>-listtime</b>	Show time in list (for dynamic hosts).
<b>-port=&lt;port number&gt;</b>	Number of the port to block/unblock.
<b>-prot={TCP   UDP   ICMP   OTHER   TCPUDP   ALL}</b>	Protocol to block/unblock.
<b>-serv=&lt;service&gt;</b>	Service to block/unblock.
<b>-show</b>	Show information about the blacklisted hosts.
<b>-time=&lt;seconds&gt;</b>	The time that the host will remain blocked.
<b>-unblock</b>	Unblock specified netobject. (Admin only)
<b>-white</b>	Show whitelist hosts only.
<b>&lt;host&gt;</b>	IP address range.

## 2.2.8. buffers

List packet buffers or the contents of a buffer.

### Description

Lists the 20 most recently freed packet buffers, or in-depth information about a specific buffer.

### Usage

```
buffers
```

List the 20 most recently freed buffers.

```
buffers -recent
```

Decode the most recently freed buffer.

```
buffers <Num>
```

Decode buffer number <Num>.

### Options

**-recent**      Decode most recently freed buffer.

**<Num>**        Decode given buffer number.

## 2.2.9. cam

CAM table information.

### Description

Show information about the CAM table(s) and their entries.

### Usage

```
cam [-num=<n>] [<Interface>] [-flush]
```

### Options

<b>-flush</b>	Flush CAM table. If interface is specified, only entries using this interface are flushed. (Admin only)
<b>-num=&lt;n&gt;</b>	Limit list to <n> entries per CAM table. (Default: 20)
<b>&lt;Interface&gt;</b>	Interface.

## 2.2.10. certcache

Show the contents of the certificate cache.

### Description

Show all certificates in the certificate cache.

### Usage

```
certcache
```

## 2.2.11. cfglog

Display configuration log.

### Description

Display the log of the last configuration read attempt.

### Usage

```
cfglog
```

## 2.2.12. connections

List current state-tracked connections.

### Description

List current state-tracked connections.

### Usage

```
connections -show [-num=<n>] [-verbose] [-srciface=<interface>]
               [-destiface=<interface>] [-protocol=<name/num>]
               [-srcport=<port>] [-destport=<port>] [-srcip=<ip addr>]
               [-destip=<ip addr>]
```

List connections.

```
connections
```

Same as "connections -show".

```
connections -hashinfo
```

Show information on hash table health.

```
connections -close [-all] [-srciface=<interface>]
                  [-destiface=<interface>] [-protocol=<name/num>]
                  [-srcport=<port>] [-destport=<port>] [-srcip=<ip addr>]
                  [-destip=<ip addr>]
```

Close connections.

## Options

<b>-all</b>	Mark all connections.
<b>-close</b>	Close all connections that match the filter expression. (Admin only)
<b>-destiface=&lt;interface&gt;</b>	Filter on destination interface.
<b>-destip=&lt;ip addr&gt;</b>	Filter on destination IP address.
<b>-destport=&lt;port&gt;</b>	Show only given destination TCP/UDP port.
<b>-hashinfo</b>	Show information on hash table health.
<b>-num=&lt;n&gt;</b>	Limit list to <n> connections. (Default: 20)
<b>-protocol=&lt;name/num&gt;</b>	Show only given IP protocol.
<b>-show</b>	Show connections.
<b>-srciface=&lt;interface&gt;</b>	Filter on source interface.
<b>-srcip=&lt;ip addr&gt;</b>	Filter on source IP address.
<b>-srcport=&lt;port&gt;</b>	Show only given source TCP/UDP port.
<b>-verbose</b>	Verbose (more information).

## 2.2.13. cpuid

Display info about the cpu.

### Description

Display the make and model of the machine's CPU.

**Usage**

```
cpuid
```

## 2.2.14. crashdump

Show the contents of the crash.dmp file.

**Description**

Show the contents of the crash.dmp file, if it exists.

**Usage**

```
crashdump
```

## 2.2.15. customlog

Show custom configured log messages.

**Description**

Show list of custom configured log messages.

**Usage**

```
customlog [-num=<num>]
```

**Options**

**-num=<num>**     Maximum number of items to list. (Default: 10)

## 2.2.16. dconsole

Displays the content of the diagnose console.

**Description**

The diagnose console is used to help troubleshooting internal problems within the security gateway

**Usage**

```
dconsole [-clean] [-flush] [-date=<date>]
```

**Options**

<b>-clean</b>	Remove all diagnose entries. (Admin only)
<b>-date=&lt;date&gt;</b>	YYYY-MM-DD. Only show entries from this date and forward.
<b>-flush</b>	Flush all diagnose entries to disk. (Admin only)

## 2.2.17. dhcp

Display information about DHCP-enabled interfaces or modify/update their leases.

### Description

Display information about a DHCP-enabled interface.

### Usage

```
dhcp
```

List DHCP enabled interfaces.

```
dhcp -list
```

List DHCP enabled interfaces.

```
dhcp -show [<interface>]
```

Show information about DHCP enabled interface.

```
dhcp -lease={RENEW | RELEASE} <interface>
```

Modify interface lease.

### Options

<b>-lease={RENEW   RELEASE}</b>	Modify interface lease.
<b>-list</b>	List all DHCP enabled interfaces.
<b>-show</b>	Show information about DHCP enabled interface.
<b>&lt;interface&gt;</b>	DHCP Interface.

## 2.2.18. dhcprelay

Show DHCP/BOOTP relay ruleset.

### Description

Display the content of the DHCP/BOOTP relay ruleset and the current routed DHCP relays.

Display filter filters relays based on interface/ip (example: if1 192.168.\*)

### Usage

```
dhcrelay
```

Show the currently relayed DHCP sessions.

```
dhcrelay -show [-rules] [-routes] [<display filter>]...
```

Show DHCP/BOOTP relay ruleset.

```
dhcrelay -release <ip address> [-interface=<Interface>]
```

Terminate relayed session.

## Options

<b>-interface=&lt;Interface&gt;</b>	Interface.
<b>-release</b>	Terminate relayed session <[interface:]ip>. (Admin only)
<b>-routes</b>	Show the currently relayed DHCP sessions.
<b>-rules</b>	Show the DHCP/BOOTP relay ruleset.
<b>-show</b>	Show ruleset.
<b>&lt;display filter&gt;</b>	Display filter, filters relays based on interface/ip.
<b>&lt;ip address&gt;</b>	IP address.

## 2.2.19. dhcpserver

Show content of the DHCP server ruleset.

### Description

Show the content of the DHCP server ruleset and various information about active/inactive leases.

Display filter filters leases based on interface/mac/ip (example: if1 192.168.\*)

### Usage

```
dhcpserver
```

Show DHCP server leases.

```
dhcpserver -show [-rules] [-leases] [-mappings] [<display  
filter>]...
```

Show DHCP server ruleset.

```
dhcpserver -release={STATIC | BLACKLIST}
```

Release static or blacklisted IP.

```
dhcpserver -releaseip <interface> <ip address>
```

Release an active IP.

## Options

<b>-leases</b>	Show DHCP server leases.
<b>-mappings</b>	Show DHCP server IP->MAC mappings.
<b>-release={STATIC   BLACK-LIST}</b>	Release static or blacklisted IP. (Admin only)
<b>-releaseip</b>	Release an active IP. (Admin only)
<b>-rules</b>	Show DHCP server rules.
<b>-show</b>	Show ruleset.
<b>&lt;display filter&gt;</b>	Display filters for leases based on interface/mac/ip (eg. if1 192.168.*).
<b>&lt;interface&gt;</b>	Interface.
<b>&lt;ip address&gt;</b>	IP address.

## 2.2.20. dns

DNS client and queries.

### Description

Show status of the DNS client and manage pending DNS queries.

### Usage

```
dns [-query=<domain name>] [-list] [-remove]
```

## Options

<b>-list</b>	List pending DNS queries.
<b>-query=&lt;domain name&gt;</b>	Resolve domain name.
<b>-remove</b>	Remove all pending DNS queries.

## 2.2.21. dnsbl

DNSBL.

### Description

Show status of DNSBL.

### Usage



```
dnsbl [-show] [<SMTP ALG>] [-clean]
```

### Options

**-clean** Clear DNSBL statistics for ALG.

**-show** Show DNSBL statistics for ALG.

**<SMTP ALG>** Name of SMTP ALG.

## 2.2.22. dynroute

Show dynamic routing policy.

### Description

Show the dynamic routing policy filter ruleset and current exports.

In the "Flags" field of the dynrouting exports, the following letters are used:

- o** Route describe the optimal path to the network
- u** Route is unexported

### Usage

```
dynroute [-rules] [-exports]
```

### Options

**-exports** Show current exports.

**-rules** Show dynamic routing, filter ruleset.

## 2.2.23. frags

Show active fragment reassemblies.

### Description

List active fragment reassemblies.

More detailed information can optionally be obtained for specific reassemblies:

**NEW** Newest reassembly

**ALL** All reassemblies

**0..1023**      Assembly 'N'

### Example 2.9. frags

```
frags NEW
frags 254
```

### Usage

```
frags [{NEW | ALL | <reassembly id>}] [-free] [-done] [-num=<n>]
```

### Options

<b>-done</b>	List done (lingering) reassemblies.
<b>-free</b>	List free instead of active.
<b>-num=&lt;n&gt;</b>	List <n> entries. (Default: 20)
<b>{NEW   ALL   &lt;reassembly id&gt;}</b>	Show in-depth info about reassembly <n>. (Default: all)

## 2.2.24. ha

Show current HA status.

### Description

Show current HA status.

### Usage

```
ha [-activate] [-deactivate]
```

### Options

<b>-activate</b>	Go active.
<b>-deactivate</b>	Go inactive.

## 2.2.25. httpposter

Display HTTPPoster\_URLx status.

### Description

Display configuration and status of configured HTTPPoster\_URLx targets.

### Usage

```
httpposter [-repost] [-display]
```

### Options

- display**      Display status.
- repost**      Re-post all URLs now. (Admin only)

## 2.2.26. hwaccel

List configured Hardware Accelerators.

### Description

Display information about configured Hardware Accelerators.

### Usage

```
hwaccel
```

## 2.2.27. ifstat

Show interface statistics.

### Description

Show list of attached interfaces, or in-depth information about a specific interface.

### Usage

```
ifstat [<Interface>] [-filter=<expr>] [-pbr=<table name>]  
      [-num=<n>] [-restart] [-allindepth]
```

### Options

- allindepth**      Show in-depth information about all interfaces.
- filter=<expr>**      Filter list of interfaces.
- num=<n>**      Limit list to <n> lines. (Default: 20)
- pbr=<table name>**      Only list members of given PBR table(s).
- restart**      Stop and restart the interface. (Admin only)

**<Interface>**                      Name of interface.

## 2.2.28. igmp

IGMP Interfaces.

### Description

Show information about the current state of the IGMP interfaces.

Send simulated messages to test configuration of the interface.

### Usage

```
igmp
```

Prints the current IGMP state.

```
igmp -state [<Interface>]
```

Prints the current IGMP state. If an interface is specified, more details are provided.

```
igmp -query <Interface> [<MC address> [<router address>]]
```

Simulate an incoming IGMP query message.

```
igmp -join <Interface> <MC address> [<host address>]
```

Simulate an incoming IGMP join message.

```
igmp -leave <Interface> <MC address> [<host address>]
```

Simulate an incoming IGMP leave message.

### Options

<b>-join</b>	Simulate an incoming IGMP join message.
<b>-leave</b>	Simulate an incoming IGMP leave message.
<b>-query</b>	Simulate an incoming IGMP query message.
<b>-state</b>	Show the current IGMP state.
<b>&lt;host address&gt;</b>	Host IP address.
<b>&lt;Interface&gt;</b>	Interface.
<b>&lt;MC address&gt;</b>	Multicast Address.
<b>&lt;router address&gt;</b>	Router IP address.

## 2.2.29. ikesnoop

Enable or disable IKE-snooping.

### Description

Turn IKE on-screen snooping on/off. Useful for troubleshooting IPsec connections.

### Usage

```
ikesnoop
```

Show IKE snooping status.

```
ikesnoop -on [<ip address>] [-verbose]
```

Enable IKE snooping.

```
ikesnoop -off
```

Disable IKE snooping.

### Options

<b>-off</b>	Turn IKE snooping off.
<b>-on</b>	Turn IKE snooping on.
<b>-verbose</b>	Enable IKE snooping with verbose output.
<b>&lt;ip address&gt;</b>	IP address to snoop.

## 2.2.30. ippool

Show IP pool information.

### Description

Show information about the current state of the configured IP pools.

### Usage

```
ippool -release [<ip address>] [-all]
```

Forcibly free IP assigned to subsystem.

```
ippool -show [-verbose]
```

Show IP pool information.

### Options

<b>-all</b>	Free all IP addresses.
<b>-release</b>	Forcibly free IP assigned to subsystem. (Admin only)

---

<b>-show</b>	Show IP pool information.
<b>-verbose</b>	Verbose output.
<b>&lt;ip address&gt;</b>	IP address to free.

## 2.2.31. ipsecglobalstats

Show global ipsec statistics.

### Description

List global IPsec statistics.

### Usage

```
ipsecglobalstats [-verbose]
```

### Options

<b>-verbose</b>	Show all statistics.
-----------------	----------------------

## 2.2.32. ipseckeealive

Show status of the IPsec ping keepalives.

### Description

Show status of the IPsec ping keepalives.

### Usage

```
ipseckeealive [-num=<n>]
```

### Options

<b>-num=&lt;n&gt;</b>	Maximum number of entries to display (default: 48).
-----------------------	---

## 2.2.33. ipsecstats

Show the SAs in use.

### Description

List the currently active IKE and IPsec SAs, optionally only showing SAs matching the pattern given for the argument "tunnel".

**Usage**

```
ipsecstats [-ike] [-ipsec] [-u] [-verbose] [-num={ALL | <Integer>}]
[<tunnel>]...
```

**Options**

<b>-ike</b>	Show IKE SAs.
<b>-ipsec</b>	Show IPsec SAs.
<b>-num={ALL   &lt;Integer&gt;}</b>	Maximum number of entries to show (default: 40/8).
<b>-u</b>	Show detailed SA statistics information.
<b>-verbose</b>	Show verbose information.
<b>&lt;tunnel&gt;</b>	Only show SAs matching pattern.

**2.2.34. killsa**

Kill all SAs belonging to the given remote SG/peer.

**Description**

Kill all (IPsec and IKE) SAs associated with a given remote IKE peer IP or optional all SA:s in the system. IKE delete messages are sent.

**Usage**

```
killsa <ip address>
```

Delete SAs belonging to provided remote SG/peer.

```
killsa -all
```

Delete all SAs.

**Options**

<b>-all</b>	Kill all SAs.
<b>&lt;ip address&gt;</b>	IP address of remote SG/peer.



**Note**  
*Requires Administrator privilege.*

**2.2.35. license**

Show contents of the license file.

### Description

Show contents of the license file.

### Usage

```
license
```

## 2.2.36. linkmon

Display link monitoring statistics.

### Description

. If link monitor hosts have been configured, linkmon will monitor host reachability to detect link/NIC problems.

### Usage

```
linkmon
```

## 2.2.37. lockdown

Enable / disable lockdown.

### Description

During local lockdown, only traffic from admin nets to the security gateway itself is allowed. Everything else is dropped.

Lockdown will not affect traffic that does not actually pass through the ruleset, e.g. traffic allowed by IPsecBeforeRules, NetconBeforeRules, SNMPBeforeRules, if such settings are enabled.

Note: If local lockdown has been set by the core itself due to licensing / configuration problems, this command will NOT remove such a lock.

### Usage

```
lockdown
```

Show lockdown status.

```
lockdown {ON | OFF}
```

Enable / disable lockdown.

### Options

**{ON | OFF}**      Enable / disable lockdown.





**Note**  
*Requires Administrator privilege.*

## 2.2.38. logout

Logout user.

### Description

Logout current user.

### Usage

```
logout
```

## 2.2.39. memory

Show memory information.

### Description

Show core memory consumption. Also show detailed memory use of some components and lists.

### Usage

```
memory
```

## 2.2.40. natpool

Show current NAT Pools.

### Description

Show current NAT Pools and in-depth information.

### Usage

```
natpool [-verbose] [<pool name> [<IP address>]] [-num=<Integer>]
```

### Options

<b>-num=&lt;Integer&gt;</b>	Maximum number of items to list (default: 20).
<b>-verbose</b>	Verbose (more information).
<b>&lt;IP address&gt;</b>	Translated IP.
<b>&lt;pool name&gt;</b>	NAT Pool name.

## 2.2.41. ospf

Show runtime OSPF information.

### Description

Show runtime information about the OSPF router process(es).

Note: `-process` is only required if there are >1 OSPF router processes.

### Usage

```
ospf
```

Show runtime information.

```
ospf -iface [<interface>] [-process=<OSPF Router Process>]
```

Show interface information.

```
ospf -area [<OSPF Area>] [-process=<OSPF Router Process>]
```

Show area information.

```
ospf -neighbor [<OSPF Neighbor>] [-process=<OSPF Router Process>]
```

Show neighbor information.

```
ospf -route [{HA | ALT}] [-process=<OSPF Router Process>]
```

Show the internal OSPF process routingtable.

```
ospf -database [-verbose] [-process=<OSPF Router Process>]
```

Show the LSA database.

```
ospf -lsa <lsaID> [-process=<OSPF Router Process>]
```

Show details for a specified LSA.

```
ospf -snoop={ON | OFF} [-process=<OSPF Router Process>]
```

Show troubleshooting messages on the console.

```
ospf -ifacedown <interface> [-process=<OSPF Router Process>]
```

Take specified interface offline.

```
ospf -ifaceup <interface> [-process=<OSPF Router Process>]
```

Take specified interface online.

```
ospf -execute={STOP | START | RESTART} [-process=<OSPF Router Process>]
```

Start/stop/restart OSPF process.

### Options

<b>-area</b>	Show area information.
<b>-database</b>	Show the LSA database.
<b>-execute={STOP   START   RE-START}</b>	Start/stop/restart OSPF process. (Admin only)
<b>-iface</b>	Show interface information.
<b>-ifacedown</b>	Take specified interface offline. (Admin only)
<b>-ifaceup</b>	Take specified interface online. (Admin only)
<b>-lsa</b>	Show details for a specified LSA <lsaID>.
<b>-neighbor</b>	Show neighbor information.
<b>-process=&lt;OSPF Router Process&gt;</b>	Required if there are >1 OSPF router processes.
<b>-route</b>	Show the internal OSPF process routingtable.
<b>-snoop={ON   OFF}</b>	Show troubleshooting messages on the console.
<b>-verbose</b>	Increase amount of information to display.
<b>&lt;interface&gt;</b>	OSPF enabled interface.
<b>&lt;interface&gt;</b>	OSPF enabled interface.
<b>&lt;lsaID&gt;</b>	LSA ID.
<b>&lt;OSPF Area&gt;</b>	OSPF Area.
<b>&lt;OSPF Neighbor&gt;</b>	Neighbor.
<b>{HA   ALT}</b>	Show HA routingtable.

## 2.2.42. pipes

Show pipes information.

### Description

Show list of configured pipes / pipe details / pipe users.

Note: The "pipes" command is not executed right away; it is queued until the end of the second, when pipe values are calculated.

### Usage

```
pipes
```

List all pipes.

```
pipes -users [<Pipe>] [-expr=<String>]
```

List users of a given pipe.

```
pipes -show [<Pipe>] [-expr=<String>]
```

Show pipe details.

### Options

<b>-expr=&lt;String&gt;</b>	Pipe wildcard(*) expression.
<b>-show</b>	Show pipe details.
<b>-users</b>	List users of a given pipe.
<b>&lt;Pipe&gt;</b>	Show pipe details.

## 2.2.43. reconfigure

Initiates a configuration re-read.

### Description

Restart the Security Gateway using the currently active configuration.

### Usage

```
reconfigure
```



#### **Note**

*Requires Administrator privilege.*

## 2.2.44. routemon

List the currently monitored interfaces and gateways.

### Description

List the currently monitored interfaces and/or gateways.

### Usage

```
routemon
```

## 2.2.45. routes

Display routing lists.

### Description

Display information about the routing table(s):

- Contents of a (named) routing table.

- The list of routing tables, along with a total count of route entries in each table, as well as how many of the entries are single-host routes.

Note that "core" routes for interface IP addresses are not normally shown. Use the *-all* switch to show core routes also.

Use the *-switched* switch to show only switched routes.

Explanation of Flags field of the routing tables:

- O** Learned via OSPF
- X** Route is Disabled
- M** Route is Monitored
- A** Published via Proxy ARP
- D** Dynamic (from e.g. DHCP relay, IPsec, L2TP/PPP servers, etc.)
- H** HA synced from cluster peer

## Usage

```
routes [-all] [<table name>] [-switched] [-flushl3cache] [-num=<n>]
      [-nonhost] [-tables] [-lookup=<ip address>] [-verbose]
```

## Options

<b>-all</b>	Also show routes for interface addresses.
<b>-flushl3cache</b>	Flush Layer 3 Cache.
<b>-lookup=&lt;ip address&gt;</b>	Lookup the route for the given IP address.
<b>-nonhost</b>	Do not show single-host routes.
<b>-num=&lt;n&gt;</b>	Limit display to <n> entries. (Default: 20)
<b>-switched</b>	Only show switched routes and L3C entries.
<b>-tables</b>	Display list of named (PBR) routing tables.
<b>-verbose</b>	Verbose.
<b>&lt;table name&gt;</b>	Name of routing table.

## 2.2.46. rules

Show rules lists.

### Description

Shows the content of the various types of rules, i.e. main ruleset, pipe ruleset, etc.

**Example 2.10. Show a range of rules**

```
rules -verbose 1-5 7-9
```

**Usage**

```
rules
```

Show all IP rules.

```
rules <rules>...
```

Show specific range of IP rules.

```
rules -type=IP [-verbose] [-schedule] [<rules>]...
```

Show IP rules.

```
rules -type={ROUTING | PIPE | IDP | THRESHOLD | IGMP} [-verbose]
        [-schedule] [<rules>]...
```

Show a specific type of rules.

**Options**

<b>-schedule</b>	Filter out rules that are not currently allowed by selected schedules.
<b>-type={IP   ROUTING   PIPE   IDP   THRESHOLD   IGMP}</b>	Type of rules to display. (Default: IP)
<b>-verbose</b>	Verbose: show all parameters of the rules.
<b>&lt;rules&gt;</b>	Range of rules to display. (default: all rules).

**2.2.47. sessionmanager**

Session Manager.

**Description**

Show information about the Session Manager, and list currently active users.

Explanation of Timeout flags for sessions:

- D** Session is disabled
- S** Session uses a timeout in its subsystem
- Session does not use timeout

**Usage**

```
sessionmanager
```

Show Session Manager status.

```
sessionmanager -status
```

Show Session Manager status.

```
sessionmanager -list [-num=<n>]
```

List active sessions.

```
sessionmanager -info <session name> <database>
```

Show in-depth information about session.

```
sessionmanager -message <session name> <database> <message text>
```

Send message to session with console.

```
sessionmanager -disconnect <session name> <database>
```

Forcibly terminate session.

### Options

<b>-disconnect</b>	Forcibly terminate session. (Admin only)
<b>-info</b>	Show in-depth information about session.
<b>-list</b>	List active sessions.
<b>-message</b>	Send message to session.
<b>-num=&lt;n&gt;</b>	List <n> number of session.
<b>-status</b>	Show Session Manager status.
<b>&lt;database&gt;</b>	Name of user database.
<b>&lt;message text&gt;</b>	Message to send.
<b>&lt;session name&gt;</b>	Name of session.

## 2.2.48. shutdown

Initiate core shutdown.

### Description

Initiate shutdown of the core. The core will normally be restarted by an external script/application.

### Usage

```
shutdown [<seconds>]
```

## Options

**<seconds>**      Seconds until shutdown. (Default: 5)



### **Note**

*Requires Administrator privilege.*

## 2.2.49. sipalg

SIP ALG.

### Description

List running SIP-ALG configurations, SIP registration and call information.

### Usage

```
sipalg -definition <alg>
```

Show running ALG configuration parameters.

```
sipalg -registration[={SHOW | FLUSH}] <alg>
```

Show or flush current registration table.

```
sipalg -calls <alg>
```

Show active calls table.

```
sipalg -session <alg>
```

Show active SIP sessions.

```
sipalg -connection <alg>
```

Show SIP connections.

```
sipalg -statistics[={SHOW | FLUSH}] <alg>
```

Show or flush SIP counters.

```
sipalg -snoop={ON | OFF} [<ipaddr>] [-verbose]
```

Control SIP snooping. Useful for troubleshooting SIP transactions.

### Options

<b>-calls</b>	Show active calls table.
<b>-connection</b>	Show SIP connections.
<b>-definition</b>	Show running ALG configuration parameters.



<b>-registration</b> [={ <b>SHOW</b>   <b>FLUSH</b> }]	Show or flush registration table. (Default: show)
<b>-session</b>	Show active SIP sessions.
<b>-snoop</b> ={ <b>ON</b>   <b>OFF</b> }	Enable or disable SIP snooping.
<b>-statistics</b> [={ <b>SHOW</b>   <b>FLUSH</b> }]	Show or flush SIP counters. (Default: show)
<b>-verbose</b>	Run SIP snooping in verbose mode.
<b>&lt;alg&gt;</b>	SIP-ALG name.
<b>&lt;ipaddr&gt;</b>	IP Address to snoop.

## 2.2.50. sshserver

SSH Server.

### Description

Show SSH Server status, or start/stop/restart SSH Server.

### Usage

```
sshserver
```

Show server status and list all connected clients.

```
sshserver -status [-verbose]
```

Show server status and list all connected clients.

```
sshserver -keygen [-b=<bits>] [-t={RSA | DSA}]
```

Generate SSH Server private keys.

```
sshserver -start <ssh server>
```

Start SSH Server.

```
sshserver -stop <ssh server>
```

Stop SSH Server.

```
sshserver -restart <ssh server>
```

Restart SSH Server.

### Options

<b>-b</b> =<bits>	Bitsize. (Default: 1024)
<b>-keygen</b>	Generate SSH Server private keys. This operation may take a long time to finish, up to several minutes!
<b>-restart</b>	Stop and start the SSH Server.

<b>-start</b>	Start the SSH Server.
<b>-status</b>	Show server status and list all connected clients.
<b>-stop</b>	Stop the SSH Server.
<b>-t={RSA   DSA}</b>	Type, (default: both RSA and DSA keys will be created).
<b>-verbose</b>	Verbose output.
<b>&lt;ssh server&gt;</b>	SSH Server.



**Note**  
*Requires Administrator privilege.*

## 2.2.51. stats

Display various general firewall statistics.

### Description

Display general information about the firewall, such as uptime, CPU load, resource consumption and other performance data.

### Usage

```
stats
```

## 2.2.52. time

Display current system time.

### Description

Display/set the system date and time.

### Usage

```
time
```

Display current system time.

```
time -set <date> <time>
```

Set system local time: <YYYY-MM-DD> <HH:MM:SS>.

```
time -sync [-force]
```

Synchronize time with timeserver(s) (specified in settings).

### Options

<b>-force</b>	Force synchronization regardless of the MaxAdjust setting.
<b>-set</b>	Set system local time: <YYYY-MM-DD> <HH:MM:SS>.
<b>-sync</b>	Synchronize time with timeserver(s) (specified in settings).
<b>&lt;date&gt;</b>	Date YYYY-MM-DD.
<b>&lt;time&gt;</b>	Time HH:MM:SS.

## 2.2.53. updatecenter

Show autoupdate status and manage IDP/AV databases.

### Description

Show autoupdate mechanism status or force an update.

### Usage

```
updatecenter [-servers] [-update[={ANTIVIRUS | IDP | ALL}]]
              [-status[={ANTIVIRUS | IDP | ALL}]]
              [-removedb={ANTIVIRUS | IDP}]
```

### Options

<b>-removedb={ANTIVIRUS   IDP}</b>	Remove the database for the specified service.
<b>-servers</b>	Show autoupdate server info.
<b>-status[={ANTIVIRUS   IDP   ALL}]</b>	Show update status and database information. (Admin only; Default: all)
<b>-update[={ANTIVIRUS   IDP   ALL}]</b>	Force an update now for the specified service. (Admin only; Default: all)

## 2.2.54. urlcache

List contents of the URL cache.

### Description

List contents of the URL cache. Used for testing during development of HTTPALG.

### Usage

```
urlcache [-verbose] [-count] [-num=<n>] [-server[={STATUS | CONNECT
| DISCONNECT}]]
```

### Options

<b>-count</b>	Only display cache count.
<b>-num=&lt;n&gt;</b>	Limit list to <n> entries. (Default: 20)
<b>-server[={STATUS   CONNECT   DISCONNECT}]</b>	Web Content Filtering Server options. (Default: status)
<b>-verbose</b>	Verbose.

## 2.2.55. userauth

Show logged-on users.

### Description

Show currently logged-on users and other information. Also allows logged-on users to be forcibly logged out.

Note: In the user listing *-list*, only privileges actually used by the policy are displayed.

### Usage

```
userauth
```

List all authenticated users.

```
userauth -list [-num=<n>]
```

List all authenticated users.

```
userauth -privilege
```

List all known privileges (usernames and groups).

```
userauth -user <user ip>
```

Show all information for user(s) with this IP address.

```
userauth -remove <user ip> <Interface>
```

Forcibly log out an authenticated user.

### Options

<b>-list</b>	List all authenticated users.
<b>-num=&lt;n&gt;</b>	Limit list of authenticated users. (Default: 20)
<b>-privilege</b>	List all known privileges (usernames and groups).
<b>-remove</b>	Forcibly log out an authenticated user. (Admin only)
<b>-user</b>	Show all information for user(s) with this IP address.
<b>&lt;Interface&gt;</b>	Interface.
<b>&lt;user ip&gt;</b>	IP address for user(s).

## 2.2.56. vlan

Show information about VLAN.

### Description

Show list of attached Virtual LAN Interfaces, or in-depth information about a specified VLAN.

### Usage

```
vlan [-vlan=<VLAN>] [-interface=<Interface>]
```

### Options

<b>-interface=&lt;Interface&gt;</b>	List VLANs connected to physical interface <Interface>.
<b>-vlan=&lt;VLAN&gt;</b>	VLAN to show information about.

## 2.2.57. vpnstats

Alias for **ipsestats**.

## 2.2.58. zonedefense

Zonedefense.

### Description

Block/unblock IP addresses/net and ethernet addresses.

### Usage

```
zonedefense [-save] [-blockip=<ip address>] [-blockenet=<ethernet  
address>] [-eraseip=<ip address>] [-eraseenet=<ethernet  
address>] [-status] [-show]
```

### Options

<b>-blockenet=&lt;ethernet address&gt;</b>	Block the specified ethernet address.
<b>-blockip=&lt;ip address&gt;</b>	Block the specified IP address/net.
<b>-eraseenet=&lt;ethernet address&gt;</b>	Unblock the specified ethernet address.
<b>-eraseip=&lt;ip address&gt;</b>	Unblock the specified IP address/net.
<b>-save</b>	Save the current zonedefense state on all switches.
<b>-show</b>	Show the current block database.
<b>-status</b>	Show the current status of the zonedefense state machine.

## 2.3. Utility

### 2.3.1. ping

Ping host.

#### Description

Sends one or more ICMP ECHO, TCP SYN or UDP datagrams to the specified IP address of a host. All datagrams are sent preloaded-style (all at once).

The data size *-length* given is the ICMP or UDP data size. 1472 bytes of ICMP data results in a 1500-byte IP datagram (1514 bytes ethernet).

#### Usage

```
ping <host> [-recvif=<interface>] [-srcip=<ip address>]
          [-pbr=<table>] [-count=<1...10>] [-length=<4...8192>]
          [-port=<0...65535>] [-udp] [-tcp] [-verbose]
```

#### Options

<b>-count=&lt;1...10&gt;</b>	Number of packets to send. (Default: 1)
<b>-length=&lt;4...8192&gt;</b>	Packet size. (Default: 4)
<b>-pbr=&lt;table&gt;</b>	Route using PBR Table.
<b>-port=&lt;0...65535&gt;</b>	Destination port of UDP or TCP ping.
<b>-recvif=&lt;interface&gt;</b>	Pass packet through the rule set, simulating that the packet was received by <recvif>.
<b>-srcip=&lt;ip address&gt;</b>	Use this source IP.
<b>-tcp</b>	Send TCP ping.
<b>-udp</b>	Send UDP ping.
<b>-verbose</b>	Verbose (more information).
<b>&lt;host&gt;</b>	IP address of host to ping.

## 2.4. Misc

### 2.4.1. help

Show help for selected topic.

#### Description

The help system contains information about commands and configuration object types.

The fastest way to get help is to simply type **help** followed by the topic that you want help with. A topic can be for example a command name (e.g. **set**) or the name of a configuration object type (e.g. **User**).

When you don't know the name of what you are looking for you can specify the category of the wanted topic with the `-category` option and use tab-completion to display a list of matching topics.

#### Usage

```
help
```

List commands alphabetically.

```
help <Topic>
```

Display help about selected topic from any category.

```
help -category={COMMANDS | TYPES} [ <Topic> ]
```

Display help from a specific topic category.

#### Options

<code>-category={COMMANDS   TYPES}</code>	Topic category.
<code>&lt;Topic&gt;</code>	Help topic.

### 2.4.2. history

Dump history to screen.

#### Description

List recently typed commands that have been stored in the command history.

#### Usage

```
history
```





---

## Chapter 3. Configuration Reference

- Access, page 66
- Address, page 68
- AdvancedScheduleProfile, page 71
- ALG, page 72
- ARP, page 77
- BlacklistWhiteHost, page 78
- Certificate, page 79
- Client, page 80
- COMPortDevice, page 83
- ConfigModePool, page 84
- DateTime, page 85
- Device, page 86
- DHCPRelay, page 87
- DHCPServer, page 88
- DNS, page 90
- Driver, page 91
- DynamicRoutingRule, page 92
- EthernetDevice, page 95
- HighAvailability, page 96
- HTTPPoster, page 97
- IDList, page 98
- IDPRule, page 99
- IKEAlgorithms, page 101
- Interface, page 102
- IPPool, page 111
- IPRule, page 112
- IPRuleFolder, page 114
- IPSecAlgorithms, page 115
- LDAPServer, page 116
- LocalUserDatabase, page 117
- LogReceiver, page 118

- NATPool, page 121
- OSPFProcess, page 122
- Pipe, page 126
- PipeRule, page 129
- PSK, page 130
- RadiusServer, page 131
- RemoteManagement, page 132
- RoutingRule, page 134
- RoutingTable, page 135
- ScheduleProfile, page 137
- Service, page 138
- Settings, page 141
- SSHClientKey, page 154
- ThresholdRule, page 155
- UpdateCenter, page 157
- UserAuthRule, page 158
- ZoneDefenseBlock, page 160
- ZoneDefenseExcludeList, page 161
- ZoneDefenseSwitch, page 162

## 3.1. Access

### Description

Use an access rule to allow or block specific source IP addresses on a specific interface.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the object.
<b>Action</b>	Accept, Expect or Drop. (Default: Drop)
<b>Interface</b>	The interface the packet must arrive on for this rule to be carried out. Exception: the Expect rule.
<b>Network</b>	The IP span that the sender must belong to for this rule to be carried out.
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)

**Comments**      Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.2. Address

This is a category that groups the following object types.

### 3.2.1. AddressFolder

#### Description

An address folder can be used to group related address objects for better overview.

#### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Comments</b>	Text describing the current object. (Optional)

#### 3.2.1.1. EthernetAddress

##### Description

Use an Ethernet Address item to define a symbolic name for an Ethernet MAC address.

##### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Address</b>	Ethernet MAC address, e.g. "12-34-56-78-ab-cd".
<b>UserAuthGroups</b>	Groups and user names that belong to this object. Objects that filter on credentials can only be used as source networks and destinations networks in rules. (Optional)
<b>NoDefinedCredentials</b>	If this property is enabled the object requires user authentication, but has no credentials (user names or groups) defined. This means that the object only requires that a user is authenticated, but ignores any kind of group membership. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

#### 3.2.1.2. EthernetAddressGroup

##### Description

An Ethernet Address Group is used for combining several Ethernet Address objects for simplified management.

##### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Members</b>	Group members.
<b>UserAuthGroups</b>	Groups and user names that belong to this object. Objects that fil-

	ter on credentials can only be used as source networks and destinations networks in rules. (Optional)
<b>NoDefinedCredentials</b>	If this property is enabled the object requires user authentication, but has no credentials (user names or groups) defined. This means that the object only requires that a user is authenticated, but ignores any kind of group membership. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.2.1.3. IP4Address

#### Description

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

#### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Address</b>	IP address, e.g. "172.16.50.8", "192.168.30.7,192.168.30.11", "192.168.7.0/24" or "172.16.25.10-172.16.25.50".
<b>UserAuthGroups</b>	Groups and user names that belong to this object. Objects that filter on credentials can only be used as source networks and destinations networks in rules. (Optional)
<b>NoDefinedCredentials</b>	If this property is enabled the object requires user authentication, but has no credentials (user names or groups) defined. This means that the object only requires that a user is authenticated, but ignores any kind of group membership. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.2.1.4. IP4Group

#### Description

An IP4 Address Group is used for combining several IP4 Address objects for simplified management.

#### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Members</b>	Group members.
<b>Exclude</b>	Addresses that will be excluded from the group. (Optional)
<b>UserAuthGroups</b>	Groups and user names that belong to this object. Objects that filter on credentials can only be used as source networks and destinations networks in rules. (Optional)
<b>NoDefinedCredentials</b>	If this property is enabled the object requires user authentication, but has no credentials (user names or groups) defined. This means that the object only requires that a user is authenticated, but ignores any kind of group membership. (Default: No)

<b>Comments</b>	Text describing the current object. (Optional)
-----------------	--

### 3.2.1.5. IP4HAAddress

#### Description

Use an IP4 HA Address item to define a name for a specific IP4 host, network or range for each node in a high availability cluster.

#### Properties

<b>Name</b>	Specifies a symbolic name for the network object. (Identifier)
<b>Address</b>	An IP address with one instance for each node in the high availability cluster.
<b>UserAuthGroups</b>	Groups and user names that belong to this object. Objects that filter on credentials can only be used as source networks and destinations networks in rules. (Optional)
<b>NoDefinedCredentials</b>	If this property is enabled the object requires user authentication, but has no credentials (user names or groups) defined. This means that the object only requires that a user is authenticated, but ignores any kind of group membership. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.2.2. EthernetAddress

The definitions here are the same as in Section 3.2.1.1, “EthernetAddress” .

## 3.2.3. EthernetAddressGroup

The definitions here are the same as in Section 3.2.1.2, “EthernetAddressGroup” .

## 3.2.4. IP4Address

The definitions here are the same as in Section 3.2.1.3, “IP4Address” .

## 3.2.5. IP4Group

The definitions here are the same as in Section 3.2.1.4, “IP4Group” .

## 3.2.6. IP4HAAddress

The definitions here are the same as in Section 3.2.1.5, “IP4HAAddress” .

## 3.3. AdvancedScheduleProfile

### Description

An advanced schedule profile contains definitions of occurrences used by various policies in the system.

### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.3.1. AdvancedScheduleOccurrence

#### Description

An advanced schedule occurrence specifies an occurrence that should happen between certain times for days in month/week

#### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>StartTime</b>	Start Time of occurrence in the format HH:MM. For example 13:30.
<b>EndTime</b>	End Time of occurrence in the format HH:MM. For example 14:15.
<b>Occurrence</b>	Specify type of occurrence. (Default: Weekly)
<b>Weekly</b>	Specifies days in week the schedule occurrence should be activated. Monday corresponds to 1 and Sunday 7. (Default: 1-7)
<b>Monthly</b>	Specifies days in month the schedule occurrence should be activated. The schedule only occurs at days that exists in the month. (Default: 1-31)
<b>Comments</b>	Text describing the current object. (Optional)



#### Note

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.4. ALG

This is a category that groups the following object types.

### 3.4.1. ALG\_FTP

#### Description

Use an FTP Application Layer Gateway to manage FTP traffic through the system.

#### Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
<b>AllowServerPassive</b>	Allow server to use passive mode (unsafe for server). (Default: No)
<b>ServerPorts</b>	Server data ports. (Default: 1024-65535)
<b>AllowClientActive</b>	Allow client to use active mode (unsafe for client). (Default: No)
<b>ClientPorts</b>	Client data ports. (Default: 1024-65535)
<b>AllowUnknownCommands</b>	Allow unknown commands. (Default: No)
<b>AllowSITEEXEC</b>	Allow SITE EXEC. (Default: No)
<b>MaxLineLength</b>	Maximum line length in control channel. (Default: 256)
<b>MaxCommandRate</b>	Maximum number of commands per second. (Default: 20)
<b>Allow8BitStrings</b>	Allow 8-bit strings in control channel. (Default: Yes)
<b>AllowResumeTransfer</b>	Allow RESUME even in case of content scanning. (Default: No)
<b>Antivirus</b>	Disabled, Audit or Protect. (Default: Disabled)
<b>ScanExclude</b>	List of files to exclude from antivirus scanning. (Optional)
<b>CompressionRatio</b>	A compression ratio higher than this value will trigger the action in Compression Ratio Action, a value of zero will disable all compression checks. (Default: 20)
<b>CompressionRatioAction</b>	The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)
<b>FileListType</b>	Specifies if the file list contains files to allow or deny. (Default: Block)
<b>FailModeBehavior</b>	Standard behaviour on error: Allow or Deny. (Default: Deny)
<b>File</b>	List of file types to allow or deny. (Optional)
<b>VerifyContentMimetype</b>	Verify that file extensions correspond to the MIME type. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)



## 3.4.2. ALG\_H323

### Description

Use an H.323 Application Layer Gateway to manage H.323 multimedia traffic.

### Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
<b>AllowTCPDataChannels</b>	Allow TCP data channels (T.120). (Default: Yes)
<b>MaxTCPDataChannels</b>	Maximum number of TCP data channels per call. (Default: 10)
<b>TranslateAddresses</b>	Automatic or Specific. (Default: Automatic)
<b>TranslateLogicalChannelAddresses</b>	Translate logical channel addresses. (Default: Yes)
<b>MaxGKRegLifeTime</b>	Max Gatekeeper Registration Lifetime. (Default: 1800)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.4.3. ALG\_HTTP

### Description

Use an HTTP Application Layer Gateway to filter HTTP traffic.

### Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
<b>RemoveCookies</b>	Remove cookies. (Default: No)
<b>RemoveScripts</b>	Remove Javascript/VBScript. (Default: No)
<b>RemoveApplets</b>	Remove Java applets. (Default: No)
<b>RemoveActiveX</b>	Remove ActiveX objects (including Flash). (Default: No)
<b>VerifyUTF8URL</b>	Verify that URLs does not contain invalid UTF8 encoding. (Default: No)
<b>BlackURLDisplayReason</b>	Message to show when there is an attempt to access a black-listed site. (Optional)
<b>MaxDownloadSize</b>	The maximal allowed file size in kB. (Optional)
<b>FileListType</b>	Specifies if the file list contains files to allow or deny. (Default: Block)
<b>FailModeBehavior</b>	Standard behaviour on error: Allow or Deny. (Default: Deny)
<b>File</b>	List of file types to allow or deny. (Optional)
<b>VerifyContentMimetype</b>	Verify that file extentions correspond to the MIME type. (Default: No)

<b>Antivirus</b>	Disabled, Audit or Protect. (Default: Disabled)
<b>ScanExclude</b>	List of files to exclude from antivirus scanning. (Optional)
<b>CompressionRatio</b>	A compression ratio higher than this value will trigger the action in Compression Ratio Action, a value of zero will disable all compression checks. (Default: 20)
<b>CompressionRatioAction</b>	The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)
<b>WebContentFilteringMode</b>	Disabled, Audit or Enable. (Default: Disabled)
<b>FilteringCategories</b>	Web content categories to block. (Optional)
<b>NonManagedAction</b>	Action to take for content that hasn't been classified. (Default: Allow)
<b>AllowFilteringOverride</b>	Allow the user to display a blocked site. (Default: No)
<b>AllowFilteringReclassification</b>	Allow reclassification of sites. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.4.3.1. ALG\_HTTP\_URL

#### Description

Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

#### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Action</b>	Whitelist or Blacklist. (Default: Blacklist)
<b>URL</b>	Specifies the URL to blacklist or whitelist.
<b>Comments</b>	Text describing the current object. (Optional)



#### **Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

### 3.4.4. ALG\_POP3

#### Description

Use an POP3 Application Layer Gateway to manage POP3 traffic through the system.

#### Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
-------------	---

<b>BlockUserPass</b>	Block clients from sending USER and PASS command. (Default: No)
<b>HideUser</b>	Prevent server from revealing that a user name do not exist. (Default: No)
<b>AllowUnknownCommands</b>	Allow unknown commands. (Default: No)
<b>FileListType</b>	Specifies if the file list contains files to allow or deny. (Default: Block)
<b>FailModeBehavior</b>	Standard behaviour on error: Allow or Deny. (Default: Deny)
<b>File</b>	List of file types to allow or deny. (Optional)
<b>VerifyContentMimetype</b>	Verify that file extentions correspond to the MIME type. (Default: No)
<b>Antivirus</b>	Disabled, Audit or Protect. (Default: Disabled)
<b>ScanExclude</b>	List of files to exclude from antivirus scanning. (Optional)
<b>CompressionRatio</b>	A compression ratio higher than this value will trigger the action in Compression Ratio Action, a value of zero will disable all compression checks. (Default: 20)
<b>CompressionRatioAction</b>	The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.4.5. ALG\_SIP

#### Description

Use a SIP ALG to manage SIP based multimedia sessions.

#### Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
<b>MaxSessionsPerId</b>	Maximum number of sessions per SIP URI. (Default: 5)
<b>MaxRegistrationTime</b>	The maximum allowed time between registration requests. (Default: 3600)
<b>SipReqRespTmout</b>	Timeout value between a request and its response. (Default: 180)
<b>SipSignalTmout</b>	Timeout value for last seen SIP message. (Default: 43200)
<b>DataChannelTmout</b>	Timeout value for data channel. (Default: 120)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.4.6. ALG\_TFTP

#### Description

Use an TFTP Application Layer Gateway to manage TFTP traffic through the system.

## Properties

<b>Name</b>	Specifies a symbolic name for the ALG. (Identifier)
<b>AllowedCommands</b>	Specifies allowed commands. (Default: ReadWrite)
<b>RemoveOptions</b>	Remove option part from request packet. (Default: No)
<b>AllowUnknownOptions</b>	Allow unknown options in request packet. (Default: No)
<b>MaxBlocksize</b>	Max value for the blksize option. (Optional)
<b>MaxFileTransferSize</b>	Max size for transferred file. (Optional)
<b>BlockDirectoryTraversal</b>	Prevent directory traversal (consecutive dots in filenames). (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.5. ARP

### Description

Use an ARP entry to publish additional IP addresses and/or MAC addresses on a specified interface.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Mode</b>	Static, Publish or XPublish. (Default: Publish)
<b>Interface</b>	Indicates the interface to which the ARP entry applies; e.g. the interface the address shall be published on.
<b>IP</b>	The IP address to be published or statically bound to a hardware address.
<b>MACAddress</b>	The hardware address associated with the IP address. (Default: 00-00-00-00-00-00)
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.6. BlacklistWhiteHost

### Description

Manually configured whitelist hosts are used to prevent from blocking a host/network on either by default or based on a schedule.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Addresses</b>	Specifies the addresses that will be whitelisted.
<b>Service</b>	Specifies the service that will be whitelisted.
<b>Schedule</b>	The schedule when the whitelist should be active. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.7. Certificate

### Description

An X. 509 certificate is used to authenticate a VPN client or gateway when establishing an IPsec tunnel.

### Properties

<b>Name</b>	Specifies a symbolic name for the certificate. (Identifier)
<b>Type</b>	Local, Remote or Request.
<b>CertificateData</b>	Certificate data.
<b>PrivateKey</b>	Private key.
<b>NoCRLs</b>	Disable CRLs (Certificate Revocation Lists). (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.8. Client

This is a category that groups the following object types.

### 3.8.1. DynDnsClientCjbNet

#### Description

Configure the parameters used to connect to the Cjb.net DynDNS service.

#### Properties

<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



#### *Note*

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

### 3.8.2. DynDnsClientDLink

#### Description

Configure the parameters used to connect to the D-Link DynDNS service.

#### Properties

<b>DNSName</b>	The DNS name excluding the .dlinkddns.com suffix.
<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



#### *Note*

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

### 3.8.3. DynDnsClientDLinkChina

#### Description

Configure the parameters used to connect to the D-Link DynDNS service (China only).

#### Properties



<b>DNSName</b>	The DNS name excluding the .dlinkddns.com suffix.
<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.8.4. DynDnsClientDyndnsOrg

**Description**

Configure the parameters used to connect to the dyndns.org DynDNS service.

**Properties**

<b>DNSName</b>	The DNS name excluding the .dyndns.org suffix.
<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.8.5. DynDnsClientDyngCx

**Description**

Configure the parameters used to connect to the dyng.cx DynDNS service.

**Properties**

<b>DNSName</b>	The DNS name excluding the .dyng.cx suffix.
<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.8.6. DynDnsClientPeanutHull

### Description

Configure the parameters used to connect to the Peanut Hull DynDNS service.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>DNSNames</b>	Specifies the DNS names separated by ";".
<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.8.7. LoginClientBigPond

### Description

Configure the parameters used to provide automatic logon to BigPond Internet service.

### Properties

<b>Username</b>	Username.
<b>Password</b>	The password for the specified username. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.9. COMPortDevice

### Description

A serial communication port, that is used for accessing the CLI.

### Properties

<b>Port</b>	Port. (Identifier)
<b>BitsPerSecond</b>	Bits per second. (Default: 9600)
<b>DataBits</b>	Data bits. (Default: 8)
<b>Parity</b>	Parity. (Default: None)
<b>StopBits</b>	Stop bits. (Default: 1)
<b>FlowControl</b>	Flow control. (Default: None)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.10. ConfigModePool

### Description

An IKE Config Mode Pool will dynamically assign the IP address, DNS server, WINS server etc. to the VPN client connecting to this gateway.

### Properties

<b>IPPoolType</b>	Specifies whether a predefined IP Pool or a static set of IP addresses should be used as IP address source.
<b>IPPool</b>	Specifies the IP pool to use for assigning IP addresses to VPN clients.
<b>IPPoolAddress</b>	Specifies the set of IP addresses to use for assigning IP addresses to VPN clients.
<b>IPPoolNetmask</b>	Specifies the netmask to assign to VPN clients.
<b>DNS</b>	Specifies the IP address of a DNS server that a VPN client should be able to connect to. (Optional)
<b>NBNSIP</b>	Specifies the IP address of a NBNS/WINS server that a VPN client should be able to connect to. (Optional)
<b>DHCP</b>	Specifies the IP address of a DHCP that that a VPN client should be able to connect to. (Optional)
<b>Subnets</b>	Specifies additional subnets behind this gateway. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.11. DateTime

### Description

Set the date, time and time zone information for this system.

### Properties

<b>TimeZone</b>	Specifies the time zone. (Default: GMT)
<b>DSTEnabled</b>	Enable daylight saving time. (Default: Yes)
<b>DSTOffset</b>	Daylight saving time offset in minutes. (Default: 60)
<b>DSTStartMonth</b>	What month daylight saving time starts. (Default: March)
<b>DSTStartDay</b>	What day of month daylight saving time starts. (Default: 1)
<b>DSTEndMonth</b>	What month daylight saving time ends. (Default: October)
<b>DSTEndDay</b>	What day of month daylight saving time ends. (Default: 1)
<b>TimeSynchronization</b>	Enable time synchronization. (Default: Disable)
<b>TimeSyncServerType</b>	Type of server for time synchronization, UDPTIME or SNTP (Simple Network Time Protocol). (Default: SNTP)
<b>TimeSyncServer1</b>	DNS hostname or IP Address of Timeserver 1.
<b>TimeSyncServer2</b>	DNS hostname or IP Address of Timeserver 2. (Optional)
<b>TimeSyncServer3</b>	DNS hostname or IP Address of Timeserver 3. (Optional)
<b>TimeSyncInterval</b>	Seconds between each resynchronization. (Default: 86400)
<b>TimeSyncMaxAdjust</b>	Maximum time drift in seconds that a server is allowed to adjust. (Default: 600)
<b>TimeSyncGroupIntervalSize</b>	Interval according to which server responses will be grouped. (Default: 10)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.12. Device

### Description

Global parameters for this device.

### Properties

<b>Name</b>	Name of the device. (Default: Device)
<b>ConfigVersion</b>	Version number of the configuration. (Default: 1)
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.13. DHCPRelay

### Description

Use a DHCP Relay to dynamically alter the routing table according to relayed DHCP leases.

### Properties

<b>Name</b>	Specifies a symbolic name for the relay rule. (Identifier)
<b>Action</b>	Ignore, Relay or BootpFwd. (Default: Ignore)
<b>SourceInterface</b>	The source interface of the DHCP packet. (Optional)
<b>TargetDHCPServer</b>	Specifies the IP of the server to send the relayed DHCP packets to.
<b>IPOfferFilter</b>	Specifies the span of IP addresses that are allowed to be relayed from the DHCP server. (Default: 1)
<b>AddRoute</b>	Enable dynamic adding of routes as leases are added and removed. (Default: No)
<b>AddRouteLocalIP</b>	The IP Address specified here will automatically be published on the interfaces where a route is added. (Optional)
<b>AddRouteGatewayIP</b>	The IP used as gateway to reach hosts on this route. (Optional)
<b>RoutingTable</b>	Specifies the routing table the clients host route should be added to. (Default: main)
<b>MaxRelaysPerInterface</b>	Specifies how many relays are allowed per interface, that means, how many DHCP clients are allowed to be relayed through each interface. (Optional)
<b>AgentIP</b>	Define what IP the relay should use as gateway IP when passing the requests to the DHCP server. (Default: Recv)
<b>AllowNULLOffers</b>	Accept server responses offering IP address "0.0.0.0" (no IP address offered). (Default: No)
<b>ProxyARPAAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes needed for the relay via Proxy ARP. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interface/interfaces on which the security gateway should publish routes needed for the relay via Proxy ARP. (Optional)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.14. DHCP Server

### Description

A DHCP Server determines a set of IP addresses and host configuration parameters to hand out to DHCP clients attached to a given interface.

### Properties

<b>Name</b>	Specifies a symbolic name for the DHCP Server rule. (Identifier)
<b>Interface</b>	The source interface to listen for DHCP requests on. This can be a single interface or a group of interfaces.
<b>IPAddressPool</b>	A range, group or network that the DHCP Server will use as IP address pool to give out DHCP leases from.
<b>Netmask</b>	Netmask sent to the DHCP Client.
<b>DefaultGateway</b>	Specifies what IP should be sent to the client for use as default gateway. If unspecified or if 0.0.0.0 is specified, the IP given to the client will be sent as gateway. (Optional)
<b>Domain</b>	Domain name used for DNS resolution. (Optional)
<b>LeaseTime</b>	The time, in seconds, that a DHCP lease should be provided to a host after this the client have to renew the lease. (Default: 86400)
<b>DNS1</b>	IP of the primary DNS server. (Optional)
<b>DNS2</b>	IP of the secondary DNS server. (Optional)
<b>NBNS1</b>	IP of the primary Windows Internet Name Service (WINS) server that is used in Microsoft environments which uses the NetBIOS Name Servers (NBNS) to assign IP addresses to NetBIOS names. (Optional)
<b>NBNS2</b>	IP of the primary Windows Internet Name Service (WINS) server that is used in Microsoft environments which uses the NetBIOS Name Servers (NBNS) to assign IP addresses to NetBIOS names. (Optional)
<b>NextServer</b>	IP address of next server in the boot process. (Optional)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.14.1. DHCP Server Pool Static Host

#### Description

Static DHCP Server host entry

#### Properties



<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Host</b>	IP Address of the host.
<b>MACAddress</b>	The hardware address of the host.
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.14.2. DHCP Server Custom Option

### Description

Extend the DHCP Server functionality by adding custom options that will be handed out to the DHCP clients.

### Properties

<b>Code</b>	The DHCP option code. (Identifier)
<b>Type</b>	What type the option is, i.e. STRING, IP4 and so on. (Default: UINT8)
<b>Param</b>	The parameter sent with the code, this can be one parameter or a comma separated list. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.15. DNS

### Description

Configure the DNS (Domain Name System) client settings.

### Properties

<b>DNSServer1</b>	IP of the primary DNS Server. (Optional)
<b>DNSServer2</b>	IP of the secondary DNS Server. (Optional)
<b>DNSServer3</b>	IP of the tertiary DNS Server. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.16. Driver

This is a category that groups the following object types.

### 3.16.1. IXP4NPEthernetDriver

#### Description

Intel (IXP4xxNPE) Fast Ethernet Adaptor.

#### Properties

**Comments**     Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

### 3.16.2. MarvellEthernetPCIDriver

#### Description

Marvell (88E8001,88E8053,88E8062) Fast and Gigabit Ethernet Adaptor.

#### Properties

**Comments**     Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

### 3.16.3. R8139EthernetPCIDriver

#### Description

RealTek (8139) Fast Ethernet Adaptor.

#### Properties

**Comments**     Text describing the current object. (Optional)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.17. DynamicRoutingRule

### Description

A Dynamic Routing Policy rule creates a filter to catch statically configured or OSPF learned routes. The matched routes can be controlled by the action rules to be either exported to OSPF processes or to be added to one or more routing tables.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule. (Optional)
<b>From</b>	OSPF or Routing table. (Default: OSPF)
<b>OSPFProcess</b>	Specifies from which OSPF process the route should be imported from into either a routing table or another OSPF process.
<b>RoutingTable</b>	Specifies from which routing table a route should be imported into the OSPF AS or copied into another routing table.
<b>DestinationInterface</b>	The interface that the policy has to match. (Optional)
<b>DestinationNetworkExactly</b>	Specifies if the route needs to match a specific network exactly. (Optional)
<b>DestinationNetworkIn</b>	Specifies if the route just needs to be within a specific network. (Optional)
<b>NextHop</b>	The next hop (router) on the route that this policy has to match. (Optional)
<b>MetricRange</b>	Specifies an interval that the metric of the routes needs to be within. (Optional)
<b>RouterID</b>	Specifies if the policy should filter on router ID. (Optional)
<b>OSPFRouteType</b>	Specifies if the policy should filter on OSPF router type. (Optional)
<b>OSPFTagRange</b>	Specifies an interval that the tag of the routers need to be within. (Optional)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

### 3.17.1. DynamicRoutingRuleExportOSPF

### Description

An OSPF action is used to manipulate and export new or changed routes to an OSPF Router Process.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>ExportToProcess</b>	Specifies to which OSPF Process the route change should be exported.
<b>SetTag</b>	Specifies a tag for this route. This tag can be used in other routers for filtering. (Optional)
<b>SetRouteType</b>	The external route type. (Optional)
<b>OffsetMetric</b>	Increases the metric of the imported route by this value. (Optional)
<b>LimitMetricRange</b>	Limits the metrics for these routes to a minimum and maximum value, if a route has a higher or lower value then specified it will be set to the specified value. (Optional)
<b>SetForward</b>	IP to route over. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



#### Note

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.17.2. DynamicRoutingRuleAddRoute

### Description

A routing action is used to manipulate and insert new or changed routes to one or more local routing tables.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Destination</b>	Specifies to which routing table the route changes to the OSPF Process should be exported.
<b>OverrideStatic</b>	Allow override of static routes. (Default: No)
<b>OverwriteDefault</b>	Allow overwrite of default route. (Default: No)
<b>OffsetMetric</b>	Increases the metric by this value. (Optional)
<b>OffsetMetricType2</b>	Increases the for Type2 routers metric by this value. (Optional)
<b>LimitMetricRange</b>	Limits the metrics for these routes to a minimum and maximum value, if a route has a higher or lower value then specified it will be set to the specified value. (Optional)

<b>ProxyARPAAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.18. EthernetDevice

### Description

Hardware settings for an Ethernet interface.

### Properties

<b>Name</b>	Specifies a symbolic name for the device. (Identifier)
<b>EthernetDriver</b>	The Ethernet PCI driver that should be used by the interface.
<b>PCIBus</b>	PCI bus number where the Ethernet adapter is installed.
<b>PCISlot</b>	PCI slot number used by the Ethernet adapter.
<b>PCIPort</b>	Some Ethernet adapters have multiple ports that share the same bus and slot number. This parameter specifies what port to be used.
<b>Media</b>	Specifies if the link speed should be auto-negotiated or locked to a static speed. (Default: Auto)
<b>Duplex</b>	Specifies if the duplex should be auto-negotiated or locked to full or half duplex. (Default: Auto)
<b>MACAddress</b>	The hardware address for the interface. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.19. HighAvailability

### Description

Configure the High Availability cluster parameters for this system.

### Properties

<b>Enabled</b>	Enable high availability. (Default: No)
<b>ClusterID</b>	A (locally) unique cluster ID to use in identifying this group of HA security gateways. (Default: 0)
<b>SyncIface</b>	Specifies the interface used for state synchronization.
<b>NodeID</b>	Master or Slave. (Default: Master)
<b>HASyncBufSize</b>	How much sync data, in KB, to buffer while waiting for acknowledgments from the cluster peer. (Default: 1024)
<b>HASyncMaxPktBurst</b>	The maximum number of state sync packets to send in a burst. (Default: 20)
<b>HAInitialSilence</b>	The number of seconds to stay silent on startup or after reconfiguration. (Default: 5)
<b>UseUniqueSharedMac</b>	Use a unique shared mac address for each interface. (Default: No)



### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*



## 3.20. HTTPPoster

### Description

Use the HTTP poster for dynamic DNS or automatic logon to services using web-based authentication.

### Properties

<b>URL1</b>	The first URL that will be posted when the security gateway is loaded. (Optional)
<b>URL2</b>	The second URL that will be posted when the security gateway is loaded. (Optional)
<b>URL3</b>	The third URL that will be posted when the security gateway is loaded. (Optional)
<b>RepDelay</b>	Delay in seconds until all URLs are refetched. (Default: 1200)
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.21. IDList

### Description

An ID list contains IDs, which are used within the authentication process when establishing an IPsec tunnel.

### Properties

<b>Name</b>	Specifies a symbolic name for the ID list. (Identifier)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.21.1. ID

#### Description

An ID is used to define parameters that are matched against the subject field in an X.509 certificate when establishing an IPsec tunnel.

#### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>Type</b>	IP, DNS, E-Mail or Distinguished name.
<b>IP</b>	IP address.
<b>Hostname</b>	Host name.
<b>CommonName</b>	Common name of the owner of the certificate. (Optional)
<b>OrganizationName</b>	Organization name of the owner of the certificate. (Optional)
<b>OrganizationalUnit</b>	Organizational unit of the owner of the certificate. (Optional)
<b>Country</b>	Specifies the country. (Optional)
<b>LocalityName</b>	Locality. (Optional)
<b>EmailAddress</b>	E-mail address. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.22. IDPRule

### Description

An IDP Rule defines a filter for matching specific network traffic. When the filter criteria is met, the IDP Rule Actions are evaluated and possible actions taken.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule. (Optional)
<b>SourceInterface</b>	Specifies the name of the receiving interface to be compared to the received packet.
<b>SourceNetwork</b>	Specifies the sender span of IP addresses to be compared to the received packet.
<b>DestinationInterface</b>	Specifies the the destination interface to be compared to the received packet.
<b>DestinationNetwork</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet.
<b>Service</b>	Specifies a service that will be used as a filter parameter when matching traffic with this rule.
<b>Schedule</b>	By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

### 3.22.1. IDPRuleAction

### Description

An IDP Rule Action specifies what signatures to search for in the network traffic, and what action to take if those signatures are found.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Action</b>	Specifies what action to take if the given signature is found. (Default: Audit)
<b>Signatures</b>	Specifies what signature(s) to search for in the network traffic. (Optional)
<b>ZoneDefense</b>	Activate ZoneDefense. (Default: No)

<b>BlackList</b>	Activate BlackList. (Default: No)
<b>BlackListTimeToBlock</b>	The number of seconds that the dynamic black list should remain. (Optional)
<b>BlackListBlockOnlyService</b>	Only block the service that triggered the blacklisting. (Default: No)
<b>BlackListIgnoreEstablished</b>	Do not drop existing connection. (Default: No)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.23. IKEAlgorithms

### Description

Configure algorithms which are used in the IKE phase of an IPsec session.

### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>NULLEnabled</b>	Enable plaintext. (Default: No)
<b>DESEnabled</b>	Enable DES encryption algorithm. (Default: No)
<b>DES3Enabled</b>	Enable 3DES encryption algorithm. (Default: No)
<b>AESEnabled</b>	Enable AES encryption algorithm. (Default: No)
<b>BlowfishEnabled</b>	Enable Blowfish encryption algorithm. (Default: No)
<b>TwofishEnabled</b>	Enable Twofish encryption algorithm. (Default: No)
<b>CAST128Enabled</b>	Enable CAST128 encryption algorithm. (Default: No)
<b>BlowfishMinKeySize</b>	Specifies the minimum Blowfish key size in bits. (Default: 128)
<b>BlowfishKeySize</b>	Specifies the Blowfish preferred key size in bits. (Default: 128)
<b>BlowfishMaxKeySize</b>	Specifies the maximum Blowfish key size in bits. (Default: 448)
<b>TwofishMinKeySize</b>	Specifies the minimum Twofish key size in bits. (Default: 128)
<b>TwofishKeySize</b>	Specifies the Twofish preferred key size in bits. (Default: 128)
<b>TwofishMaxKeySize</b>	Specifies the maximum Twofish key size in bits. (Default: 256)
<b>AESMinKeySize</b>	Specifies the minimum AES key size in bits. (Default: 128)
<b>AESKeySize</b>	Specifies the preferred AES key size in bits. (Default: 128)
<b>AESMaxKeySize</b>	Specifies the maximum AES key size in bits. (Default: 256)
<b>MD5Enabled</b>	Enable MD5 integrity algorithm. (Default: No)
<b>SHA1Enabled</b>	Enable SHA1 integrity algorithm. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.24. Interface

This is a category that groups the following object types.

### 3.24.1. DefaultInterface

#### Description

A special interface used to represent internal mechanisms in the system as well as an abstract "any" interface.

#### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.24.2. Ethernet

#### Description

An Ethernet interface represents a logical endpoint for Ethernet traffic.

#### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>IP</b>	The IP address of the interface.
<b>Network</b>	The network of the interface.
<b>DefaultGateway</b>	The default gateway of the interface. (Optional)
<b>Broadcast</b>	The broadcast address of the connected network. (Optional)
<b>PrivateIP</b>	The private IP address of this high availability node. (Optional)
<b>NOCHB</b>	This will disable sending Cluster Heartbeats from this interface (used by HA to detect if a node is online and working). (Optional)
<b>MTU</b>	Specifies the size (in bytes) of the largest packet that can be passed onward. (Default: 1500)
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 100)
<b>DHCPEnabled</b>	Specifies that DHCP should be enabled on this interface. (Default: No)
<b>DHCPHostName</b>	Optional DHCP Host Name. Leave blank to use default name. (Optional)
<b>EthernetDevice</b>	Hardware settings for the Ethernet interface.
<b>AutoSwitchRoute</b>	Enable transparent mode, which means that a switch route is added automatically for this interface. (Default: No)

<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this interface using the given network. (Default: Yes)
<b>AutoDefaultGatewayRoute</b>	Automatically add a default route for this interface using the given default gateway. (Default: Yes)
<b>DHCPDNS1</b>	IP of the primary DNS server. (Optional)
<b>DHCPDNS2</b>	IP of the secondary DNS server. (Optional)
<b>ReceiveMulticastTraffic</b>	Sets the multicast receive mode of the interface. (Default: Auto)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.24.3. GRE Tunnel

#### Description

A GRE interface is a Generic Routing Encapsulation (no encryption, no authentication, only encapsulation) tunnel over an existing IP network.

#### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>IP</b>	Specifies the IP address of the GRE interface.
<b>Network</b>	Specifies the network address of the GRE interface.
<b>RemoteEndpoint</b>	Specifies the IP address of the remote endpoint.
<b>EncapsulationChecksum</b>	Add an extra level of checksum above the one provided by the IPv4 layer. (Default: No)
<b>OriginatorIPType</b>	Specifies what IP address to use as source IP in e.g. NAT. (Default: LocalInterface)
<b>OriginatorIP</b>	Manually specified originator IP address to use as source IP in e.g. NAT.
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 90)
<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this interface using the given remote network. (Default: Yes)
<b>UseSessionKey</b> <b>SessionKey</b> <b>Comments</b>	Text describing the current object. (Optional)

### 3.24.4. InterfaceGroup

#### Description

Use an interface group to combine several interfaces for a simplified security policy.

#### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>Equivalent</b>	Specifies if the interfaces should be considered security equivalent, that means that if enabled the interface group can be used as a destination interface in rules where connections might need to be moved between the two interfaces. (Default: No)
<b>Members</b>	Specifies the interfaces that are included in the interface group.
<b>Comments</b>	Text describing the current object. (Optional)

## 3.24.5. IPSecTunnel

### Description

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the interface.
<b>LocalNetwork</b>	The network on "this side" of the IPsec tunnel. The IPsec tunnel will be established between this network and the remote network.
<b>RemoteNetwork</b>	The network connected to the remote gateway. The IPsec tunnel will be established between the local network and this network.
<b>RemoteEndpoint</b>	Specifies the IP address of the remote endpoint. This is the address the security gateway will establish the IPsec tunnel to. It also dictates from where inbound IPsec tunnels are allowed. (Optional)
<b>IKEConfigModePool</b>	Selects IKE Config Mode Pool to use for the tunnel. (Optional)
<b>IKEAlgorithms</b>	Specifies the IKE Proposal list used with the tunnel.
<b>IPSecAlgorithms</b>	Specifies the IPsec Proposal list used with the tunnel.
<b>IKELifeTimeSeconds</b>	The lifetime of the IKE connection in seconds. Whenever it expires, a new phase-1 exchange will be performed. (Default: 28800)
<b>IPSecLifeTimeSeconds</b>	The lifetime of the IPsec connection in seconds. Whenever it's exceeded, a re-key will be initiated, providing new IPsec encryption and authentication session keys. (Default: 3600)
<b>IPSecLifeTimeKilobytes</b>	The lifetime of the IPsec connection in kilobytes. (Default: 0)
<b>EncapsulationMode</b>	Specifies if the IPsec tunnel should use Tunnel or Transport mode. (Default: Tunnel)
<b>AuthMethod</b>	Certificate or Pre-shared key. (Default: PSK)
<b>PSK</b>	Selects the Pre-shared key to use with this IPsec Tunnel.



---

<b>LocalIDType</b>	Selects the type of Local ID to use. (Default: Auto)
<b>LocalIDValue</b>	Specify the local identity of the tunnel ID.
<b>GatewayCertificate</b>	Selects the certificate the security gateway uses to authenticate itself to the other IPsec peer.
<b>RootCertificates</b>	Selects one or more root certificates to use with this IPsec Tunnel.
<b>IDList</b>	Selects the identification list to use with this IPsec Tunnel. An identification list is a list of the identities that are allowed to establish a IPsec tunnel. (Optional)
<b>XAuth</b>	Off, Required for inbound or Pass to peer gateway. (Default: Off)
<b>XAuthUsername</b>	Specifies the username to pass to the remote gateway via IKE XAuth.
<b>XAuthPassword</b>	Specifies the password to pass to the remote gateway via IKE XAuth.
<b>DHCPOverIPSec</b>	Allow DHCP over IPsec from single-host clients. (Default: No)
<b>AddRouteToRemoteNet</b>	Dynamically add route to the remote networks when a tunnel is established. (Default: No)
<b>PlaintextMTU</b>	Specifies the size in bytes at which to fragment plaintext packets (rather than fragmenting IPsec). (Default: 1424)
<b>OriginatorIPType</b>	Specifies what IP address to use as source IP in e.g. NAT. (Default: LocalInterface)
<b>OriginatorIP</b>	Manually specified originator IP address to use as source IP in e.g. NAT.
<b>IKEMode</b>	Specifies which IKE mode to use: main or aggressive. (Default: Main)
<b>DHGroup</b>	Specifies the Diffie-Hellman group to use when doing key exchanges in IKE. (Default: 2)
<b>PFS</b>	Specifies whether PFS should be used or not. (Default: None)
<b>PFS DHGroup</b>	Specifies which Diffie-Hellman group to use with PFS. (Default: 2)
<b>SetupSAPer</b>	Setup security association per network, host or port. (Default: Net)
<b>DeadPeerDetection</b>	Enable Dead Peer Detection. (Default: Yes)
<b>NATTraversal</b>	Enable or disable NAT traversal. (Default: OnIfNeeded)
<b>KeepAlive</b>	Disabled, Auto or Manual. (Default: Disabled)
<b>KeepAliveSourceIP</b>	Source IP address used when sending keep-alive ICMP pings.
<b>KeepAliveDestinationIP</b>	Destination IP address used when sending keep-alive ICMP pings.
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 90)

---

<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this interface using the given remote network. (Default: Yes)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.24.6. L2TPClient

### Description

A PPTP/L2TP client interface is a PPP (Point-to-Point Protocol) tunnel over an existing IP network. Its IP address and DNS servers are dynamically assigned.

### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>IP</b>	The host name to store the assigned IP address in, if this network object exists and have a value other than 0.0.0.0 the PPTP/L2TP client will try to get that one from the PPTP/L2TP server as preferred IP. (Optional)
<b>Network</b>	The network from which traffic should be routed into the tunnel.
<b>RemoteEndpoint</b>	The IP address of the L2TP/PPTP server.
<b>TunnelProtocol</b>	Specifies if PPTP or L2TP should be used for this tunnel. (Default: PPTP)
<b>OriginatorIPType</b>	Specifies what IP address to use as source IP in e.g. NAT. (Default: LocalInterface)
<b>OriginatorIP</b>	Manually specified originator IP address to use as source IP in e.g. NAT.
<b>DNS1</b>	IP of the primary DNS server. (Optional)
<b>DNS2</b>	IP of the secondary DNS server. (Optional)
<b>Username</b>	Specifies the username to use for this PPTP/L2TP interface.
<b>Password</b>	The password to use for this PPTP/L2TP interface.
<b>PPPAuthNoAuth</b>	Allow no authentication for this tunnel. (Default: No)
<b>PPPAuthPAP</b>	Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)
<b>PPPAuthCHAP</b>	Use CHAP authentication protocol for this tunnel. (Default: Yes)
<b>PPPAuthMSCHAP</b>	Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)

<b>PPPAuthMSCHAPv2</b>	Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)
<b>MPPENone</b>	Allow authentication without Microsoft Point-to-Point Encryption (MPPE). (Default: Yes)
<b>MPPERC440</b>	Use an RC4 40 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)
<b>MPPERC456</b>	Use an RC4 56 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)
<b>MPPERC4128</b>	Use an RC4 128 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)
<b>DialOnDemand</b>	Enable Dial-on-demand which means that the L2TP/PPTP tunnel will not be setup until traffic is sent on the interface. (Default: No)
<b>ActivitySensing</b>	Specifies if the dial-on-demand should trigger on inbound or outbound traffic or both. (Default: BiDirectional)
<b>IdleTimeout</b>	Idle timeout in seconds for dial-on-demand. (Default: 3600)
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 90)
<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this interface using the given remote network. (Default: Yes)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.24.7. L2TPServer

### Description

A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.

### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>IP</b>	The IP address of the PPTP/L2TP server interface.
<b>TunnelProtocol</b>	Specifies if PPTP or L2TP should be used for this tunnel. (Default: PPTP)
<b>Interface</b>	The interface that the PPTP/L2TP Server should be listening on.
<b>ServerIP</b>	Specifies the IP that the PPTP/L2TP server should listen on, this can be an IP of a interface, or for example an ARP published IP.
<b>UseUserAuth</b>	Enable the use of user authentication rules on this server. (Default: Yes)
<b>MPPENone</b>	Allow no authentication for this tunnel. (Default: Yes)
<b>MPPERC440</b>	Use an RC4 40 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)

<b>MPPER456</b>	Use an RC4 56 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)
<b>MPPER4128</b>	Use an RC4 128 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)
<b>IPPool</b>	A range, group or network that the PPTP/L2TP server will use as IP address pool to give out IP addresses to the clients from.
<b>DNS1</b>	IP of the primary DNS server. (Optional)
<b>DNS2</b>	IP of the secondary DNS server. (Optional)
<b>NBNS1</b>	IP of the primary Windows Internet Name Service (WINS) server that is used in Microsoft environments which uses the NetBIOS Name Servers (NBNS) to assign IP addresses to NetBIOS names. (Optional)
<b>NBNS2</b>	IP of the primary Windows Internet Name Service (WINS) server that is used in Microsoft environments which uses the NetBIOS Name Servers (NBNS) to assign IP addresses to NetBIOS names. (Optional)
<b>AllowedRoutes</b>	Restricts networks for which routes may automatically be added. (Default: all-nets)
<b>ProxyARPAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.24.8. PPPoETunnel

### Description

A PPPoE interface is a PPP (point-to-point protocol) tunnel over an existing physical Ethernet interface. Its IP address is dynamically assigned.

### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>EthernetInterface</b>	The physical Ethernet interface that connects to the PPPoE server network.
<b>IP</b>	The host name to store the assigned IP address in. (Optional)
<b>Network</b>	The network from which traffic should be routed into the tunnel.
<b>DNS1</b>	IP of the primary DNS server. (Optional)
<b>DNS2</b>	IP of the secondary DNS server. (Optional)
<b>Username</b>	Specifies the username to use for this PPPoE tunnel.
<b>Password</b>	The password to use for this PPPoE tunnel.

<b>ServiceName</b>	Specifies the PPPoE server service name used to distinguish between two or more PPPoE servers attached to the same network. (Optional)
<b>PPPAuthNoAuth</b>	Allow no authentication for this tunnel. (Default: No)
<b>PPPAuthPAP</b>	Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)
<b>PPPAuthCHAP</b>	Use CHAP authentication protocol for this tunnel. (Default: Yes)
<b>PPPAuthMSCHAP</b>	Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)
<b>PPPAuthMSCHAPv2</b>	Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)
<b>DialOnDemand</b>	Enable Dial-on-demand which means that the PPPoE tunnel will not be setup until traffic is sent on the interface. (Default: No)
<b>ActivitySensing</b>	Specifies if the dial-on-demand should trigger on inbound or outbound traffic or both. (Default: BiDirectional)
<b>IdleTimeout</b>	Idle timeout in seconds for dial-on-demand. (Default: 3600)
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 90)
<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this interface using the given remote network. (Default: Yes)
<b>Schedule</b>	The schedule defines when the PPPoE tunnel should be active. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.24.9. VLAN

### Description

Use a VLAN to define a virtual interface compatible with the IEEE 802.1Q Virtual LAN standard.

### Properties

<b>Name</b>	Specifies a symbolic name for the interface. (Identifier)
<b>Ethernet</b>	Specifies on which Ethernet interface the virtual LAN is defined.
<b>VLANID</b>	Specifies the virtual LAN ID used for this virtual LAN interface. Two virtual LANs cannot have the same VLAN ID if they are defined on the same Ethernet interface. (Default: 0)
<b>IP</b>	Specifies the IP address of the virtual LAN interface, if other than the IP of the Ethernet interface.
<b>Network</b>	Specifies the network address of the virtual LAN interface.
<b>DefaultGateway</b>	The default gateway of the virtual LAN interface. (Optional)

<b>Broadcast</b>	Specifies the broadcast address of the virtual LAN interface. (Optional)
<b>PrivateIP</b>	The private IP address of this high availability node. (Optional)
<b>Metric</b>	Specifies the metric for the auto-created route. (Default: 100)
<b>AutoSwitchRoute</b>	Enable transparent mode, which means that a switch route is added automatically for this virtual LAN interface. (Default: No)
<b>AutoInterfaceNetworkRoute</b>	Automatically add a route for this virtual LAN interface using the given network. (Default: Yes)
<b>AutoDefaultGatewayRoute</b>	Automatically add a default route for this virtual LAN interface using the given default gateway. (Default: Yes)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.25. IPPool

### Description

An IPPool is a dynamic object which consists of IP leases that are fetched from a DHCP Server. The IPPool itself is used as resource of addresses by subsystems that may need to distribute addresses, e.g. by IPsec in Configuration mode.

### Properties

<b>Name</b>	Specifies a symbolic name for the IP Pool. (Identifier)
<b>DHCPSType</b>	Should server address be specified or should broadcast on a interface be used. (Default: Interface)
<b>ServerIP</b>	DHCP Server Address.
<b>ServerFilter</b>	Specifies which DHCP server that leases should be accepted from. (Optional)
<b>Interface</b>	Specifies the interface on which is found the DHCP server that leases are accepted from.
<b>IPFilter</b>	Specifies which IP addresses that are accepted from the DHCP server. (Optional)
<b>RoutingTable</b>	The routing table to use in communication with the DHCP server. (Default: main)
<b>ReceiveInterface</b>	Which interface to use when communicating with the DHCP server. (Optional)
<b>PrefetchLeases</b>	Specifies the number of leases an IP Pool will keep prefetched. (Default: 3)
<b>MaxFree</b>	Maximum number of free address that the IP pool will keep, others will be returned back to DHCP server. (Optional)
<b>MaxClients</b>	Maximum number clients that the IP pool is allowed to contain. (Optional)
<b>MacRangeStart</b>	Specifies the lower boundary of MAC addresses that DHCP Clients will use in communication with a server. (Optional)
<b>MacRangeEnd</b>	Specifies the upper boundary of MAC addresses that DHCP Clients will use in communication with a server. (Optional)
<b>SenderIP</b>	The local IP that should be used when communication with the DHCP server. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.26. IPRule

### Description

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule. (Optional)
<b>Action</b>	Reject, Drop, FwdFast, Allow, NAT, SAT or SLB_SAT.
<b>SourceInterface</b>	Specifies the name of the receiving interface to be compared to the received packet.
<b>SourceNetwork</b>	Specifies the sender span of IP addresses to be compared to the received packet.
<b>DestinationInterface</b>	Specifies the the destination interface to be compared to the received packet.
<b>DestinationNetwork</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet.
<b>Service</b>	Specifies a service that will be used as a filter parameter when matching traffic with this rule.
<b>Schedule</b>	By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)
<b>NATAction</b>	Specify sender address or Use interface address. (Default: UseInterfaceAddress)
<b>NATSenderAddress</b>	Specifies which sender address will be used.
<b>NATSenderPort</b>	Translate to this port. (Optional)
<b>NATPool</b>	Specifies which sender address will be used.
<b>SATTranslate</b>	Specifies whether to translate source IP or destination IP. (Default: DestinationIP)
<b>SATTranslateToIP</b>	Translate to this IP address.
<b>SATTranslateToPort</b>	Translate to this port. (Optional)
<b>SATAllToOne</b>	Rewrite all destination IPs to a single IP. (Default: No)
<b>SLBStickiness</b>	Specifies stickiness mode. (Default: None)
<b>SLBIdleTimeout</b>	New connections that arrive within the idle timeout are assigned to the same real server as previous connections from that address. The timeout is refreshed after each new connection. (Default: 30)
<b>SLBMaxSlots</b>	Specifies maximum number of slots for IP and network stickiness. (Default: 2048)
<b>SLBNetSize</b>	Specifies network size for network stickiness. (Default: 24)



<b>SLBMonitorPing</b>	Enable monitoring using ICMP Ping packets. (Default: No)
<b>SLBMonitorTCP</b>	Enable monitoring using TCP packets. (Default: No)
<b>SLBPingUseSharedIP</b>	Use the shared IP of a HA cluster instead of the private IP of the node. (Default: Yes)
<b>SLBTCPUseSharedIP</b>	Use the shared IP of a HA cluster instead of the private IP of the node. (Default: Yes)
<b>SLBPingInterval</b>	Ping interval in milliseconds. (Default: 10000)
<b>SLBPingMaxLoss</b>	Ping maximum packet loss. (Default: 5)
<b>SLBTCPInterval</b>	TCP interval in milliseconds. (Default: 10000)
<b>SLBTCPMaxLoss</b>	TCP maximum packet loss. (Default: 5)
<b>SLBTCPPorts</b>	Specifies which ports will be monitored.
<b>SLBDistribution</b>	Specifies the algorithm used for the load distribution tasks. (Default: RoundRobin)
<b>SLBWindowTime</b>	Specifies the window time used for counting the number of seconds back in time to summarize the number of new connections for connection-rate algorithm. (Default: 10)
<b>SLBAddresses</b>	The IP addresses of the servers in the server farm.
<b>RequireIGMP</b>	Multicast traffic must have been requested using IGMP before it is forwarded. (Default: Yes)
<b>MultiplexArgument</b>	Specifies how the traffic should be forwarded and translated.
<b>MultiplexAllToOne</b>	Rewrite all destination IPs to a single IP. (Default: No)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

## 3.27. IPRuleFolder

### Description

An IP Rule folder can be used to group IP Rules into logical groups for better overview and simplified management.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies the name of the folder.
<b>Comments</b>	Text describing the current object. (Optional)



### **Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

### 3.27.1. IPRule

The definitions here are the same as in Section 3.26, “IPRule” .

## 3.28. IPSecAlgorithms

### Description

Configure algorithms which are used in the IPsec phase of an IPsec session.

### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>NULLEnabled</b>	Enable plaintext. (Default: No)
<b>DESEnabled</b>	Enable DES encryption algorithm. (Default: No)
<b>DES3Enabled</b>	Enable 3DES encryption algorithm. (Default: No)
<b>AESEnabled</b>	Enable AES encryption algorithm. (Default: No)
<b>BlowfishEnabled</b>	Enable Blowfish encryption algorithm. (Default: No)
<b>TwofishEnabled</b>	Enable Twofish encryption algorithm. (Default: No)
<b>CAST128Enabled</b>	Enable CAST128 encryption algorithm. (Default: No)
<b>BlowfishMinKeySize</b>	Specifies the minimum Blowfish key size in bits. (Default: 128)
<b>BlowfishKeySize</b>	Specifies the Blowfish preferred key size in bits. (Default: 128)
<b>BlowfishMaxKeySize</b>	Specifies the maximum Blowfish key size in bits. (Default: 448)
<b>TwofishMinKeySize</b>	Specifies the minimum Twofish key size in bits. (Default: 128)
<b>TwofishKeySize</b>	Specifies the Twofish preferred key size in bits. (Default: 128)
<b>TwofishMaxKeySize</b>	Specifies the maximum Twofish key size in bits. (Default: 256)
<b>AESMinKeySize</b>	Specifies the minimum AES key size in bits. (Default: 128)
<b>AESKeySize</b>	Specifies the preferred AES key size in bits. (Default: 128)
<b>AESMaxKeySize</b>	Specifies the maximum AES key size in bits. (Default: 256)
<b>MD5Enabled</b>	Enable MD5 integrity algorithm. (Default: No)
<b>SHA1Enabled</b>	Enable SHA1 integrity algorithm. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.29. LDAPServer

### Description

An LDAP server is used as a central repository of certificates and CRLs that the security gateway can download when necessary.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Host</b>	Specifies the IP address or hostname of the LDAP server.
<b>Username</b>	Specifies the username to use when accessing the LDAP server. (Optional)
<b>Password</b>	Specifies the password to use when accessing the LDAP server. (Optional)
<b>Port</b>	Specifies the LDAP service port number. (Default: 389)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.30. LocalUserDatabase

### Description

A local user database contains user accounts used for authentication purposes.

### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.30.1. User

#### Description

User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

#### Properties

<b>Name</b>	Specifies the username to add into the user database. (Identifier)
<b>Password</b>	The password for this user.
<b>Groups</b>	Specifies the user groups that this user is a member of, e.g. Administrators. (Optional)
<b>IPPool</b>	If the user is logging in over PPTP/L2TP it will be assigned this static IP. (Optional)
<b>AutoAddRouteNet</b>	PPTP/L2TP networks behind the user. (Optional)
<b>AutoAddRouteMetric</b>	Metric for the network. (Optional)
<b>SSHKeys</b>	Public keys used to log in via SSH. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.31. LogReceiver

This is a category that groups the following object types.

### 3.31.1. EventReceiverSNMP2c

#### Description

A SNMP2c event receiver is used to receive SNMP events from the system.

#### Properties

<b>Name</b>	Specifies a symbolic name for the log receiver. (Identifier)
<b>IPAddress</b> <b>Port</b>	(Default: 162)
<b>Community</b> <b>RepeatCount</b> <b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency,Alert,Critical>Error,Warning,Notice,Info)
<b>Comments</b>	Text describing the current object. (Optional)

#### 3.31.1.1. LogReceiverMessageException

##### Description

A log message exception is used to override the severity filter in the log receiver.

##### Properties

<b>LogID</b>	The ID number of the log message. (Identifier)
<b>LogType</b>	EXCLUDE or INCLUDE. (Default: EXCLUDE)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.31.2. LogReceiverMemory

#### Description

A memory log receiver is used to receive and keep log events in system RAM.

#### Properties

<b>Name</b>	Specifies a symbolic name for the log receiver. (Identifier)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency,Alert,Critical>Error,Warning,Notice,Info)

<b>Comments</b>	Text describing the current object. (Optional)
-----------------	--

### 3.31.3. LogReceiverSMTP

#### Description

An SMTP event receiver is used for receiving emails for IDP events.

#### Properties

<b>Name</b>	Specifies a symbolic name for the log receiver. (Identifier)
<b>IPAddress</b>	The IP address of the SMTP server.
<b>Port</b>	Specifies the which port to use to connect to the SMTP server. (Default: 25)
<b>Receiver1</b>	The email address that the event information is sent to.
<b>Receiver2</b>	Alternate email receiver. (Optional)
<b>Receiver3</b>	Alternate email receiver. (Optional)
<b>Sender</b>	Specifies which sender the email will have. (Default: hostmaster)
<b>Identity</b>	Specifies which identity to write in the email header. (Default: hostmaster)
<b>XMailer</b>	Specifies the X-mailer information to write in the email header. (Optional)
<b>Subject</b>	The subject of the email. (Default: "Log event from D-Link DFL Firewall")
<b>HoldTime</b>	The hold time in seconds during which the log threshold must be reached for an email to be sent. (Default: 120)
<b>MinRepeatDelay</b>	The amount of seconds the security gateway will wait before sending another email. (Default: 600)
<b>LogThreshold</b>	The number of events that have to occur within the hold time for an email to be sent. (Default: 2)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.31.4. LogReceiverSyslog

#### Description

A Syslog receiver is used to receive log events from the system in the standard Syslog format.

#### Properties

<b>Name</b>	Specifies a symbolic name for the log receiver. (Identifier)
<b>IPAddress</b>	Specifies the IP address of the log receiver.
<b>Port</b>	Specifies the port number of the log service. (Default: 514)
<b>Facility</b>	Specifies what facility is used when logging. (Default: local0)

<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency,Alert,Critical>Error,Warning,Notice,Info)
<b>Comments</b>	Text describing the current object. (Optional)

#### 3.31.4.1. LogReceiverMessageException

The definitions here are the same as in Section 3.31.1.1, “LogReceiverMessageException” .



## 3.32. NATPool

### Description

A NAT Pool is used for NATing multiple concurrent connections to using different source IP addresses.

### Properties

<b>Name</b>	Specifies a symbolic name for the NAT Pool. (Identifier)
<b>Type</b>	Specifies how NAT'ed connections are assigned a NAT IP address. (Default: stateful)
<b>IPSource</b>	Specify which IP Address source to use. (Default: IPRange)
<b>IPRange</b>	Specifies the range of IP addresses used for NAT translation.
<b>IPPool</b>	Specifies the IP Pool used for retrieving IP addresses for NAT translation.
<b>IPPoolIPs</b>	The number of IP addresses to get from the IP Pool.
<b>StateKeepAlive</b>	The number of seconds that stateful NAT state will be kept in absence of new connections. (Default: 120)
<b>MaxStates</b>	Maximum number of statefully tracked NATPool states. (Default: 16384)
<b>ProxyARPAAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes needed for receiving traffic on NATPool addresses. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interface/interfaces on which the security gateway should publish routes needed for the relay via Proxy ARP. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.33. OSPFProcess

### Description

An OSPF Router Process defines a group of routers exchanging routing information via the Open Shortest Path First routing protocol.

### Properties

<b>Name</b>	Specifies a symbolic name for the OSPF process. (Identifier)
<b>RouterID</b>	Specifies the IP address that is used to identify the router. If no router ID is configured, it will be computed automatically based on the highest IP address of any interface participating in the OSPF process. (Optional)
<b>PrivRouterID</b>	The private router ID of this high availability node. (Optional)
<b>RFC1583</b>	Enable this if the security gateway will be used in an environment that consists of routers that only support RFC 1583. (Default: No)
<b>SPFHoldTime</b>	Specifies the minimum time, in seconds, between two SPF calculations. (Default: 10)
<b>SPFDelayTime</b>	Specifies the delay time, in seconds, between when OSPF receives a topology change and when it starts a SPF calculation. (Default: 5)
<b>LSAGroupPacing</b>	This specifies the time in seconds at which interval the OSPF LSAs are collected into a group and refreshed. (Default: 10)
<b>RoutesHoldtime</b>	This specifies the time in seconds that the routing table will be kept unchanged after a reconfiguration of OSPF entries or a HA failover. (Default: 45)
<b>RefBandwidthValue</b>	Set the reference bandwidth that is used when calculating the default interface cost for routes. (Default: 1)
<b>RefBandwidthUnit</b>	Sets the reference bandwidth unit. (Default: Gbps)
<b>MemoryMaxUsage</b>	Maximum amount in kilobytes of RAM that the OSPF process is allowed to use. The default is 1% of installed RAM. Specifying 0 indicates that the OSPF process is allowed to use all available RAM. (Optional)
<b>DebugPacket</b>	Enables or disabled logging of general packet parsing events and also specifies the details of the log. (Default: Off)
<b>DebugHello</b>	Enables or disabled logging of hello packets and also specifies the details of the log. (Default: Off)
<b>DebugDDesc</b>	Enables or disabled logging of database description packets and also specifies the details of the log. (Default: Off)
<b>DebugExchange</b>	Enables or disabled logging of exchange packets and also specifies the details of the log. (Default: Off)
<b>DebugLSA</b>	Enables or disabled logging of LSA events and also specifies the details of the log. (Default: Off)
<b>DebugSPF</b>	Enables or disabled logging of SPF calculation events and also specifies the details of the log. (Default: Off)

<b>DebugRoute</b>	Enables or disabled logging of routing table manipulation events and also specifies the details of the log. (Default: Off)
<b>AuthType</b>	Specifies the authentication type for the OSPF protocol exchanges. (Default: None)
<b>AuthPassphrase</b>	Specifies the passphrase used for authentication. (Optional)
<b>AuthMD5ID</b>	Specifies the MD5 key ID used for MD5 digest authentication.
<b>AuthMD5Key</b>	A 128-bit key used to produce the MD5 digest. (Optional)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.33.1. OSPFArea

### Description

An OSPF area is a sub-domain within the OSPF process which collects OSPF interfaces, neighbors, aggregates and virtual links.

### Properties

<b>Name</b>	Specifies a symbolic name for the area. (Identifier)
<b>AreaID</b>	Specifies the area id, if 0.0.0.0 is specified this is the backbone area.
<b>Stub</b>	Enable to make the router automatically advertises a default route so that routers in the stub area can reach destinations outside the area. (Default: No)
<b>StubSummarize</b>	Become a default router for stub area (Summarize). (Default: Yes)
<b>StubMetric</b>	Route metric for stub area. (Optional)
<b>FilterExternal</b>	Specifies the network addresses allowed to be imported into this area from external routing sources. (Optional)
<b>FilterInterArea</b>	Specifies the network addresses allowed to be imported from other routers inside the area. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.33.1.1. OSPFInterface

### Description

Select and define the properties of an interface that should be made a member of the Router Process.

### Properties

<b>Interface</b>	Specifies which interface in the security gateway will be used for this OS-
------------------	---

	PF interface. (Identifier)
<b>Type</b>	Auto, Broadcast, Point-to-point or Point-to-multipoint. (Default: Auto)
<b>MetricType</b>	Metric value or Bandwidth. (Default: MetricValue)
<b>Metric</b>	Specifies the routing metric for this OSPF interface.
<b>BandwidthValue</b>	Specifies the bandwidth for this OSPF interface.
<b>BandwidthUnit</b>	Specifies the bandwidth unit. (Default: Mbps)
<b>UseDefaultAuth</b>	Use the authentication configuration specified in the OSPF process. (Default: Yes)
<b>AuthType</b>	Specifies the authentication type for the OSPF protocol exchanges. (Default: None)
<b>AuthPassphrase</b>	Specifies the passphrase used for authentication. (Optional)
<b>AuthMD5ID</b>	Specifies the MD5 key ID used for MD5 digest authentication.
<b>AuthMD5Key</b>	A 128-bit key used to produce the MD5 digest. (Optional)
<b>HelloInterval</b>	Specifies the number of seconds between HELLO packets sent from the interface. (Default: 10)
<b>RtrDeadInterval</b>	If no HELLO packets are received from a neighbor within this interval (in seconds), that neighbor router will be declared to be down. (Default: 40)
<b>RxmtInterval</b>	Specifies the number of seconds between retransmissions of LSAs to neighbors on this interface. (Default: 5)
<b>RtrPrio</b>	Specifies the router priority, a higher number increases this routers chance of becoming DR or BDR, if 0 is specified this router will not be eligible in the DR/BDR election. (Default: 1)
<b>InfTransDelay</b>	Specifies the estimated transmit delay for the interface in seconds. This value represents the maximum time it takes to forward a LSA packet through the router. (Default: 1)
<b>WaitInterval</b>	Specifies the number of seconds between the time when the interface brought up and the election of the DR and BDR. This value should be higher than the hello interval. (Default: 40)
<b>Passive</b>	Enable to make it possible to include networks into the OSPF routing process, without running OSPF on the interface connected to that network. (Default: No)
<b>IgnoreMTU</b>	Enable to allow OSPF MTU mismatches. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.33.1.2. OSPFNeighbor

#### Description

For point-to-point and point-to-multipoint networks, specify the IP addresses of directly connected routers.

#### Properties

<b>Interface</b>	Specifies the OSPF interface of the neighbor. (Identifier)
<b>IPAddress</b>	IP Address of the neighbor.
<b>Metric</b>	Specifies the metric of the neighbor. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.33.1.3. OSPFAggregate

#### Description

An aggregate is used to replace any number of smaller networks belonging to the local (intra) area with one contiguous network which may then be advertised or hidden.

#### Properties

<b>Network</b>	The aggregate network used to combine several small routes. (Identifier)
<b>Advertise</b>	Advertise the aggregate. (Default: Yes)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.33.1.4. OSPFVLink

#### Description

An area that does not have a direct connection to the backbone must have at least one area border router with a virtual link to a backbone router, or to another router with a link to the backbone.

#### Properties

<b>Name</b>	Specifies a symbolic name for the virtual link. (Identifier)
<b>RouterID</b>	The ID of the router on the other side of the virtual link.
<b>UseDefaultAuth</b>	Use the authentication configuration specified in the OSPF process. (Default: Yes)
<b>AuthType</b>	Specifies the authentication type for the OSPF protocol exchanges. (Default: None)
<b>AuthPassphrase</b>	Specifies the passphrase used for authentication. (Optional)
<b>AuthMD5ID</b>	Specifies the MD5 key ID used for MD5 digest authentication.
<b>AuthMD5Key</b>	A 128-bit key used to produce the MD5 digest. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.34. Pipe

### Description

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

### Properties

<b>Name</b>	Specifies a symbolic name for the pipe. (Identifier)
<b>LimitKbpsTotal</b>	Total bandwidth limit for this pipe in kilobits per second. (Optional)
<b>LimitPPSTotal</b>	Total packet per second limit for this pipe. (Optional)
<b>LimitKbps0</b>	Specifies the bandwidth limit in kbps for precedence 0 (the lowest precedence). (Optional)
<b>LimitPPS0</b>	Specifies the packet per second limit for precedence 0 (the lowest precedence). (Optional)
<b>LimitKbps1</b>	Specifies the bandwidth limit in kbps for precedence 1. (Optional)
<b>LimitPPS1</b>	Specifies the packet per second limit for precedence 1. (Optional)
<b>LimitKbps2</b>	Specifies the bandwidth limit in kbps for precedence 2. (Optional)
<b>LimitPPS2</b>	Specifies the packet per second limit for precedence 2. (Optional)
<b>LimitKbps3</b>	Specifies the bandwidth limit in kbps for precedence 3. (Optional)
<b>LimitPPS3</b>	Specifies the packet per second limit for precedence 3. (Optional)
<b>LimitKbps4</b>	Specifies the bandwidth limit in kbps for precedence 4. (Optional)
<b>LimitPPS4</b>	Specifies the packet per second limit for precedence 4. (Optional)
<b>LimitKbps5</b>	Specifies the bandwidth limit in kbps for precedence 5. (Optional)
<b>LimitPPS5</b>	Specifies the packet per second limit for precedence 5. (Optional)
<b>LimitKbps6</b>	Specifies the bandwidth limit in kbps for precedence 6. (Optional)
<b>LimitPPS6</b>	Specifies the packet per second limit for precedence 6. (Optional)
<b>LimitKbps7</b>	Specifies the bandwidth limit in kbps for precedence 7 (the highest precedence). (Optional)
<b>LimitPPS7</b>	Specifies the packet per second limit for precedence 7 (the highest precedence). (Optional)
<b>UserLimitKbpsTotal</b>	Total bandwidth limit per group in the pipe in kilobits per second. (Optional)
<b>UserLimitPPSTotal</b>	Total throughput limit per group in the pipe in packets per second. (Optional)
<b>UserLimitKbps0</b>	Specifies the bandwidth limit per group in kbps for precedence 0 (the lowest precedence). (Optional)
<b>UserLimitPPS0</b>	Specifies the throughput limit per group in PPS for precedence 0

---

	(the lowest precedence). (Optional)
<b>UserLimitKbps1</b>	Specifies the bandwidth limit per group in kbps for precedence 1. (Optional)
<b>UserLimitPPS1</b>	Specifies the throughput limit per group in PPS for precedence 1. (Optional)
<b>UserLimitKbps2</b>	Specifies the bandwidth limit per group in kbps for precedence 2. (Optional)
<b>UserLimitPPS2</b>	Specifies the throughput limit per group in PPS for precedence 2. (Optional)
<b>UserLimitKbps3</b>	Specifies the bandwidth limit per group in kbps for precedence 3. (Optional)
<b>UserLimitPPS3</b>	Specifies the throughput limit per group in PPS for precedence 3. (Optional)
<b>UserLimitKbps4</b>	Specifies the bandwidth limit per group in kbps for precedence 4. (Optional)
<b>UserLimitPPS4</b>	Specifies the throughput limit per group in PPS for precedence 4. (Optional)
<b>UserLimitKbps5</b>	Specifies the bandwidth limit per group in kbps for precedence 5. (Optional)
<b>UserLimitPPS5</b>	Specifies the throughput limit per group in PPS for precedence 5. (Optional)
<b>UserLimitKbps6</b>	Specifies the bandwidth limit per group in kbps for precedence 6. (Optional)
<b>UserLimitPPS6</b>	Specifies the throughput limit per group in PPS for precedence 6. (Optional)
<b>UserLimitKbps7</b>	Specifies the bandwidth limit per group in kbps for precedence 7 (the highest precedence). (Optional)
<b>UserLimitPPS7</b>	Specifies the throughput limit per group in PPS for precedence 7 (the highest precedence). (Optional)
<b>Grouping</b>	Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups. (Default: None)
<b>GroupingNetworkSize</b>	If users are grouped according to source or destination network, the size of the network has to be specified by this setting. (Default: 0)
<b>Dynamic</b>	Enable dynamic balancing of groups. (Default: No)
<b>PrecedenceMin</b>	Specifies the lowest allowed precedence for traffic in this pipe. If a packet with a lower precedence enters, its precedence is raised to this value. (Default: 0)
<b>PrecedenceDefault</b>	Specifies the default precedence for the pipe. If a packet enters this pipe without a set precedence, it gets assigned this value. Should be higher than or equal to the minimum precedence. (Default: 0)
<b>PrecedenceMax</b>	Specifies the highest allowed precedence for traffic in this pipe. If a packet with a higher precedence enters, its precedence is lowered to this value. Should be higher than or equal to the default precedence. (Default: 7)

---

**Comments**

Text describing the current object. (Optional)



## 3.35. PipeRule

### Description

A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the object. (Optional)
<b>SourceInterface</b>	Specifies the name of the receiving interface to be compared to the received packet.
<b>SourceNetwork</b>	Specifies the sender span of IP addresses to be compared to the received packet.
<b>DestinationInterface</b>	Specifies the the destination interface to be compared to the received packet.
<b>DestinationNetwork</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet.
<b>Service</b>	Specifies a service that will be used as a filter parameter when matching traffic with this rule.
<b>Schedule</b>	By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)
<b>ForwardChain</b>	Specifies one or more pipes to be used for forward traffic. (Optional)
<b>ReturnChain</b>	Specifies one or more pipes to be used for return traffic. (Optional)
<b>Precedence</b>	Specifies what precedence should be assigned to the packets before sent into a pipe. (Default: FromPipe)
<b>FixedPrecedence</b>	Specifies the fixed precedence.
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

## 3.36. PSK

### Description

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

### Properties

<b>Name</b>	Specifies a symbolic name for the pre-shared key. (Identifier)
<b>Type</b>	Specifies the type of the shared key.
<b>PSKAscii</b>	Specifies the PSK as a passphrase.
<b>PSKHex</b>	Specifies the PSK as a hexadecimal key.
<b>Comments</b>	Text describing the current object. (Optional)

## 3.37. RadiusServer

### Description

External RADIUS server used to verify user names and passwords.

### Properties

<b>Name</b>	Specifies a symbolic name for the server. (Identifier)
<b>IPAddress</b>	The IP address of the server.
<b>Port</b>	The UDP port of the server. (Default: 1812)
<b>RetryTimeout</b>	The retry timeout, in seconds, used when trying to contact the RADIUS accounting server. If no response has been given after for example 2 seconds, the security gateway will try again by sending a new AccountingRequest packet. (Default: 2)
<b>SharedSecret</b>	The shared secret phrase for the Authenticator generation.
<b>Comments</b>	Text describing the current object. (Optional)

## 3.38. RemoteManagement

This is a category that groups the following object types.

### 3.38.1. RemoteMgmtHTTP

#### Description

HTTP/HTTPS management.

#### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>AccessLevel</b>	The access level to grant the user that logs in. (Default: Admin)
<b>LocalUserDatabase</b>	Specifies the local user database to use for login.
<b>HTTP</b>	Enable remote management via HTTP. (Default: No)
<b>HTTPS</b>	Enable remote management via HTTPS. (Default: No)
<b>Interface</b>	Specifies the interface for which remote access is granted.
<b>Network</b>	Specifies the network for which remote access is granted.
<b>Comments</b>	Text describing the current object. (Optional)

### 3.38.2. RemoteMgmtSNMP

#### Description

SNMP management.

#### Properties

<b>Name</b>	Specifies a symbolic name for the object. (Identifier)
<b>SNMPGetCommunity</b>	Specifies the name of the community to be granted rights to remotely monitor the security gateway.
<b>Interface</b>	Specifies the interface for which remote access is granted.
<b>Network</b>	Specifies the network for which remote access is granted.
<b>Comments</b>	Text describing the current object. (Optional)

### 3.38.3. RemoteMgmtSSH

#### Description

Secure Shell (SSH) Server.

#### Properties

---

<b>Name</b>	Specifies a symbolic name for the SSH server. (Identifier)
<b>Port</b>	The listening port for the SSH server. (Default: 22)
<b>AllowAuthMethodPassword</b>	Allow password client authentication. (Default: Yes)
<b>AllowAuthMethodPublicKey</b>	Allow public key client authentication. (Default: Yes)
<b>AllowHostKeyDSA</b>	Allow DSA public key algorithm. (Default: Yes)
<b>AllowHostKeyRSA</b>	Allow RSA public key algorithm. (Default: Yes)
<b>AllowKexDH14</b>	Allow Diffie-Hellman Group 1 key exchange algorithm. (Default: Yes)
<b>AllowKexDH1</b>	Allow Diffie-Hellman Group 14 key exchange algorithm. (Default: Yes)
<b>AllowAES128</b>	Allow AES-128 encryption algorithm. (Default: Yes)
<b>AllowAES192</b>	Allow AES-192 encryption algorithm. (Default: Yes)
<b>AllowAES256</b>	Allow AES-256 encryption algorithm. (Default: Yes)
<b>AllowBlowfish</b>	Allow Blowfish encryption algorithm. (Default: Yes)
<b>Allow3DES</b>	Allow 3DES encryption algorithm. (Default: Yes)
<b>AllowMACSHA1</b>	Allow SHA1 integrity algorithm. (Default: Yes)
<b>AllowMACMD5</b>	Allow MD5 integrity algorithm. (Default: Yes)
<b>AllowMACSHA196</b>	Allow SHA1-96 integrity algorithm. (Default: Yes)
<b>AllowMACMD596</b>	Allow MD5-96 integrity algorithm. (Default: Yes)
<b>Banner</b>	Specifies the greeting message to display when the user logs in. (Optional)
<b>MaxSessions</b>	The maximum number of clients that can be connected at the same time. (Default: 5)
<b>SessionIdleTime</b>	The number of seconds a user can be idle before the session is closed. (Default: 1800)
<b>LoginGraceTime</b>	When the user has supplied the username, the password has to be provided within this number of seconds or the session will be closed. (Default: 30)
<b>AuthenticationRetries</b>	The number of retries allowed before the session is closed. (Default: 5)
<b>AccessLevel</b>	The access level to grant the user that logs in. (Default: Admin)
<b>LocalUserDatabase</b>	Specifies the local user database to use for login.
<b>Interface</b>	Specifies the interface for which remote access is granted.
<b>Network</b>	Specifies the network for which remote access is granted.
<b>Comments</b>	Text describing the current object. (Optional)

---

## 3.39. RoutingRule

### Description

A Routing Rule forces the use of a routing table in the forward and/or return direction of traffic on a connection. The ordering parameter of the routing table determines if it is consulted before or after the main routing table.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule. (Optional)
<b>ForwardRoutingTable</b>	The forward routing table will be used for packets from the connection originator to the connection endpoint.
<b>ReturnRoutingTable</b>	The return routing table will be used for packets traveling in the reverse direction.
<b>SourceInterface</b>	Specifies the name of the receiving interface to be compared to the received packet.
<b>SourceNetwork</b>	Specifies the sender span of IP addresses to be compared to the received packet.
<b>DestinationInterface</b>	Specifies the the destination interface to be compared to the received packet.
<b>DestinationNetwork</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet.
<b>Service</b>	Specifies a service that will be used as a filter parameter when matching traffic with this rule.
<b>Schedule</b>	By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

## 3.40. RoutingTable

### Description

The system has a predefined main routing table. Alternate routing tables can be defined by the user.

### Properties

<b>Name</b>	Specifies a symbolic name for the routing table. (Identifier)
<b>Ordering</b>	Specifies how a route lookup is done in a named routing table. (Default: Only)
<b>RemoveInterfaceIPRoutes</b>	Removes the interface routes. Makes the security gateway completely transparent. (Default: No)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.40.1. Route

#### Description

A route defines what interface and gateway to use in order to reach a specified network.

#### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the object. (Optional)
<b>Interface</b>	Specifies which interface packets destined for this route shall be sent through.
<b>Gateway</b>	Specifies the IP address of the next router hop used to reach the destination network. If the network is directly connected to the security gateway interface, no gateway address is specified. (Optional)
<b>LocalIP</b>	The IP address specified here will be automatically published on the corresponding interface. This address will also be used as the sender address in ARP queries. If no address is specified, the security gateway's interface IP address will be used. (Optional)
<b>RouteMonitor</b>	Specifies if this route should be monitored for route changes for route failover purposes. (Default: No)
<b>MonitorLinkStatus</b>	Mark the route as down if the interface link status changes to down. (Default: No)
<b>MonitorGateway</b>	Mark the route as down if the next hop does not answer on ARP lookups during a specified time. (Default: No)
<b>MonitorGatewayManualARP</b>	Enable a manually specified ARP lookup interval. (Default: No)
<b>MonitorGatewayARPInterval</b>	Specifies the ARP lookup interval in milliseconds. (Default:

	1000)
<b>Network</b>	Specifies the network address for this route.
<b>Metric</b>	Specifies the metric for this route. (Default: 0)
<b>ProxyARPAAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.40.2. SwitchRoute

### Description

A switch route defines which interfaces the specified network can be reached on. Proxy ARP defines between which interfaces ARP is allowed.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the object. (Optional)
<b>Interface</b>	Specifies which interface packets destined for this route shall be sent through.
<b>Network</b>	Specifies the network address for this route.
<b>Metric</b>	Specifies the metric for this route. (Default: 0)
<b>ProxyARPAAllInterfaces</b>	Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)
<b>ProxyARPInterfaces</b>	Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*



## 3.41. ScheduleProfile

### Description

A Schedule Profile defines days and dates and are then used by the various policies in the system.

### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>Mon</b>	Specifies during which intervals the schedule profile is active on Mondays. (Optional)
<b>Tue</b>	Specifies during which intervals the schedule profile is active on Tuesdays. (Optional)
<b>Wed</b>	Specifies during which intervals the schedule profile is active on Wednesdays. (Optional)
<b>Thu</b>	Specifies during which intervals the schedule profile is active on Thursdays. (Optional)
<b>Fri</b>	Specifies during which intervals the schedule profile is active on Fridays. (Optional)
<b>Sat</b>	Specifies during which intervals the schedule profile is active on Saturdays. (Optional)
<b>Sun</b>	Specifies during which intervals the schedule profile is active on Sundays. (Optional)
<b>StartDate</b>	The date after which this Schedule should be active. (Optional)
<b>EndDate</b>	The date after which this Schedule is not active anymore. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.42. Service

This is a category that groups the following object types.

### 3.42.1. ServiceGroup

#### Description

A Service Group is a collection of service objects, which can then be used by different policies in the system.

#### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>Members</b>	Group members.
<b>Comments</b>	Text describing the current object. (Optional)

### 3.42.2. ServiceICMP

#### Description

An ICMP Service is an object definition representing ICMP traffic with specific parameters.

#### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>MessageTypes</b>	Specifies the ICMP message types that are applicable to this service. (Default: All)
<b>EchoRequest</b>	Enable matching of Echo Request messages. (Default: No)
<b>EchoRequestCodes</b>	Specifies which Echo Request message codes should be matched. (Default: 0-255)
<b>DestinationUnreachable</b>	Enable matching of Destination Unreachable messages. (Default: No)
<b>DestinationUnreachableCodes</b>	Specifies which Destination Unreachable message codes should be matched. (Default: 0-255)
<b>Redirect</b>	Enable matching of Redirect messages. (Default: No)
<b>RedirectCodes</b>	Specifies which Redirect message codes should be matched. (Default: 0-255)
<b>ParameterProblem</b>	Enable matching of Parameter Problem messages. (Default: No)
<b>ParameterProblemCodes</b>	Specifies which Parameter Problem message codes should be matched. (Default: 0-255)
<b>EchoReply</b>	Enable matching of Echo Reply messages. (Default: No)
<b>EchoReplyCodes</b>	Specifies which Echo Reply message codes should be

	matched. (Default: 0-255)
<b>SourceQuenching</b>	Enable matching of Source Quenching messages. (Default: No)
<b>SourceQuenchingCodes</b>	Specifies which Source Quenching message codes should be matched. (Default: 0-255)
<b>TimeExceeded</b>	Enable matching of Time Exceeded messages. (Default: No)
<b>TimeExceededCodes</b>	Specifies which Time Exceeded message codes should be matched. (Default: 0-255)
<b>PassICMPReturn</b>	Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)
<b>ALG</b>	An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)
<b>MaxSessions</b>	Specifies how many concurrent sessions that are permitted using this service. (Default: 200)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.42.3. ServiceIPProto

#### Description

An IP Protocol Service is a definition of an IP protocol with specific parameters.

#### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>IPProto</b>	IP protocol number or range, e.g. "1-4,7" will match the protocols ICMP, IGMP, GGP, IP-in-IP and CBT. (Default: 0-255)
<b>PassICMPReturn</b>	Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)
<b>ALG</b>	An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)
<b>MaxSessions</b>	Specifies how many concurrent sessions that are permitted using this service. (Default: 200)
<b>Comments</b>	Text describing the current object. (Optional)

### 3.42.4. ServiceTCPUDP

#### Description

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

#### Properties

<b>Name</b>	Specifies a symbolic name for the service. (Identifier)
<b>DestinationPorts</b>	Specifies the destination port or the port ranges applicable to this service.
<b>Type</b>	Specifies whether this service uses the TCP or UDP protocol or both. (Default: TCP)
<b>SourcePorts</b>	Specifies the source port or the port ranges applicable to this service. (Default: 0-65535)
<b>SYNRelay</b>	Enable SYN flood protection (SYN Relay). (Default: No)
<b>PassICMPReturn</b>	Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)
<b>ALG</b>	An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)
<b>MaxSessions</b>	Specifies how many concurrent sessions that are permitted using this service. (Default: 200)
<b>Comments</b>	Text describing the current object. (Optional)

## 3.43. Settings

This is a category that groups the following object types.

### 3.43.1. ARPTableSettings

#### Description

Advanced ARP-table settings.

#### Properties

<b>ARPMatchEnetSender</b>	The Ethernet Sender address matching the hardware address in the ARP data. (Default: DropLog)
<b>ARPQueryNoSenderIP</b>	If the IP source address of an ARP query (NOT response!) is "0.0.0.0". (Default: DropLog)
<b>ARPSenderIP</b>	The IP Source address in ARP packets. (Default: Validate)
<b>UnsolicitedARPReplies</b>	Unsolicited ARP replies. (Default: DropLog)
<b>ARPRequests</b>	Specifies whether or not the ARP requests should automatically be added to the ARP table. (Default: Drop)
<b>ARPChanges</b>	ARP packets that would cause an entry to be changed. (Default: AcceptLog)
<b>StaticARPChanges</b>	ARP packets that would cause static entries to be changed. (Default: DropLog)
<b>ARPExpire</b>	Lifetime of an ARP entry in seconds. (Default: 900)
<b>ARPExpireUnknown</b>	Lifetime of an "unknown" ARP entry in seconds. (Default: 3)
<b>ARPMulticast</b>	ARP packets claiming to be multicast addresses; may need to be enabled for some load balancers/redundancy solutions. (Default: DropLog)
<b>ARPBroadcast</b>	ARP packets claiming to be broadcast addresses; should never need to be enabled. (Default: DropLog)
<b>ARPCacheSize</b>	Number of ARP entries in cache, total. (Default: 4096)
<b>ARPHashSize</b>	Number of ARP hash buckets per physical interface. (Default: 512)
<b>ARPHashSizeVLAN</b>	Number of ARP hash buckets per VLAN interface. (Default: 64)



#### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

### 3.43.2. ConnTimeoutSettings

#### Description

Timeout settings for various protocols.

### Properties

<b>ConnLife_TCP_SYN</b>	Connection idle lifetime for TCP connections being formed. (Default: 60)
<b>ConnLife_TCP</b>	Connection idle lifetime for TCP. (Default: 262144)
<b>ConnLife_TCP_FIN</b>	Connection idle lifetime for TCP connections being closed. (Default: 80)
<b>ConnLife_UDP</b>	Connection idle lifetime for UDP. (Default: 130)
<b>AllowBothSidesToKeepConnAlive_UDP</b>	Allow both sides to keep a UDP connection alive. (Default: No)
<b>ConnLife_Ping</b>	Connection timeout for Ping. (Default: 8)
<b>ConnLife_Other</b>	Idle lifetime for other protocols. (Default: 130)
<b>ConnLife_IGMP</b>	Connection idle lifetime for IGMP. (Default: 12)



#### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.3. DHCPRelaySettings

### Description

Advanced DHCP relay settings.

### Properties

<b>MaxTransactions</b>	Maximum number of concurrent BOOTP/DHCP transactions. (Default: 32)
<b>TransactionTimeout</b>	Timeout for each transaction (in seconds). (Default: 10)
<b>MaxPPMPerIfc</b>	Maximum packets per minute that are relayed from clients to the server, per interface. (Default: 500)
<b>MaxHops</b>	Requests/responses that have traversed more than this many relays will not be relayed. (Default: 5)
<b>MaxLeaseTime</b>	Maximum lease time (seconds) allowed from the DHCP server (too high times will be lowered silently). (Default: 10000)
<b>MaxAutoRoutes</b>	Maximum number of DHCP client IPs automatically added to the routing table. (Default: 256)
<b>AutoSaveRelayPolicy</b>	Policy for saving the relay list to disk. (Default: ReconfShut)
<b>AutoSaveRelayInterval</b>	Seconds between auto saving the relay list to disk. (Default: 86400)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.4. DHCP Server Settings

### Description

Advanced DHCP server settings.

### Properties

<b>AutoSaveLeasePolicy</b>	Policy for saving the lease database to disk. (Default: ReconfShut)
<b>AutoSaveLeaseInterval</b>	Seconds between auto saving the lease database to disk. (Default: 86400)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.5. Frag Settings

### Description

Settings related to fragmented packets.

### Properties

<b>PseudoReass_MaxConcurrent</b>	Maximum number of concurrent fragment reassemblies. Set to 0 to drop all fragments. (Default: 1024)
<b>IllegalFrag</b>	Illegally constructed fragments; partial overlaps, bad sizes, etc. (Default: DropLog)
<b>DuplicateFragData</b>	On receipt of duplicate fragments, verify matching data... (Default: Check8)
<b>FragReassemblyFail</b>	Failed packet reassembly attempts - due to timeouts or packet losses. (Default: LogSuspectSubseq)
<b>DroppedFrag</b>	Fragments of packets dropped due to rule base. (Default: LogSuspect)
<b>DuplicateFrag</b>	Duplicate fragments received. (Default: LogSuspect)
<b>FragmentedICMP</b>	Fragmented ICMP messages other than Ping; normally invalid. (Default: DropLog)
<b>MinimumFragLength</b>	Minimum allowed length of non-last fragments. (Default: 8)
<b>ReassTimeout</b>	Timeout of a reassembly, since previous received fragment.

	(Default: 65)
<b>ReassTimeLimit</b>	Maximum lifetime of a reassembly, since first received fragment. (Default: 90)
<b>ReassDoneLinger</b>	How long to remember a completed reassembly (watching for old dups). (Default: 20)
<b>ReassIllegalLinger</b>	How long to remember an illegal reassembly (watching for more fragments). (Default: 60)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.6. ICMPSettings

### Description

Settings related to the ICMP protocol.

### Properties

<b>ICMPSendPerSecLimit</b>	Maximum number of ICMP responses that will be sent each second. (Default: 500)
<b>SilentlyDropStateICMPErrors</b>	Silently drop ICMP errors regarding statefully tracked open connections. (Default: Yes)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.7. IPSecTunnelSettings

### Description

Settings for the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

### Properties

<b>IPsecMaxTunnels</b>	Amount of IPsec tunnels allowed (0 = automatic). (Default: 0)
<b>IPsecMaxRules</b>	Amount of IPsec rules allowed (0 = automatic). (Default: 0)
<b>IKESendInitialContact</b>	Send 'initial contact' messages. (Default: Yes)
<b>IKESendCRLs</b>	Send CRLs in the IKE exchange. (Default: Yes)
<b>IKECRLValidityTime</b>	Maximum number of seconds a CRL is considered valid (0=obey the 'next update' field in the CRL). (Default: 86400)



<b>IKEMaxCAPath</b>	Maximum number of CA certificates in a certificate path. (Default: 15)
<b>IPsecCertCacheMaxCerts</b>	Maximum number of entries in the certificate cache. (Default: 1024)
<b>IPsecBeforeRules</b>	Pass IKE & IPsec (ESP/AH) traffic sent to the security gateway directly to the IPsec engine without consulting the ruleset. (Default: Yes)
<b>IPsecGWNameCacheTime</b>	Amount of time to keep an IPsec tunnel open when the remote DNS name fails to resolve. (Default: 14400)
<b>DPDMetric</b>	Metric 10s of seconds with no traffic or other evidence of life in tunnel before SA is removed. (Default: 3)
<b>DPDKeepTime</b>	Number 10s of seconds a SA will remain in dead cache after a delete. DPD will not trigger if peer already is cached as dead. (Default: 2)
<b>DPDExpireTime</b>	Number of seconds that DPD-R-U-THERE messages will be sent. (Default: 15)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.8. IPSettings

### Description

Settings related to the IP protocol.

### Properties

<b>LogChecksumErrors</b>	Log IP packets with bad checksums. (Default: Yes)
<b>LogNonIP4</b>	Log occurrences of non-IPv4 packets. (Default: Yes)
<b>LogReceivedTTL0</b>	Log received packets with TTL=0; this should never happen! (Default: Yes)
<b>Block0000Src</b>	Block 0.0.0.0 as source address. (Default: Drop)
<b>Block0Net</b>	Block 0.* source addresses. (Default: DropLog)
<b>Block127Net</b>	Block 127.* source addresses. (Default: DropLog)
<b>BlockMulticastSrc</b>	Block multicast source addresses (224.0.0.0--255.255.255.255). (Default: DropLog)
<b>TTLMin</b>	The minimum IP Time-To-Live value accepted on receipt. (Default: 3)
<b>TTLOnLow</b>	What action to take on too low unicast TTL values. (Default: DropLog)
<b>TTLMinMulticast</b>	The minimum IP multicast Time-To-Live value accepted on

	receipt. (Default: 3)
<b>TTLonLowMulticast</b>	What action to take on too low multicast TTL values. (Default: DropLog)
<b>DefaultTTL</b>	The default IP Time-To-Live of packets originated by the security gateway (32-255). (Default: 255)
<b>LayerSizeConsistency</b>	TCP/UDP/ICMP/etc layer data and header sizes matching lower layer size information. (Default: ValidateLogBad)
<b>SecuRemoteUDPEncapCompat</b>	Allow IP data to contain eight bytes more than the UDP total length field specifies -- Checkpoint SecuRemote violates NAT-T drafts. (Default: No)
<b>IPOptionSizes</b>	Validity of IP header option sizes. (Default: ValidateLogBad)
<b>IPOPT_SR</b>	How to handle IP packets with contained source or return routes. (Default: DropLog)
<b>IPOPT_TS</b>	How to handle IP packets with contained Timestamps. (Default: DropLog)
<b>IPOPT_RTRALT</b>	How to handle IP packets with contained route alert. (Default: ValidateLogBad)
<b>IPOPT_OTHER</b>	How to handle IP options not specified above. (Default: DropLog)
<b>DirectedBroadcasts</b>	How to handle directed broadcasts being passed from one interface to another. (Default: DropLog)
<b>IPRF</b>	How to handle the IP Reserved Flag, if set; it should never be. (Default: DropLog)
<b>StripDFOnSmall</b>	Strip the "DontFragment" flag for packets of this size or smaller. (Default: 65535)
<b>MulticastIPEnetOnMismatch</b>	What action to take when ethernet and IP multicast addresses does not match. (Default: DropLog)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.9. L2TPServerSettings

### Description

PPTP/L2TP server settings.

### Properties

<b>L2TPBeforeRules</b>	Pass L2TP connections sent to the security gateway directly to the L2TP engine without consulting the ruleset. (Default: Yes)
<b>PPTPBeforeRules</b>	Pass PPTP connections sent to the security gateway directly to the PPTP engine without consulting the ruleset. (Default: Yes)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.10. LengthLimSettings

### Description

Length limitations for various protocols.

### Properties

<b>MaxTCPLen</b>	TCP; Sometimes has to be increased if tunneling protocols are used. (Default: 1480)
<b>MaxUDPLen</b>	UDP; Many interactive applications use large UDP packets, may otherwise be decreased to 1480. (Default: 60000)
<b>MaxICMPLen</b>	ICMP; May be decreased to 1480 if desired. (Default: 10000)
<b>MaxGRELen</b>	Encapsulated (tunneled transport), used by PPTP. (Default: 2000)
<b>MaxESPLen</b>	IPsec ESP; Encrypted communication. (Default: 2000)
<b>MaxAHLen</b>	IPsec AH; Authenticated communication. (Default: 2000)
<b>MaxSKIPLen</b>	SKIP; Simple Key management for IP, VPN protocol. (Default: 2000)
<b>MaxOSPFLen</b>	OSPF; Open Shortest Path First, routing protocol. (Default: 1480)
<b>MaxIPIPLen</b>	IPIP/FWZ; Encapsulated (tunneled) transport, used by VPN-1. (Default: 2000)
<b>MaxIPCompLen</b>	IPsec IPComp; Compressed communication. (Default: 2000)
<b>MaxL2TPLen</b>	L2TP; Layer 2 Tunneling Protocol. (Default: 2000)
<b>MaxOtherSubIPLen</b>	Others; sometimes has to be increased if unknown tunneling protocols are used. (Default: 1480)
<b>LogOversizedPackets</b>	Log occurrences of oversized packets. (Default: Yes)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.11. LocalReassSettings

### Description

Parameters use for local fragment reassembly.

### Properties

<b>LocalReass_MaxConcurrent</b>	Maximum number of concurrent local reassemblies. (Default: 256)
<b>LocalReass_MaxSize</b>	Maximum size of a locally reassembled packet. (Default: 10000)
<b>LocalReass_NumLarge</b>	Number of large (>2K) local reassembly buffers (of the above size). (Default: 32)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.12. LogSettings

**Description**

Advanced log settings.

**Properties**

<b>LogSendPerSecLimit</b>	Limits how many log packets the security gateway may send out per second. (Default: 2000)
---------------------------	---

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.13. MiscSettings

**Description**

Miscellaneous Settings

**Properties**

<b>UDPSrcPort0</b>	How to treat UDP packets with source port 0. (Default: DropLog)
<b>Port0</b>	How to treat TCP/UDP packets with destination port 0 and TCP packets with source port 0. (Default: DropLog)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.14. RemoteMgmtSettings

**Description**

Setup and configure methods and permissions for remote management of this system.

### Properties

<b>NetconBiDirTimeout</b>	Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration. (Default: 30)
<b>WebUIBeforeRules</b>	Enable HTTP(S) traffic to the security gateway regardless of configured IP Rules. (Default: Yes)
<b>WWWSrv_HTTPPort</b>	Specifies the HTTP port for the web user interface. (Default: 80)
<b>WWWSrv_HTTPSPort</b>	Specifies the HTTP(S) port for the web user interface. (Default: 443)
<b>SSHBeforeRules</b>	Enable SSH traffic to the security gateway regardless of configured IP Rules. (Default: Yes)
<b>HTTPSCertificate</b>	Specifies which certificate to use for HTTPS traffic. (Optional)
<b>SNMPBeforeRules</b>	Enable SNMP traffic to the security gateway regardless of configured IP Rules. (Default: Yes)
<b>SNMPRequestLimit</b>	Maximum number of SNMP packets that will be processed each second. (Default: 100)
<b>SNMPSysContact</b>	The contact person for this managed node. (Default: N/A)
<b>SNMPSysName</b>	The name for this managed node. (Default: N/A)
<b>SNMPSysLocation</b>	The physical location of this node. (Default: N/A)
<b>SNMPIfDescription</b>	What to display in the SNMP MIB-II ifDescr variables. (Default: Name)
<b>SNMPIfAlias</b>	What to display in the SNMP ifMIB ifAlias variables. (Default: Hardware)
<b>LocalConsoleIdleTimeout</b>	Number of seconds of inactivity until the local console user is automatically logged out. (Default: 900)
<b>WebUIIdleTimeout</b>	Number of seconds of inactivity until the HTTP(S) session is closed. (Default: 900)



#### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.15. RoutingSettings

### Description

Configure the routing capabilities of the system.

### Properties

<b>RouteFailOver_IfacePollInterval</b>	Time (ms) between polling of interface failure. (Default: 500)
<b>RouteFailOver_ARPPollInterval</b>	Time (ms) between ARP-lookup of gateways. May be overridden for each route. (Default: 1000)
<b>RouteFailOver_PingPollInterval</b>	Time (ms) between PING'ing of gateways. (Default: 1000)
<b>RouteFailOver_GraceTime</b>	Time (s) between startup/reconfigure and monitoring start. (Default: 30)
<b>RouteFailOver_ConsecFails</b>	Number of consecutive failures before route is marked as unavailable. (Default: 5)
<b>RouteFailOver_ConsecSuccess</b>	Number of consecutive success before route is marked as available. (Default: 5)
<b>Transp_CAMToL3CDestLearning</b>	Do L3 Cache learning based on destination IPs and MACs in combination with CAM table contents. (Default: Yes)
<b>Transp_DecrementTTL</b>	Decrement TTL on packets forwarded between transparent interfaces. (Default: No)
<b>Transp_CAMSize_Dynamic</b>	Allocate the CAM Size value dynamically. (Default: Yes)
<b>Transp_CAMSize</b>	Maximum number of entries in each CAM table. (Default: 8192)
<b>Transp_L3CSize_Dynamic</b>	Allocate the L3 Cache Size value dynamically. (Default: Yes)
<b>Transp_L3CSize</b>	Maximum number of entries in each Layer 3 Cache. (Default: 8192)
<b>Transp_RelaySTP</b>	Relay Spanning-Tree (STP, RSTP and MSTP) Bridge Protocol Data Units to all switch interfaces. (Default: Drop)
<b>Transp_RelayMPLS</b>	Forward MPLS packets to all switch interfaces. (Default: Drop)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.16. SSLSettings

### Description

Settings related to SSL (Secure Sockets Layer).

### Properties

<b>SSL_ProcessingPriority</b>	The amount of of CPU time that SSL processing is allowed to use. (Default: Normal)
<b>TLS_RSA_WITH_3DES_168_SHA1</b>	Enable cipher RSA_WITH_3DES_168_SHA1. (Default: Yes)
<b>TLS_RSA_WITH_RC4_128_SHA1</b>	Enable cipher RSA_WITH_RC4_128_SHA1. (Default: Yes)

<b>TLS_RSA_WITH_RC4_128_MD5</b>	Enable cipher TLS_RSA_WITH_RC4_128_MD5. (Default: Yes)
<b>TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1</b>	Enable cipher TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1. (Default: Yes)
<b>TLS_RSA_EXPORT512_WITH_RC4_40_MD5</b>	Enable cipher TLS_RSA_EXPORT1024_WITH_RC4_40_MD5. (Default: No)
<b>TLS_RSA_EXPORT512_WITH_RC2_40_MD5</b>	Enable cipher TLS_RSA_EXPORT1024_WITH_RC2_40_MD5. (Default: No)
<b>TLS_RSA_EXPORT_WITH_NULL_SHA1</b>	Enable cipher TLS_RSA_EXPORT_WITH_NULL_SHA1 (no encryption, just message validation). (Default: No)
<b>TLS_RSA_EXPORT_WITH_NULL_MD5</b>	Enable cipher TLS_RSA_EXPORT_WITH_NULL_MD5 (no encryption, just message validation). (Default: No)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.17. StateSettings

### Description

Parameters for the state engine in the system.

### Properties

<b>ConnReplace</b>	What to do when the connection table is full. (Default: ReplaceLog)
<b>LogOpenFails</b>	Log packets that are neither part of open connections nor valid new connections. (Default: Yes)
<b>LogReverseOpens</b>	Log reverse connection attempts through an established connection. (Default: Yes)
<b>LogStateViolations</b>	Log packets that violate stateful tracking rules; for instance, TCP connect sequences. (Default: Yes)
<b>LogConnections</b>	Log connections opening and closing. (Default: Log)
<b>LogConnectionUsage</b>	Log for every packet that passes through a connection. (Default: No)
<b>MaxConnections_Dynamic</b>	Allocate the Max Connection value dynamically. (Default: Yes)
<b>MaxConnections</b>	Maximum number of simultaneous connections. (Default: 8192)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.18. TCPSettings

### Description

Settings related to the TCP protocol.

### Properties

<b>TCPOptionSizes</b>	Validity of TCP header option sizes. (Default: ValidateLogBad)
<b>TCPMSSMin</b>	Minimum allowed TCP MSS (Maximum Segment Size). (Default: 100)
<b>TCPMSSOnLow</b>	How to handle too low MSS values. (Default: DropLog)
<b>TCPMSSMax</b>	Maximum allowed TCP MSS (Maximum Segment Size). (Default: 1460)
<b>TCPMSSVPNMax</b>	Limits TCP MSS for VPN connections; minimizes fragmentation. (Default: 1400)
<b>TCPMSSOnHigh</b>	How to handle too high MSS values. (Default: Adjust)
<b>TCPMSSLogLevel</b>	When to log regarding too high TCP MSS, if not logged by "TCP MSS on high". (Default: 7000)
<b>TCPMSSAutoClamping</b>	Automatically clamp TCP MSS according to MTU of involved interfaces - in addition to "TCP MSS max". (Default: Yes)
<b>TCPZeroUnusedACK</b>	Force unused ACK fields to zero; helps prevent connection spoofing. (Default: Yes)
<b>TCPZeroUnusedURG</b>	Force unused URG fields to zero; prevents small information leak. (Default: Yes)
<b>TCPOPT_WSOPT</b>	The WSOPT (Window Scale) option (common). (Default: ValidateLogBad)
<b>TCPOPT_SACK</b>	The SACK/SACKPERMIT (Selective ACK) options (common). (Default: ValidateLogBad)
<b>TCPOPT_TSOPT</b>	The TSOPT (Timestamp) option (common). (Default: ValidateLogBad)
<b>TCPOPT_ALTCHKREQ</b>	The ALTCHKREQ (Alternate Checksum Request) option. (Default: StripLog)
<b>TCP- OPT_ALTCHKDATA</b>	The ALTCHKDATA (Alternate Checksum Data) option. (Default: StripLog)
<b>TCPOPT_CC</b>	The CC (Connection Count) option series (semi common). (Default: StripLogBad)
<b>TCPOPT_OTHER</b>	How to handle TCP options not specified above. (Default: StripLog)



<b>TCPSynUrg</b>	The TCP URG flag together with SYN; normally invalid (strip=strip URG). (Default: DropLog)
<b>TCPSynPsh</b>	The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH). (Default: StripSilent)
<b>TCPSynRst</b>	The TCP RST flag together with SYN; normally invalid (strip=strip RST). (Default: DropLog)
<b>TCPSynFin</b>	The TCP FIN flag together with SYN; normally invalid (strip=strip FIN). (Default: DropLog)
<b>TCPFinUrg</b>	The TCP URG flag together with FIN; normally invalid (strip=strip URG). (Default: DropLog)
<b>TCPUrg</b>	The TCP URG flag; many operating systems cannot handle this correctly. (Default: StripLog)
<b>TCPECN</b>	The Explicit Congestion Notification (ECN) flags. Previously known as "XMAS"/"YMAS" flags. Also used in OS fingerprinting. (Default: StripLog)
<b>TCPRF</b>	The TCP Reserved field: should be zero. Used in OS fingerprinting. Also part of ECN extension. (Default: StripLog)
<b>TCPNULL</b>	TCP "NULL" packets without SYN, ACK, FIN or RST; normally invalid, used by scanners. (Default: DropLog)
<b>TCPSequenceNumbers</b>	Validation of TCP sequence numbers. (Default: ValidateLogBad)
<b>TCPAllowReopen</b>	Allow clients to re-open TCP connections that are in the closed state. (Default: No)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.43.19. VLANSettings

### Description

Settings for IEEE 802.1Q based Virtual LAN interfaces.

### Properties

**UnknownVLANTags** VLAN packets tagged with an unknown ID. (Default: DropLog)

**Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.44. SSHClientKey

### Description

The public key of the client connecting to the SSH server.

### Properties

<b>Name</b>	Specifies a symbolic name for the key. (Identifier)
<b>Type</b>	DSA or RSA. (Default: DSA)
<b>Subject</b>	Value of the Subject header tag of the public key file. (Optional)
<b>PublicKey</b>	Specifies the public key.
<b>Comments</b>	Text describing the current object. (Optional)

## 3.45. ThresholdRule

### Description

A Threshold Rule defines a filter for matching specific network traffic. When the filter criteria is met, the Threshold Rule Actions are evaluated and possible actions taken.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule. (Optional)
<b>SourceInterface</b>	Specifies the name of the receiving interface to be compared to the received packet.
<b>SourceNetwork</b>	Specifies the sender span of IP addresses to be compared to the received packet.
<b>DestinationInterface</b>	Specifies the the destination interface to be compared to the received packet.
<b>DestinationNetwork</b>	Specifies the span of IP addresses to be compared to the destination IP of the received packet.
<b>Service</b>	Specifies a service that will be used as a filter parameter when matching traffic with this rule.
<b>Schedule</b>	By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no Index is specified when creating an instance of this type, the object will be placed last in the list and the Index will be equal to the length of the list.*

### 3.45.1. ThresholdAction

### Description

A Threshold Rule Action specifies what thresholds to measure, and what action to take if those thresholds are reached.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Action</b>	Protect or Audit. (Default: Protect)
<b>GroupBy</b>	Specifies whether the threshold should be host- or network-based. (Default: SourceIP)
<b>Threshold</b>	Specifies the threshold.

---

<b>ThresholdUnit</b>	Specifies the threshold unit. (Default: ConnsSec)
<b>ZoneDefense</b>	Activate ZoneDefense. (Default: No)
<b>BlackList</b>	Activate BlackList. (Default: No)
<b>BlackListTimeToBlock</b>	The number of seconds that the dynamic black list should remain. (Optional)
<b>BlackListBlockOnlyService</b>	Only block the service that triggered the blacklisting. (Default: No)
<b>BlackListIgnoreEstablished</b>	Do not drop existing connection. (Default: No)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.46. UpdateCenter

### Description

Configure automatical updates.

### Properties

<b>AVEnabled</b>	Automatic updates of antivirus definitions and engine. (Default: No)
<b>IDPEnabled</b>	Automatic updates of IDP maintenance signatures. (Default: No)
<b>AdvancedIDPEnabled</b>	Automatic updates of Advanced IDP signatures. (Default: No)
<b>UpdateInterval</b>	Specifies the interval at which the automatic update runs. (Default: Daily)
<b>UpdateDate</b>	Specifies the day of month when the automatic update is runs.
<b>UpdateWeekday</b>	Specifies the day of week when the automatic update is runs. (Default: mon)
<b>Hourly</b>	Specififes the number of hours between periodical updates.
<b>UpdateHour</b>	Specifies the hour when the update is run. (Default: 0)
<b>UpdateMinute</b>	Specifies the minute when the update is run. (Default: 0)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.47. UserAuthRule

### Description

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Name</b>	Specifies a symbolic name for the rule.
<b>Agent</b>	HTTP, HTTPS, XAUTH, PPP or EAP. (Default: HTTP)
<b>AuthSource</b>	Disallow, Radius or Local.
<b>Interface</b>	The interface on which the connection was received.
<b>OriginatorIP</b>	The network object that the incoming IP address must be a part of.
<b>TerminatorIP</b>	Specifies the destination IP configured on the PPTP/L2TP server configuration. Only used when agent is PPP.
<b>RadiusServers</b>	Specifies the authentication servers that will be used to authenticate users matching this rule.
<b>RadiusMethod</b>	Specifies the authentication method used for encrypting the user password. (Default: PAP)
<b>LocalUserDB</b>	Specifies the local user database that will be used to authenticate users matching this rule.
<b>LoginType</b>	HTML form or Basic authentication. (Default: HTMLForm)
<b>RealmString</b>	The string that is presented as a part of the 401 - Authentication Required message.
<b>HostCertificate</b>	Specifies the host certificate that the security gateway sends to the client.
<b>RootCertificate</b>	Specifies the root certificate that was used to sign the host certificate. (Optional)
<b>PPPAuthNoAuth</b>	Allow no authentication. (Default: No)
<b>PPPAuthPAP</b>	Use PAP authentication protocol. User name and password are sent in plaintext. (Default: Yes)
<b>PPPAuthCHAP</b>	Use CHAP authentication protocol. (Default: Yes)
<b>PPPAuthMSCHAP</b>	Use MS-CHAP authentication protocol. (Default: Yes)
<b>PPPAuthMSCHAPv2</b>	Use MS-CHAP v2 authentication protocol. (Default: Yes)
<b>IdleTimeout</b>	If a user has successfully been authenticated, and no traffic has been seen from his IP address for this number of seconds, he/she will automatically be logged out. (Default: 1800)
<b>SessionTimeout</b>	If a user has successfully been authenticated, he/she will auto-

	atically be logged out after this many seconds, regardless of if there has been activity from the user or not. (Optional)
<b>UseServerTimeouts</b>	Use timeouts received from the authentication server. If no values are received, the manually specified values will be used. (Default: No)
<b>MultipleUsernameLogins</b>	Specifies how multiple username logins will be handled. (Default: AllowMultiple)
<b>ReplaceIdleTime</b>	Replace existing user if idle for more than this number of seconds. (Default: 10)
<b>AccountingServers</b>	Specifies the accounting servers that will be used to report user usage matching this rule. (Optional)
<b>BytesSent</b>	Enable reporting of the number of bytes sent by the user. (Default: Yes)
<b>PacketsSent</b>	Enable reporting of the number of packets sent by the user. (Default: Yes)
<b>BytesReceived</b>	Enable reporting of the number of bytes received by the user. (Default: Yes)
<b>PacketsReceived</b>	Enable reporting of the number of packets received by the user. (Default: Yes)
<b>SessionTime</b>	Enable reporting of the number of seconds the session lasted. (Default: Yes)
<b>SupportInterimAccounting</b>	Enable Interim Accounting Messages to update the accounting server with the current status of an authenticated user. (Default: No)
<b>ServerInterimControl</b>	Let the RADIUS server determine the interval that interim accounting events should be sent. (Default: Yes)
<b>InterimValue</b>	The interval in seconds in which interim accounting events should be sent. (Default: 600)
<b>LogEnabled</b>	Enable logging. (Default: No)
<b>LogSeverity</b>	Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)
<b>Comments</b>	Text describing the current object. (Optional)

**Note**

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*

## 3.48. ZoneDefenseBlock

### Description

Manually configured blocks are used to block a host/network on the switches either by default or based on schedule.

### Properties

<b>Index</b>	The index of the object, starting at 1. (Identifier)
<b>Addresses</b>	Specifies the addresses to block.
<b>Protocol</b>	All, TCP, UDP or ICMP. (Default: All)
<b>Port</b>	Specifies which UDP or TCP port to use. (Default: 0)
<b>Schedule</b>	Specifies the schedule when the given addresses should be blocked. (Optional)
<b>Comments</b>	Text describing the current object. (Optional)



### Note

*If no `Index` is specified when creating an instance of this type, the object will be placed last in the list and the `Index` will be equal to the length of the list.*



## 3.49. ZoneDefenseExcludeList

### Description

The exclude list is used exclude certain hosts/networks from being blocked out by IDP/Threshold rule violations.

### Properties

**Addresses**      Specifies the addresses that should not be blocked. (Optional)

**Comments**      Text describing the current object. (Optional)



### **Note**

*This object type does not have an identifier and is identified by the name of the type only. There can only be one instance of this type.*

## 3.50. ZoneDefenseSwitch

### Description

A ZoneDefense switch will have its ACLs controlled and hosts/networks violating the IDP/Threshold rules will be blocked directly on the switch.

### Properties

<b>Name</b>	Specifies a symbolic name for the ZoneDefense switch. (Identifier)
<b>SwitchModel</b>	Specifies the switch model type. (Default: DES-3226S)
<b>IP</b>	The IP address of the management interface of the switch.
<b>Enabled</b>	Enable the ZoneDefense switch. (Default: Yes)
<b>SNMPCommunity</b>	The SNMP community string (write access).
<b>Comments</b>	Text describing the current object. (Optional)



---

# Index

## Commands

### A

about, 30  
activate, 19  
add, 19  
alarm, 30  
arp, 30  
arpsnoop, 31  
ats, 32

### B

bigpond, 32  
blacklist, 33  
buffers, 34

### C

cam, 34  
cancel, 20  
cc, 20  
certcache, 35  
cfglog, 35  
commit, 21  
connections, 35  
copy, 22  
cpuid, 36  
crashdump, 37  
customlog, 37

### D

dconsole, 37  
delete, 22  
dhcp, 38  
dhcprelay, 38  
dhcpserver, 39  
dns, 40  
dnsbl, 40  
dynroute, 41

### F

frags, 41

### H

ha, 42  
help, 63  
history, 63  
httpposter, 42  
hwaccel, 43

### I

ifstat, 43  
igmp, 44  
ikesnoop, 44  
ippool, 45

ipsecglobalstats, 46  
ipseckeealive, 46  
ipsecstats, 46

### K

killsa, 47

### L

license, 47  
linkmon, 48  
lockdown, 48  
logout, 49

### M

memory, 49

### N

natpool, 49

### O

ospf, 50

### P

ping, 62  
pipes, 51  
pskgen, 23

### R

reconfigure, 52  
reject, 24  
reset, 25  
routemon, 52  
routes, 52  
rules, 53

### S

sessionmanager, 54  
set, 25  
show, 26  
shutdown, 55  
sipalg, 56  
sshserver, 57  
stats, 58

### T

time, 58

### U

undelete, 28  
updatecenter, 59  
urlcache, 59  
userauth, 60

### V

vlan, 61  
vpnstats, 61  
(see also ipsecstats)

**Z**

zonedefense, 61

# Object types

**A**

Access, 66  
AddressFolder, 68  
AdvancedScheduleOccurrence, 71  
AdvancedScheduleProfile, 71  
ALG\_FTP, 72  
ALG\_H323, 73  
ALG\_HTTP, 73  
ALG\_HTTP\_URL, 74  
ALG\_POP3, 74  
ALG\_SIP, 75  
ALG\_TFTP, 75  
ARP, 77  
ARPTTableSettings, 141

**B**

BlacklistWhiteHost, 78

**C**

Certificate, 79  
COMPortDevice, 83  
ConfigModePool, 84  
ConnTimeoutSettings, 141

**D**

DateTime, 85  
DefaultInterface, 102  
Device, 86  
DHCPRelay, 87  
DHCPRelaySettings, 142  
DHCPServer, 88  
DHCPServerCustomOption, 89  
DHCPServerPoolStaticHost, 88  
DHCPServerSettings, 143  
DNS, 90  
DynamicRoutingRule, 92  
DynamicRoutingRuleAddRoute, 93  
DynamicRoutingRuleExportOSPF, 92  
DynDnsClientCjbNet, 80  
DynDnsClientDLink, 80  
DynDnsClientDLinkChina, 80  
DynDnsClientDynDnsOrg, 81  
DynDnsClientDynaCx, 81  
DynDnsClientPeanutHull, 82

**E**

Ethernet, 102  
EthernetAddress, 68, 70  
EthernetAddressGroup, 68, 70  
EthernetDevice, 95  
EventReceiverSNMP2c, 118

**F**

FragSettings, 143

**G**

GRE Tunnel, 103

**H**

HighAvailability, 96  
HTTPPoster, 97

**I**

ICMPSettings, 144  
ID, 98  
IDList, 98  
IDPRule, 99  
IDPRuleAction, 99  
IKEAlgorithms, 101  
InterfaceGroup, 103  
IP4Address, 69, 70  
IP4Group, 69, 70  
IP4HAddress, 70, 70  
IPPool, 111  
IPRule, 112, 114  
IPRuleFolder, 114  
IPSecAlgorithms, 115  
IPSecTunnel, 104  
IPSecTunnelSettings, 144  
IPSettings, 145  
IXP4NPEEthernetDriver, 91

**L**

L2TPClient, 106  
L2TPServer, 107  
L2TPServerSettings, 146  
LDAPServer, 116  
LengthLimSettings, 147  
LocalReassSettings, 147  
LocalUserDatabase, 117  
LoginClientBigPond, 82  
LogReceiverMemory, 118  
LogReceiverMessageException, 118, 120  
LogReceiverSMTP, 119  
LogReceiverSyslog, 119  
LogSettings, 148

**M**

MarvellEthernetPCIDriver, 91  
MiscSettings, 148

**N**

NATPool, 121

**O**

OSPFAggregate, 125  
OSPFArea, 123  
OSPFInterface, 123  
OSPFNeighbor, 124

OSPFProcess, 122  
OSPFVLink, 125

## P

Pipe, 126  
PipeRule, 129  
PPPoETunnel, 108  
PSK, 130

## R

R8139EthernetPCIDriver, 91  
RadiusServer, 131  
RemoteMgmtHTTP, 132  
RemoteMgmtSettings, 148  
RemoteMgmtSNMP, 132  
RemoteMgmtSSH, 132  
Route, 135  
RoutingRule, 134  
RoutingSettings, 149  
RoutingTable, 135

## S

ScheduleProfile, 137  
ServiceGroup, 138  
ServiceICMP, 138  
ServiceIPProto, 139  
ServiceTCPUDP, 139  
SSHClientKey, 154  
SSLSettings, 150  
StateSettings, 151  
SwitchRoute, 136

## T

TCPSettings, 152  
ThresholdAction, 155  
ThresholdRule, 155

## U

UpdateCenter, 157  
User, 117  
UserAuthRule, 158

## V

VLAN, 109  
VLANSettings, 153

## Z

ZoneDefenseBlock, 160  
ZoneDefenseExcludeList, 161  
ZoneDefenseSwitch, 162