CLI Reference Guide
DFL-260E/860E/1660/2560/2560G

NetDefendOS version 2.40.03
Published 2013-02-20
Copyright © 2013

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 the written consent of D-Link.

Disclaimer
The information in this document is subject to change without notice. D-Link makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. D-Link reserves the right to revise this publication and to make changes from time to time in the content hereof without any obligation to notify any person or parties 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 ............................................................................................................... 10
1. Introduction ................................................................................................... 12
   1.1. Running a command ............................................................................ 12
   1.2. Help .................................................................................................. 13
      1.2.1. Help for commands .................................................................... 13
      1.2.2. Help for object types ................................................................. 13
   1.3. Function keys ..................................................................................... 14
   1.4. Command line history ........................................................................ 15
   1.5. Tab completion .................................................................................. 16
      1.5.1. Inline help ................................................................................ 16
      1.5.2. Autocompleting Current and Default value ............................... 16
      1.5.3. Configuration object type categories ......................................... 17
   1.6. User roles .......................................................................................... 18
2. Command Reference ..................................................................................... 20
   2.1. Configuration ..................................................................................... 20
      2.1.1. activate ...................................................................................... 20
      2.1.2. add ............................................................................................ 20
      2.1.3. cancel ........................................................................................ 21
      2.1.4. cc ............................................................................................. 22
      2.1.5. commit ....................................................................................... 23
      2.1.6. delete ........................................................................................ 23
      2.1.7. pskgen ...................................................................................... 24
      2.1.8. reject ......................................................................................... 24
      2.1.9. reset .......................................................................................... 26
      2.1.10. set ........................................................................................... 26
      2.1.11. show ........................................................................................ 27
      2.1.12. undelete ................................................................................... 29
   2.2. Runtime ............................................................................................... 31
      2.2.1. about ......................................................................................... 31
      2.2.2. alarm ......................................................................................... 31
      2.2.3. arp ............................................................................................. 31
      2.2.4. arpsnoop .................................................................................... 32
      2.2.5. ats ............................................................................................. 33
      2.2.6. bigpond ...................................................................................... 33
      2.2.7. blacklist ..................................................................................... 34
      2.2.8. buffers ....................................................................................... 35
      2.2.9. cam ............................................................................................ 36
      2.2.10. certcache .................................................................................. 36
      2.2.11. cfglog ...................................................................................... 37
      2.2.12. connections .............................................................................. 37
      2.2.13. cpuid ....................................................................................... 38
      2.2.14. crashdump ............................................................................... 38
      2.2.15. cryptostat ................................................................................. 38
      2.2.16. dconsole .................................................................................. 39
      2.2.17. dhcp ......................................................................................... 39
      2.2.18. dhcrelay .................................................................................. 40
      2.2.19. dhcpserver .............................................................................. 41
      2.2.20. dns .......................................................................................... 42
      2.2.21. dnsbl ....................................................................................... 42
      2.2.22. dynroute .................................................................................. 42
      2.2.23. frags ......................................................................................... 43
      2.2.24. ha ........................................................................................... 44
      2.2.25. hostmon ................................................................................... 44
      2.2.26. httpdlg .................................................................................... 45
      2.2.27. httpposter ............................................................................... 45
      2.2.28. hwm ......................................................................................... 46
      2.2.29. idppipes ................................................................................... 46
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.30. ifstat</td>
<td>47</td>
</tr>
<tr>
<td>2.2.31. igmp</td>
<td>47</td>
</tr>
<tr>
<td>2.2.32. ikesnoop</td>
<td>48</td>
</tr>
<tr>
<td>2.2.33. ippool</td>
<td>49</td>
</tr>
<tr>
<td>2.2.34. ipseceglobalstats</td>
<td>49</td>
</tr>
<tr>
<td>2.2.35. ipseckeepalive</td>
<td>50</td>
</tr>
<tr>
<td>2.2.36. ipsecestats</td>
<td>50</td>
</tr>
<tr>
<td>2.2.37. ipsectunnels</td>
<td>51</td>
</tr>
<tr>
<td>2.2.38. killsa</td>
<td>51</td>
</tr>
<tr>
<td>2.2.39. languagefiles</td>
<td>52</td>
</tr>
<tr>
<td>2.2.40. ldap</td>
<td>52</td>
</tr>
<tr>
<td>2.2.41. license</td>
<td>53</td>
</tr>
<tr>
<td>2.2.42. linkmon</td>
<td>53</td>
</tr>
<tr>
<td>2.2.43. logout</td>
<td>54</td>
</tr>
<tr>
<td>2.2.44. memory</td>
<td>54</td>
</tr>
<tr>
<td>2.2.45. natpool</td>
<td>54</td>
</tr>
<tr>
<td>2.2.46. nd</td>
<td>55</td>
</tr>
<tr>
<td>2.2.47. ndsnoop</td>
<td>56</td>
</tr>
<tr>
<td>2.2.48. netobjects</td>
<td>56</td>
</tr>
<tr>
<td>2.2.49. ospf</td>
<td>57</td>
</tr>
<tr>
<td>2.2.50. pcapdump</td>
<td>59</td>
</tr>
<tr>
<td>2.2.51. pipes</td>
<td>61</td>
</tr>
<tr>
<td>2.2.52. ppptpalg</td>
<td>61</td>
</tr>
<tr>
<td>2.2.53. reconfigure</td>
<td>62</td>
</tr>
<tr>
<td>2.2.54. routemon</td>
<td>62</td>
</tr>
<tr>
<td>2.2.55. routes</td>
<td>62</td>
</tr>
<tr>
<td>2.2.56. rules</td>
<td>64</td>
</tr>
<tr>
<td>2.2.57. selftest</td>
<td>64</td>
</tr>
<tr>
<td>2.2.58. services</td>
<td>66</td>
</tr>
<tr>
<td>2.2.59. sessionmanager</td>
<td>67</td>
</tr>
<tr>
<td>2.2.60. settings</td>
<td>68</td>
</tr>
<tr>
<td>2.2.61. shutdown</td>
<td>69</td>
</tr>
<tr>
<td>2.2.62. sipalg</td>
<td>69</td>
</tr>
<tr>
<td>2.2.63. sshserver</td>
<td>71</td>
</tr>
<tr>
<td>2.2.64. sslvpn</td>
<td>72</td>
</tr>
<tr>
<td>2.2.65. stats</td>
<td>72</td>
</tr>
<tr>
<td>2.2.66. sysmsgs</td>
<td>73</td>
</tr>
<tr>
<td>2.2.67. techsupport</td>
<td>73</td>
</tr>
<tr>
<td>2.2.68. time</td>
<td>73</td>
</tr>
<tr>
<td>2.2.69. uarules</td>
<td>74</td>
</tr>
<tr>
<td>2.2.70. updatecenter</td>
<td>75</td>
</tr>
<tr>
<td>2.2.71. userauth</td>
<td>75</td>
</tr>
<tr>
<td>2.2.72. vlan</td>
<td>76</td>
</tr>
<tr>
<td>2.2.73. vpnstats</td>
<td>77</td>
</tr>
<tr>
<td>2.2.74. zonedefense</td>
<td>77</td>
</tr>
<tr>
<td>2.3. Utility</td>
<td>78</td>
</tr>
<tr>
<td>2.3.1. ping</td>
<td>78</td>
</tr>
<tr>
<td>2.4. Misc</td>
<td>79</td>
</tr>
<tr>
<td>2.4.1. echo</td>
<td>79</td>
</tr>
<tr>
<td>2.4.2. help</td>
<td>79</td>
</tr>
<tr>
<td>2.4.3. history</td>
<td>80</td>
</tr>
<tr>
<td>2.4.4. is</td>
<td>80</td>
</tr>
<tr>
<td>2.4.5. script</td>
<td>81</td>
</tr>
<tr>
<td>3. Configuration Reference</td>
<td>84</td>
</tr>
<tr>
<td>3.1. Access</td>
<td>85</td>
</tr>
<tr>
<td>3.2. Address</td>
<td>87</td>
</tr>
<tr>
<td>3.2.1. AddressFolder</td>
<td>87</td>
</tr>
<tr>
<td>3.2.2. EthernetAddress</td>
<td>90</td>
</tr>
<tr>
<td>3.2.3. EthernetAddressGroup</td>
<td>90</td>
</tr>
<tr>
<td>3.2.4. IP4Address</td>
<td>90</td>
</tr>
<tr>
<td>3.2.5. IP4Group</td>
<td>90</td>
</tr>
<tr>
<td>3.2.6. IP4HAAddress</td>
<td>90</td>
</tr>
<tr>
<td>3.2.7. IP6Address</td>
<td>90</td>
</tr>
</tbody>
</table>
3.2.8. IP6Group .............................................................. 90
3.3. AdvancedScheduleProfile .............................................. 91
  3.3.1. AdvancedScheduleOccurrence ............................. 91
3.4. ALG ................................................................. 92
  3.4.1. ALG_FTP .......................................................... 92
  3.4.2. ALG_H323 ......................................................... 93
  3.4.3. ALG_HTTP ........................................................ 93
  3.4.4. ALG_POP3 ......................................................... 95
  3.4.5. ALG_PPTP ........................................................ 96
  3.4.6. ALG_SIP .......................................................... 96
  3.4.7. ALG_SMTP ......................................................... 97
  3.4.8. ALG_TFTP ........................................................ 99
  3.4.9. ALG_TLS .......................................................... 99
3.5. ARPND ........................................................... 100
3.6. BlacklistWhiteHost ...................................................... 101
3.7. Certificate .......................................................... 102
3.8. Client .............................................................. 103
  3.8.1. DynDnsClientCjbNet .......................................... 103
  3.8.2. DynDnsClientDLink ............................................ 103
  3.8.3. DynDnsClientDLinkChina ................................... 103
  3.8.4. DynDnsClientDynDnsOrg ...................................... 104
  3.8.5. DynDnsClientDynsCx .......................................... 104
  3.8.6. DynDnsClientPeanutHull ..................................... 105
  3.8.7. LoginClientBigPond ............................................ 105
3.9. COMPortDevice ...................................................... 106
3.10. ConfigModePool .................................................... 107
3.11. DateTime ........................................................... 108
3.12. Device ............................................................. 109
3.13. DHCP Relay ......................................................... 110
3.14. DHCP Server ........................................................ 111
  3.14.1. DHCP ServerPoolStaticHost .............................. 112
  3.14.2. DHCP ServerCustomOption .............................. 112
3.15. DNS .............................................................. 113
3.16. Driver ............................................................. 114
  3.16.1. E1000EthernetPCIDriver .................................... 114
  3.16.2. ixgbeEthernetPCIDriver ..................................... 114
  3.16.3. IXP4NPEEthernetDriver ..................................... 115
  3.16.4. MarvellEthernetPCIDriver .................................. 115
  3.16.5. R8139EthernetPCIDriver .................................... 115
  3.16.6. R8169EthernetPCIDriver .................................... 115
3.17. DynamicRoutingRule ................................................ 117
  3.17.1. DynamicRoutingRuleExportOSPF ..................... 118
  3.17.2. DynamicRoutingRuleAddRoute ....................... 118
3.18. EthernetDevice ..................................................... 120
3.19. HighAvailability .................................................. 121
3.20. HTTP ALG Banners ............................................... 122
3.21. HTTP Auth Banners ............................................... 123
3.22. HTTP Poster ........................................................ 124
3.23. HWM .............................................................. 125
3.24. ID List ............................................................. 126
  3.24.1. ID .............................................................. 126
3.25. IDP Rule .......................................................... 127
  3.25.1. IDP RuleAction ............................................... 127
3.26. IGMP Rule ........................................................ 129
3.27. IGMP Setting ........................................................ 131
3.28. IKE Algorithms ..................................................... 132
3.29. Interface .......................................................... 133
  3.29.1. Default Interface ............................................ 133
  3.29.2. Ethernet ........................................................ 133
  3.29.3. GRE Tunnel ..................................................... 134
  3.29.4. Interface Group ............................................... 134
  3.29.5. IPsec Tunnel ..................................................... 135
  3.29.6. L2TP Client ...................................................... 137
List of Examples

1. Command option notation ................................................................. 10
1.1. Help for commands ................................................................. 13
1.2. Help for object types ................................................................. 13
1.3. Command line history ................................................................. 15
1.4. Tab completion ................................................................. 16
1.5. Inline help ................................................................. 16
1.6. Edit an existing property value ................................................................. 17
1.7. Using categories with tab completion ................................................................. 17
2.1. Create a new object ................................................................. 21
2.2. Change context ................................................................. 22
2.3. Delete an object ................................................................. 23
2.4. Reject changes ................................................................. 25
2.5. Set property values ................................................................. 27
2.6. Show objects ................................................................. 28
2.7. Undelete an object ................................................................. 29
2.8. Block hosts ................................................................. 34
2.9. frags ................................................................. 43
2.10. List network objects which have names containing "net". ................................................................. 57
2.11. Show a range of rules ................................................................. 64
2.12. Interface ping test between all interfaces ................................................................. 65
2.13. Interface ping test between interfaces 'if1' and 'if2' ................................................................. 65
2.14. Start 30 min burn-in, testing RAM, storage media and crypto accelerator ................................................................. 65
2.15. List all services which names begin with "http" ................................................................. 67
2.16. Show a range of rules ................................................................. 74
2.17. Hello World ................................................................. 79
2.18. Transfer script files to and from the device ................................................................. 80
2.19. Upload license data ................................................................. 80
2.20. Upload certificate data ................................................................. 81
2.21. Upload ssh public key data ................................................................. 81
2.22. Execute script ................................................................. 81
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:

- **Angle brackets** `<name>` or `-option=<description>`
  - Used for specifying the name of an option or a description of a value.

- **Square brackets** `[option]` or `-option[=value]`
  - Used for specifying that an option or a value for an option is optional and can be omitted.

- **Curly brackets** `{value1 | value2 | value3}`
  - Used for specifying the available values for an option.

- **Ellipsis** `...`
  - Used for specifying that more than one 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 12
- Help, page 13
- Function keys, page 14
- Command line history, page 15
- Tab completion, page 16
- User roles, page 18

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 2.4.2, “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.

**Backspace**  
Delete the character to the left of the cursor.

**Tab**  
Complete current word.

**Ctrl-A or Home**  
Move the cursor to the beginning of the line.

**Ctrl-B or Left Arrow**  
Move the cursor one character to the left.

**Ctrl-C**  
Clear line or cancel page view if more than one page of information is shown.

**Ctrl-D or Delete**  
Delete the character to the right of the cursor.

**Ctrl-E or End**  
Move the cursor to the end of the line.

**Ctrl-F or Right Arrow**  
Move the cursor one character to the right.

**Ctrl-K**  
Delete from the cursor to the end of the line.

**Ctrl-N or Down Arrow**  
Show the next entry in the command history.

**Ctrl-P or Up Arrow**  
Show the previous entry in the command history.

**Ctrl-T**  
Transpose the current and the previous character.

**Ctrl-U**  
Delete from the cursor to the beginning of line.

**Ctrl-W**  
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 2.4.3, “history”.

Example 1.3. Command line history

Using the command line history via the arrow keys:

```plaintext
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", and 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=example_ip (tab)  
gw-world:/> set Address IP4Group examplegroup Members=example_ip  
("example_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 and Default value

Another special character that can be used together with tab completion is the period "." character.
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.

The "<" character before a tab can be used to automatically fill in the default value for a parameter if no value has yet been set. If the ",," character is used, all possible values will be shown and these can then be edited with the back arrow and backspace keys.

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

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 Adress (the category is autocompleted)

gw-world:/> show Adress ip4a (tab)

gw-world:/> show Adress IP4Address (the type is autocompleted)

gw-world:/> show Adress 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 20
• Runtime, page 31
• Utility, page 78
• Misc, page 79

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>] [-force] [-silent] [<key-value pair>]...
```

### Options

- `-force`  
  Add object, even if it has errors.
- `-silent`  
  Do not show any errors.
- `<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
```
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 "exampldb". Only objects in the current context can be accessed.

Example 2.2. Change context

Change to a sub/child context:
```
gw-world:/> cc LocalUserDatabase exampldb
gw-world:/exampldb>
```
Go back to the parent context:
```
gw-world:/ospf1/area1> cc ..
gw-world:/ospf1>
gw-world:/>
```
Go back to the root context:
```
gw-world:/ospf1/area1> cc
gw-world:/>
or
```
```
gw-world:/ospf1/area1> 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

```
-print
```
Print the current context.

```
<Category>
```
Category that groups object types.

```
<Identifier>
```
The property that identifies the configuration object.
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. 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 examplerule)
gw-world:/> set IPRule examplerule SourceNetwork=examplenet
SourceNetwork=examplenet

Usage

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

-force
Force object to be deleted even if it's used by other objects or has children.

<Category>
Category that groups object types.

<Identifier>
The property that identifies the configuration object. May not be applicable depending on the specified <Type>.

<Type>
Type of configuration object to perform operation on.

Note
Requires Administrator privilege.

2.1.7. pskgen
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

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

Options

-<comments>=<String>
Comments for this key.

-<size>=
Number of bits of data in the generated key. (Default: 64)

2.1.8. reject
Reject changes.

Note
Requires Administrator privilege.
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
```

Reject changes recursively:

```
gw-world:/> set Address IP4Address example_ip2 Address=1.2.3.4
Comments="This whole object will be removed"
gw-world:/> reject Address IP4Address example_ip2
```

Reject all changes:

```
gw-world:/exampledb> set User user1 Comments="Something"
gw-world:/exampledb> set User user2 Comments="that will be"
gw-world:/exampledb> set User user3 Comments="rejected"
gw-world:/exampledb> cc ..
gw-world:/> reject LocalUserDatabase exampledb -recursive
```

Usage

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

Reject changes made to the specified object.

```
reject -all
```

Reject all changes in the configuration.

Options

- **-all**  
  Reject all changes in the configuration.

- **-recursive**  
  Recursively reject changes.

- **<Category>**  
  Category that groups object types.

- **<Identifier>**  
  The property that identifies the configuration object. May not be applicable depending on the specified <Type>. 
Type of configuration object to perform operation on.

Note
Requires Administrator privilege.

2.1.9. reset

Reset unit configuration and/or binaries.

Description
Reset configuration or binaries to factory defaults.

Usage

reset -configuration
Reset the configuration to factory defaults.

reset -unit
Reset the unit to factory defaults.

Options

-configuration
Reset configuration to factory default.

-unit
Reset unit to factory defaults.

Note
Requires Administrator privilege.

2.1.10. 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 propertynames 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:

```
> 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"
```

Set properties for an object without identifier:

```
> gw-world:/> set DynDnsClientDyndns0rg Username=example
```

Usage

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

Options

- **-disable**
  Disable object. This option is not available if the object is already disabled.

- **-enable**
  Enable object. This option is not available if the object is already enabled.

- **-force**
  Set values, even if they contain errors.

- **<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.

2.1.11. 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.
- The object is disabled.
! The object has errors.
+ The object is newly created.
* The object is modified.

Additional flags:

D The object has dynamic properties which are updated by the system.

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:/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`
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

- changes  Show all changes in the current configuration.
- disabled  Show disabled properties.
- errors     Show all errors in the current configuration.
- references Show all references to this object from other objects.
- verbose    Show error details.

<Category>  Category that groups object types.
<Identifier> The property that identifies the configuration object.
May not be applicable depending on the specified <Type>.

<Type>     Type of configuration object to perform operation on.

2.1.12. 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 examplerule)
gw-world:/> set IPRule examplerule SourceNetwork=examplenet
gw-world:/> delete Address IP4Address examplenet -force
gw-world:/> undelete Address IP4Address examplenet

Usage

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

<Category> Category that groups object types.

<Identifier> The property that identifies the configuration object. May not be applicable depending on the specified <Type>.

<Type> 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 specified interface.

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

Send gratuitous ARP for IP.

**Options**

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

### 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**
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`

Show ALL BigPond information.

`bigpond <interface>`
Show BigPond information of specified 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


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

-all Show all the information.

-black Show blacklist hosts only.

-block Block specified netobject. (Admin only)
-creati
time
-dest=<ip address>
-dynam
ic
-force
-info
-listtime
-prot={TCP | UDP | ICMP | OTHER | TCPUDP | ALL}
-port=<port number>
-show
-time=<seconds>
-unblock
-white
<host>

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.
2.2.9. cam

CAM table information.

**Description**

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

**Usage**

```
cam -num=<n>
```

Show CAM table information.

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

Show interface-specified CAM table information.

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

Flush CAM table information of specified interface.

```
cam -flush
```

Flush CAM table information.

**Options**

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


List connections.

connections

Same as "connections -show".


Close connections.

Options

-all Mark all connections.
-close Close all connections that match the filter expression. (Admin only)

-destiface=<interface> Filter on destination interface.

-destip=<ip addr> Filter on destination IP address.

-destport=<port> Show only given destination TCP/UDP port.
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. cryptostat

Show information about crypto accelerators.

**Description**

Show information about installed crypto accelerators.

**Usage**
cryptostat

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>] [-onlyhigh] [-blockoutput]

Options
- **-clean** Remove all diagnose entries. (Admin only)
- **-date=<date>** YYYY-MM-DD. Only show entries from this date and forward.
- **-flush** Flush all diagnose entries to disk. (Admin only)
- **-onlyhigh** Only show entries with severity high. (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.
2.2.18. dhcprelay

Show DHCP/BOOTP relayer ruleset.

**Description**

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

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

**Usage**

dhcprelay

Show the currently relayed DHCP sessions.

dhcprelay -show [-rules] [-routes] [<display filter>]...

Show DHCP/BOOTP relayer ruleset.

dhcprelay -release <ip address> [-interface=<Interface>]

Terminate relayed session.

**Options**

- `interface=<Interface>` Interface.
- `release` Terminate relayed session <[interface:]ip>. (Admin only)
- `routes` Show the currently relayed DHCP sessions.
- `rules` Show the DHCP/BOOTP relayer ruleset.
- `show` Show ruleset.
- `<display filter>` Display filter, filters relays based on interface/ip.
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] [-num=<Integer>] [-fromentry=<Integer>] [-mappings] [<display filter>]...
```

Show DHCP server ruleset.

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

Release a specific types of IPs.

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

Release an active IP.

**Options**

- `-fromentry=<Integer>`
  - Shows dhcp server lease list from offset `<n>`.
- `-leases`
  - Show DHCP server leases.
- `-mappings`
  - Show DHCP server IP mappings.
- `-num=<Integer>`
  - Limit list to `<n>` leases.
- `-release={BLACKLIST}`
  - Release specific type of IPs. (Admin only)
- `-releaseip`
  - Release an active IP. (Admin only)
- `-rules`
  - Show DHCP server rules.
- `-show`
  - Show ruleset.
- `<display filter>`
  - Display filters for leases based on interface/mac/ip (eg. if1 192.168.*).
- `<interface>`
  - Interface.
- `<ip address>`
  - IP address.
### 2.2.20. dns

DNS client and queries.

**Description**

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

**Usage**

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

**Options**

- **-list**  
  List pending DNS queries.
- **-query=<domain name>**  
  Resolve domain name.
- **-remove**  
  Remove all pending DNS queries.

### 2.2.21. dnsbl

DNSBL.

**Description**

Show status of DNSBL.

**Usage**

```bash
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**
-done List done (lingering) reassemblies.
-free List free instead of active.
-num=<n> List <n> entries. (Default: 20)
{NEW | ALL | <reassembly id>} 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

-activate Go active.
-deactivate Go inactive.

2.2.25. hostmon

Show Host Monitor statistics.

Description

Show active Host Monitor sessions.

Usage

hostmon [-verbose] [-num=<n>]

Options

-num=<n> Limit list to <n> entries. (Default: 20)
-verbose Verbose output.
2.2.26. httpalg

Commands related to the HTTP Application Layer Gateway.

Description

Show information about the WCF cache or list the overridden WCF hosts.

Usage

httpalg -override [-flush]

List or flush hosts that have overridden the wcf filter.


Display URL cache information.

Options

- count
  Only display cache count.
- flush
  Removes all entries.
- num=<n>
  Limit list to <n> entries. (Default: 20)
- override
  List hosts that have overridden the wcf filter.
- server={STATUS | CONNECT | DISCONNECT]
  Web Content Filtering Server options. (Default: status)
- show
  Show Web Content Filtering cache data.
- url=<String>
  Limits the output from the show command to only match the specified characters.
- verbose
  Verbose.
- wcfcache
  Show statistics of WCF functionality.

2.2.27. httpposter

Display HTTP Poster status.

Description

Display configuration and status of configured HTTPPoster_URLx targets.

Usage

httpposter [-repost=<Integer>]
Options

-repost=<Integer> Re-post URL now. (Admin only)

2.2.28. hwm

Show hardware monitor sensor status.

Description
Show hardware monitor sensor status.

Usage

hwm [-all] [-verbose]

Options

-all Show ALL sensors, WARNING: use at own risk, may take long time for highspeed ifaces to cope.

-verbose Show sensor number, type and limits.

2.2.29. idppipes

Show and remove hosts that are piped by IDP.

Description
Show list of currently piped hosts.

Usage

idppipes -show [-host=<ip addr>]

Lists hosts for which new connections are piped by IDP.

idppipes -unpipe [-all] [-host=<ip addr>]

Remove piping for the specified host.

Options

-all mark all hosts.
**2.2.30. ifstat**

Show interface statistics.

**Description**

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

**Usage**

```
```

**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.

**2.2.31. 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**

- **-join**
  
  Simulate an incoming IGMP join message.

- **-leave**
  
  Simulate an incoming IGMP leave message.

- **-query**
  
  Simulate an incoming IGMP query message.

- **-state**
  
  Show the current IGMP state.

- `<host address>`
  
  Host IP address.

- `<Interface>`
  
  Interface.

- `<MC address>`
  
  Multicast Address.

- `<router address>`
  
  Router IP address.

**2.2.32. 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

- **-off** Turn IKE snooping off.
- **-on** Turn IKE snooping on.
- **-verbose** Enable IKE snooping with verbose output.
- **<ip address>** IP address to snoop.

### 2.2.33. 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] [-max=<n>]
```

Show IP pool information.

**Options**

- **-all** Free all IP addresses.
- **-max=<n>** Limit list to <n> entries. (Default: 10)
- **-release** Forcibly free IP assigned to subsystem. (Admin only)
- **-show** Show IP pool information.
- **-verbose** Verbose output.
- **<ip address>** IP address to free.

### 2.2.34. ipsecglobalstats

Show global ipsec statistics.

**Description**
List global IPsec statistics.

**Usage**

`ipsecglobalstats [-verbose]`

**Options**

- `-verbose` Show all statistics.

### 2.2.35. ipseckeepalive

Show status of the IPsec ping keepalives.

**Description**

Show status of the IPsec ping keepalives.

**Usage**

`ipseckeepalive [-num=<n>]`

**Options**

- `-num=<n>` Maximum number of entries to display (default: 48).

### 2.2.36. 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] [<tunnel>] [-ipsec] [-usage] [-verbose] [-num={ALL | <Integer>}] [-force]`

**Options**
2.2.37. ipsectunnels

Lists the current IPsec configuration.

**Description**

Lists the current IPsec configuration.

**Usage**

```bash
ipsectunnels -iface=<recv iface>
```

Show specific interface.

```bash
ipsectunnels -num={ALL | <Integer>} [-force]
```

Show specific number if interface.

```bash
ipsectunnels
```

Show interfaces.

**Options**

- **-force**
  Bypass confirmation question.

- **-iface=<recv iface>**
  IPsec interface to show information about.

- **-num={ALL | <Integer>}**
  Maximum number of entries to show (default: 40).

2.2.38. 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.
2.2.39. languagefiles

Manage language files on disk.

Description

Manage language files on disk

Usage

languagefiles

Show all language files on disk.

languagefiles -remove=<String>

Remove a language file from disk.

Options

-remove=<String> Specify language file to delete.

2.2.40. ldap

LDAP information.

Description
Status and statistics for the configured LDAP databases.

**Usage**

```bash
ldap
```
List all LDAP databases.

```bash
ldap -list
```
List all LDAP databases.

```bash
ldap -show [<LDAP Server>]
```
Show LDAP database status and statistics.

```bash
ldap -reset [<LDAP Server>]
```
Reset LDAP database.

**Options**

- `-list` List all LDAP databases.
- `-reset` Reset status for LDAP database.
- `-show` Show status and statistics.
- `<LDAP Server>` LDAP database.

---

### 2.2.41. license

Show contents of the license file.

**Description**

Show contents of the license file.

**Usage**

```bash
license
```

---

### 2.2.42. linkmon

Display link monitoring statistics.

**Description**

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

Logout user.

Usage

logout

2.2.44. memory

Show memory information.

Description

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

Usage

memory

2.2.45. natpool

Show current NAT Pools.

Description

Show current NAT Pools and in-depth information.

Usage

natpool [-verbose] [<pool name> [IP4 Address]] [-num=<Integer>]
Options

- **-num=<Integer>**  Maximum number of items to list (default: 20).
- **-verbose**  Verbose (more information).
- **<IP4 Address>**  Translated IP.
- **<pool name>**  NAT Pool name.

## 2.2.46. nd

Show Neighbor Discovery entries for given interface.

### Description

List the Neighbor Discovery cache entries of specified interfaces.

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

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

### Usage

```
nd
```

Show all Neighbor Discovery entries.

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

Show Neighbor Discovery entries.

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

Show information on hash table health.

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

Flush Neighbor Discovery cache of specified interface.

```
nd -query=<ip> <Interface>
```

Send Neighbor Solicitation for IP.

```
nd -del=<ip> <Interface>
```

Delete ND cache entry.

### Options

- **-del=<ip>**  Delete ND cache entry <ip>.
2.2.47. ndsnoop

Toggle snooping and displaying of ARP requests.

Description

Toggle snooping and displaying of Neighbor Discovery queries and responses on-screen.

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

Usage

ndsnoop

Show snooped interfaces.

ndsnoop {ALL | NONE | <interface>} [-verbose]

Snoop specified interface.

Options

-verbose

Verbose.

{ALL | NONE | <interface>}

Interface name.

2.2.48. netobjects

Show runtime values of network objects.

Description
Displays named network objects and their contents.

Example 2.10. List network objects which have names containing "net".

```
netobjects *net*
```

Usage

```
netobjects [<String>] [-num=<num>]
```

Options

```
-num=<num>  Number of entries to show. (Default: 20)
<String>  Name or pattern.
```

2.2.49. 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 routing table.
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**

- **-area**
  - Show area information.

- **-database**
  - Show the LSA database.

- **-execute={STOP | START | RESTART}**
  - Start/stop/restart OSPF process. (Admin only)

- **-iface**
  - Show interface information.

- **-ifacedown**
  - Take specified interface offline. (Admin only)

- **-ifaceup**
  - Take specified interface online. (Admin only)

- **-lsa**
  - Show details for a specified LSA <lsaID>.

- **-neighbor**
  - Show neighbor information.

- **-process=<OSPF Router Process>**
  - Required if there are >1 OSPF router processes.

- **-route**
  - Show the internal OSPF process routingtable.

- **-snoop={ON | OFF}**
  - Show troubleshooting messages on the console.

- **-verbose**
  - Increase amount of information to display.

- **<interface>**
  - OSPF enabled interface.

- **<interface>**
  - OSPF enabled interface.

- **<lsaID>**
  - LSA ID.

- **<OSPF Area>**
  - OSPF Area.

- **<OSPF Neighbor>**
  - Neighbor.
2.2.50. pcapdump

Packet capturing.

Description

Packet capture engine

Usage

pcapdump

Show capture status.

```
pcapdump -start [<interface(s)>] [-size=<value>] [-snaplen=<value>]
 [-count=<value>] [-out] [-out-nocap]
 [-eth=<Ethernet Address>] [-ethsrc=<Ethernet Address>]
 [-ethdest=<Ethernet Address>] [-ip=<IP4 Address>]
 [-ipsrc=<IP4 Address>] [-ipdest=<IP4 Address>]
 [-port=<0...65535>] [-sport=<0...65535>]
 [-dport=<0...65535>] [-sport=<0...255>] [-icmp] [-tcp]
 [-udp] [-promisc] [-ipversion=<1...15>]
```

Start capture.

pcapdump -stop [<interface(s)>]

Stop capture.

pcapdump -status

Show capture status.

pcapdump -show [<interface(s)>]

Show a captured packets brief.

pcapdump -write [<interface(s)>] [-filename=<String>]

Write the captured packets to disk.

pcapdump -wipe

Remove all captured packets from memory.

pcapdump -cleanup

Remove all captured packets, release capture mode and delete all written capture files from disk.

Options

- -cleanup Remove all captured packets, release capture mode
and delete all written capture files from disk.

-\texttt{-count=\langle\texttt{value}\rangle}\quad\text{Number of packets to capture.}
-\texttt{-destport=\langle0...65535\rangle}\quad\text{Destination TCP/UDP port filter.}
-\texttt{-eth=\langle\texttt{Ethernet Address}\rangle}\quad\text{Ethernet address filter.}
-\texttt{-ethdest=\langle\texttt{Ethernet Address}\rangle}\quad\text{Ethernet destination address filter.}
-\texttt{-ethsrc=\langle\texttt{Ethernet Address}\rangle}\quad\text{Ethernet source address filter.}
-\texttt{-filename=\langle\texttt{String}\rangle}\quad\text{Filename for capture file.}
-\texttt{-icmp}\quad\text{ICMP filter.}
-\texttt{-ip=\langle\texttt{IP4 Address}\rangle}\quad\text{IP address filter.}
-\texttt{-ipdest=\langle\texttt{IP4 Address}\rangle}\quad\text{Destination IP address filter.}
-\texttt{-ipsrc=\langle\texttt{IP4 Address}\rangle}\quad\text{Source IP address filter.}
-\texttt{-ipversion=\langle1...15\rangle}\quad\text{IP version filter.}
-\texttt{-out}\quad\text{Realtime packet brief dumped to console.}
-\texttt{-out-nocap}\quad\text{Unbuffered (not stored in memory) realtime packet brief dumped to console.}
-\texttt{-port=\langle0...65535\rangle}\quad\text{TCP/UDP port filter.}
-\texttt{-promisc}\quad\text{Set iface in promiscuous mode.}
-\texttt{-proto=\langle0...255\rangle}\quad\text{IP protocol filter.}
-\texttt{-show}\quad\text{Show a captured packets brief.}
-\texttt{-size=\langle\texttt{value}\rangle}\quad\text{Size (kb) of buffer to store captured packets in memory (default 512kb).}
-\texttt{-snaplen=\langle\texttt{value}\rangle}\quad\text{Maximum length of each packet to capture.}
-\texttt{-srcport=\langle0...65535\rangle}\quad\text{Source TCP/UDP port filter.}
-\texttt{-start}\quad\text{Start capture.}
-\texttt{-status}\quad\text{Show capture status.}
-\texttt{-stop}\quad\text{Stop capture.}
-\texttt{-tcp}\quad\text{TCP filter.}
-\texttt{-udp}\quad\text{UDP filter.}
-\texttt{-wipe}\quad\text{Remove all captured packets from memory.}
-\texttt{-write}\quad\text{Write the captured packets to disk.}
\texttt{<interface(s)>}\quad\text{Name of interface(s)}.

\textbf{Note}
\textit{Requires Administrator privilege.}
2.2.51. 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

-expr=<String>  Pipe wildcard(*) expression.
-show           Show pipe details.
-users          List users of a given pipe.
<Pipe>          Show pipe details.

2.2.52. pptpalg

Show PPTP ALG information.

Description
Shows information and statistics of the PPTP ALGs.

Usage

pptpalg
Show all configured PPTP ALGs.

pptpalg -sessions <PPTP ALG> [-verbose] [-num=<Integer>]
List all PPTP sessions.

```
pptpalg -services <PPTP ALG>
```

List all services attached to PPTP ALG.

**Options**

- `-num=<Integer>` Number of entries to list.
- `-services` List all services attached to PPTP ALG.
- `-sessions` List all session using a PPTP tunnel.
- `-verbose` Verbose output.
- `<PPTP ALG>` PPTP ALG.

### 2.2.53. reconfigure

Initiates a configuration re-read.

**Description**

Restart the Security Gateway using the currently active configuration.

**Usage**

```
reconfigure
```

*Note*

Requires Administrator privilege.

### 2.2.54. routemon

List the currently monitored interfaces and gateways.

**Description**

List the currently monitored interfaces and/or gateways.

**Usage**

```
routemon
```

### 2.2.55. 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

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

Show rules lists.

Description

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

Example 2.11. Show a range of rules

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

Usage

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

Options

- **-schedule**
  Filter out rules that are not currently allowed by selected schedules.

- **-type={IP | ROUTING | PIPE | IDP | THRESHOLD | IGMP}**
  Type of rules to display. (Default: IP)

- **-verbose**
  Verbose: show all parameters of the rules.

- **<rules>**
  Range of rules to display. (default: all rules).

2.2.57. selftest

Run appliance self tests.

Description

The appliance self tests are used to verify the correct function of hardware components.

Normal SGW operations might be disrupted during the test(s).

The outcome of the throughput crypto accelerator tests are dependent on configuration values. If the number of large buffers (LocalReassSettings->LocalReass_NumLarge) too low, it might lower throughput result. In the field 'Drop/Fail', the 'Drop' column contains the number of packets that were dropped before ever reaching the crypto accelerator and the 'Fail' column contains the number of packets that for some reason failed encryption. The 'Pkt In/Out' field shows the total number of packets sent to, and returned from the accelerator.

The interface tests 'traffic' and 'throughput' are dependent on the settings for the NIC ring sizes and possibly also license limitations. The 'traffic' test uses a uniform random distribution of six packet sizes between 60 and 1518 bytes. The content of each received packet is validated. The 'throughput' test uses only the largest packet size, and does not validate the contents of the received packets.
Example 2.12. Interface ping test between all interfaces

selftest -ping

Example 2.13. Interface ping test between interfaces 'if1' and 'if2'

selftest -ping -interfaces=if1,if2

Example 2.14. Start 30 min burn-in, testing RAM, storage media and crypto accelerator

selftest -burnin -minutes 30 -media -memory -cryptoaccel

Usage

selftest -memory [-num=<Integer>]
Check the sanity of the RAM.

selftest -media [-size=<Integer>]
Check the sanity of the disk drive.

selftest -mac
Check if there are MAC address collisions on the interfaces.

selftest -ping [-interfaces=<Interface>]
Run a ping test over the interfaces.

selftest -throughput [-interfaces=<Interface>]
Run a throughput test over the interfaces.

selftest -traffic [-interfaces=<Interface>]
Run a traffic test over the interfaces.

selftest -cryptoaccel
Verify the correct functioning of the accelerator cards.

selftest -burnin [-hours[=<Integer>]] [-minutes[=<Integer>]]
[-cryptoaccel]
Run burn-in tests for a set of sub tests. If no sub tests are specified the following are included:
memory, -ping, -traffic, -cryptoaccel.

**selftest -abort**

Abort a running self test.

**selftest**

Show the status of a running test.

## Options

- **-abort**
  Abort a running self test.

- **-burnin**
  Run burn-in tests for a selected set of sub tests.

- **-cryptoaccel**
  Verify the correct functioning of available crypto accelerator cards.

- **-hours[=<Integer>]**
  Test duration in hours. (Default: 48)

- **-interfaces=<Interface>**
  Ethernet interface(s).

- **-mac**
  Check if there are MAC address collisions on the interfaces.

- **-media**
  Check the sanity of the disk drive.

- **-memory**
  Check the sanity of the RAM.

- **-minutes[=<Integer>]**
  Test duration in minutes. (Default: 0)

- **-num=<Integer>**
  Number of times to execute the test. (Default: 1)

- **-ping**
  Run a ping test over the interfaces.

- **-size=<Integer>**
  Size of media space to utilize in the test. Set in MB. (Default: 1)

- **-throughput**
  Run a throughput test over the interfaces. This will show the maximal achievable interface throughput.

- **-traffic**
  Run a traffic test over the interfaces. The traffic test uses mixed frame sizes and verifies the content of each received frame.

**Note**

Requires Administrator privilege.

### 2.2.58. services

Show runtime values of configured services.

## Description

Shows the runtime values of all configured services.
Example 2.15. List all services which names begin with "http"

services http*

Usage

services [<String>]

Options

<String> Name or pattern.

2.2.59. 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(s).
sessionmanager -message <session name> <database> <message text>

Send message to session with console.

sessionmanager -disconnect <session name> <database> [<IP Address> [{LOCAL | SSH | HTTP | HTTPS}]]

Forcibly terminate session(s).

Options

- **-disconnect**
  Forcibly terminate session(s). (Admin only)

- **-info**
  Show in-depth information about session.

- **-list**
  List active sessions.

- **-message**
  Send message to session.

- **-num=<n>**
  List <n> number of session.

- **-status**
  Show Session Manager status.

- **<database>**
  Name of user database.

- **<IP Address>**
  IP address.

- **<message text>**
  Message to send.

- **<session name>**
  Name of session.

- **{LOCAL | SSH | HTTP | HTTPS}**
  Session type.

### 2.2.60. settings

Show settings.

**Description**

Show the contents of the settings section, category by category.

**Usage**

```text
settings
```

Show list of categories.

```text
settings <category>
```

Show settings in category.

**Options**
2.2.61. shutdown

Initiate core or system shutdown.

Description

Initiate restart of the core/system.

Usage

```
shutdown [<seconds>] [-normal] [-reboot]
```

Options

- **-normal**
  
  Initiate core shutdown.

- **-reboot**
  
  Initiate system reboot.

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

*Note*

Requires Administrator privilege.

2.2.62. sipalg

SIP ALG.

Description

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

The -flags option with -snoop allows any combination of the following values:

- 0x00000001 GENERAL
- 0x00000002 ERRORS
- 0x00000004 OPTIONS
- 0x00000008 PARSE
- 0x00000010 VALIDATE
- 0x00000020 SDP
- 0x00000040 ALLOW CHANGES
- 0x00000080 SUPPORTED_CHANGES
- 0x00000100 2543COMPLIANCE
- 0x00000200 RECEPTION
- 0x00000400 SESSION
- 0x00000800 REQUEST
- 0x00001000 RESPONSE
- 0x00002000 TOPO_CHANGES
- 0x00004000 MEDIA
- 0x00008000 CONTACT
- 0x00010000 CONN
- 0x00020000 PING
- 0x00040000 TRANSACTION
- 0x00080000 CALLLEG
- 0x00100000 REGISTRY

Flags can be added in the usual way. The default value is 0x00000003 (GENERAL and ERRORS).

NOTE: ‘verbose’ option outputs a lot of information on the console which may lead to system instability. Use with caution.

**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 | VERBOSE} [<ipaddr>] [-flags=<String>]

Control SIP snooping. Useful for troubleshooting SIP transactions. NOTE: 'verbose' option outputs a lot of information on the console which may lead to system instability. Use with caution.

Options

- **-calls**
  Show active calls table.

- **-connection**
  Show SIP connections.

- **-definition**
  Show running ALG configuration parameters.

- **-flags=<String>**
  SIP snooping for certain levels. Expected number in hexadecimal notation.

- **-registration[={SHOW | FLUSH}]**
  Show or flush registration table. (Default: show)

- **-session**
  Show active SIP sessions.

- **-snoop={ON | OFF | VERBOSEL**
  Enable or disable SIP snooping. NOTE: 'verbose' option outputs a lot of information on the console which may lead to system instability. Use with caution.

- **-statistics[={SHOW | FLUSH}]**
  Show or flush SIP counters. (Default: show)

- **<alg>**
  SIP-ALG name.

- **<ipaddr>**
  IP Address to snoop.

### 2.2.63. sshsserver

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 -restart <ssh server>
```
Restart SSH Server.

**Options**

- **-b=<bits>**
  Bitsize. (Default: 1024)

- **-keygen**
  Generate SSH Server private keys. This operation may take a long time to finish, up to several minutes!

- **-restart**
  Stop and start the SSH Server.

- **-status**
  Show server status and list all connected clients.

- **-t={RSA | DSA}**
  Type. (default: both RSA and DSA keys will be created).

- **-verbose**
  Verbose output.

- **<ssh server>**
  SSH Server.

*Note*
Requires Administrator privilege.

### 2.2.64. sslvpn

SSLVPN tunnels.

**Description**
List running SSLVPN configurations, SSLVPN active tunnels and call information.

**Usage**

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

**Options**

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

### 2.2.65. stats

Display various general firewall statistics.

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

System messages.

**Description**

Show contents of the FWLoader sysmsg buffer.

**Usage**

```
stats
```

2.2.67. techsupport

Technical Support information.

**Description**

Generate information useful for technical support.

Due to the large amount of output, this command might show a truncated result when execute from the local console.

**Usage**

```
techsupport
```

2.2.68. 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**

- **-force**  
  Force synchronization regardless of the MaxAdjust setting.

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

- **-sync**  
  Synchronize time with timeserver(s) (specified in settings).

- **<date>**  
  Date YYYY-MM-DD.

- **<time>**  
  Time HH:MM:SS.

### 2.2.69. uarules

Show user authentication rules.

**Description**

Displays the contents of the user authentication ruleset.

**Example 2.16. Show a range of rules**

uarules -v 1-2,4-5

**Usage**

uarules [-verbose] [<Integer Range>]

**Options**

- **-verbose**  
  Verbose output.

- **<Integer Range>**  
  Range of rules to list.
2.2.70. updatecenter

Show autoupdate status and manage IDP/AV databases.

Description

Show autoupdate mechanism status or force an update.

Usage

updatecenter -update[={ANTIVIRUS | IDP | ALL}]

Initiate an update check of the specified database.

updatecenter -removedb={ANTIVIRUS | IDP}

Remove the specified signature database.

updatecenter -status[={ANTIVIRUS | IDP | ALL}]

Show update status and database information.

updatecenter -servers

Show status of update servers.

Options

-removedb={ANTIVIRUS | IDP} Remove the database for the specified service.
-servers Show status of update servers.
-status[={ANTIVIRUS | IDP | ALL}] Show update status and database information. (Admin only; Default: all)
-update[={ANTIVIRUS | IDP | ALL}] Force an update now for the specified service. (Admin only; Default: all)

2.2.71. 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

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

2.2.72. vlan

Show information about VLAN.

Description

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

Usage

vlan

List attached VLANs.

vlan -num[=<n>] [-page[=<n>]]

Set number of display lines per page and display page.

vlan <Interface>
Display VLANs connected to physical iface <iface>.

**Options**

- **-num[=<n>]** Limit display lines to <n> entries in page. (Default: 20)
- **-page[=<n>]** Set page <n> for lines to display. (Default: 1)
- **<Interface>** Display VLAN information about this interface.

### 2.2.73. vpnstats

Alias for ipsecstats.

#### 2.2.74. 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**

- **-blockenet=<ethernet address>** Block the specified ethernet address.
- **-blockip=<ip address>** Block the specified IP address/net.
- **-eraseenet=<ethernet address>** Unblock the specified ethernet address.
- **-eraseip=<ip address>** Unblock the specified IP address/net.
- **-save** Save the current zonedefense state on all switches.
- **-show** Show the current block database.
- **-status** 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=<2...8192>]
[-port=<0...65535>] [-udp] [-tcp] [-tos=<0...255>] [-verbose]
```

Options

- `-count=<1...10>`
  Number of packets to send. (Default: 1)
- `-length=<2...8192>`
  Packet size. (Default: 4)
- `-pbr=<table>`
  Route using PBR Table.
- `-port=<0...65535>`
  Destination port of UDP or TCP ping.
- `-recvif=<interface>`
  Pass packet through the rule set, simulating that the packet was received by `<recvif>`.
- `-srcip=<ip address>`
  Use this source IP.
- `-tcp`
  Send TCP ping.
- `-tos=<0...255>`
  Type of service.
- `-udp`
  Send UDP ping.
- `-verbose`
  Verbose (more information).
- `<host>`
  IP address of host to ping.
2.4. Misc

2.4.1. echo

Print text.

**Description**

Print text to the console.

**Example 2.17. Hello World**

```bash
echo Hello World
```

**Usage**

```
echo [<String>]...
```

**Options**

* `<String>` Text to print.*

2.4.2. 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>
```
2.4.3. history

Dump history to screen.

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

Usage

history

2.4.4. ls

Lists device data accessible by SCP.

Description
Lists device data which are available through SCP.

Example 2.18. Transfer script files to and from the device

Upload:    scp myscript user@sgw-ip:script/myscript
Download:  scp user@sgw-ip:script/myscript ./myscript

In addition to the files listed it is possible to upload license, certificates and ssh public key files.

Example 2.19. Upload license data

scp licence.lic user@sgw-ip:license.lic

Certificates and ssh client key objects are created if they do not exist.
Example 2.20. Upload certificate data

scp certificate.cer user@sgw-ip:certificate/certificate_name
scp certificate.key user@sgw-ip:certificate/certificate_name

Example 2.21. Upload ssh public key data

scp sshkey.pub user@sgw-ip:sshclientkey/sshclientkey_name

Usage

Options

-long
Enable long listing format.

<File>
File to list.

2.4.5. script

Handle CLI scripts.

Description

Run, create, show, store or delete script files.

Script files are transferred to and from the device by the SCP protocol. On the device they are stored in the "/script" folder.

Example 2.22. Execute script

"script.sgs":
add IP4Address Name=$1 Address=$2 Comment="$0: \$100"
is executed as line:
add IP4Address Name=ip_test Address=127.0.0.1 Comment="script.sgs: $100"

Usage

script -create [[<Category>] <Type> [<Identifier>]] [-name=<Name>]
Create configuration script from specified object, class or category.

script -execute [-verbose] [-force] [-quiet] -name=<Name> [<Parameters>]...
2.4.5. script

Execute script.

```
script -show [-all] [-name=<Name>]
```

Show script in console window.

```
script -store [-all] [-name=<Name>]
```

Store a script to persistent storage.

```
script -remove [-all] [-name=<Name>]
```

Remove script.

```
script
```

List script files.

**Options**

- `-all`  
  Apply to all scripts.

- `-create`  
  Create configuration script from specified object, class or category.

- `-execute`  
  Execute script.

- `-force`  
  Force script execution.

- `-name=<Name>`  
  Name of script.

- `-quiet`  
  Quiet script execution.

- `-remove`  
  Remove script.

- `-show`  
  Show script in console window.

- `-store`  
  Store a script to persistent storage.

- `-verbose`  
  Verbose mode.

- `<Category>`  
  Category that groups object types.

- `<Identifier>`  
  The property that identifies the configuration object. May not be applicable depending on the specified `<Type>`.

- `<Parameters>`  
  List of input arguments.

- `<Type>`  
  Type of configuration object to perform operation on.

**Note**

Requires Administrator privilege.
Chapter 3. Configuration Reference

• Access, page 85
• Address, page 87
• AdvancedScheduleProfile, page 91
• ALG, page 92
• ARPND, page 100
• BlacklistWhiteHost, page 101
• Certificate, page 102
• Client, page 103
• COMPortDevice, page 106
• ConfigModePool, page 107
• DateTime, page 108
• Device, page 109
• DHCPRelay, page 110
• DHCPServer, page 111
• DNS, page 113
• Driver, page 114
• DynamicRoutingRule, page 117
• EthernetDevice, page 120
• HighAvailability, page 121
• HTTPALGBanners, page 122
• HTTPAuthBanners, page 123
• HTTPPoster, page 124
• HWM, page 125
• IDList, page 126
• IDPRule, page 127
• IGMPRule, page 129
• IGMPSetting, page 131
• IKEAlgorithms, page 132
• Interface, page 133
• IPPool, page 144
• IPRule, page 145
3.1. Access
Description

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

Properties

**Index**
- The index of the object, starting at 1. (Identifier)

**Name**
- Specifies a symbolic name for the object.

**Action**
- Accept, Expect or Drop. (Default: Drop)

**Interface**
- The interface the packet must arrive on for this rule to be carried out. Exception: the Expect rule.

**Network**
- The IP span that the sender must belong to for this rule to be carried out.

**LogEnabled**
- Enable logging. (Default: Yes)

**LogSeverity**
- 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

Name
Specifies a symbolic name for the network object. (Identifier)

Comments
Text describing the current object. (Optional)

3.2.1.1. IP6Address

Description

Use an IP6 Address item to define a name for a specific IP6 host, network or range.

Properties

Name
Specifies a symbolic name for the network object. (Identifier)

Address
IPv6 address, e.g. "1:2:3::4", "1234:5678:9abc:def0:1234:5678:9abc:def0", "1:2::/32" or "1:2::10-1:2::20".

Comments
Text describing the current object. (Optional)

3.2.1.2. IP6Group

Description

An IP6 Address Group is used for combining several IP6 Address objects for simplified management.

Properties

Name
Specifies a symbolic name for the network object. (Identifier)

Members
Group members.

Comments
Text describing the current object. (Optional)
3.2.1.3. EthernetAddress

**Description**

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

**Properties**

- **Name**
  - Specifies a symbolic name for the network object. (Identifier)

- **Address**
  - Ethernet MAC address, e.g. "12-34-56-78-ab-cd".

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

3.2.1.4. EthernetAddressGroup

**Description**

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

**Properties**

- **Name**
  - Specifies a symbolic name for the network object. (Identifier)

- **Members**
  - Group members.

- **Comments**
  - 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**

- **Name**
  - Specifies a symbolic name for the network object. (Identifier)

- **Address**
  - An IP address with one instance for each node in the high availability cluster.

- **UserAuthGroups**
  - 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)
NoDefinedCredentials
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)

Comments
Text describing the current object. (Optional)

3.2.1.6. IP4Group

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

Properties

Name
Specifies a symbolic name for the network object. (Identifier)

Members
Group members.

UserAuthGroups
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)

NoDefinedCredentials
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)

Comments
Text describing the current object. (Optional)

3.2.1.7. IP4Address

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

Properties

Name
Specifies a symbolic name for the network object. (Identifier)

Address
IP address, e.g. "172.16.50.8", "192.168.7.0/24" or "172.16.25.10-172.16.25.50".

ActiveAddress
The dynamically set address used by e.g. DHCP enabled Ethernet interfaces. (Optional)

UserAuthGroups
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.
3.2.2. EthernetAddress

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

3.2.3. EthernetAddressGroup

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

3.2.4. IP4Address

The definitions here are the same as in Section 3.2.1.7, “IP4Address”.

3.2.5. IP4Group

The definitions here are the same as in Section 3.2.1.6, “IP4Group”.

3.2.6. IP4HAAddress

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

3.2.7. IP6Address

The definitions here are the same as in Section 3.2.1.1, “IP6Address”.

3.2.8. IP6Group

The definitions here are the same as in Section 3.2.1.2, “IP6Group”.

NoDefinedCredentials

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)

Comments

Text describing the current object. (Optional)
3.3. AdvancedScheduleProfile

Description

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the service. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.3.1. AdvancedScheduleOccurrence

Description

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

Properties

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

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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the ALG. (Identifier)</td>
</tr>
<tr>
<td>AllowServerPassive</td>
<td>Allow server to use passive mode (unsafe for server). (Default: No)</td>
</tr>
<tr>
<td>ServerPorts</td>
<td>Server data ports. (Default: 1024-65535)</td>
</tr>
<tr>
<td>AllowClientActive</td>
<td>Allow client to use active mode (unsafe for client). (Default: No)</td>
</tr>
<tr>
<td>ClientPorts</td>
<td>Client data ports. (Default: 1024-65535)</td>
</tr>
<tr>
<td>AllowUnknownCommands</td>
<td>Allow unknown commands. (Default: No)</td>
</tr>
<tr>
<td>AllowSITEEXEC</td>
<td>Allow SITE EXEC. (Default: No)</td>
</tr>
<tr>
<td>MaxLineLength</td>
<td>Maximum line length in control channel. (Default: 256)</td>
</tr>
<tr>
<td>MaxCommandRate</td>
<td>Maximum number of commands per second. (Default: 20)</td>
</tr>
<tr>
<td>Allow8BitStrings</td>
<td>Allow 8-bit strings in control channel. (Default: Yes)</td>
</tr>
<tr>
<td>AllowResumeTransfer</td>
<td>Allow RESUME even in case of content scanning. (Default: No)</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Disabled, Audit or Protect. (Default: Disabled)</td>
</tr>
<tr>
<td>ScanExclude</td>
<td>List of files to exclude from antivirus scanning. (Optional)</td>
</tr>
<tr>
<td>CompressionRatio</td>
<td>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)</td>
</tr>
<tr>
<td>CompressionRatioAction</td>
<td>The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)</td>
</tr>
<tr>
<td>AllowEncryptedZip</td>
<td>Allow encrypted zip files, even though the contents can not be scanned. (Default: No)</td>
</tr>
<tr>
<td>ZDEnabled</td>
<td>Enable ZoneDefense Block. (Default: No)</td>
</tr>
<tr>
<td>ZDNetwork</td>
<td>Hosts within this network will be blocked at switches if a virus is found.</td>
</tr>
</tbody>
</table>
### 3.4.2. ALG_H323

**Description**

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

**Properties**

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

### 3.4.3. ALG_HTTP

**Description**

Use an HTTP Application Layer Gateway to filter HTTP traffic.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the ALG. (Identifier)</td>
</tr>
<tr>
<td>RemoveCookies</td>
<td>Remove cookies. (Default: No)</td>
</tr>
<tr>
<td>RemoveScripts</td>
<td>Remove Javascript/VBScript. (Default: No)</td>
</tr>
<tr>
<td>RemoveApplets</td>
<td>Remove Java applets. (Default: No)</td>
</tr>
<tr>
<td>RemoveActiveX</td>
<td>Remove ActiveX objects (including Flash). (Default: No)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>VerifyUTF8URL</td>
<td>Verify that URLs do not contain invalid UTF8 encoding. (Default: No)</td>
</tr>
<tr>
<td>BlackURLDisplayReason</td>
<td>Message to show when there is an attempt to access a blacklisted site. (Optional)</td>
</tr>
<tr>
<td>HTTPBanners</td>
<td>HTTP ALG HTML Banners. (Default: Default)</td>
</tr>
<tr>
<td>MaxDownloadSize</td>
<td>The maximal allowed file size in kB. (Optional)</td>
</tr>
<tr>
<td>FileListType</td>
<td>Specifies if the file list contains files to allow or deny. (Default: Block)</td>
</tr>
<tr>
<td>FailModeBehavior</td>
<td>Standard behaviour on error: Allow or Deny. (Default: Deny)</td>
</tr>
<tr>
<td>File</td>
<td>List of file types to allow or deny. (Optional)</td>
</tr>
<tr>
<td>VerifyContentMimetype</td>
<td>Verify that file extentions correspond to the MIME type. (Default: No)</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Disabled, Audit or Protect. (Default: Disabled)</td>
</tr>
<tr>
<td>ScanExclude</td>
<td>List of files to exclude from antivirus scanning. (Optional)</td>
</tr>
<tr>
<td>CompressionRatio</td>
<td>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)</td>
</tr>
<tr>
<td>CompressionRatioAction</td>
<td>The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)</td>
</tr>
<tr>
<td>AllowEncryptedZip</td>
<td>Allow encrypted zip files, even though the contents can not be scanned. (Default: No)</td>
</tr>
<tr>
<td>ZDEnabled</td>
<td>Enable ZoneDefense Block. (Default: No)</td>
</tr>
<tr>
<td>ZDNetwork</td>
<td>Hosts within this network will be blocked at switches if a virus is found.</td>
</tr>
<tr>
<td>WebContentFilteringMode</td>
<td>Disabled, Audit or Enable. (Default: Disabled)</td>
</tr>
<tr>
<td>FilteringCategories</td>
<td>Web content categories to block. (Optional)</td>
</tr>
<tr>
<td>NonManagedAction</td>
<td>Action to take for content that hasn't been classified. (Default: Allow)</td>
</tr>
<tr>
<td>AllowFilteringOverride</td>
<td>Allow the user to display a blocked site. (Default: No)</td>
</tr>
<tr>
<td>OverrideUpdateOnAccess</td>
<td>Restart the override timer on each new access to disallowed categories. (Default: Yes)</td>
</tr>
<tr>
<td>OverrideTimeToLive</td>
<td>Seconds that all disallowed categories will be allowed for the host that requested the override. (Default: 300)</td>
</tr>
<tr>
<td>AllowFilteringReclassification</td>
<td>Allow reclassification of sites. (Default: No)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
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

Action
Whitelist or Blacklist. (Default: Blacklist)

URL
Specifies the URL to blacklist or whitelist.

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.

3.4.4. ALG_POP3

Description

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

Properties

Name
Specifies a symbolic name for the ALG. (Identifier)

BlockUserPass
Block clients from sending USER and PASS command. (Default: No)

HideUser
Prevent server from revealing that a user name does not exist. (Default: No)

AllowUnknownCommands
Allow unknown commands. (Default: No)

FileListType
Specifies if the file list contains files to allow or deny. (Default: Block)

FailModeBehavior
Standard behaviour on error: Allow or Deny. (Default: Deny)

File
List of file types to allow or deny. (Optional)

VerifyContentMimetype
Verify that file extensions correspond to the MIME type. (Default: No)

Antivirus
Disabled, Audit or Protect. (Default: Disabled)

ScanExclude
List of files to exclude from antivirus scanning. (Optional)

CompressionRatio
A compression ratio higher than this value will trig-
ger the action in Compression Ratio Action, a value of zero will disable all compression checks. (Default: 20)

**CompressionRatioAction**
The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)

**AllowEncryptedZip**
Allow encrypted zip files, even though the contents can not be scanned. (Default: No)

**ZDEnabled**
Enable ZoneDefense Block. (Default: No)

**ZDNetwork**
Hosts within this network will be blocked at switches if a virus is found.

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

### 3.4.5. ALG_PPTP

**Description**
Use a PPTP Application Layer Gateway to manage PPTP traffic through the system.

**Properties**

- **Name**
  Specifies a symbolic name for the ALG. (Identifier)

- **EchoTimeout**
  Specifies idle timeout for Echo messages in the PPTP tunnel. (Default: 0)

- **IdleTimeout**
  Specifies idle timeout for user traffic in the PPTP tunnel. (Default: 0)

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

### 3.4.6. ALG_SIP

**Description**
Use a SIP ALG to manage SIP based multimedia sessions.

**Properties**

- **Name**
  Specifies a symbolic name for the ALG. (Identifier)

- **MaxSessionsPerId**
  Maximum number of sessions per SIP URI. (Default: 5)

- **MaxRegistrationTime**
  The maximum allowed time in seconds between registration requests. (Default: 3600)

- **SipSignalTmout**
  Timeout value for last seen SIP message (in seconds). (Default: 43200)

- **DataChannelTmout**
  Timeout value for data channel (in seconds).
AllowMediaByPass | Allow clients to exchange media directly when possible. (Default: Yes)
---|---
AllowTCPDataChannels | Allow TCP data channels. (Default: Yes)
MaxTCPDataChannels | Maximum number of TCP data channels per call. (Default: 5)
Comments | Text describing the current object. (Optional)

### 3.4.7. ALG_SMTP

#### Description

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

#### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the ALG. (Identifier)</td>
</tr>
<tr>
<td>VerifySenderEmail</td>
<td>Check emails for mismatching SMTP command From address and email header From address. (Default: No)</td>
</tr>
<tr>
<td>VerifySenderEmailAction</td>
<td>...and block them. (Default: Deny)</td>
</tr>
<tr>
<td>VerifySenderEmailSpamTag</td>
<td>Spam Tag that is inserted into the subject. (Default: &quot;*** SPAM ***&quot;)</td>
</tr>
<tr>
<td>VerifySenderEmailDomainOnly</td>
<td>Only check domain names in email From addresses. (Default: No)</td>
</tr>
<tr>
<td>MaxEmailPerMinute</td>
<td>Specifies the maximum amount of emails per minute from the same host. (Optional)</td>
</tr>
<tr>
<td>MaxEmailSize</td>
<td>Specifies the maximum allowed email size in kB. (Optional)</td>
</tr>
<tr>
<td>FileListType</td>
<td>Specifies if the file list contains files to allow or deny. (Default: Block)</td>
</tr>
<tr>
<td>FailModeBehavior</td>
<td>Standard behaviour on error: Allow or Deny. (Default: Deny)</td>
</tr>
<tr>
<td>File</td>
<td>List of file types to allow or deny. (Optional)</td>
</tr>
<tr>
<td>VerifyContentMimetype</td>
<td>Verify that file extensions correspond to the MIME type. (Default: No)</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Disabled, Audit or Protect. (Default: Disabled)</td>
</tr>
<tr>
<td>ScanExclude</td>
<td>List of files to exclude from antivirus scanning. (Optional)</td>
</tr>
<tr>
<td>CompressionRatio</td>
<td>A compression ratio higher than this value will trigger the action in Compression Ratio Action, a value of zero will disable all compression checks.</td>
</tr>
</tbody>
</table>
CompressionRatioAction
The action to take when high compression threshold is violated, all actions are logged. (Default: Drop)

AllowEncryptedZip
Allow encrypted zip files, even though the contents can not be scanned. (Default: No)

ZDEnabled
Enable ZoneDefense Block. (Default: No)

ZDNetwork
Hosts within this network will be blocked at switches if a virus is found.

DNSBL
Disable or Enable DNSBL. (Default: No)

SpamThreshold
Spam Threshold defines when an email should be considered as Spam. (Default: 10)

DropThreshold
Drop Threshold defines when an email should be considered malicious and be dropped. (Default: 20)

SpamTag
Spam Tag that is inserted into the subject for an email considered as Spam or malicious. (Default: "*** SPAM ***")

ForwardBlockedMail
Forward blocked mails to DropAddress. (Default: No)

DropAddress
Email address that emails reaching the drop threshold will be rerouted to.

AppendTXT
Use TXT records (will only be used if reaching the drop threshold). (Default: No)

CacheSize
Size of the IP Cache of checked sender IP addresses. (Default: 0)

CacheTimeout
Timeout in seconds before a cached IP address is removed. (Default: 600)

DNSBlackLists
Specifies the BlackList domain and its weighted value.

Comments
Text describing the current object. (Optional)

3.4.7.1. ALG_SMTP_Email

Description
Used to whitelist or blacklist an email sender/recipient.

Properties

Type
Specifies if the email address is the sender or the recipient. (Default: Sender)

Action
Specifies whether to whitelist (allow) or blacklist (deny) this address. (Default: Blacklist)
3.4.8. ALG_TFTP

Description

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

Properties

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

3.4.9. ALG_TLS

Description

TLS Alg

Properties

Name  Specifies a symbolic name for the ALG. (Identifier)
HostCert  Specifies the host certificate.
RootCert  Specifies the root certificate. (Optional)
Comments  Text describing the current object. (Optional)
3.5. ARPND

Description

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

Properties

- **Mode**: Static, Publish or XPublish. (Default: Publish)
- **Interface**: Indicates the interface to which the ARP entry applies; e.g. the interface the address shall be published on.
- **IP**: The IP address to be published or statically bound to a hardware address.
- **MACAddress**: The hardware address associated with the IP address. (Default: 00-00-00-00-00-00)
- **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.*
3.6. BlacklistWhiteHost

**Description**

Hosts and networks added to this whitelist can never be blacklisted by IDP or Threshold Rules.

**Properties**

- **Addresses**: Specifies the addresses that will be whitelisted.
- **Service**: Specifies the service that will be whitelisted.
- **Schedule**: The schedule when the whitelist should be active. (Optional)
- **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.*
### 3.7. Certificate

#### Description

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

#### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the certificate. (Identifier)</td>
</tr>
<tr>
<td>Type</td>
<td>Local, Remote or Request.</td>
</tr>
<tr>
<td>CertificateData</td>
<td>Certificate data.</td>
</tr>
<tr>
<td>PrivateKey</td>
<td>Private key.</td>
</tr>
<tr>
<td>NoCRLs</td>
<td>Disable CRLs (Certificate Revocation Lists). (Default: No)</td>
</tr>
<tr>
<td>PKAType</td>
<td>Encryption algorithm of the public key. (Default: Unknown)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*

3.8.2. DynDnsClientDLink

Description

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSName</td>
<td>The DNS name excluding the .dlinkddns.com suffix.</td>
</tr>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*

3.8.3. DynDnsClientDLinkChina

Description

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

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSName</td>
<td>The DNS name excluding the .dyndns.org suffix.</td>
</tr>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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.

3.8.5. DynDnsClientDynsCx

Description
Configure the parameters used to connect to the dyns.cx DynDNS service.

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSName</td>
<td>The DNS name excluding the .dyns.cx suffix.</td>
</tr>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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.
**3.8.6. DynDnsClientPeanutHull**

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSNames</td>
<td>Specifies the DNS names separated by &quot;;&quot;.</td>
</tr>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Username.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the specified username. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port. (Identifier)</td>
</tr>
<tr>
<td>BitsPerSecond</td>
<td>Bits per second. (Default: 9600)</td>
</tr>
<tr>
<td>DataBits</td>
<td>Data bits. (Default: 8)</td>
</tr>
<tr>
<td>Parity</td>
<td>Parity. (Default: None)</td>
</tr>
<tr>
<td>StopBits</td>
<td>Stop bits. (Default: 1)</td>
</tr>
<tr>
<td>FlowControl</td>
<td>Flow control. (Default: None)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
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

IPPoolType  Specifies whether a predefined IP Pool or a static set of IP addresses should be used as IP address source.

IPPool  Specifies the IP pool to use for assigning IP addresses to VPN clients.

IPPoolAddress  Specifies the set of IP addresses to use for assigning IP addresses to VPN clients.

IPPoolNetmask  Specifies the netmask to assign to VPN clients.

DNS  Specifies the IP address of a DNS server that a VPN client should be able to connect to. (Optional)

NBNSIP  Specifies the IP address of a NBNS/WINS server that a VPN client should be able to connect to. (Optional)

DHCP  Specifies the IP address of a DHCP that a VPN client should be able to connect to. (Optional)

Subnets  Specifies additional subnets behind this gateway. (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.
3.11. DateTime

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

Properties

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

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.
3.12. Device

Description
Global parameters for this device.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the device. (Default: Device)</td>
</tr>
<tr>
<td>LocalCfgVersion</td>
<td>Local version number of the configuration. (Default: 1)</td>
</tr>
<tr>
<td>ConfigUser</td>
<td>Name of the user who committed the current configuration. (Default: BaseConfiguration)</td>
</tr>
<tr>
<td>ConfigSession</td>
<td>Session type used when the current configuration was committed. (Default: BaseConfiguration)</td>
</tr>
<tr>
<td>ConfigIP</td>
<td>IP address of the user who committed the current configuration. (Optional)</td>
</tr>
<tr>
<td>ConfigDate</td>
<td>Date when the current configuration was committed. (Optional)</td>
</tr>
<tr>
<td>HWModel</td>
<td>System hardware model. (Default: SOFTWARE)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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

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

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

Index

The index of the object, starting at 1. (Identifier)

Name

Specifies a symbolic name for the DHCP Server rule. (Identifier)

Interface

The source interface to listen for DHCP requests on. This can be a single interface or a group of interfaces.

RelayerFilter

A range, group or network that will allow specific DHCP Relayers access to the DHCP Server. (Default: 0/0)

IPAddressPool

A range, group or network that the DHCP Server will use as IP address pool to give out DHCP leases from.

Netmask

Netmask sent to the DHCP Client.

DefaultGateway

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)

Domain

Domain name used for DNS resolution. (Optional)

LeaseTime

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)

DNS1

IP of the primary DNS server. (Optional)

DNS2

IP of the secondary DNS server. (Optional)

NBNS1

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)

NBNS2

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)

NextServer

IP address of next server in the boot process. (Optional)

LogEnabled

Enable logging. (Default: Yes)
LogSeverity
Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)

Comments
Text describing the current object. (Optional)

3.14.1. DHCPServerPoolStaticHost

Description
Static DHCP Server host entry

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP Address of the host.</td>
</tr>
<tr>
<td>StaticHostType</td>
<td>Identifier for host. (Default: MACAddress)</td>
</tr>
<tr>
<td>MACAddress</td>
<td>The hardware address of the host.</td>
</tr>
<tr>
<td>ClientIdentType</td>
<td>Type of client identifier specified. (Default: Ascii)</td>
</tr>
<tr>
<td>ClientIdent</td>
<td>The client identifier for the host.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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. DHCPServerCustomOption

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

Properties

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

Description

Configure the DNS (Domain Name System) client settings.

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNSServer1</td>
<td>IP of the primary DNS Server. (Optional)</td>
</tr>
<tr>
<td>DNSServer2</td>
<td>IP of the secondary DNS Server. (Optional)</td>
</tr>
<tr>
<td>DNSServer3</td>
<td>IP of the tertiary DNS Server. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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. E1000EthernetPCIDriver

**Description**
Intel (E1000) Gigabit Ethernet Adaptor.

**Properties**

- **RxRingsize**
  Rx ringsize. (Default: 64)
- **TxRingsize**
  Rx ringsize. (Default: 256)
- **EnableMonitoring**
  Enable monitoring. (Default: No)
- **BelowCPULoad**
  Below CPU load. (Default: 80)
- **BelowInterfaceLoad**
  Below interface load. (Default: 70)
- **MinInterval**
  Minimum interval. (Default: 30)
- **RxErrorPercentage**
  Rx error percentage. (Default: 20)
- **TxErrorPercentage**
  Tx error percentage. (Default: 7)
- **ErrorTime**
  Error time. (Default: 10)
- **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. ixgbeEthernetPCIDriver

**Description**
Intel (IXGBE) 10 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. IXP4NPEEthernetDriver

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.

3.16.4. 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.

3.16.5. 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.

3.16.6. R8169EthernetPCIDriver
Description
RealTek (8169, 8110) 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.
3.17. 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

Index

The index of the object, starting at 1. (Identifier)

Name

Specifies a symbolic name for the rule. (Optional)

From

OSPF or Routing table. (Default: OSPF)

OSPFProcess

Specifies from which OSPF process the route should be imported from into either a routing table or another OSPF process.

RoutingTable

Specifies from which routing table a route should be imported into the OSPF AS or copied into another routing table.

DestinationInterface

The interface that the policy has to match. (Optional)

DestinationNetworkExactly

Specifies if the route needs to match a specific network exactly. (Optional)

DestinationNetworkIn

Specifies if the route just needs to be within a specific network. (Optional)

NextHop

The next hop (router) on the route that this policy has to match. (Optional)

MetricRange

Specifies an interval that the metric of the routes needs to be within. (Optional)

RouterID

Specifies if the policy should filter on router ID. (Optional)

OSPFRouteType

Specifies if the policy should filter on OSPF router type. (Optional)

OSPFTagRange

Specifies an interval that the tag of the routers need to be within. (Optional)

LogEnabled

Enable logging. (Default: Yes)

LogSeverity

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.
3.17.1. DynamicRoutingRuleExportOSPF

Description

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

Properties

ExportToProcess Specifies to which OSPF Process the route change should be exported.

SetTag Specifies a tag for this route. This tag can be used in other routers for filtering. (Optional)

SetRouteType The external route type. (Optional)

OffsetMetric Increases the metric of the imported route by this value. (Optional)

LimitMetricRange 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)

SetForward IP to route over. (Optional)

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.

3.17.2. DynamicRoutingRuleAddRoute

Description

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

Properties

Destination Specifies to which routing table the route changes to the OSPF Process should be exported.

OverrideStatic Allow override of static routes. (Default: No)

OverwriteDefault Allow overwrite of default route. (Default: No)

OffsetMetric Increases the metric by this value. (Optional)

OffsetMetricType2 Increases the for Type2 routers metric by this value. (Optional)
### 3.17.2. DynamicRoutingRuleAddRoute

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LimitMetricRange</td>
<td>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)</td>
</tr>
<tr>
<td>ProxyARPAllInterfaces</td>
<td>Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)</td>
</tr>
<tr>
<td>ProxyARPInterfaces</td>
<td>Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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

Name
Specifies a symbolic name for the device. (Identifier)

EthernetDriver
The Ethernet PCI driver that should be used by the interface.

PCIBus
PCI bus number where the Ethernet adapter is installed.

PCISlot
PCI slot number used by the Ethernet adapter.

PCIPort
Some Ethernet adapters have multiple ports that share the same bus and slot number. This parameter specifies what port to be used.

Media
Specifies if the link speed should be auto-negotiated or locked to a static speed. (Default: Auto)

Duplex
Specifies if the duplex should be auto-negotiated or locked to full or half duplex. (Default: Auto)

MACAddress
The hardware address for the interface. (Optional)

Comments
Text describing the current object. (Optional)
3.19. HighAvailability

Description

Configure the High Availability cluster parameters for this system.

Properties

**Enabled**
Enable high availability. (Default: No)

**ClusterID**
A (locally) unique cluster ID to use in identifying this group of HA security gateways. (Default: 0)

**SyncIface**
Specifies the interface used for state synchronization.

**NodeID**
Master or Slave. (Default: Master)

**HASyncBufSize**
How much sync data, in KB, to buffer while waiting for acknowledgments from the cluster peer. (Default: 1024)

**HASyncMaxPktBurst**
The maximum number of state sync packets to send in a burst. (Default: 20)

**HAInitialSilence**
The number of seconds to stay silent on startup or after reconfiguration. (Default: 5)

**UseUniqueSharedMac**
Use a unique shared mac address for each interface. (Default: Yes)

**HADeactivateBeforeReconf**
Deactivate(hand over) before Reconfiguration if Active. (Default: Yes)

**ReconfFailoverTime**
Number of non-responsive seconds before failover at HA reconf (0=immediate failover). (Default: 0)

**HAFailoverTime**
Number of milliseconds before failover when active HA node becomes non-responsive. (Default: 750)

*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. HTTPALGBanners

Description
HTTP banner files specifies the look and feel of HTTP ALG restriction web pages.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the HTTP Banner Files. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompressionForbidden</td>
<td>HTML for the CompressionForbidden.html web page.</td>
</tr>
<tr>
<td>ContentForbidden</td>
<td>HTML for the ContentForbidden.html web page.</td>
</tr>
<tr>
<td>URLForbidden</td>
<td>HTML for the URLForbidden.html web page.</td>
</tr>
<tr>
<td>RestrictedSiteNotice</td>
<td>HTML for the RestrictedSiteNotice.html web page.</td>
</tr>
<tr>
<td>ReclassifyURL</td>
<td>HTML for the ReclassifyURL.html web page.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.21. HTTPAuthBanners

Description
HTTP banner files specify the look and feel of HTML authentication web pages.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the HTTP Banner Files. (Identifier)</td>
</tr>
<tr>
<td>FormLogin</td>
<td>HTML for the FormLogin.html web page.</td>
</tr>
<tr>
<td>LoginSuccess</td>
<td>HTML for the LoginSuccess.html web page.</td>
</tr>
<tr>
<td>LoginFailure</td>
<td>HTML for the LoginFailure.html web page.</td>
</tr>
<tr>
<td>LoginAlreadyDone</td>
<td>HTML for the LoginAlreadyDone.html web page.</td>
</tr>
<tr>
<td>LoginChallenge</td>
<td>HTML for the LoginChallenge.html web page.</td>
</tr>
<tr>
<td>LoginChallengeTimeout</td>
<td>HTML for the LoginChallenge.html Timeout web page.</td>
</tr>
<tr>
<td>LogoutSuccess</td>
<td>HTML for the LogoutSuccess.html web page.</td>
</tr>
<tr>
<td>LogoutSuccessBasicAuth</td>
<td>HTML for the LogoutSuccessBasicAuth.html web page.</td>
</tr>
<tr>
<td>LogoutFailure</td>
<td>HTML for the LogoutFailure.html web page.</td>
</tr>
<tr>
<td>FileNotFound</td>
<td>HTML for the FileNotFound.html web page.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.22. HTTPPoster

**Description**

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

**Properties**

- **URL**
  - The URL that will be posted when the security gateway is loaded.

- **RepostDelay**
  - Delay in seconds until the URL is refetched. (Default: 1200)

- **AlwaysRepost**
  - Repost on each reconfiguration. (Default: No)

- **PostValues**
  - HTTP POST the values. (Default: No)

- **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.*
3.23. HWM

Description

Hardware Monitoring allows monitoring of hardware sensors.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the object.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Type of monitoring.</td>
</tr>
<tr>
<td>Sensor</td>
<td>Sensor index.</td>
</tr>
<tr>
<td>MinLimit</td>
<td>Lower limit. (Optional)</td>
</tr>
<tr>
<td>MaxLimit</td>
<td>Upper limit. (Optional)</td>
</tr>
<tr>
<td>EnableMonitoring</td>
<td>Enable/disable monitoring. (Default: No)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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. IDList

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the ID list. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.24.1. 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the object. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>IP, DNS, E-Mail or Distinguished name.</td>
</tr>
<tr>
<td>IP</td>
<td>IP address.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Host name.</td>
</tr>
<tr>
<td>CommonName</td>
<td>Common name of the owner of the certificate. (Optional)</td>
</tr>
<tr>
<td>OrganizationName</td>
<td>Organization name of the owner of the certificate. (Optional)</td>
</tr>
<tr>
<td>OrganizationalUnit</td>
<td>Organizational unit of the owner of the certificate. (Optional)</td>
</tr>
<tr>
<td>Country</td>
<td>Specifies the country. (Optional)</td>
</tr>
<tr>
<td>LocalityName</td>
<td>Locality. (Optional)</td>
</tr>
<tr>
<td>EMailAddress</td>
<td>E-mail address. (Optional)</td>
</tr>
<tr>
<td>DN Tuples</td>
<td>Enter the most common DN types above, or as a comma seperated list of types below. E.g. 'SN=12345, S=Smith' for serial number and surname. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.25. IDPRule

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the rule. (Optional)</td>
</tr>
<tr>
<td>SourceInterface</td>
<td>Specifies the name of the receiving interface to be compared to the received packet.</td>
</tr>
<tr>
<td>SourceNetwork</td>
<td>Specifies the sender span of IP addresses to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationInterface</td>
<td>Specifies the the destination interface to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationNetwork</td>
<td>Specifies the span of IP addresses to be compared to the destination IP of the received packet.</td>
</tr>
<tr>
<td>Service</td>
<td>Specifies a service that will be used as a filter parameter when matching traffic with this rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)</td>
</tr>
<tr>
<td>InsertionEvasion</td>
<td>Protect against insertion/evastion attacks. (Default: Yes)</td>
</tr>
<tr>
<td>URIIllegalUTF8</td>
<td>Specifies what action to take if invalid UTF-8 characters are seen in a HTTP URI. (Default: Log)</td>
</tr>
<tr>
<td>URIIllegalHex</td>
<td>Specifies what action to take when invalid hexencoding (%xx) is seen in a HTTP URI. (Default: DropLog)</td>
</tr>
<tr>
<td>URIDoubleEncode</td>
<td>Specifies what action to take when seeing double encoded characters in a HTTP URI. (Default: Ignore)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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.

3.25.1. 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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Specifies what action to take if the given signature is found. (Default: Audit)</td>
</tr>
<tr>
<td>Signatures</td>
<td>Specifies what signature(s) to search for in the network traffic. (Optional)</td>
</tr>
<tr>
<td>ZoneDefense</td>
<td>Activate ZoneDefense. (Default: No)</td>
</tr>
<tr>
<td>BlackList</td>
<td>Activate BlackList. (Default: No)</td>
</tr>
<tr>
<td>BlackListTimeToBlock</td>
<td>The number of seconds that the dynamic black list should remain. (Optional)</td>
</tr>
<tr>
<td>BlackListBlockOnlyService</td>
<td>Only block the service that triggered the blacklisting. (Default: No)</td>
</tr>
<tr>
<td>BlackListIgnoreEstablished</td>
<td>Do not drop existing connection. (Default: No)</td>
</tr>
<tr>
<td>PipeLimit</td>
<td>Specifies the bandwidth limit in kbps for hosts triggered by this action.</td>
</tr>
<tr>
<td>PipeNetwork</td>
<td>Traffic shaping will only apply to hosts that are within this network. (Default: 0/0)</td>
</tr>
<tr>
<td>PipeNewConnections</td>
<td>Enable piping of new connections from and to the same host. (Default: No)</td>
</tr>
<tr>
<td>PipeTimeWindow</td>
<td>Throttling of new connections to and from the triggering host will stop after the configured amount of time. (Default: 10)</td>
</tr>
<tr>
<td>LogEnabled</td>
<td>Enable logging. (Default: Yes)</td>
</tr>
<tr>
<td>LogSeverity</td>
<td>Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*
### 3.26. IGMPRule

**Description**

An IGMP rule specifies how to handle inbound IGMP reports and outbound IGMP queries.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Index</strong></td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>Specifies a symbolic name for the rule. (Optional)</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The type of IGMP messages the rule applies to. (Default: Report)</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Drop, Snoop, Proxy or PIM. (Default: Drop)</td>
</tr>
<tr>
<td><strong>SourceInterface</strong></td>
<td>Specifies the name of the receiving interface to be compared to the received packet.</td>
</tr>
<tr>
<td><strong>SourceNetwork</strong></td>
<td>Specifies the sender span of IP addresses to be compared to the received packet.</td>
</tr>
<tr>
<td><strong>DestinationInterface</strong></td>
<td>Specifies the destination interface to be compared to the received packet. (Default: core)</td>
</tr>
<tr>
<td><strong>MulticastGroup</strong></td>
<td>Specifies the multicast group to be compared to the received packet.</td>
</tr>
<tr>
<td><strong>MulticastSource</strong></td>
<td>Specifies the multicast source to be compared to the received packet.</td>
</tr>
<tr>
<td><strong>RelayInterface</strong></td>
<td>Specifies the interface via which to relay IGMP messages.</td>
</tr>
<tr>
<td><strong>TranslateMGroup</strong></td>
<td>Translate the multicast group for packets matching this rule. (Default: No)</td>
</tr>
<tr>
<td><strong>GrpAllToOne</strong></td>
<td>Rewrite all multicast groups to a single IP. (Default: No)</td>
</tr>
<tr>
<td><strong>NewGrpIP</strong></td>
<td>Translate the multicast group to this address.</td>
</tr>
<tr>
<td><strong>TranslateMSource</strong></td>
<td>Translate the multicast source for packets matching this rule. (Default: No)</td>
</tr>
<tr>
<td><strong>SrcAllToOne</strong></td>
<td>Rewrite all multicast sources to a single IP. (Default: No)</td>
</tr>
<tr>
<td><strong>NewSrcIP</strong></td>
<td>Translate the multicast source to this address.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>Pass IGMP data not matching this rule to the next rule. (Default: Yes)</td>
</tr>
<tr>
<td><strong>LogEnabled</strong></td>
<td>Enable logging. (Default: Yes)</td>
</tr>
<tr>
<td><strong>LogSeverity</strong></td>
<td>Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)</td>
</tr>
<tr>
<td><strong>Comments</strong></td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
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. IGMPSetting

Description
IGMP parameters can be tuned for one, or a group of interfaces in order to match the characteristics of a network.

Properties

Name
Specifies a symbolic name for the object. (Identifier)

Interface
The interfaces that these settings should apply to.

RobustnessVariable
IGMP is robust to (Robustness Variable - 1) packet losses. (Default: 2)

MaxRequestsPerSecond
Maximum number of IGMP requests to process each second and interface. (Default: 100)

RouterVersion
Multiple IGMP querying routers on a network must use the same IGMP version. (Default: IGMPv3)

LowestCompatibleVersion
The lowest IGMP version to allow on incoming requests. (Default: IGMPv1)

QueryInterval
The interval between general queries sent by the security gateway. (Default: 125000)

QueryResponseInterval
The maximum time until a host (client) has to send an answer to a query. (Default: 10000)

LastMemberQueryInterval
The maximum time until a host (client) has to send an answer to a group and group-and-source specific query. (Default: 10000)

LastMemberQueryCount
The number of group and group-and-source specific queries sent until the security gateway decides there are no more subscribers to a specific multicast group. (Default: 2)

StartupQueryInterval
The general query interval to use during the startup phase. (Default: 30000)

StartupQueryCount
The number of startup queries to send during the startup phase. (Default: 2)

UnsolicitedReportInterval
The time between repetitions of a host’s initial membership reports to a group. (Default: 1000)

ReactToOwnQueries
Should the system respond to Member Report Queries originating from itself. (Default: No)

Comments
Text describing the current object. (Optional)
3.28. IKEAlgorithms

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

Properties

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

This is a category that groups the following object types.

3.29.1. DefaultInterface

Description

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the interface. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.29.2. Ethernet

Description

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the interface. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>Network</td>
<td>The network of the interface.</td>
</tr>
<tr>
<td>DefaultGateway</td>
<td>The default gateway of the interface. (Optional)</td>
</tr>
<tr>
<td>Broadcast</td>
<td>The broadcast address of the connected network. (Optional)</td>
</tr>
<tr>
<td>EnableIPv6</td>
<td>Enable processing of IPv6 traffic on this interface. (Default: No)</td>
</tr>
<tr>
<td>IPv6IP</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>IPv6Network</td>
<td>The network of the interface.</td>
</tr>
<tr>
<td>IPv6DefaultGateway</td>
<td>The default gateway of the interface. (Optional)</td>
</tr>
<tr>
<td>PrivateIP</td>
<td>The private IP address of this high availability node. (Optional)</td>
</tr>
<tr>
<td>NOCHB</td>
<td>This will disable sending Cluster Heartbeats from this interface (used by HA to detect if a node is online and working). (Optional)</td>
</tr>
<tr>
<td>MTU</td>
<td>Specifies the size (in bytes) of the largest packet that</td>
</tr>
</tbody>
</table>
3.29.3. GRETunnel

Description

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the interface. (Identifier)</td>
</tr>
<tr>
<td>IP</td>
<td>Specifies the IP address of the GRE interface.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network address of the GRE interface.</td>
</tr>
<tr>
<td>RemoteEndpoint</td>
<td>Specifies the IP address of the remote endpoint.</td>
</tr>
<tr>
<td>EncapsulationChecksum</td>
<td>Add an extra level of checksum above the one provided by the IPv4 layer. (Default: No)</td>
</tr>
</tbody>
</table>
### OriginatorIPType
Specifies what IP address to use as source IP in e.g. NAT. (Default: LocalInterface)

### OriginatorIP
Manually specified originator IP address to use as source IP in e.g. NAT.

### Metric
Specifies the metric for the auto-created route. (Default: 90)

### AutoInterfaceNetworkRoute
Automatically add a route for this interface using the given remote network. (Default: Yes)

### UseSessionKey
Specify whether or not to use a session key. (Default: No)

### SessionKey
Session key. (Default: 0)

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

### 3.29.4. InterfaceGroup

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the interface. (Identifier)</td>
</tr>
<tr>
<td>Equivalent</td>
<td>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)</td>
</tr>
<tr>
<td>Members</td>
<td>Specifies the interfaces that are included in the interface group.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

### 3.29.5. IPsecTunnel

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the interface. (Identifier)</td>
</tr>
</tbody>
</table>
LocalNetwork
The network on "this side" of the IPsec tunnel. The IPsec tunnel will be established between this network and the remote network.

RemoteNetwork
The network connected to the remote gateway. The IPsec tunnel will be established between the local network and this network.

RemoteEndpoint
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)

IKEConfigModePool
Selects IKE Config Mode Pool to use for the tunnel. (Optional)

IKEAlgorithms
Specifies the IKE Proposal list used with the tunnel.

IPsecAlgorithms
Specifies the IPsec Proposal list used with the tunnel.

IKELifeTimeSeconds
The lifetime of the IKE connection in seconds. Whenever it expires, a new phase-1 exchange will be performed. (Default: 28800)

IPsecLifeTimeSeconds
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)

IPsecLifeTimeKilobytes
The lifetime of the IPsec connection in kilobytes. (Default: 0)

EncapsulationMode
Specifies if the IPsec tunnel should use Tunnel or Transport mode. (Default: Tunnel)

AuthMethod
Certificate or Pre-shared key.

PSK
Selects the Pre-shared key to use with this IPsec Tunnel.

LocalIDType
Selects the type of Local ID to use. (Default: Auto)

LocalIDValue
Specify the local identity of the tunnel ID.

GatewayCertificate
Selects the certificate the security gateway uses to authenticate itself to the other IPsec peer.

RootCertificates
Selects one or more root certificates to use with this IPsec Tunnel.

IDList
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)

XAuth
Off, Required for inbound or Pass to peer gateway. (Default: Off)

XAuthUsername
Specifies the username to pass to the remote gateway via IKE XAuth.

XAuthPassword
Specifies the password to pass to the remote gateway via IKE XAuth.
DHCPOverIPsec  
Allow DHCP over IPsec from single-host clients.  
(Default: No)

AddRouteToRemoteNet  
Dynamically add route to the remote networks when a tunnel is established.  
(Default: No)

PlaintextMTU  
Specifies the size in bytes at which to fragment plaintext packets (rather than fragmenting IPsec).  
(Default: 1420)

OriginatorIPType  
Specifies what IP address to use as source IP in e.g. NAT.  
(Default: LocalInterface)

OriginatorIP  
Manually specified originator IP address to use as source IP in e.g. NAT.

OriginatorHAIP  
Manually specified private originator IP address for use in HA.  
(Optional)

IKEMode  
Specifies which IKE mode to use: main or aggressive.  
(Default: Main)

DHGroup  
Specifies the Diffie-Hellman group to use when doing key exchanges in IKE.  
(Default: 2)

PFS  
Specifies whether PFS should be used or not.  
(Default: None)

PFSDHGroup  
Specifies which Diffie-Hellman group to use with PFS.  
(Default: 2)

SetupSAPer  
Setup security association per network, host or port.  
(Default: Net)

DeadPeerDetection  
Enable Dead Peer Detection.  
(Default: Yes)

NATTraversal  
Enable or disable NAT traversal.  
(Default: OnIfNeeded)

KeepAlive  
Disabled, Auto or Manual.  
(Default: Disabled)

KeepAliveSourceIP  
Source IP address used when sending keep-alive ICMP pings.

KeepAliveDestinationIP  
Destination IP address used when sending keep-alive ICMP pings.

Metric  
Specifies the metric for the auto-created route.  
(Default: 90)

AutoInterfaceNetworkRoute  
Automatically add a route for this interface using the given remote network.  
(Default: Yes)

LocalGateway  
Specifies on which local address this tunnel should accept incoming IKE/IPsec traffic.  
(Optional)

Comments  
Text describing the current object.  
(Optional)

3.29.6. 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**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the interface. (Identifier)</td>
</tr>
<tr>
<td>IP</td>
<td>The host name to store the assigned IP address in, if this network object exists and have a value other then 0.0.0.0 the PPTP/L2TP client will try to get that one from the PPTP/L2TP server as preferred IP. (Optional)</td>
</tr>
<tr>
<td>Network</td>
<td>The network from which traffic should be routed into the tunnel.</td>
</tr>
<tr>
<td>RemoteEndpoint</td>
<td>The IP address of the L2TP/PPTP server.</td>
</tr>
<tr>
<td>TunnelProtocol</td>
<td>Specifies if PPTP or L2TP should be used for this tunnel. (Default: PPTP)</td>
</tr>
<tr>
<td>OriginatorIPType</td>
<td>Specifies what IP address to use as source IP in e.g. NAT. (Default: LocalInterface)</td>
</tr>
<tr>
<td>OriginatorIP</td>
<td>Manually specified originator IP address to use as source IP in e.g. NAT.</td>
</tr>
<tr>
<td>DNS1</td>
<td>IP of the primary DNS server. (Optional)</td>
</tr>
<tr>
<td>DNS2</td>
<td>IP of the secondary DNS server. (Optional)</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the username to use for this PPTP/L2TP interface.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for this PPTP/L2TP interface.</td>
</tr>
<tr>
<td>PPPAuthNoAuth</td>
<td>Allow no authentication for this tunnel. (Default: No)</td>
</tr>
<tr>
<td>PPPAuthPAP</td>
<td>Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthCHAP</td>
<td>Use CHAP authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthMSCHAP</td>
<td>Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthMSCHAPv2</td>
<td>Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>MPPENone</td>
<td>Allow authentication without Microsoft Point-to-Point Encryption (MPPE). (Default: Yes)</td>
</tr>
<tr>
<td>MPPERC440</td>
<td>Use an RC4 40 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)</td>
</tr>
<tr>
<td>MPPERC456</td>
<td>Use an RC4 56 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)</td>
</tr>
</tbody>
</table>
MPPERC4128
Use an RC4 128 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)

DialOnDemand
Enable Dial-on-demand which means that the L2TP/PPTP tunnel will not be setup until traffic is sent on the interface. (Default: No)

ActivitySensing
Specifies if the dial-on-demand should trigger on inbound or outbound traffic or both. (Default: BiDirectional)

IdleTimeout
Idle timeout in seconds for dial-on-demand. (Default: 3600)

Metric
Specifies the metric for the auto-created route. (Default: 90)

MTU
Specifies the size (in bytes) of the largest packet that can be passed onward. (Default: 1456)

AutoInterfaceNetworkRoute
Automatically add a route for this interface using the given remote network. (Default: Yes)

MPPEAllowStateful
Allow usage of Stateful MPPE (less secure, use only for compatibility). (Default: No)

Comments
Text describing the current object. (Optional)

3.29.7. L2TPServer

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

Properties

Name
Specifies a symbolic name for the interface. (Identifier)

IP
The IP address of the PPTP/L2TP server interface.

TunnelProtocol
Specifies if PPTP or L2TP should be used for this tunnel. (Default: PPTP)

Interface
The interface that the PPTP/L2TP Server should be listening on.

ServerIP
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.

UseUserAuth
Enable the use of user authentication rules on this server. (Default: Yes)

MPPENone
Allow no authentication for this tunnel. (Default: Yes)
### MPPERC440
Use an RC4 40 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)

### MPPERC456
Use an RC4 56 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)

### MPPERC4128
Use an RC4 128 bit MPPE session key with MS-CHAP or MS-CHAP v2 authentication protocol. (Default: Yes)

### IPPool
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.

### DNS1
IP of the primary DNS server. (Optional)

### DNS2
IP of the secondary DNS server. (Optional)

### NBNS1
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)

### NBNS2
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)

### AllowedRoutes
Restricts networks for which routes may automatically be added. (Default: all-nets)

### MPPEAllowStateful
Allow usage of Stateful MPPE (less secure, use only for compatibility). (Default: No)

### ProxyARPAllInterfaces
Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)

### ProxyARPInterfaces
Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)

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

## 3.29.8. 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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the interface.</td>
</tr>
<tr>
<td></td>
<td>(Identifier)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EthernetInterface</td>
<td>The physical Ethernet interface that connects to the PPPoE server network.</td>
</tr>
<tr>
<td>IP</td>
<td>The host name to store the assigned IP address in.</td>
</tr>
<tr>
<td>Network</td>
<td>The network from which traffic should be routed into the tunnel.</td>
</tr>
<tr>
<td>DNS1</td>
<td>IP of the primary DNS server. (Optional)</td>
</tr>
<tr>
<td>DNS2</td>
<td>IP of the secondary DNS server. (Optional)</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the username to use for this PPPoE tunnel.</td>
</tr>
<tr>
<td>Password</td>
<td>The password to use for this PPPoE tunnel.</td>
</tr>
<tr>
<td>ServiceName</td>
<td>Specifies the PPPoE server service name used to distinguish between two or more PPPoE servers attached to the same network. (Optional)</td>
</tr>
<tr>
<td>PPPAuthNoAuth</td>
<td>Allow no authentication for this tunnel. (Default: No)</td>
</tr>
<tr>
<td>PPPAuthPAP</td>
<td>Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthCHAP</td>
<td>Use CHAP authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthMSCHAP</td>
<td>Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>PPPAuthMSCHAPv2</td>
<td>Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)</td>
</tr>
<tr>
<td>DialOnDemand</td>
<td>Enable Dial-on-demand which means that the PPPoE tunnel will not be setup until traffic is sent on the interface. (Default: No)</td>
</tr>
<tr>
<td>ActivitySensing</td>
<td>Specifies if the dial-on-demand should trigger on inbound or outbound traffic or both. (Default: BiDirectional)</td>
</tr>
<tr>
<td>IdleTimeout</td>
<td>Idle timeout in seconds for dial-on-demand. (Default: 3600)</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies the metric for the auto-created route. (Default: 90)</td>
</tr>
<tr>
<td>AutoInterfaceNetworkRoute</td>
<td>Automatically add a route for this interface using the given remote network. (Default: Yes)</td>
</tr>
<tr>
<td>Schedule</td>
<td>The schedule defines when the PPPoE tunnel should be active. (Optional)</td>
</tr>
<tr>
<td>ForceUnnumbered</td>
<td>Force the PPPoE tunnel to be unnumbered. (Default: No)</td>
</tr>
<tr>
<td>SpecifyManually</td>
<td>Make it possible to manually specify IP Address object. (Default: No)</td>
</tr>
<tr>
<td>MTU</td>
<td>Specifies the size (in bytes) of the largest packet that can be passed onward. (Default: 1492)</td>
</tr>
</tbody>
</table>
3.29.9. SSLVPNInterface

Description

An SSL VPN interface, together with the bundled client, creates an easy to use tunnel solution for roaming users.

Properties

Name
Specifies a symbolic name for the interface.
(Identifier)

OuterInterface
The physical interface that the SSL VPN interface will listen on.

ServerPort
The listening port for the SSL VPN interface.
(Default: 443)

ServerIP
Listening IP for the SSL VPN interface.

ServerFQDN
Optional. FQDN of the SSL VPN server given to clients, eg: (sslvpn.example.com). (Optional)

IPAddressPool
A range, group or network that will be the IP pool from which the SSL VPN clients will receive their IP addresses.

InnerIP
Local IP for the SSL VPN interface.

PrimaryDNS
IP of the primary DNS Server. (Optional)

SecondaryDNS
IP of the secondary DNS Server. (Optional)

ProxyARPAllInterfaces
Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)

ProxyARPInterfaces
Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)

Comments
Text describing the current object. (Optional)

3.29.10. VLAN

Description

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

Properties

Name
Specifies a symbolic name for the interface.
(Identifier)
Ethernet  Specifies on which Ethernet interface the virtual
LAN is defined.

VLANID  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 Eth-
ernet interface. (Default: 0)

IP  Specifies the IP address of the virtual LAN interface,
if other than the IP of the Ethernet interface.

Network  Specifies the network address of the virtual LAN in-
terface.

DefaultGateway  The default gateway of the virtual LAN interface.
(Optional)

Broadcast  Specifies the broadcast address of the virtual LAN
interface. (Optional)

EnableIPv6  Enable processing of IPv6 traffic on this interface.
(Default: No)

IPv6IP  Specifies the IP address of the virtual LAN interface.

IPv6Network  Specifies the network of the virtual LAN interface.

IPv6DefaultGateway  The default gateway of the virtual LAN interface.
(Optional)

PrivateIP  The private IP address of this high availability node.
(Optional)

Metric  Specifies the metric for the auto-created route.
(Default: 100)

AutoSwitchRoute  Enable transparent mode, which means that a switch
route is added automatically for this virtual LAN inter-
face. (Default: No)

AutoInterfaceNetworkRoute  Automatically add a route for this virtual LAN inter-
face using the given network. (Default: Yes)

AutoDefaultGatewayRoute  Automatically add a default route for this virtual
LAN interface using the given default gateway.
(Default: Yes)

PrioCopyPolicy  Set the QoS to VLAN priority copy policy. (Default: InheritFromPhys)

EnableRouterAdvertisement  Enable Router Advertisement for this interface.
(Default: No)

Comments  Text describing the current object. (Optional)
### 3.30. IPPool

**Description**

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the IP Pool. (Identifier)</td>
</tr>
<tr>
<td>DHCPServerType</td>
<td>Should server address be specified or should broadcast on a interface be used. (Default: Interface)</td>
</tr>
<tr>
<td>ServerIP</td>
<td>DHCP Server Address.</td>
</tr>
<tr>
<td>ServerFilter</td>
<td>Specifies which DHCP server that leases should be accepted from. (Optional)</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies the interface which has the DHCP server that leases are accepted from.</td>
</tr>
<tr>
<td>IPFilter</td>
<td>Specifies which IP addresses that are accepted from the DHCP server. (Optional)</td>
</tr>
<tr>
<td>ReceiveInterface</td>
<td>Which interface to use when communicating with the DHCP server. (Optional)</td>
</tr>
<tr>
<td>PrefetchLeases</td>
<td>Specifies the number of leases an IP Pool will keep prefetched. (Default: 3)</td>
</tr>
<tr>
<td>MaxFree</td>
<td>Maximum number of free address that the IP pool will keep, others will be returned back to DHCP server. (Optional)</td>
</tr>
<tr>
<td>MaxClients</td>
<td>Maximum number clients that the IP pool is allowed to contain. (Optional)</td>
</tr>
<tr>
<td>MacRangeStart</td>
<td>Specifies the lower boundary of MAC addresses that DHCP Clients will use in communication with a server. (Optional)</td>
</tr>
<tr>
<td>MacRangeEnd</td>
<td>Specifies the upper boundary of MAC addresses that DHCP Clients will use in communication with a server. (Optional)</td>
</tr>
<tr>
<td>SenderIP</td>
<td>The local IP that should be used when communication with the DHCP server. (Optional)</td>
</tr>
<tr>
<td>AscendingFreeList</td>
<td>Enabling this will result in the IPs being fetched in a predictable manner from the free list. (Default: No)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.31. IPRule

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the rule. (Optional)</td>
</tr>
<tr>
<td>Action</td>
<td>Reject, Drop, FwdFast, Allow, NAT, SAT or SLB_SAT.</td>
</tr>
<tr>
<td>SourceInterface</td>
<td>Specifies the name of the receiving interface to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationInterface</td>
<td>Specifies the destination interface to be compared to the received packet.</td>
</tr>
<tr>
<td>SourceNetwork</td>
<td>Specifies the sender span of IP addresses to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationNetwork</td>
<td>Specifies the span of IP addresses to be compared to the destination IP of the received packet.</td>
</tr>
<tr>
<td>Service</td>
<td>Specifies a service that will be used as a filter parameter when matching traffic with this rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)</td>
</tr>
<tr>
<td>NATAction</td>
<td>Specify sender address or Use interface address. (Default: UseInterfaceAddress)</td>
</tr>
<tr>
<td>NATSenderAddress</td>
<td>Specifies which sender address will be used.</td>
</tr>
<tr>
<td>NATPool</td>
<td>Specifies which sender address will be used.</td>
</tr>
<tr>
<td>SATTranslate</td>
<td>Specifies whether to translate source IP or destination IP. (Default: DestinationIP)</td>
</tr>
<tr>
<td>SATTranslateToIP</td>
<td>Translate to this IP address.</td>
</tr>
<tr>
<td>SATTranslateToPort</td>
<td>Translate to this port. (Optional)</td>
</tr>
<tr>
<td>SATAllToOne</td>
<td>Rewrite all destination IPs to a single IP. (Default: No)</td>
</tr>
<tr>
<td>SLBAAddresses</td>
<td>The IP addresses of the servers in the server farm.</td>
</tr>
<tr>
<td>SLBStickiness</td>
<td>Specifies stickiness mode. (Default: None)</td>
</tr>
<tr>
<td>SLBIdleTimeOut</td>
<td>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)</td>
</tr>
</tbody>
</table>
SLBMaxSlots
Specifies maximum number of slots for IP and network stickiness. (Default: 2048)

SLBNetSize
Specifies network size for network stickiness. (Default: 24)

SLBNewPort
Rewrite destination port to this port. (Optional)

SLBMonitorRoutingTable
Routing table used for server monitoring. (Default: main)

SLBMonitorPing
Enable monitoring using ICMP Ping packets. (Default: No)

SLBPingPollingInterval
Delay in milliseconds between each ping interval. (Default: 5000)

SLBPingSamples
Specifies the number of attempts to use for statistical calculations. (Default: 10)

SLBPingMaxPollFails
Specifies the maximum number of failed ping attempts until host is considered to be unreachable. (Default: 2)

SLBPingMaxAverageLatency
Specifies the max average latency for the sample attempts. (Default: 800)

SLBMonitorTCP
Enable monitoring using TCP handshakes. (Default: No)

SLBTCPPorts
Specifies the ports that will be monitored.

SLBTCPPollingInterval
Delay in milliseconds between each TCP handshake. (Default: 10000)

SLBTCPSamples
Specifies the number of attempts to use for statistical calculations. (Default: 10)

SLBTCPPMaxPollFails
Specifies the maximum number of failed TCP attempts until host is considered to be unreachable. (Default: 2)

SLBTCPPMaxAverageLatency
Specifies the max average latency for the sample attempts. (Default: 800)

SLBMonitorHTTP
Enable monitoring using HTTP requests. (Default: No)

SLBHTTPPorts
Specifies the ports that will be monitored. (Default: 80)

SLBHTTPPollingInterval
Delay in milliseconds between each monitor interval. (Default: 10000)

SLBHTTPSamples
Specifies the number of attempts to use for statistical calculations. (Default: 10)

SLBHTTPMaxPollFails
Specifies the maximum number of failed HTTP attempts until host is considered to be unreachable. (Default: 2)

SLBHTTPMaxAverageLatency
Specifies the max average latency for the sample attempts. (Default: 800)
SLBHTTPURLType
Defines how the request URL should be interpreted. (Default: FQDN)

SLBHTTPRequestURL
Specifies the HTTP URL to monitor.

SLBHTTPExpectedResponse
Expected HTTP response.

SLBDistribution
Specifies the algorithm used for the load distribution tasks. (Default: RoundRobin)

SLBWindowTime
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)

RequireIGMP
Multicast traffic must have been requested using IGMP before it is forwarded. (Default: Yes)

MultiplexArgument
Specifies how the traffic should be forwarded and translated.

MultiplexAllToOne
Rewrite all destination IPs to a single IP. (Default: No)

LogEnabled
Enable logging. (Default: Yes)

LogSeverity
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.
3.32. IPRuleFolder

Description

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies the name of the folder.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

*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.

3.32.1. IPRule

The definitions here are the same as in Section 3.31, “IPRule”.
# 3.33. IPsecAlgorithms

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the object. (Identifier)</td>
</tr>
<tr>
<td>NULLEnabled</td>
<td>Enable plaintext. (Default: No)</td>
</tr>
<tr>
<td>DESEnabled</td>
<td>Enable DES encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>DES3Enabled</td>
<td>Enable 3DES encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>AESEnabled</td>
<td>Enable AES encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>BlowfishEnabled</td>
<td>Enable Blowfish encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>TwofishEnabled</td>
<td>Enable Twofish encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>CAST128Enabled</td>
<td>Enable CAST128 encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>SDT2Enabled</td>
<td>Enable SDT2 encryption algorithm. (Default: No)</td>
</tr>
<tr>
<td>BlowfishMinKeySize</td>
<td>Specifies the minimum Blowfish key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>BlowfishKeySize</td>
<td>Specifies the Blowfish preferred key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>BlowfishMaxKeySize</td>
<td>Specifies the maximum Blowfish key size in bits. (Default: 448)</td>
</tr>
<tr>
<td>TwofishMinKeySize</td>
<td>Specifies the minimum Twofish key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>TwofishKeySize</td>
<td>Specifies the Twofish preferred key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>TwofishMaxKeySize</td>
<td>Specifies the maximum Twofish key size in bits. (Default: 256)</td>
</tr>
<tr>
<td>AESMinKeySize</td>
<td>Specifies the minimum AES key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>AESKeySize</td>
<td>Specifies the preferred AES key size in bits. (Default: 128)</td>
</tr>
<tr>
<td>AESMaxKeySize</td>
<td>Specifies the maximum AES key size in bits. (Default: 256)</td>
</tr>
<tr>
<td>MD5Enabled</td>
<td>Enable MD5 integrity algorithm. (Default: No)</td>
</tr>
<tr>
<td>SHA1Enabled</td>
<td>Enable SHA1 integrity algorithm. (Default: No)</td>
</tr>
<tr>
<td>XCBCEnabled</td>
<td>Enable XCBC-AES integrity algorithm. (Default: No)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
### 3.34. LDAPDatabase

**Description**

External LDAP server used to verify user names and passwords.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the server. (Identifier)</td>
</tr>
<tr>
<td>IP</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP port of the server. (Default: 389)</td>
</tr>
<tr>
<td>Timeout</td>
<td>The timeout, in milliseconds, used when processing requests. (Default: 5)</td>
</tr>
<tr>
<td>NameAttr</td>
<td>Specifies a name attribute in LDAP database. (Default: uid)</td>
</tr>
<tr>
<td>PassAttr</td>
<td>Specifies a password attribute in LDAP database. (Optional)</td>
</tr>
<tr>
<td>GroupsAttr</td>
<td>Specifies the group membership attribute used in the LDAP database. (Default: memberOf)</td>
</tr>
<tr>
<td>GetGroups</td>
<td>Retrieve group membership for users. (Default: Yes)</td>
</tr>
<tr>
<td>DomainName</td>
<td>The domain name of the server. (Optional)</td>
</tr>
<tr>
<td>BaseObject</td>
<td>Specifies a base object to search. (Optional)</td>
</tr>
<tr>
<td>UserName</td>
<td>Specifies a user name. (Optional)</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies a user password. (Optional)</td>
</tr>
<tr>
<td>Type</td>
<td>Add domain name to username. (Default: 0)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.35. LDAPServer

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Specifies the IP address or hostname of the LDAP server.</td>
</tr>
<tr>
<td>Username</td>
<td>Specifies the username to use when accessing the LDAP server. (Optional)</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password to use when accessing the LDAP server. (Optional)</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the LDAP service port number. (Default: 389)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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. LinkMonitor

**Description**

The Link Monitor allows the system to monitor one or more hosts and take action if they are unreachable.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Specifies what action the system should take.</td>
</tr>
<tr>
<td>Addresses</td>
<td>Specifies the addresses that should be monitored.</td>
</tr>
<tr>
<td>MaxLoss</td>
<td>A single host is considered unreachable if this number of consecutive ping responses to that host are not replied to. (Default: 7)</td>
</tr>
<tr>
<td>PingInterval</td>
<td>Milliseconds between each monitor attempt. (Default: 250)</td>
</tr>
<tr>
<td>InitGracePeriod</td>
<td>Do not allow triggering of the link monitor for this number of seconds after the last reconfiguration. (Default: 45)</td>
</tr>
<tr>
<td>UseSharedIP</td>
<td>Use the shared IP of an HA cluster instead of the private IP of the node. (Default: No)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*
3.37. LocalUserDatabase

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

**Properties**

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the object. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.37.1. 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**

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

This is a category that groups the following object types.

3.38.1. EventReceiverSNMP2c

Description

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

Properties

- **Name**: Specifies a symbolic name for the log receiver. (Identifier)
- **IPAddress**: Destination IP address.
- **Port**: Destination port. (Default: 162)
- **Community**: Community string. (Default: public)
- **RepeatCount**: Repetition counter. (Default: 0)
- **LogSeverity**: Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency, Alert, Critical, Error, Warning, Notice, Info)
- **Comments**: Text describing the current object. (Optional)

3.38.1.1. LogReceiverMessageException

Description

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

Properties

- **LogCategory**: The Category of the log message.
- **LogID**: The ID number of the log message, a empty value selects all messages of this category. (Optional)
- **LogType**: EXCLUDE or INCLUDE. (Default: EXCLUDE)
- **LogSeverity**: 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.
3.38.2. LogReceiverMemory

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the log receiver. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogSeverity</td>
<td>Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency, Alert, Critical, Error, Warning, Notice, Info)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.38.2.1. LogReceiverMessageException

The definitions here are the same as in Section 3.38.1.1, “LogReceiverMessageException”.

3.38.3. LogReceiverSMTP

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the log receiver. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>The IP address of the SMTP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the which port to use to connect to the SMTP server. (Default: 25)</td>
</tr>
<tr>
<td>Receiver1</td>
<td>The email address that the event information is sent to.</td>
</tr>
<tr>
<td>Receiver2</td>
<td>Alternate email receiver. (Optional)</td>
</tr>
<tr>
<td>Receiver3</td>
<td>Alternate email receiver. (Optional)</td>
</tr>
<tr>
<td>Sender</td>
<td>Specifies which sender the email will have. (Default: hostmaster)</td>
</tr>
<tr>
<td>Identity</td>
<td>Specifies which identity to write in the email header. (Default: hostmaster)</td>
</tr>
<tr>
<td>XMailer</td>
<td>Specifies the X-mailer information to write in the email header. (Optional)</td>
</tr>
<tr>
<td>Subject</td>
<td>Specifies the subject.</td>
</tr>
</tbody>
</table>
HoldTime

The hold time in seconds during which the log threshold must be reached for an email to be sent. (Default: 120)

MinRepeatDelay

The amount of seconds the security gateway will wait before sending another email. (Default: 600)

LogThreshold

The number of events that have to occur within the hold time for an email to be sent. (Default: 2)

Comments

Text describing the current object. (Optional)

3.38.4. LogReceiverSyslog

Description

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

Properties

Name

Specifies a symbolic name for the log receiver. (Identifier)

IPAddress

Specifies the IP address of the log receiver.

Port

Specifies the port number of the log service. (Default: 514)

Facility

Specifies what facility is used when logging. (Default: local0)

LogSeverity

Specifies with what severity log events will be sent to the specified log receivers. (Optional; Default: Emergency,Alert,Critical,Error,Warning,Notice,Info)

Comments

Text describing the current object. (Optional)

3.38.4.1. LogReceiverMessageException

The definitions here are the same as in Section 3.38.1.1, “LogReceiverMessageException”.
3.39. NATPool

Description

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

Properties

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

**Description**

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the OSPF process. (Identifier)</td>
</tr>
<tr>
<td>RouterID</td>
<td>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)</td>
</tr>
<tr>
<td>PrivRouterID</td>
<td>The private router ID of this high availability node. (Optional)</td>
</tr>
<tr>
<td>RFC1583</td>
<td>Enable this if the security gateway will be used in an environment that consists of routers that only support RFC 1583. (Default: No)</td>
</tr>
<tr>
<td>SPFHoldTime</td>
<td>Specifies the minimum time, in seconds, between two SPF calculations. (Default: 10)</td>
</tr>
<tr>
<td>SPFDelayTime</td>
<td>Specifies the delay time, in seconds, between when OSPF receives a topology change and when it starts a SPF calculation. (Default: 5)</td>
</tr>
<tr>
<td>LSAGroupPacing</td>
<td>This specifies the time in seconds at which interval the OSPF LSAs are collected into a group and refreshed. (Default: 10)</td>
</tr>
<tr>
<td>RoutesHoldtime</td>
<td>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)</td>
</tr>
<tr>
<td>RefBandwidthValue</td>
<td>Set the reference bandwidth that is used when calculating the default interface cost for routes. (Default: 1)</td>
</tr>
<tr>
<td>RefBandwidthUnit</td>
<td>Sets the reference bandwidth unit. (Default: Gbps)</td>
</tr>
<tr>
<td>MemoryMaxUsage</td>
<td>Maximum amount in bytes of RAM that the OSPF process is allowed to use. The default is one percent of installed RAM. Specifying 0 indicates that the OSPF process is allowed to use all available RAM. (Optional)</td>
</tr>
<tr>
<td>DebugPacket</td>
<td>Enables or disabled logging of general packet parsing events and also specifies the details of the log. (Default: Off)</td>
</tr>
<tr>
<td>DebugHello</td>
<td>Enables or disabled logging of hello packets and also specifies the details of the log. (Default: Off)</td>
</tr>
<tr>
<td>DebugDDesc</td>
<td>Enables or disabled logging of database description</td>
</tr>
</tbody>
</table>
packets and also specifies the details of the log. (Default: Off)

**DebugExchange**
Enables or disabled logging of exchange packets and also specifies the details of the log. (Default: Off)

**DebugLSA**
Enables or disabled logging of LSA events and also specifies the details of the log. (Default: Off)

**DebugSPF**
Enables or disabled logging of SPF calculation events and also specifies the details of the log. (Default: Off)

**DebugRoute**
Enables or disabled logging of routing table manipulation events and also specifies the details of the log. (Default: Off)

**AuthType**
Specifies the authentication type for the OSPF protocol exchanges. (Default: None)

**AuthPassphrase**
Specifies the passphrase used for authentication. (Optional)

**AuthMD5ID**
Specifies the MD5 key ID used for MD5 digest authentication.

**AuthMD5Key**
A 128-bit key used to produce the MD5 digest. (Optional)

**LogEnabled**
Enable logging. (Default: Yes)

**LogSeverity**
Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)

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

### 3.40.1. OSPFArea

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

#### Properties

**Name**
Specifies a symbolic name for the area. (Identifier)

**AreaID**
Specifies the area id, if 0.0.0.0 is specified this is the backbone area.

**Stub**
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)

**StubSummarize**
Become a default router for stub area (Summarize). (Default: Yes)

**StubMetric**
Route metric for stub area. (Optional)
FilterExternal
Specifies the network addresses allowed to be imported into this area from external routing sources. (Optional)

FilterInterArea
Specifies the network addresses allowed to be imported from other routers inside the area. (Optional)

Comments
Text describing the current object. (Optional)

3.40.1. OSPFInterface

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

Properties

Interface
Specifies which interface in the security gateway will be used for this OSPF interface. (Identifier)

Type
Auto, Broadcast, Point-to-point or Point-to-multipoint. (Default: Auto)

Network
Specifies the network related to the configured OSPF interface. (Optional)

MetricType
Metric value or Bandwidth. (Default: MetricValue)

Metric
Specifies the routing metric for this OSPF interface. (Default: 10)

BandwidthValue
Specifies the bandwidth for this OSPF interface.

BandwidthUnit
Specifies the bandwidth unit. (Default: Mbps)

UseDefaultAuth
Use the authentication configuration specified in the OSPF process. (Default: Yes)

AuthType
Specifies the authentication type for the OSPF protocol exchanges. (Default: None)

AuthPassphrase
Specifies the passphrase used for authentication. (Optional)

AuthMD5ID
Specifies the MD5 key ID used for MD5 digest authentication.

AuthMD5Key
A 128-bit key used to produce the MD5 digest. (Optional)

HelloInterval
Specifies the number of seconds between HELLO packets sent from the interface. (Default: 10)

RtrDeadInterval
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)

RxmtInterval
Specifies the number of seconds between retransmissions of LSAs to neighbors on this interface.
### RtrPrio
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)

### InfTransDelay
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)

### WaitInterval
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)

### Passive
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)

### IgnoreMTU
Enable to allow OSPF MTU mismatches. (Default: No)

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

### 3.40.1.2. OSPFNeighbor

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

**Properties**

- **Interface**
  Specifies the OSPF interface of the neighbor.

- **IPAddress**
  IP Address of the neighbor.

- **Metric**
  Specifies the metric of the neighbor. (Optional)

- **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.*

### 3.40.1.3. 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

<table>
<thead>
<tr>
<th>Network</th>
<th>The aggregate network used to combine several small routes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertise</td>
<td>Advertise the aggregate. (Default: Yes)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.

### 3.40.1.4. 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

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

**Description**

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

**Properties**

- **Name**: Specifies a symbolic name for the pipe. (Identifier)
- **LimitKbpsTotal**: Total bandwidth limit for this pipe in kilobits per second. (Optional)
- **LimitPPSTotal**: Total packet per second limit for this pipe. (Optional)
- **LimitKbps0**: Specifies the bandwidth limit in kbps for precedence 0 (the lowest precedence). (Optional)
- **LimitPPS0**: Specifies the packet per second limit for precedence 0 (the lowest precedence). (Optional)
- **LimitKbps1**: Specifies the bandwidth limit in kbps for precedence 1. (Optional)
- **LimitPPS1**: Specifies the packet per second limit for precedence 1. (Optional)
- **LimitKbps2**: Specifies the bandwidth limit in kbps for precedence 2. (Optional)
- **LimitPPS2**: Specifies the packet per second limit for precedence 2. (Optional)
- **LimitKbps3**: Specifies the bandwidth limit in kbps for precedence 3. (Optional)
- **LimitPPS3**: Specifies the packet per second limit for precedence 3. (Optional)
- **LimitKbps4**: Specifies the bandwidth limit in kbps for precedence 4. (Optional)
- **LimitPPS4**: Specifies the packet per second limit for precedence 4. (Optional)
- **LimitKbps5**: Specifies the bandwidth limit in kbps for precedence 5. (Optional)
- **LimitPPS5**: Specifies the packet per second limit for precedence 5. (Optional)
- **LimitKbps6**: Specifies the bandwidth limit in kbps for precedence 6. (Optional)
- **LimitPPS6**: Specifies the packet per second limit for precedence 6. (Optional)
- **LimitKbps7**: Specifies the bandwidth limit in kbps for precedence 7. (Optional)
LimitPPS7
Specifies the packet per second limit for precedence 7 (the highest precedence). (Optional)

UserLimitKbpsTotal
Total bandwidth limit per group in the pipe in kilobits per second. (Optional)

UserLimitPPSTotal
Total throughput limit per group in the pipe in packets per second. (Optional)

UserLimitKbps0
Specifies the bandwidth limit per group in kbps for precedence 0 (the lowest precedence). (Optional)

UserLimitPPS0
Specifies the throughput limit per group in PPS for precedence 0 (the lowest precedence). (Optional)

UserLimitKbps1
Specifies the bandwidth limit per group in kbps for precedence 1. (Optional)

UserLimitPPS1
Specifies the throughput limit per group in PPS for precedence 1. (Optional)

UserLimitKbps2
Specifies the bandwidth limit per group in kbps for precedence 2. (Optional)

UserLimitPPS2
Specifies the throughput limit per group in PPS for precedence 2. (Optional)

UserLimitKbps3
Specifies the bandwidth limit per group in kbps for precedence 3. (Optional)

UserLimitPPS3
Specifies the throughput limit per group in PPS for precedence 3. (Optional)

UserLimitKbps4
Specifies the bandwidth limit per group in kbps for precedence 4. (Optional)

UserLimitPPS4
Specifies the throughput limit per group in PPS for precedence 4. (Optional)

UserLimitKbps5
Specifies the bandwidth limit per group in kbps for precedence 5. (Optional)

UserLimitPPS5
Specifies the throughput limit per group in PPS for precedence 5. (Optional)

UserLimitKbps6
Specifies the bandwidth limit per group in kbps for precedence 6. (Optional)

UserLimitPPS6
Specifies the throughput limit per group in PPS for precedence 6. (Optional)

UserLimitKbps7
Specifies the bandwidth limit per group in kbps for precedence 7 (the highest precedence). (Optional)

UserLimitPPS7
Specifies the throughput limit per group in PPS for precedence 7 (the highest precedence). (Optional)

Grouping
Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups. (Default: None)

GroupingNetworkSize
If users are grouped according to source or destina-
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic</td>
<td>Enable dynamic balancing of groups. (Default: No)</td>
</tr>
<tr>
<td>PrecedenceMin</td>
<td>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)</td>
</tr>
<tr>
<td>PrecedenceDefault</td>
<td>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)</td>
</tr>
<tr>
<td>PrecedenceMax</td>
<td>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)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.42. 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

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

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.
3.43. PSK

Description

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the pre-shared key. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the type of the shared key.</td>
</tr>
<tr>
<td>PSKAscii</td>
<td>Specifies the PSK as a passphrase.</td>
</tr>
<tr>
<td>PSKHex</td>
<td>Specifies the PSK as a hexadecimal key.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.44. RadiusAccounting

Description

External RADIUS server used to collect user statistics.

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the server. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td>Port</td>
<td>The UDP port of the server. (Default: 1813)</td>
</tr>
<tr>
<td>RetryTimeout</td>
<td>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)</td>
</tr>
<tr>
<td>SharedSecret</td>
<td>The shared secret phrase for the Authenticator generation.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.45. RadiusServer

Description

External RADIUS server used to verify user names and passwords.

Properties

Name
Specifies a symbolic name for the server. (Identifier)

IPAddress
The IP address of the server.

Port
The UDP port of the server. (Default: 1812)

RetryTimeout
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)

SharedSecret
The shared secret phrase for the Authenticator generation.

Comments
Text describing the current object. (Optional)
3.46. RemoteIDList

Description
List of Remote IDs that are allowed access when using Pre Shared Keys as authentication method.

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the type of the shared key.</td>
</tr>
<tr>
<td>PSKAscii</td>
<td>Specifies the PSK as a passphrase.</td>
</tr>
<tr>
<td>PSKHex</td>
<td>Specifies the PSK as a hexadecimal key.</td>
</tr>
<tr>
<td>IDType</td>
<td>Selects the type of remote identity to use.</td>
</tr>
<tr>
<td>IDValue</td>
<td>Specify the remote identity of the tunnel ID.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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.
3.47. RemoteManagement

This is a category that groups the following object types.

3.47.1. RemoteMgmtHTTP

Description
Configure HTTP/HTTPS management to enable remote management to the system.

Properties

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

3.47.2. RemoteMgmtSNMP

Description
Configure SNMP management to enable SNMP polling.

Properties

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

Description
Configure a Secure Shell (SSH) Server to enable remote management access to the system.

Properties

Name
Specifies a symbolic name for the SSH server.

Interface
Specifies the interface for which remote access is granted.

Port
The listening port for the SSH server. (Default: 22)

AllowAuthMethodPassword
Allow password client authentication. (Default: Yes)

AllowAuthMethodPublicKey
Allow public key client authentication. (Default: Yes)

AllowHostKeyDSA
Allow DSA public key algorithm. (Default: Yes)

AllowHostKeyRSA
Allow RSA public key algorithm. (Default: Yes)

AllowKexDH14
Allow Diffie-Hellman Group 14 key exchange algorithm. (Default: Yes)

AllowKexDH1
Allow Diffie-Hellman Group 1 key exchange algorithm. (Default: Yes)

AllowAES128
Allow AES-128 encryption algorithm. (Default: Yes)

AllowAES192
Allow AES-192 encryption algorithm. (Default: Yes)

AllowAES256
Allow AES-256 encryption algorithm. (Default: Yes)

AllowBlowfish
Allow Blowfish encryption algorithm. (Default: Yes)

Allow3DES
Allow 3DES encryption algorithm. (Default: Yes)

AllowMACSHA1
Allow SHA1 integrity algorithm. (Default: Yes)

AllowMACMD5
Allow MD5 integrity algorithm. (Default: Yes)

AllowMACSHA196
Allow SHA1-96 integrity algorithm. (Default: Yes)

AllowMACMD596
Allow MD5-96 integrity algorithm. (Default: Yes)

Banner
Specifies the greeting message to display when the user logs in. (Optional)

MaxSessions
The maximum number of clients that can be connected at the same time. (Default: 5)

SessionIdleTime
The number of seconds a user can be idle before the session is closed. (Default: 1800)
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoginGraceTime</td>
<td>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)</td>
</tr>
<tr>
<td>AuthenticationRetries</td>
<td>The number of retries allowed before the session is closed. (Default: 3)</td>
</tr>
<tr>
<td>AccessLevel</td>
<td>The access level to grant the user that logs in. (Default: Admin)</td>
</tr>
<tr>
<td>LocalUserDatabase</td>
<td>Specifies the local user database to use for login.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network for which remote access is granted.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.48. RouteBalancingInstance

Description

A route balancing instance is associated with a routing table and defines how to make use of multiple routes to the same destination.

Properties

RoutingTable
Specify routing table to deploy route load balancing in. (Identifier)

Algorithm
Specify which algorithm to use when balancing the routes. (Default: RoundRobin)

Comments
Text describing the current object. (Optional)
3.49. RouteBalancingSpilloverSettings

Description

Settings associated with the spillover algorithm.

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface to threshold limit. (Identifier)</td>
</tr>
<tr>
<td>HoldTime</td>
<td>Number of consecutive seconds over/under the threshold limit to trigger state change for the affected routes. (Default: 30)</td>
</tr>
<tr>
<td>OutboundThreshold</td>
<td>Outbound threshold limit. (Optional)</td>
</tr>
<tr>
<td>OutboundUnit</td>
<td>The outbound units. (Default: kbps)</td>
</tr>
<tr>
<td>InboundThreshold</td>
<td>Inbound threshold limit. (Optional)</td>
</tr>
<tr>
<td>InboundUnit</td>
<td>The inbound units. (Default: kbps)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.50. RouterAdvertisement

Description

Enabling Router Advertisement will answer Solicitations and periodically send out Advertisements. Stateless address autoconfiguration (SLAAC) will only work correctly if the configured network prefix is 64 (RFC4862).

Properties

| Index | The index of the object, starting at 1. (Identifier) |
| Name | Specifies a symbolic name for the Router Advertisement. |
| Interface | Specifies the name of the interface to advertise on. |
| AdvUseGlobal | Use global RA advanced settings. (Default: Yes) |
| MaxRtrAdvInterval | Maximum time between sending unsolicited multicast Router Advertisement. (Default: 600s). (Default: 600) |
| MinRtrAdvInterval | Minimum time between sending unsolicited multicast Router Advertisement. Will be automatically adjusted if set to less than 3 seconds or greater than .75 * MaxRtrInterval). (Default: 200) |
| AutoLifetime | Auto adjust the Router Lifetime field using the following formula; 3 * MaxRtrAdvInterval. (Default: Yes) |
| AdvDefaultLifetime | The value to be placed in the Router Lifetime field of Router Advertisements sent from the SGW, in seconds. (Default: 1800s). (Default: 1800) |
| AdvReachableTime | The value to be placed in the Reachable Time field in the Router Advertisement messages SGW. The value zero means unspecified. (Default: 0s). (Default: 0) |
| AdvRetransTimer | The value to be placed in the Retrans Timer field in the Router Advertisement messages sent by the SGW. The value zero means unspecified. (Default: 0s). (Default: 0) |
| AdvManagedFlag | Indicates that addresses are available via DHCPv6. (Default: False). (Default: No) |
| AdvOtherConfigFlag | Indicates that other configuration information is available via DHCPv6. (Default: False). (Default: No) |
| AdvCurHopLimit | The default value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the SGW. The value zero means unspecified. (Default: 64). (Default: 64) |
| AdvLinkMTU | The value to be placed in MTU options sent. A value of zero indicates that no MTU options are sent. |
3.50.1. RA_PrefixInformation

Description

Specifies a Router Advertisement Prefix Information option.

Properties

Name

Specifies a symbolic name for the Prefix Information.

Prefix

Specifies the network prefix.

AdvValidLifetime

The value to be placed in the Valid Lifetime in the Prefix Information option. The value of 999999999 represents infinity. (Default: 2592000s). (Default: 2592000)

AdvPreferredLifetime

The value to be placed in the Preferred Lifetime in the Prefix Information option. The value of 999999999 represents infinity. (Default: 604800s). (Default: 604800)

AdvOnLinkFlag

Indicates that the advertised prefix can be used for on-link determination. (Default: True). (Default: Yes)

AdvAutonomousFlag

Indicates that the advertised prefix can be used for stateless address configuration. (Default: True). (Default: Yes)

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.
## 3.51. 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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the rule. (Optional)</td>
</tr>
<tr>
<td>ForwardRoutingTable</td>
<td>The forward routing table will be used for packets from the connection originator to the connection endpoint.</td>
</tr>
<tr>
<td>ReturnRoutingTable</td>
<td>The return routing table will be used for packets traveling in the reverse direction.</td>
</tr>
<tr>
<td>SourceNetwork</td>
<td>Specifies the sender span of IP addresses to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationNetwork</td>
<td>Specifies the span of IP addresses to be compared to the destination IP of the received packet.</td>
</tr>
<tr>
<td>SourceInterface</td>
<td>Specifies the name of the receiving interface to be compared to the received packet.</td>
</tr>
<tr>
<td>DestinationInterface</td>
<td>Specifies the destination interface to be compared to the received packet.</td>
</tr>
<tr>
<td>Service</td>
<td>Specifies a service that will be used as a filter parameter when matching traffic with this rule.</td>
</tr>
<tr>
<td>Schedule</td>
<td>By adding a schedule to a rule, the security gateway will only allow that rule to trigger at those designated times. (Optional)</td>
</tr>
<tr>
<td>LogEnabled</td>
<td>Enable logging. (Default: Yes)</td>
</tr>
<tr>
<td>LogSeverity</td>
<td>Specifies with what severity log events will be sent to the specified log receivers. (Default: Default)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*
3.52. RoutingTable

**Description**

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

**Properties**

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

3.52.1. Route

**Description**

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the object. (Optional)</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies which interface packets destined for this route shall be sent through.</td>
</tr>
<tr>
<td>Gateway</td>
<td>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)</td>
</tr>
<tr>
<td>LocalIP</td>
<td>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)</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network address for this route.</td>
</tr>
<tr>
<td>RouteMonitor</td>
<td>Specifies if this route should be monitored for route changes for route failover purposes. (Default: No)</td>
</tr>
<tr>
<td>MonitorLinkStatus</td>
<td>Mark the route as down if the interface link status changes to down. (Default: No)</td>
</tr>
<tr>
<td>MonitorGateway</td>
<td>Mark the route as down if the next hop does not answer on ARP lookups during a specified time. (Default: No)</td>
</tr>
</tbody>
</table>
3.52.1. Route

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MonitorGatewayManualARP</td>
<td>Enable a manually specified ARP lookup interval. (Default: No)</td>
</tr>
<tr>
<td>MonitorGatewayARPInterval</td>
<td>Specifies the ARP lookup interval in milliseconds. (Default: 1000)</td>
</tr>
<tr>
<td>EnableHostMonitoring</td>
<td>Enables the Host Monitoring functionality. (Default: No)</td>
</tr>
<tr>
<td>Reachability</td>
<td>Specifies the number of hosts that are required to be reachable to consider the route to be active. (Default: ALL)</td>
</tr>
<tr>
<td>GracePeriod</td>
<td>Specifies the time to wait after a reconfiguration until the monitoring begins. (Default: 5)</td>
</tr>
<tr>
<td>ReachabilityCount</td>
<td>Minimum number of reachable hosts to consider the route to be active.</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies the metric for this route. (Default: 0)</td>
</tr>
<tr>
<td>ProxyARPAllInterfaces</td>
<td>Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)</td>
</tr>
<tr>
<td>ProxyARPIFInterfaces</td>
<td>Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

**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.*

3.52.1.1. MonitoredHost

**Description**

Specify a host and a monitoring method.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method</td>
<td>Monitoring method. (Default: ICMP)</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Specifies the IP address of the host to monitor.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the TCP port to monitor.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>Delay in milliseconds between each monitor attempt. (Default: 10000)</td>
</tr>
<tr>
<td>ReachabilityRequired</td>
<td>Specifies if this host is required to be reachable for monitoring to be successful. (Default: No)</td>
</tr>
<tr>
<td>Samples</td>
<td>Specifies the number of attempts to use for statistical calculations. (Default: 10)</td>
</tr>
</tbody>
</table>
MaxPollFails Specifies the maximum number of failed attempts until host is considered to be unreachable. (Default: 2)

MaxAverageLatency Specifies the max average latency for the sample attempts. (Default: 800)

RequestURL Specifies the HTTP URL to monitor.

ExpectedResponse Expected HTTP response.

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.*

### 3.52.2. Route6

**Description**

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

**Properties**

**Name** Specifies a symbolic name for the object. (Optional)

**Network** Specifies the network address for this route.

**Interface** Specifies which interface packets destined for this route shall be sent through.

**Gateway** Specifies the IPv6 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)

**LocalIP** The IPv6 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 IPv6 address will be used. (Optional)

**Metric** Specifies the metric for this route. (Default: 0)

**ProxyNDAllInterfaces** Always select all interfaces, including new ones, for publishing routes via Proxy Neighbor Discovery. (Default: No)

**ProxyNDInterfaces** Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)

**Comments** Text describing the current object. (Optional)
3.52.3. 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

<table>
<thead>
<tr>
<th>Property</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the object. (Optional)</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies which interface packets destined for this route shall be sent through.</td>
</tr>
<tr>
<td>Network</td>
<td>Specifies the network address for this route.</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies the metric for this route. (Default: 0)</td>
</tr>
<tr>
<td>ProxyARPAllInterfaces</td>
<td>Always select all interfaces, including new ones, for publishing routes via Proxy ARP. (Default: No)</td>
</tr>
<tr>
<td>ProxyARPInterfaces</td>
<td>Specifies the interfaces on which the security gateway should publish routes via Proxy ARP. (Optional)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

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.
### 3.53. ScheduleProfile

**Description**

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

**Properties**

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

This is a category that groups the following object types.

3.54.1. ServiceGroup

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the service. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members</td>
<td>Group members.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

3.54.2. ServiceICMP

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

Properties

<table>
<thead>
<tr>
<th>Name</th>
<th>Specifies a symbolic name for the service. (Identifier)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MessageTypes</td>
<td>Specifies the ICMP message types that are applicable to this service. (Default: All)</td>
</tr>
<tr>
<td>EchoRequest</td>
<td>Enable matching of Echo Request messages. (Default: No)</td>
</tr>
<tr>
<td>EchoRequestCodes</td>
<td>Specifies which Echo Request message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>DestinationUnreachable</td>
<td>Enable matching of Destination Unreachable messages. (Default: No)</td>
</tr>
<tr>
<td>DestinationUnreachableCodes</td>
<td>Specifies which Destination Unreachable message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>Redirect</td>
<td>Enable matching of Redirect messages. (Default: No)</td>
</tr>
<tr>
<td>RedirectCodes</td>
<td>Specifies which Redirect message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>ParameterProblem</td>
<td>Enable matching of Parameter Problem messages. (Default: No)</td>
</tr>
</tbody>
</table>
### 3.54.3. ServiceICMPv6

**Description**

An IPv6-ICMP Service is an object definition representing IPv6-ICMP traffic with specific parameters.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the service. (Identifier)</td>
</tr>
<tr>
<td>MessageTypes</td>
<td>Specifies the IPv6-ICMP message types that are applicable to this service. (Default: All)</td>
</tr>
<tr>
<td>EchoRequest</td>
<td>Enable matching of Echo Request messages. (Default: No)</td>
</tr>
<tr>
<td>EchoRequestCodes</td>
<td>Specifies which Echo Request message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>EchoReply</td>
<td>Enable matching of Echo Reply messages. (Default: No)</td>
</tr>
<tr>
<td>EchoReplyCodes</td>
<td>Specifies which Echo Reply message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>SourceQuenching</td>
<td>Enable matching of Source Quenching messages. (Default: No)</td>
</tr>
<tr>
<td>SourceQuenchingCodes</td>
<td>Specifies which Source Quenching message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>TimeExceeded</td>
<td>Enable matching of Time Exceeded messages. (Default: No)</td>
</tr>
<tr>
<td>TimeExceededCodes</td>
<td>Specifies which Time Exceeded message codes should be matched. (Default: 0-255)</td>
</tr>
<tr>
<td>PassICMPReturn</td>
<td>Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)</td>
</tr>
<tr>
<td>ALG</td>
<td>An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)</td>
</tr>
<tr>
<td>MaxSessions</td>
<td>Specifies how many concurrent sessions that are permitted using this service. (Default: 200)</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>

---

ParameterProblemCodes Specifies which Parameter Problem message codes should be matched. (Default: 0-255)

EchoReply Enable matching of Echo Reply messages. (Default: No)

EchoReplyCodes Specifies which Echo Reply message codes should be matched. (Default: 0-255)

SourceQuenching Enable matching of Source Quenching messages. (Default: No)

SourceQuenchingCodes Specifies which Source Quenching message codes should be matched. (Default: 0-255)

TimeExceeded Enable matching of Time Exceeded messages. (Default: No)

TimeExceededCodes Specifies which Time Exceeded message codes should be matched. (Default: 0-255)

PassICMPReturn Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)

ALG An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)

MaxSessions Specifies how many concurrent sessions that are permitted using this service. (Default: 200)

Comments Text describing the current object. (Optional)
3.54.4. ServiceIPProto

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

Properties

Name
Specifies a symbolic name for the service. (Identifier)

IPProto
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)

PassICMPReturn
Enable passing an ICMP error message only if it is related to an existing connection using this service. (Default: No)

ALG
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service. (Optional)

MaxSessions
Specifies how many concurrent sessions that are permitted using this service. (Default: 200)

Comments
Text describing the current object. (Optional)
### 3.54.5. ServiceTCPUDP

**Description**

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

**Properties**

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

This is a category that groups the following object types.

### 3.55.1. ARPNDSettings

**Description**

Advanced ARP/Neighbor Discovery-table settings.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARPMatchEnetSender</td>
<td>The Ethernet Sender address matching the hardware address in the ARP data. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPQueryNoSenderIP</td>
<td>If the IP source address of an ARP query (NOT response!) is &quot;0.0.0.0&quot;. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPSenderIP</td>
<td>The IP Source address in ARP packets. (Default: Validate)</td>
</tr>
<tr>
<td>UnsolicitedARPReplies</td>
<td>Unsolicited ARP replies. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPRequests</td>
<td>Specifies whether or not the ARP requests should automatically be added to the ARP table. (Default: Drop)</td>
</tr>
<tr>
<td>ARPChanges</td>
<td>ARP packets that would cause an entry to be changed. (Default: AcceptLog)</td>
</tr>
<tr>
<td>StaticARPChanges</td>
<td>ARP packets that would cause static entries to be changed. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPExpire</td>
<td>Lifetime of an ARP entry in seconds. (Default: 900)</td>
</tr>
<tr>
<td>ARPExpireUnknown</td>
<td>Lifetime of an &quot;unknown&quot; ARP entry in seconds. (Default: 3)</td>
</tr>
<tr>
<td>ARPMulticast</td>
<td>ARP packets claiming to be multicast addresses; may need to be enabled for some load balancers/redundancy solutions. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPBroadcast</td>
<td>ARP packets claiming to be broadcast addresses; should never need to be enabled. (Default: DropLog)</td>
</tr>
<tr>
<td>ARPCacheSize</td>
<td>Number of ARP entries in cache, total. (Default: 4096)</td>
</tr>
<tr>
<td>ARPHashSize</td>
<td>Number of ARP hash buckets per physical interface. (Default: 512)</td>
</tr>
<tr>
<td>ARPHashSizeVLAN</td>
<td>Number of ARP hash buckets per VLAN interface. (Default: 64)</td>
</tr>
<tr>
<td>ARPLogResolveSuccess</td>
<td>Specifies whether or not to log when ARP Resolve succeeds. (Default: No)</td>
</tr>
<tr>
<td>LogResolveFailure</td>
<td>Specifies whether or not to log failed ARP Resolves. (Default: Yes)</td>
</tr>
</tbody>
</table>
### ARPNDSettings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDRateLimit</td>
<td>Rate limit originated ND packets. (Default: 1000)</td>
</tr>
<tr>
<td>MaxAnycastDelayTime</td>
<td>Randomized time to delay proxied and anycast advertisements. (Default: 100)</td>
</tr>
<tr>
<td>ProxyClearOverrideFlag</td>
<td>Clear the Override flag on proxy ND advertisements. (Default: Yes)</td>
</tr>
<tr>
<td>NDMatchEnetSender</td>
<td>Ignore ND packets with mismatching sender- and options MAC-addresses. (Default: Yes)</td>
</tr>
<tr>
<td>NDValSenderIP</td>
<td>Validate the IP source address of the ND packet. (Default: Yes)</td>
</tr>
<tr>
<td>NDLogResolveSuccess</td>
<td>Specifies whether or not to log when ND Resolve succeeds. (Default: No)</td>
</tr>
<tr>
<td>NDChanges</td>
<td>Action to take when ND packets are received that would modify an existing entry. (Default: FavorOld)</td>
</tr>
<tr>
<td>StaticNDChanges</td>
<td>Action to take when ND packets are received that would modify a static entry. (Default: DropLog)</td>
</tr>
<tr>
<td>NDValidation</td>
<td>Action to take when the stateless validation of a ND packet fail. (Default: DropLog)</td>
</tr>
<tr>
<td>NDCacheSize</td>
<td>Number of cached IP/L2 address tuples. (Per iface). (Default: 1024)</td>
</tr>
<tr>
<td>NDMaxMulticastSolicit</td>
<td>Number of Neighbor Solicitations before giving up address resolution. (Default: 3)</td>
</tr>
<tr>
<td>NDMaxUnicastSolicit</td>
<td>Number of Neighbor Solicitations before giving up a zombie during dead peer detection. (Default: 3)</td>
</tr>
<tr>
<td>NDBaseReachableTime</td>
<td>Multiple of randomized time factor in seconds, resulting in the time before a ND entry becomes a zombie. (Default: 30)</td>
</tr>
<tr>
<td>NDDelayFirstProbeTime</td>
<td>Time in seconds for a cache entry to go from DELAY to PROBE state unless resolved. (Default: 5)</td>
</tr>
<tr>
<td>NDRetransTimer</td>
<td>Number of seconds between each Neighbor Solicitation during address resolution and dead peer detection. (Default: 1)</td>
</tr>
<tr>
<td>MaxRtrAdvInterval</td>
<td>Maximum time between sending unsolicited multicast Router Advertisement. (Default: 600s). (Default: 600)</td>
</tr>
<tr>
<td>MinRtrAdvInterval</td>
<td>Minimum time between sending unsolicited multicast Router Advertisement. Will be automatically adjusted if set to less than 3 seconds or greater than .75 * MaxRtrAdvInterval. (Default: 200)</td>
</tr>
<tr>
<td>AutoLifetime</td>
<td>Auto adjust the Router Lifetime field using the following formula; 3 * MaxRtrAdvInterval. (Default: Yes)</td>
</tr>
<tr>
<td>AdvDefaultLifetime</td>
<td>The value to be placed in the Router Lifetime field of Router Advertisements sent from the SGW, in seconds. (Default: 1800s). (Default: 1800)</td>
</tr>
</tbody>
</table>
### AdvReachableTime
The value to be placed in the Reachable Time field in the Router Advertisement messages sent by the SGW. The value zero means unspecified. (Default: 0s). (Default: 0)

### AdvRetransTimer
The value to be placed in the Retrans Timer field in the Router Advertisement messages sent by the SGW. The value zero means unspecified. (Default: 0s). (Default: 0)

### AdvManagedFlag
Indicates that addresses are available via DHCPv6. (Default: False). (Default: No)

### AdvOtherConfigFlag
Indicates that other configuration information is available via DHCPv6. (Default: False). (Default: No)

### AdvCurHopLimit
The default value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the SGW. The value zero means unspecified. (Default: 64). (Default: 64)

### AdvLinkMTU
The value to be placed in MTU options sent. A value of zero indicates that no MTU options are sent. (Default: 0). (Default: 0)

### AdvValidLifetime
The value to be placed in the Valid Lifetime in the Prefix Information option. The value of 999999999 represents infinity. (Default: 2592000s). (Default: 2592000)

### AdvPreferredLifetime
The value to be placed in the Preferred Lifetime in the Prefix Information option. The value of 999999999 represents infinity. (Default: 604800s). (Default: 604800)

### AdvOnLinkFlag
Indicates that the advertised prefix can be used for on-link determination. (Default: True). (Default: Yes)

### AdvAutonomousFlag
Indicates that the advertised prefix can be used for stateless address configuration. (Default: True). (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.

### 3.55.2. AuthenticationSettings

**Description**
Settings related to Authentication and Accounting.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogoutAccUsersAtShutdown</td>
<td>Logout authenticated accounting users and send Ac-</td>
</tr>
</tbody>
</table>
3.55.3. ConnTimeoutSettings

**Description**

Timeout settings for various protocols.

**Properties**

- **ConnLife_TCP_SYN**
  
  Connection idle lifetime for TCP connections being formed. (Default: 60)

- **ConnLife_TCP**
  
  Connection idle lifetime for TCP. (Default: 262144)

- **ConnLife_TCP_FIN**
  
  Connection idle lifetime for TCP connections being closed. (Default: 80)

- **ConnLife_UDP**
  
  Connection idle lifetime for UDP. (Default: 130)

- **AllowBothSidesToKeepConnAlive_UDP**
  
  Allow both sides to keep a UDP connection alive. (Default: No)

- **ConnLife_Ping**
  
  Connection timeout for Ping. (Default: 8)

- **ConnLife_Other**
  
  Idle lifetime for other protocols. (Default: 130)

- **ConnLife_IGMP**
  
  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.

3.55.4. DHCPRelaySettings

**Description**
Advanced DHCP relay settings.

**Properties**

MaxTransactions
Maximum number of concurrent BOOTP/DHCP transactions. (Default: 32)

TransactionTimeout
Timeout for each transaction (in seconds). (Default: 10)

MaxPPMPerInterface
Maximum packets per minute that are relayed from clients to the server, per interface. (Default: 500)

MaxHops
Requests/responses that have traversed more than this many relays will not be relayed. (Default: 5)

MaxLeaseTime
Maximum lease time (seconds) allowed from the DHCP server (too high times will be lowered silently). (Default: 10000)

MaxAutoRoutes
Maximum number of DHCP client IPs automatically added to the routing table. (Default: 256)

AutoSaveRelayPolicy
Policy for saving the relay list to disk. (Default: ReconfShut)

AutoSaveRelayInterval
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.

### 3.55.5. DHCPServerSettings

**Description**
Advanced DHCP server settings.

**Properties**

AutoSaveLeasePolicy
Policy for saving the lease database to disk. (Default: ReconfShut)

AutoSaveLeaseInterval
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.

### 3.55.6. FragSettings
Description
Settings related to fragmented packets.

Properties

**PseudoReass\_MaxConcurrent**  Maximum number of concurrent fragment reassemblies. Set to 0 to drop all fragments. (Default: 1024)

**IllegalFrags**  Illegally constructed fragments; partial overlaps, bad sizes, etc. (Default: DropLog)

**DuplicateFragData**  On receipt of duplicate fragments, verify matching data... (Default: Check8)

**FragReassemblyFail**  Failed packet reassembly attempts - due to timeouts or packet losses. (Default: LogSuspectSubseq)

**DroppedFrags**  Fragments of packets dropped due to rule base. (Default: LogSuspect)

**DuplicateFrags**  Duplicate fragments received. (Default: LogSuspect)

**FragmentedICMP**  Fragmented ICMP messages other than Ping; normally invalid. (Default: DropLog)

**MinimumFragLength**  Minimum allowed length of non-last fragments. (Default: 8)

**ReassTimeout**  Timeout of a reassembly, since previous received fragment. (Default: 65)

**ReassTimeLimit**  Maximum lifetime of a reassembly, since first received fragment. (Default: 90)

**ReassDoneLinger**  How long to remember a completed reassembly (watching for old dupns). (Default: 20)

**ReassIllegalLinger**  How long to remember an illegal reassembly (watching for more fragments). (Default: 60)

**IP6IllegalFrags**  Illegally constructed fragments; partial overlaps, bad sizes, etc. (Default: DropLog)

**IP6DuplicateFragData**  On receipt of duplicate fragments, verify matching data... (Default: Check8)

**IP6FragReassemblyFail**  Failed packet reassembly attempts - due to timeouts or packet losses. (Default: LogSuspectSubseq)

**IP6DroppedFrags**  Fragments of packets dropped due to rule base. (Default: LogSuspect)

**IP6DuplicateFrags**  Duplicate fragments received. (Default: LogSuspect)

**IP6RejectBadFragLength**  Send Parameter Problem error upon reception of fragments with bad data length. (Default: No)

**IP6IgnoreStubFrags**  Ignore fragments with M flag cleared and fragment offset zero. (Default: No)
3.55.7. HWMSets

**Description**

General settings for Hardware Monitoring

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnableSensors</td>
<td>Enable/disable all HWM functionality. (Default: No)</td>
</tr>
<tr>
<td>SensorPollInterval</td>
<td>Sensor polling interval. (Default: 500)</td>
</tr>
<tr>
<td>MemoryPollInterval</td>
<td>Memory polling interval in minutes. (Default: 15)</td>
</tr>
<tr>
<td>MemoryUsePercent</td>
<td>Should mem monitor use percentage as unit for monitoring, else it is megabyte. (Default: Yes)</td>
</tr>
<tr>
<td>MemoryLogRepetition</td>
<td>Should a log message be sent for each poll result that is in the Alert, Critical or Warning level, or should a log message only be sent when a new level is reached. (Default: No)</td>
</tr>
<tr>
<td>MemoryAlertLevel</td>
<td>Alert log message if free memory is below this value, disable by using 0. (Default: 0)</td>
</tr>
<tr>
<td>MemoryCriticalLevel</td>
<td>Critical log message if free memory is below this value, disable by using 0. (Default: 0)</td>
</tr>
<tr>
<td>MemoryWarningLevel</td>
<td>Warning log message if free memory is below this value, disable by using 0. (Default: 0)</td>
</tr>
</tbody>
</table>

**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.
3.55.8. ICMPSettings

**Description**
Settings related to the ICMP protocol.

**Properties**

- **ICMP_sendPerSecLimit**: Maximum number of ICMP responses that will be sent each second. (Default: 500)
- **SilentlyDropStateICMPErrors**: 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.

3.55.9. IPsecTunnelSettings

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

**Properties**

- **IPsecMaxTunnels**: Amount of IPsec tunnels allowed (0 = automatic). (Default: 0)
- **IPsecMaxRules**: Amount of IPsec rules allowed (0 = automatic). (Default: 0)
- **IKESendInitialContact**: Send 'initial contact' messages. (Default: Yes)
- **IKESendCRLs**: Send CRLs in the IKE exchange. (Default: Yes)
- **IKECRLValidityTime**: Maximum number of seconds a CRL is considered valid (0 = obey the 'next update' field in the CRL). (Default: 86400)
- **IKEMaxCAPath**: Maximum number of CA certificates in a certificate path. (Default: 15)
- **IPsecCertCacheMaxCerts**: Maximum number of entries in the certificate cache. (Default: 1024)
IPsecBeforeRules
Pass IKE & IPsec (ESP/AH) traffic sent to the security gateway directly to the IPsec engine without consulting the ruleset. (Default: Yes)

IPsecGWNameCacheTime
Amount of time to keep an IPsec tunnel open when the remote DNS name fails to resolve. (Default: 14400)

DPDMetric
Metric 10s of seconds with no traffic or other evidence of life in tunnel before SA is removed. (Default: 3)

FlowMetric
Minimum number of seconds without data traffic in a flow to activate IKE DPD liveness checks from the corresponding IKE SA. (Default: 15)

IPsecDPDN�数WaitWorryTime
Do not wait for 10 times the value of DPDMetric after the value of Flow Metric has expired without aliveness sign before activating IKE DPD. (Default: No)

DPDKeepTime
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)

DPDExpireTime
Number of seconds that DPD-R-U-THERE messages will be sent. (Default: 15)

IPsecHardwareAcceleration
IPsec hardware acceleration. (Default: Inline)

IPsecDisablePKAccel
Disable hardware acceleration for public-key operations. (Default: No)

AESSNIEnable
Enable AES-NI acceleration for processors that support it. (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.

3.55.10. IPSettings

Description
Settings related to the IP protocol.

Properties

EnableIPv6
Enable processing of IPv6 traffic. (Default: No)

LogReceivedHopLimit0
Log received packets with Hop-Limit=0; this should never happen! (Default: Yes)

HopLimitMin
The minimum IP Hop-Limit value accepted on receipt. (Default: 3)

HopLimitOnLow
What action to take on too low unicast Hop-Limit
HopLimitMinMulticast
The minimum IP multicast Hop-Limit value accepted on receipt. (Default: 3)

HopLimitOnLowMulticast
What action to take on too low multicast Hop-Limit values. (Default: DropLog)

DefaultHopLimit
The default IP Hop-Limit of packets originated by the security gateway (32-255). (Default: 255)

IP6FL
Validate IPV6 Flow label header field. (Default: Ignore)

IP6TC
Validate IPV6 Traffic class header field. (Default: Ignore)

IP6MaxExtHdr
Maximum allowed size of all IP6 extension headers. (Default: 256)

IP6OnMaxExtHdr
Validate the extension header length when it goes beyond IP6MaxExtHdr. (Default: DropLog)

RejectUnorderedExtHdr
Send an ICMPv6 error when encountering extension headers out of order. (Default: No)

IP6MaxOptHdr
Total number of options allowed per IP6 extension header. (Default: 8)

IP6OnMaxOptHdr
Validate the number of options per extension header when it goes beyond IP6MaxOptHdr. (Default: DropLog)

IP6ValidateSyntax
Validate ipv6 syntax violation. (Default: ValidateLogBad)

IP6OPT_PADN
Validate when ipv6 padn option data fields are non-zero. (Default: StripLog)

IP6OPT_JUMBO
Validate jumbogram packets. (Default: ValidateLog)

IP6OPT_RA
Validate Router Alert packets. (Default: Ignore)

IP6OPT_HA
Validate Home Address option packets. (Default: Ignore)

IP6OPT_OTH
Validate unknown option types. (Default: RFC2460Log)

IP6_RH0
Validate routing header type 0 option. (Default: RFC5095NoSupportLog)

IP6_RH2
Validate routing header type 2 option. (Default: RFC2460NoSupportLog)

IP6_RHOther
Validate routing header other than type 0 or 2 option. (Default: RFC2460NoSupportLog)

LogCheckSumErrors
Log IP packets with bad checksums. (Default: Yes)

LogNonIPv4IPv6
Log occurrences of non-IPv4/IPv6 packets. (Default: Yes)

LogReceivedTTLO
Log received packets with TTL=0; this should never
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log0000Src</td>
<td>Log invalid 0.0.0.0 source address. (Default: Drop)</td>
</tr>
<tr>
<td>Block0Net</td>
<td>Block 0.* source addresses. (Default: DropLog)</td>
</tr>
<tr>
<td>Block127Net</td>
<td>Block 127.* source addresses. (Default: DropLog)</td>
</tr>
<tr>
<td>BlockMulticastSrc</td>
<td>Block multicast source addresses (224.0.0.0--255.255.255). (Default: DropLog)</td>
</tr>
<tr>
<td>TTLMin</td>
<td>The minimum IP Time-To-Live value accepted on receipt. (Default: 3)</td>
</tr>
<tr>
<td>TTLOnLow</td>
<td>What action to take on too low unicast TTL values. (Default: DropLog)</td>
</tr>
<tr>
<td>TTLMinMulticast</td>
<td>The minimum IP multicast Time-To-Live value accepted on receipt. (Default: 3)</td>
</tr>
<tr>
<td>TTLOnLowMulticast</td>
<td>What action to take on too low multicast TTL values. (Default: DropLog)</td>
</tr>
<tr>
<td>DefaultTTL</td>
<td>The default IP Time-To-Live of packets originated by the security gateway (32-255). (Default: 255)</td>
</tr>
<tr>
<td>LayerSizeConsistency</td>
<td>TCP/UDP/ICMP/etc layer data and header sizes matching lower layer size information. (Default: ValidateLogBad)</td>
</tr>
<tr>
<td>SecuRemoteUDPEncapCompat</td>
<td>Allow IP data to contain eight bytes more than the UDP total length field specifies -- Checkpoint SecuRemote violates NAT-T drafts. (Default: No)</td>
</tr>
<tr>
<td>IPOptionSizes</td>
<td>Validity of IP header option sizes. (Default: ValidateLogBad)</td>
</tr>
<tr>
<td>IPOPT_SR</td>
<td>How to handle IP packets with contained source or return routes. (Default: DropLog)</td>
</tr>
<tr>
<td>IPOPT_TS</td>
<td>How to handle IP packets with contained Timestamps. (Default: DropLog)</td>
</tr>
<tr>
<td>IPOPT_RTRALT</td>
<td>How to handle IP packets with contained route alert. (Default: ValidateLogBad)</td>
</tr>
<tr>
<td>IPOPT_OTHER</td>
<td>How to handle IP options not specified above. (Default: DropLog)</td>
</tr>
<tr>
<td>DirectedBroadcasts</td>
<td>How to handle directed broadcasts being passed from one interface to another. (Default: DropLog)</td>
</tr>
<tr>
<td>IPRF</td>
<td>How to handle the IP Reserved Flag, if set; it should never be. (Default: DropLog)</td>
</tr>
<tr>
<td>StripDFOnSmall</td>
<td>Strip the &quot;DontFragment&quot; flag for packets of this size or smaller. (Default: 65535)</td>
</tr>
<tr>
<td>MulticastIPEnetOnMismatch</td>
<td>What action to take when ethernet and IP multicast addresses do not match. (Default: DropLog)</td>
</tr>
</tbody>
</table>
3.55.11. L2TPServerSettings

Description

PPTP/L2TP server settings.

Properties

L2TPBeforeRules
Pass L2TP connections sent to the security gateway directly to the L2TP engine without consulting the ruleset. (Default: Yes)

PPTPBeforeRules
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.

3.55.12. LengthLimSettings

Description

Length limitations for various protocols.

Properties

MaxTCPLen
TCP; Sometimes has to be increased if tunneling protocols are used. (Default: 1480)

MaxUDPLen
UDP; Many interactive applications use large UDP packets, may otherwise be decreased to 1480. (Default: 60000)

MaxICMPLen
ICMP; May be decreased to 1480 if desired. (Default: 10000)

MaxICMPv6Len
ICMPv6; May be decreased to 1280 if desired. (Default: 10000)

MaxGRELen
Encapsulated (tunneled transport), used by PPTP. (Default: 2000)

MaxESPLen
IPsec ESP; Encrypted communication. (Default: 2000)
# 3.55.13. LocalReassSettings

**Description**
Parameters use for local fragment reassembly.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LocalReass_MaxConcurrent</td>
<td>Maximum number of concurrent local reassemblies. (Default: 256)</td>
</tr>
<tr>
<td>LocalReass_MaxSize</td>
<td>Maximum size of a locally reassembled packet. (Default: 10000)</td>
</tr>
<tr>
<td>LocalReass_NumLarge</td>
<td>Number of large (&gt;2K) local reassembly buffers (of the above size). (Default: 32)</td>
</tr>
</tbody>
</table>

*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.

# 3.55.14. LogSettings

**Description**
Advanced log settings.

Advanced log settings.
3.55.15. MiscSettings

Description
Miscellaneous Settings

Properties

LogSendPerSecLimit
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.

3.55.15. MiscSettings

Description
Miscellaneous Settings

Properties

UDPSrcPort0
How to treat UDP packets with source port 0. (Default: DropLog)

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

HighBuffers_Dynamic
Allocate the HighBuffers value dynamically. (Default: Yes)

HighBuffers
Number of packet buffers to allocate in addition to the ~200 initial buffers. (Default: 1024)

LocalUndelivered
How to treat (allowed) packets to the Security Gateway that do not match open ports (snmp, scp, netcon, etc). (Default: DropLog)

WCFPerfLog
Enables periodical logging of Web Contentent Filtering resolving performance. (Default: Disabled)

AVSW_Engine
Antivirus Software Engine Selection. (Default: Auto)

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.

3.55.16. MulticastSettings

Description
Advanced Multicast Settings.
### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoAddMulticastCoreRoute</td>
<td>Auto generate core route for &quot;224.0.0.1-239.255.255.255&quot;. (Default: Yes)</td>
</tr>
<tr>
<td>IGMPBeforeRules</td>
<td>Allows IGMP traffic to enter the Security Gateway by default. (Default: Yes)</td>
</tr>
<tr>
<td>IGMPMaxGlobalRequestsPerSecond</td>
<td>Maximum number of requests per second. (Default: 1000)</td>
</tr>
<tr>
<td>IGMPMaxRequestsPerSecond</td>
<td>Maximum number of requests per interface per second. (Default: 100)</td>
</tr>
<tr>
<td>IGMPReactToOwnQueries</td>
<td>The Security Gateway should always respond with Member Reports, even to Queries originating from itself. (Default: No)</td>
</tr>
<tr>
<td>IGMPRobustnessVariable</td>
<td>IGMP is robust to 'value' - 1 packet losses. (Default: 2)</td>
</tr>
<tr>
<td>IGMPQueryInterval</td>
<td>The interval (ms) between general queries sent by the Security Gateway. (Default: 125000)</td>
</tr>
<tr>
<td>IGMPQueryResponseInterval</td>
<td>The maximum time (ms) until a host/client has to send an answer to a query. (Default: 10000)</td>
</tr>
<tr>
<td>IGMPStartupQueryInterval</td>
<td>The general query interval (ms) to use during the startup phase (default: 1/4 of the 'IGMP Query Interval' parameter. (Default: 30000)</td>
</tr>
<tr>
<td>IGMPStartupQueryCount</td>
<td>The number of startup queries to send during the startup phase. (Default: 2)</td>
</tr>
<tr>
<td>IGMPLastMemberQueryInterval</td>
<td>The maximum time (ms) until a host/client has to send an answer to a group and group-and-source specific query. (Default: 5000)</td>
</tr>
<tr>
<td>IGMPUnsolicitedReportInterval</td>
<td>The time between repetitions (ms) of an initial membership report. (Default: 1000)</td>
</tr>
<tr>
<td>IGMPRouterVersion</td>
<td>Multiple IGMP querying routers on a network must use the same IGMP version. (Default: IGMPv3)</td>
</tr>
<tr>
<td>IGMP LowestCompatibleVersion</td>
<td>Lowest IGMP compatibility mode. (Default: IGMPv1)</td>
</tr>
</tbody>
</table>

**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.

### 3.55.17. PPPSettings

#### Description

Settings related to the PPP protocol.
3.55.18. RemoteMgmtSettings

Description

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

Properties

**InitialResendTime**

Initial time in milliseconds to wait before sending a new configuration request if no server response is received. (Default: 200)

*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.

**3.55.18. RemoteMgmtSettings**

**Properties**

**NetconBiDirTimeout**

Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration. (Default: 30)

**WebUIBeforeRules**

Enable HTTP(S) traffic to the security gateway regardless of configured IP Rules. (Default: Yes)

**WWW_srv_HTTPPort**

Specifies the HTTP port for the web user interface. (Default: 80)

**WWW_srv_HTTPSPort**

Specifies the HTTPS port for the web user interface. (Default: 443)

**WebUIAllowLoginAutoComplete**

Allow the web browser to remember the username and password on the login page. (Default: Yes)

**SSHBeforeRules**

Enable SSH traffic to the security gateway regardless of configured IP Rules. (Default: Yes)

**HTTPSCertificate**

Specifies which certificate to use for HTTPS traffic. Only RSA certificates are supported. (Optional)

**SNMPBeforeRules**

Enable SNMP traffic to the security gateway regardless of configured IP Rules. (Default: Yes)

**SNMPRequestLimit**

Maximum number of SNMP packets that will be processed each second. (Default: 100)

**SNMPSysContact**

The contact person for this managed node. (Default: N/A)

**SNMPSysName**

The name for this managed node. (Default: N/A)

**SNMPSysLocation**

The physical location of this node. (Default: N/A)

**SNMPIfDescription**

What to display in the SNMP MIB-II ifDescr variables. (Default: Name)
### 3.55.19. RoutingSettings

**Description**

Configure the routing capabilities of the system.

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RouteFailOver_IfacePollInterval</td>
<td>Time (ms) between polling of interface failure. (Default: 500)</td>
</tr>
<tr>
<td>RouteFailOver_ARPPollInterval</td>
<td>Time (ms) between ARP-lookup of gateways. May be overridden for each route. (Default: 1000)</td>
</tr>
<tr>
<td>RouteFailOver_PingPollInterval</td>
<td>Time (ms) between PING'ing of gateways. (Default: 1000)</td>
</tr>
<tr>
<td>RouteFailOver_GraceTime</td>
<td>Time (s) between startup/reconfigure and monitoring start. (Default: 30)</td>
</tr>
<tr>
<td>RouteFailOver_ConsecFails</td>
<td>Number of consecutive failures before route is marked as unavailable. (Default: 5)</td>
</tr>
<tr>
<td>RouteFailOver_ConsecSuccess</td>
<td>Number of consecutive success before route is marked as available. (Default: 5)</td>
</tr>
<tr>
<td>Transp_CAMToL3CDestLearning</td>
<td>Do L3 Cache learning based on destination IPs and MACs in combination with CAM table contents. (Default: Yes)</td>
</tr>
<tr>
<td>Transp_DecrementTTL</td>
<td>Decrement TTL on packets forwarded between transparent interfaces. (Default: No)</td>
</tr>
<tr>
<td>Transp_CAMSize_Dynamic</td>
<td>Allocate the CAM Size value dynamically. (Default: Yes)</td>
</tr>
<tr>
<td>Transp_CAMSize</td>
<td>Maximum number of entries in each CAM table. (Default: 8192)</td>
</tr>
<tr>
<td>Transp_L3CSIZE_Dynamic</td>
<td>Allocate the L3 Cache Size value dynamically. (Default: Yes)</td>
</tr>
<tr>
<td>Transp_L3CSIZE</td>
<td>Maximum number of entries in each Layer 3 Cache. (Default: 8192)</td>
</tr>
</tbody>
</table>

*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._
### 3.55.20. SSLSettings

**Description**

Settings related to SSL (Secure Sockets Layer).

**Properties**

- **SSL_ProcessingPriority**
  - The amount of CPU time that SSL processing is allowed to use. (Default: Normal)

- **TLS_RSA_WITH_3DES_168_SHA1**
  - Enable cipher RSA_WITH_3DES_168_SHA1. (Default: Yes)

- **TLS_RSA_WITH_RC4_128_SHA1**
  - Enable cipher RSA_WITH_RC4_128_SHA1. (Default: Yes)

- **TLS_RSA_WITH_RC4_128_MD5**
  - Enable cipher TLS_RSA_WITH_RC4_128_MD5. (Default: Yes)

- **TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1**
  - Enable cipher TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1. (Default: Yes)

- **TLS_RSA_EXPORT512_WITH_RC4_40_MD5**
  - Enable cipher TLS_RSA_EXPORT512_WITH_RC4_40_MD5. (Default: No)

- **TLS_RSA_EXPORT512_WITH_RC2_40_MD5**
  - Enable cipher TLS_RSA_EXPORT512_WITH_RC2_40_MD5. (Default: No)

- **TLS_RSA_EXPORT_WITH_NULL_SHA1**
  - Enable cipher TLS_RSA_EXPORT_WITH_NULL_SHA1 (no encryption, just message validation). (Default: No)

- **TLS_RSA_EXPORT_WITH_NULL_MD5**
  - 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.
3.55.21. SSLVPNInterfaceSettings

**Description**

SSL VPN interface settings.

**Properties**

**SSLVPNBeforeRules**

Pass SSL VPN connections sent to the security gateway directly to the SSL VPN 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.*

3.55.22. StateSettings

**Description**

Parameters for the state engine in the system.

**Properties**

**ConnReplace**

What to do when the connection table is full. (Default: ReplaceLog)

**LogOpenFails**

Log packets that are neither part of open connections nor valid new connections. (Default: Yes)

**LogReverseOpens**

Log reverse connection attempts through an established connection. (Default: Yes)

**LogStateViolations**

Log packets that violate stateful tracking rules; for instance, TCP connect sequences. (Default: Yes)

**LogConnections**

Log connections opening and closing. (Default: Log)

**LogConnectionUsage**

Log for every packet that passes through a connection. (Default: No)

**MaxConnections_Dynamic**

Allocate the Max Connection value dynamically. (Default: Yes)

**MaxConnections**

Maximum number of simultaneous connections. (Default: 8192)

**ErrorOnUnrecognized**

Reply with ICMP error when receiving IPv6 packets containing unrecognized headers destined to the SGW. (Not recommended). (Default: No)
3.55.23. TCPSettings

Description

Settings related to the TCP protocol.

Properties

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

TCPOPT_OTHER
How to handle TCP options not specified above. (Default: StripLog)

TCPSynUrg
The TCP URG flag together with SYN; normally invalid (strip=strip URG). (Default: DropLog)

TCPSynPsh
The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH). (Default: StripSilent)

TCPSynRst
The TCP RST flag together with SYN; normally invalid (strip=strip RST). (Default: DropLog)

TCPSynFin
The TCP FIN flag together with SYN; normally invalid (strip=strip FIN). (Default: StripLog)

TCPUrg
The TCP URG flag; many operating systems cannot handle this correctly. (Default: StripLog)

TCPECN
The Explicit Congestion Notification (ECN) flags. Previously known as "XMAS"/"YMAS" flags. Also used in OS fingerprinting. (Default: StripLog)

TCPRF
The TCP Reserved field: should be zero. Used in OS fingerprinting. Also part of ECN extension. (Default: StripLog)

TCPNULL
TCP "NULL" packets without SYN, ACK, FIN or RST; normally invalid, used by scanners. (Default: DropLog)

TCPSequenceNumbers
Validation of TCP sequence numbers. (Default: ValidateLogBad)

TCPAllowReopen
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.

3.55.24. 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.
3.56. SSHClientKey

**Description**

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

**Properties**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the key. (Identifier)</td>
</tr>
<tr>
<td>Type</td>
<td>DSA or RSA. (Default: DSA)</td>
</tr>
<tr>
<td>Subject</td>
<td>Value of the Subject header tag of the public key file. (Optional)</td>
</tr>
<tr>
<td>PublicKey</td>
<td>Specifies the public key.</td>
</tr>
<tr>
<td>Comments</td>
<td>Text describing the current object. (Optional)</td>
</tr>
</tbody>
</table>
3.57. ThresholdRule

Description

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

Properties

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

**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.*

3.57.1. ThresholdAction

Description

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Protect or Audit. (Default: Protect)</td>
</tr>
<tr>
<td>GroupBy</td>
<td>Specifies whether the threshold should be host- or network-based. (Default: SourceIP)</td>
</tr>
<tr>
<td>Threshold</td>
<td>Specifies the threshold.</td>
</tr>
</tbody>
</table>
### 3.57.1. ThresholdAction

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

**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.*
3.58. UpdateCenter

Description
Configure automatical updates.

Properties

**AVEnabled**
Automatic updates of antivirus definitions and engine. (Default: No)

**IDPEnabled**
Automatic updates of IDP maintenance signatures. (Default: No)

**AdvancedIDPEnabled**
Automatic updates of Advanced IDP signatures. (Default: No)

**UpdateInterval**
Specifies the interval at which the automatic update runs. (Default: Daily)

**UpdateDate**
Specifies the day of month when the automatic update is runs.

**UpdateWeekday**
Specifies the day of week when the automatic update is runs. (Default: mon)

**Hourly**
Specifies the number of hours between periodical updates.

**UpdateHour**
 Specifies the hour when the update is run. (Default: 0)

**UpdateMinute**
Specifies the minute when the update is run. (Default: 0)

**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.
3.59. UserAuthRule

Description

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

Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The index of the object, starting at 1. (Identifier)</td>
</tr>
<tr>
<td>Name</td>
<td>Specifies a symbolic name for the rule. (Optional)</td>
</tr>
<tr>
<td>Agent</td>
<td>HTTP, HTTPS, XAUTH, PPP or EAP. (Default: HTTP)</td>
</tr>
<tr>
<td>ChallengeExpire</td>
<td>How long, in seconds, before RADIUS challenge expires. (Default: 160)</td>
</tr>
<tr>
<td>AuthSource</td>
<td>Disallow, LDAP, RADIUS or Local.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface on which the connection was received.</td>
</tr>
<tr>
<td>OriginatorIP</td>
<td>The network object that the incoming IP address must be a part of.</td>
</tr>
<tr>
<td>TerminatorIP</td>
<td>Specifies the destination IP configured on the PPTP/L2TP server configuration. Only used when agent is PPP or SSL. With SSL, this is the IP address of the listening interface.</td>
</tr>
<tr>
<td>RadiusServers</td>
<td>Specifies the authentication servers that will be used to authenticate users matching this rule.</td>
</tr>
<tr>
<td>LDAPServers</td>
<td>Specifies the authentication servers that will be used to authenticate users matching this rule.</td>
</tr>
<tr>
<td>RadiusMethod</td>
<td>Specifies the authentication method used for encrypting the user password. (Default: PAP)</td>
</tr>
<tr>
<td>LocalUserDB</td>
<td>Specifies the local user database that will be used to authenticate users matching this rule.</td>
</tr>
<tr>
<td>LoginType</td>
<td>HTML form or Basic authentication. (Default: HTMLForm)</td>
</tr>
<tr>
<td>MACAuthSecret</td>
<td>Password used to authenticate MAC user, if empty the MAC address will be sent as password. (Optional)</td>
</tr>
<tr>
<td>MACAllowRouter</td>
<td>Allow cliente connected through an Router. (Default: No)</td>
</tr>
<tr>
<td>HTTPBanners</td>
<td>HTTP Authentication HTML Banners. (Default: Default)</td>
</tr>
<tr>
<td>RealmString</td>
<td>The string that is presented as a part of the 401 - Authentication Required message. (Optional)</td>
</tr>
<tr>
<td>HostCertificate</td>
<td>Specifies the host certificate that the security gate-</td>
</tr>
</tbody>
</table>
**RootCertificate**  
Specifies the root certificate that was used to sign the host certificate. Only RSA certificates are supported. (Optional)

**PPPAuthNoAuth**  
Allow no authentication. (Default: No)

**PPPAuthPAP**  
Use PAP authentication protocol. User name and password are sent in plaintext. (Default: Yes)

**PPPAuthCHAP**  
Use CHAP authentication protocol. (Default: Yes)

**PPPAuthMSCHAP**  
Use MS-CHAP authentication protocol. (Default: Yes)

**PPPAuthMSCHAPv2**  
Use MS-CHAP v2 authentication protocol. (Default: Yes)

**IdleTimeout**  
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)

**SessionTimeout**  
If a user has successfully been authenticated, he/she will automatically be logged out after this many seconds, regardless of if there has been activity from the user or not. (Optional)

**UseServerTimeouts**  
Use timeouts received from the authentication server. If no values are received, the manually specified values will be used. (Default: No)

**MultipleUsernameLogins**  
Specifies how multiple username logins will be handled. (Default: AllowMultiple)

**ReplaceIdleTime**  
Replace existing user if idle for more than this number of seconds. (Default: 10)

**AccountingServers**  
Specifies the accounting servers that will be used to report user usage matching this rule. (Optional)

**BytesSent**  
Enable reporting of the number of bytes sent by the user. (Default: Yes)

**PacketsSent**  
Enable reporting of the number of packets sent by the user. (Default: Yes)

**BytesReceived**  
Enable reporting of the number of bytes received by the user. (Default: Yes)

**PacketsReceived**  
Enable reporting of the number of packets received by the user. (Default: Yes)

**SessionTime**  
Enable reporting of the number of seconds the session lasted. (Default: Yes)

**SupportInterimAccounting**  
Enable Interim Accounting Messages to update the accounting server with the current status of an authenticated user. (Default: No)

**ServerInterimControl**  
Let the RADIUS server determine the interval that interim accounting events should be sent. (Default:
InterimValue

The interval in seconds in which interim accounting events should be sent. (Default: 600)

LogEnabled

Enable logging. (Default: Yes)

LogSeverity

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.*
3.60. ZoneDefenseBlock

Description

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

Properties

Addresses
Specifies the addresses to block.

Protocol
All, TCP, UDP or ICMP. (Default: All)

Port
Specifies which UDP or TCP port to use. (Default: 0)

Schedule
Specifies the schedule when the given addresses should be blocked. (Optional)

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.
3.61. ZoneDefenseExcludeList

Description

The exclude list is used to 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.
3.62. 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

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

Commands

A
about, 31
activate, 20
add, 20
alarm, 31
arp, 31
arpmsnooop, 32
ats, 33

B
bigpond, 33
blacklist, 34
buffers, 35

C
cam, 36
cancel, 21
cce, 22
certcache, 36
cfglog, 37
commit, 23
connections, 37
cpuid, 38
crashdump, 38
cryptostat, 38

D
dconsole, 39
delete, 23
dhcp, 39
dhcprelay, 40
dhcpserver, 41
dns, 42
dnsbl, 42
dynroute, 42

E
echo, 79

F
frags, 43

H
ha, 44
help, 79
history, 80
hostmon, 44
httpalp, 45
httpposter, 45
hwm, 46

I
idppipes, 46
ifstat, 47
igmp, 47
ikesnooop, 48
ippool, 49
ipsecglobalstats, 49
ipsekeepalive, 50
ipsecstats, 50
ipsectunnels, 51

K
killsa, 51

L
languagefiles, 52
ldap, 52
license, 53
linkmon, 53
logout, 54
ls, 80
memory, 54

N
natpool, 54
nd, 55
ndsnooop, 56
netobjects, 56

O
ospf, 57

P
pcapdump, 59
ping, 78
pipes, 61
psktpalg, 61
pskgen, 24

R
reconfigure, 62
reject, 24
reset, 26
routemon, 62
routes, 62
rules, 64

S
script, 81
selftest, 64
services, 66
sessionmanager, 67
set, 26
settings, 68
show, 27
shutdown, 69
sipalg, 69
sshserver, 71
sslvpn, 72
stats, 72
sysmsgs, 73

T
technsupport, 73
time, 73

U
uarules, 74
undelete, 29
updatecenter, 75
userauth, 75

V
vlan, 76
vpstats, 77
(see also ipsecstats)

Z
zonedefense, 77

Object types

A
Access, 85
AddressFolder, 87
AdvancedScheduleOccurrence, 91
AdvancedScheduleProfile, 91
ALG_FTP, 92
ALG_H323, 93
ALG_HTTP, 93
ALG_HTTP_URL, 95
ALG_POP3, 95
ALG_PPTP, 96
ALG_SIP, 96
ALG_SMTP, 97
ALG_SMTP_Email, 98
ALG_TFTP, 99
ALG_TLS, 99
ARPND, 100
ARPNDSettings, 189
AuthenticationSettings, 191

B
BlacklistWhiteHost, 101

C
Certificate, 102
COMPortDevice, 106
ConfigModePool, 107
ConnTimeoutSettings, 192

D
DateTime, 108
DefaultInterface, 133
Device, 109
DHCPRelay, 110
DHCPRelaySettings, 192
DHCPServer, 111
DHCPServerCustomOption, 112
DHCPServerPoolStaticHost, 112
DHCPServerSettings, 193
DNS, 113
DynamicRoutingRule, 117
DynamicRoutingRuleAddRoute, 118
DynamicRoutingRuleExportOSPF, 118
DynDnsClientCjbNet, 103
DynDnsClientDLink, 103
DynDnsClientDLinkChina, 103
DynDnsClientDynDNSOrg, 104
DynDnsClientDynsCx, 104
DynDnsClientPeanutHull, 105
E1000EthernetPCIDriver, 114
Ethernet, 133
EthernetAddress, 88, 90
EthernetAddressGroup, 88, 90
EthernetDevice, 120
EventReceiverSNMP2c, 155

F
FragSettings, 193

G
GRE Tunnel, 134

H
HighAvailability, 121
HTTPALGBanners, 122
HTTPAuthBanners, 123
HTTPPoster, 124
HWM, 125
HWMSettings, 195

I
ICMPSets, 196
ID, 126
IDList, 126
IDPRule, 127
IDPRuleAction, 127
IGMPRule, 129
IGMPSetting, 131
IKEAlgorithms, 132
InterfaceGroup, 135
IP4Address, 89, 90
IP4Group, 89, 90
IP4HAAddress, 88, 90
IP6Address, 87, 90
IP6Group, 87, 90
IPPool, 144
IPRule, 145, 148
IPRuleFolder, 148
IPsecAlgorithms, 149
IPsecTunnel, 135
IPsecTunnelSettings, 196
IPSettings, 197
ixgbeEthernetPCIDriver, 114
IXP4NPEEthernetDriver, 115

L
L2TPClient, 137
L2TPServer, 139
L2TPServerSettings, 200
LDAPDatabase, 151
LDAPServer, 152
LengthLimSettings, 200
LinkMonitor, 153
LocalReassSettings, 201
LocalUserDatabase, 154
LoginClientBigPond, 105
LogReceiverMemory, 156
LogReceiverMessageException, 155, 156, 157
LogReceiverSMTP, 156
LogReceiverSyslog, 157
LogSettings, 201

M
MarvellEthernetPCIDriver, 115
MiscSettings, 202
MonitoredHost, 181
MulticastSettings, 202

N
NATPool, 158

O
OSPFAggregate, 162
OSPFArea, 160
OSPFInterface, 161
OSPFNeighbor, 162
OSPFProcess, 159
OSPFVLink, 163

P
Pipe, 164
PipeRule, 167
PPPoETunnel, 140
PPPSets, 203
PSK, 168

R
R8139EthernetPCIDriver, 115
R8169EthernetPCIDriver, 115
RA_PrefixInformation, 178
RadiusAccounting, 169
RadiusServer, 170
RemoteIDLList, 171
RemoteMgmtHTTP, 172
RemoteMgmtSettings, 204
RemoteMgmtSNMP, 172
RemoteMgmtSSH, 173

Route, 180
Route6, 182
RouteBalancingInstance, 175
RouteBalancingSpilloverSettings, 176
RouterAdvertisement, 177
RoutingRule, 179
RoutingSettings, 205
RoutingTable, 180

S
ScheduleProfile, 184
ServiceGroup, 185
ServiceICMP, 185
ServiceICMPv6, 186
ServiceIPProto, 187
ServiceTCPUDP, 188
SSHClientKey, 211
SSLSettings, 206
SSLVPNInterface, 142
SSLVPNInterfaceSettings, 207
StateSettings, 207
SwitchRoute, 183

T
TCPSettings, 208
ThresholdAction, 212
ThresholdRule, 212

U
UpdateCenter, 214
User, 154
UserAuthRule, 215

V
VLAN, 142
VLANSettings, 209

Z
ZoneDefenseBlock, 218
ZoneDefenseExcludeList, 219
ZoneDefenseSwitch, 220