D-Link®
Building Networks for People

Network Security Firewall CLI Reference Guide

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

Ver. 1.02

Network Security Solution http://www.dlink.com

NetDefend

CLI Reference Guide

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

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

Published 2007-12-24
Copyright © 2007

CLI Reference Guide
DFL-210/260/800/860/1600/2500
NetDefendOS version 2.20

Published 2007-12-24

Copyright © 2007

Copyright Notice

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

Disclaimer

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

Limitations of Liability

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

Table of Contents

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

2.2.29. ikesnoop 44
2.2.30. ippool 45
2.2.31. ipsecglobalstats 46
2.2.32. ipseckeepalive 46
2.2.33. ipsecstats 46
2.2.34. killsa 47
2.2.35. license 47
2.2.36. linkmon 48
2.2.37. lockdown 48
2.2.38. logout 49
2.2.39. memory 49
2.2.40. natpool 49
2.2.41. ospf 50
2.2.42. pipes 51
2.2.43. reconfigure 52
2.2.44. routemon 52
2.2.45. routes 52
2.2.46. rules 53
2.2.47. sessionmanager 54
2.2.48. shutdown 55
2.2.49. sipalg 56
2.2.50. sshserver 57
2.2.51. stats 58
2.2.52. time 58
2.2.53. updatecenter 59
2.2.54. urlcache 59
2.2.55. userauth 60
2.2.56. vlan 61
2.2.57. vpnstats 61
2.2.58. zonedefense 61
2.3. Utility 62
2.3.1. ping 62
2.4. Misc 63
2.4.1. help 63
2.4.2. history 63
3. Configuration Reference 65
3.1. Access 66
3.2. Address 68
3.2.1. AddressFolder 68
3.2.2. EthernetAddress 70
3.2.3. EthernetAddressGroup 70
3.2.4. IP4Address 70
3.2.5. IP4Group 70
3.2.6. IP4HAAddress 70
3.3. AdvancedScheduleProfile 71
3.3.1. AdvancedScheduleOccurrence 71
3.4. ALG 72
3.4.1. ALG_FTP 72
3.4.2. ALG_H323 73
3.4.3. ALG_HTTP 73
3.4.4. ALG_POP3 74
3.4.5. ALG_SIP 75
3.4.6. ALG_TFTP 75
3.5. ARP 77
3.6. BlacklistWhiteHost 78
3.7. Certificate 79
3.8. Client 80
3.8.1. DynDnsClientCjbNet 80
3.8.2. DynDnsClientDLink 80
3.8.3. DynDnsClientDLinkChina 80
3.8.4. DynDnsClientDyndnsOrg 81
3.8.5. DynDnsClientDynsCx 81
3.8.6. DynDnsClientPeanutHull 82

3.8.7. LoginClientBigPond 82
3.9. COMPortDevice 83
3.10. ConfigModePool 84
3.11. DateTime 85
3.12. Device 86
3.13. DHCPRelay 87
3.14. DHCPServer 88
3.14.1. DHCPServerPoolStaticHost 88
3.14.2. DHCPServerCustomOption 89
3.15. DNS 90
3.16. Driver 91
3.16.1. IXP4NPEEthernetDriver 91
3.16.2. MarvellEthernetPCIDriver 91
3.16.3. R8139EthernetPCIDriver 91
3.17. DynamicRoutingRule 92
3.17.1. DynamicRoutingRuleExportOSPF 92
3.17.2. DynamicRoutingRuleAddRoute 93
3.18. EthernetDevice 95
3.19. HighAvailability 96
3.20. HTTPPoster 97
3.21. IDList 98
3.21.1. ID 98
3.22. IDPRule 99
3.22.1. IDPRuleAction 99
3.23. IKEAlgorithms 101
3.24. Interface 102
3.24.1. DefaultInterface 102
3.24.2. Ethernet 102
3.24.3. GRETunnel 103
3.24.4. InterfaceGroup 103
3.24.5. IPSecTunnel 104
3.24.6. L2TPClient 106
3.24.7. L2TPServer 107
3.24.8. PPPoETunnel 108
3.24.9. VLAN 109
3.25. IPPool 111
3.26. IPRule 112
3.27. IPRuleFolder 114
3.27.1. IPRule 114
3.28. IPSecAlgorithms 115
3.29. LDAPServer 116
3.30. LocalUserDatabase 117
3.30.1. User 117
3.31. LogReceiver 118
3.31.1. EventReceiverSNMP2c 118
3.31.2. LogReceiverMemory 118
3.31.3. LogReceiverSMTP 119
3.31.4. LogReceiverSyslog 119
3.32. NATPool 121
3.33. OSPFProcess 122
3.33.1. OSPFArea 123
3.34. Pipe 126
3.35. PipeRule 129
3.36. PSK 130
3.37. RadiusServer 131
3.38. RemoteManagement 132
3.38.1. RemoteMgmtHTTP 132
3.38.2. RemoteMgmtSNMP 132
3.38.3. RemoteMgmtSSH 132
3.39. RoutingRule 134
3.40. RoutingTable 135
3.40.1. Route 135
3.40.2. SwitchRoute 136

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

List of Examples

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

Preface

Audience

The target audience for this reference guide is:

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

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

Notation

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

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 11

• Help, page 12

• Function keys, page 13

• Command line history, page 14

• Tab completion, page 15

• User roles, page 17

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

1.1. Running a command

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

1.2. Help

1.2.1. Help for commands

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

Example 1.1. Help for commands

Brief help for the **activate** command:

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

Full help for **activate**:

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

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

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

List all available commands:

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

1.2.2. Help for object types

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

Example 1.2. Help for object types

Full help for `IP4Address`:

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

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

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

1.3. Function keys

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

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 2.4.2, “history”.

Example 1.3. Command line history

Using the command line history via the arrow keys:

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

1.5. Tab completion

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

Example 1.4. Tab completion

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

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

Tab completion of references:

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

1.5.1. Inline help

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

Example 1.5. Inline help

Get inline help for all properties of an IP4Address:

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

Getting inline help for the Address property:

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

1.5.2. Autocompleting current value and default value

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

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

Example 1.6. Edit an existing property value

Edit the current value:

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

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

Edit the default value:

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

1.5.3. Configuration object type categories

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

Example 1.7. Using categories with tab completion

Accessing an IP4Address object with the use of categories:

```
gw-world:/> show ad (tab)
gw-world:/> show 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 priviege. This is indicated in this guide by a note following the command or "Admin only" written next to an option.

Chapter 2. Command Reference

• Configuration, page 19

• Runtime, page 30

• Utility, page 62

• Misc, page 63

2.1. Configuration

2.1.1. activate

Activate changes.

Description

Activate the latest changes.

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

Usage

```
activate
```

Note
Requires Administrator privilege.

2.1.2. add

Create a new object.

Description

Create a new object and add it to the configuration.

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

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

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

Example 2.1. Create a new object

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

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

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

Usage

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

Options

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

Note
Requires Administrator privilege.

2.1.3. cancel

Cancel ongoing commit.

Description

Cancel commit operation immediately, without waiting for the timeout.

Usage

```
cancel
```

Note
Requires Administrator privilege.

2.1.4. cc

Change the current context.

Description

Change the current configuration context.

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

Example 2.2. Change context

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

Go back to the parent context:
 gw-world:/ospf1/area1> cc ..
 gw-world:/ospf1> cc ..
 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. May not be applicable depending on the specified <Type>.
<Type>	Type of configuration object to perform operation on.

2.1.5. commit

Save new configuration to media.

Description

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

command.

Usage

```
commit
```

Note
Requires Administrator privilege.

2.1.6. copy

Copy object.

Description

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

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

Usage

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

Options

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

2.1.7. delete

Delete specified objects.

Description

Delete the specified object, removing it from the configuration.

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

See also: **undelete**

Example 2.3. Delete an object

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

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

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.

2.1.8. 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={64 | 128 | 256 | 512 | 1024 | 2048 | 4096}	Number of bits of data in the generated key. (Default: 64)
<Name>	Name of key.

Note
Requires Administrator privilege.

2.1.9. reject

Reject changes.

Description

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

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

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

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

Example 2.4. Reject changes

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

Reject changes recursively:
(will reject changes in the user database and all users)
 gw-world:/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

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

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

Usage

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

Reject changes made to the specified object.

```
reject -all
```

Reject all changes in the configuration.

Options

-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>	Type of configuration object to perform operation on.

Note
Requires Administrator privilege.

2.1.10. reset

Reset unit configuraition and/or binaries.

Description

Reset configuration or binaries to factory defaults.

Usage

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

Options

-configuration	Reset configuration to factory default.
-unit	Reset unit to factory defaults.

Note
Requires Administrator privilege.

2.1.11. set

Set property values.

Description

Set property values of configuration objects.

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

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

See also: **add**

Example 2.5. Set property values

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

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

Usage

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

Options

-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.
<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.

2.1.12. show

Show objects.

Description

Show objects.

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

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

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

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

Unchanged objects are not indicated by a flag.

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

Example 2.6. Show objects

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

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

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

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

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

Usage

```
show
```

Show the types and categories available in the current context.

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

Show an object or list a type or category.

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

Show all errors.

```
show -changes
```

Show all changes.

Options

-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.

2.1.13. undelete

Restore previously deleted objects.

Description

Restore a previously deleted object.

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

See also: **delete**

Example 2.7. Undelete an object

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

Undelete a referenced object:
(will remove the error in 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 all specified interfaces.

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

Send gratuitous ARP for IP.

Options

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

2.2.4. arpsnoop

Toggle snooping and displaying of ARP requests.

Description

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

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

Usage

```
arpsnoop
```

Show snooped interfaces.

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

Snoop all interfaces.

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

Snoop specified interface.

```
arpsnoop -disable
```

Disable all snooping.

Options

-all Snoop all interfaces.

-disable Disable all snooping.

-verbose Verbose.

<interface> Interface name.

2.2.5. ats

Show active ARP Transaction States.

Description

Show active ARP Transaction States.

Usage

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

Options

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

2.2.6. bigpond

Show BigPond information.

Description

Show the BigPond information about specified interface.

Usage

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

Options

<interface> Interface to show BigPond information.

2.2.7. blacklist

Blacklist.

Description

Block and unblock hosts on the black and white list.

Note: Static blacklist hosts cannot be unblocked.

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

Example 2.8. Block hosts

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

Usage

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

Show information about the blacklisted hosts.

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

Block specified netobject.

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

Unblock specified netobject.

Options

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

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

2.2.8. buffers

List packet buffers or the contents of a buffer.

Description

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

Usage

```
buffers
```

List the 20 most recently freed buffers.

```
buffers -recent
```

Decode the most recently freed buffer.

```
buffers <Num>
```

Decode buffer number <Num>.

Options

-recent	Decode most recently freed buffer.
<Num>	Decode given buffer number.

2.2.9. cam

CAM table information.

Description

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

Usage

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

Options

-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

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

List connections.

```
connections
```

Same as "connections -show".

```
connections -hashinfo
```

Show information on hash table health.

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

Close connections.

Options

-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.
-hashinfo	Show information on hash table health.
-num=<n>	Limit list to <n> connections. (Default: 20)
-protocol=<name/num>	Show only given IP protocol.
-show	Show connections.
-srciface=<interface>	Filter on source interface.
-srcip=<ip addr>	Filter on source IP address.
-srcport=<port>	Show only given source TCP/UDP port.
-verbose	Verbose (more information).

2.2.13. cpuid

Display info about the cpu.

Description

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

Usage

```
cpuid
```

2.2.14. crashdump

Show the contents of the crash.dmp file.

Description

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

Usage

```
crashdump
```

2.2.15. customlog

Show custom configured log messages.

Description

Show list of custom configured log messages.

Usage

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

Options

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

2.2.16. dconsole

Displays the content of the diagnose console.

Description

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

Usage

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

Options

-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)

2.2.17. dhcp

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

Description

Display information about a DHCP-enabled interface.

Usage

```
dhcp
```

List DHCP enabled interfaces.

```
dhcp -list
```

List DHCP enabled interfaces.

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

Show information about DHCP enabled interface.

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

Modify interface lease.

Options

-lease={RENEW | RELEASE}	Modify interface lease.
-list	List all DHCP enabled interfaces.
-show	Show information about DHCP enabled interface.
<interface>	DHCP 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.
<ip address>	IP address.

2.2.19. dhcpserver

Show content of the DHCP server ruleset.

Description

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

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

Usage

```
dhcpserver
```

Show DHCP server leases.

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

Show DHCP server ruleset.

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

Release static or blacklisted IP.

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

Release an active IP.

Options

-leases	Show DHCP server leases.
-mappings	Show DHCP server IP->MAC mappings.
-release={STATIC | BLACK-LIST}	Release static or blacklisted IP. (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

```
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

```
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. httpposter

Display HTTPPoster_URLx status.

Description

Display configuration and status of configured HTTPPoster_URLx targets.

Usage

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

Options

-display Display status.

-repost Re-post all URLs now. (Admin only)

2.2.26. hwaccel

List configured Hardware Accelerators.

Description

Display information about configured Hardware Accelarators.

Usage

```
hwaccel
```

2.2.27. ifstat

Show interface statistics.

Description

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

Usage

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

Options

-allindepth Show in-depth information about all interfaces.

-filter=<expr> Filter list of interfaces.

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

-pbr=<table name> Only list members of given PBR table(s).

-restart Stop and restart the interface. (Admin only)

<Interface> Name of interface.

2.2.28. igmp

IGMP Interfaces.

Description

Show information about the current state of the IGMP interfaces.

Send simulated messages to test configuration of the interface.

Usage

```
igmp
```

Prints the current IGMP state.

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

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

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

Simulate an incoming IGMP query message.

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

Simulate an incoming IGMP join message.

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

Simulate an incoming IGMP leave message.

Options

-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.

2.2.29. ikesnoop

Enable or disable IKE-snooping.

Description

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

Usage

```
ikesnoop
```

Show IKE snooping status.

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

Enable IKE snooping.

```
ikesnoop -off
```

Disable IKE snooping.

Options

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

2.2.30. ippool

Show IP pool information.

Description

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

Usage

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

Forcibly free IP assigned to subsystem.

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

Show IP pool information.

Options

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

-show	Show IP pool information.
-verbose	Verbose output.
<ip address>	IP address to free.

2.2.31. ipsecglobalstats

Show global ipsec statistics.

Description

List global IPsec statistics.

Usage

```
ipsecglobalstats [-verbose]
```

Options

-verbose	Show all statistics.

2.2.32. 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).

2.2.33. ipsecstats

Show the SAs in use.

Description

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

Usage

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

Options

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

2.2.34. killsa

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

Description

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

Usage

```
killsa <ip address>
```

Delete SAs belonging to provided remote SG/peer.

```
killsa -all
```

Delete all SAs.

Options

-all	Kill all SAs.
<ip address>	IP address of remote SG/peer.

Note
Requires Administrator privilege.

2.2.35. license

Show contents of the license file.

Description

Show contents of the license file.

Usage

```
license
```

2.2.36. linkmon

Display link montitoring statistics.

Description

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

Usage

```
linkmon
```

2.2.37. lockdown

Enable / disable lockdown.

Description

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

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

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

Usage

```
lockdown
```

Show lockdown status.

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

Enable / disable lockdown.

Options

{ON | OFF} Enable / disable lockdown.

Note
Requires Administrator privilege.

2.2.38. logout

Logout user.

Description

Logout current user.

Usage

```
logout
```

2.2.39. memory

Show memory information.

Description

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

Usage

```
memory
```

2.2.40. natpool

Show current NAT Pools.

Description

Show current NAT Pools and in-depth information.

Usage

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

Options

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

2.2.41. ospf

Show runtime OSPF information.

Description

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

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

Usage

```
ospf
```

Show runtime information.

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

Show interface information.

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

Show area information.

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

Show neighbor information.

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

Show the internal OSPF process routingtable.

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

Show the LSA database.

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

Show details for a specified LSA.

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

Show troubleshooting messages on the console.

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

Take specified interface offline.

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

Take specified interface online.

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

Start/stop/restart OSPF process.

Options

-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.
{HA | ALT}	Show HA routingtable.

2.2.42. pipes

Show pipes information.

Description

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

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

Usage

```
pipes
```

List all pipes.

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

List users of a given pipe.

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

Show pipe details.

Options

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

2.2.43. reconfigure

Initiates a configuration re-read.

Description

Restart the Security Gateway using the currently active configuration.

Usage

```
reconfigure
```

Note
Requires Administrator privilege.

2.2.44. routemon

List the currently monitored interfaces and gateways.

Description

List the currently monitored interfaces and/or gateways.

Usage

```
routemon
```

2.2.45. routes

Display routing lists.

Description

Display information about the routing table(s):

- Contents of a (named) routing table.

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

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

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

Explanation of Flags field of the routing tables:

O Learned via OSPF

X Route is Disabled

M Route is Monitored

A Published via Proxy ARP

D Dynamic (from e.g. DHCP relay, IPsec, L2TP/PPP servers, etc.)

H HA synced from cluster peer

Usage

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

Options

-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.

2.2.46. rules

Show rules lists.

Description

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

Example 2.10. Show a range of rules

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

Usage

```
rules
```

Show all IP rules.

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

Show specific range of IP rules.

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

Show IP rules.

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

Show a specific type of rules.

Options

-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).

2.2.47. sessionmanager

Session Manager.

Description

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

Explanation of Timeout flags for sessions:

D Session is disabled

S Session uses a timeout in its subsystem

- Session does not use timeout

Usage

```
sessionmanager
```

Show Session Manager status.

```
sessionmanager -status
```

Show Session Manager status.

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

List active sessions.

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

Show in-depth information about session.

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

Send message to session with console.

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

Forcibly terminate session.

Options

-disconnect	Forcibly terminate session. (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.
<message text>	Message to send.
<session name>	Name of session.

2.2.48. shutdown

Initiate core shutdown.

Description

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

Usage

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

Options

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

Note
Requires Administrator privilege.

2.2.49. sipalg

SIP ALG.

Description

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

Usage

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

Show running ALG configuration parameters.

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

Show or flush current registration table.

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

Show active calls table.

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

Show active SIP sessions.

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

Show SIP connections.

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

Show or flush SIP counters.

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

Control SIP snooping. Useful for troubleshooting SIP transactions.

Options

-calls	Show active calls table.
-connection	Show SIP connections.
-definition	Show running ALG configuration parameters.

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

2.2.50. sshserver

SSH Server.

Description

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

Usage

```
sshserver
```

Show server status and list all connected clients.

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

Show server status and list all connected clients.

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

Generate SSH Server private keys.

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

Start SSH Server.

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

Stop SSH Server.

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

Restart SSH Server.

Options

-b=<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.

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

Note
Requires Administrator privilege.

2.2.51. stats

Display various general firewall statistics.

Description

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

Usage

```
stats
```

2.2.52. time

Display current system time.

Description

Display/set the system date and time.

Usage

```
time
```

Display current system time.

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

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

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

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

Options

-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.

2.2.53. updatecenter

Show autoupdate status and manage IDP/AV databases.

Description

Show autoupdate mechanism status or force an update.

Usage

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

Options

-removedb={ANTIVIRUS | IDP}	Remove the database for the specified service.
-servers	Show autoupdate server info.
-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)

2.2.54. urlcache

List contents of the URL cache.

Description

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

Usage

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

Options

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

2.2.55. userauth

Show logged-on users.

Description

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

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

Usage

```
userauth
```

List all authenticated users.

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

List all authenticated users.

```
userauth -privilege
```

List all known privileges (usernames and groups).

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

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

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

Forcibly log out an authenticated user.

Options

-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).

2.2.56. vlan

Show information about VLAN.

Description

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

Usage

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

Options

-interface=<Interface>	List VLANs connected to physical interface <Interface>.
-vlan=<VLAN>	VLAN to show information about.

2.2.57. vpnstats

Alias for **ipsecstats**.

2.2.58. zonedefense

Zonedefense.

Description

Block/unblock IP addresses/net and ethernet addresses.

Usage

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

Options

-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=<4...8192>]
     [-port=<0...65535>] [-udp] [-tcp] [-verbose]
```

Options

-count=<1...10>	Number of packets to send. (Default: 1)
-length=<4...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.
-udp	Send UDP ping.
-verbose	Verbose (more information).
<host>	IP address of host to ping.

2.4. Misc

2.4.1. help

Show help for selected topic.

Description

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

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

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

Usage

```
help
```

List commands alphabetically.

```
help <Topic>
```

Display help about selected topic from any category.

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

Display help from a specific topic category.

Options

-category={COMMANDS | TYPES}	Topic category.
<**Topic**>	Help topic.

2.4.2. history

Dump history to screen.

Description

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

Usage

```
history
```

Chapter 3. Configuration Reference

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

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

3.1. Access

Description

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

Properties

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: No)
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. 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".
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)

3.2.1.2. 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.
UserAuthGroups	Groups and user names that belong to this object. Objects that fil-

	ter on credentials can only be used as source networks and destinations networks in rules. (Optional)
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)

3.2.1.3. 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", "192.168.30.7,192.168.30.11", "192.168.7.0/24" or "172.16.25.10-172.16.25.50".
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)

3.2.1.4. 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.
Exclude	Addresses that will be excluded from the group. (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. (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)

3.2.1.5. 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)

3.2.2. EthernetAddress

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

3.2.3. EthernetAddressGroup

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

3.2.4. IP4Address

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

3.2.5. IP4Group

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

3.2.6. IP4HAAddress

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

3.3. AdvancedScheduleProfile

Description

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

Properties

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

3.3.1. AdvancedScheduleOccurrence

Description

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

Properties

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

Name	Specifies a symbolic name for the ALG. (Identifier)
AllowServerPassive	Allow server to use passive mode (unsafe for server). (Default: No)
ServerPorts	Server data ports. (Default: 1024-65535)
AllowClientActive	Allow client to use active mode (unsafe for client). (Default: No)
ClientPorts	Client data ports. (Default: 1024-65535)
AllowUnknownCommands	Allow unknown commands. (Default: No)
AllowSITEEXEC	Allow SITE EXEC. (Default: No)
MaxLineLength	Maximum line length in control channel. (Default: 256)
MaxCommandRate	Maximum number of commands per second. (Default: 20)
Allow8BitStrings	Allow 8-bit strings in control channel. (Default: Yes)
AllowResumeTransfer	Allow RESUME even in case of content scanning. (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 trigger 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)
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 extentions correspond to the MIME type. (Default: No)
Comments	Text describing the current object. (Optional)

3.4.2. ALG_H323

Description

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

Properties

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

3.4.3. ALG_HTTP

Description

Use an HTTP Application Layer Gateway to filter HTTP traffic.

Properties

Name	Specifies a symbolic name for the ALG. (Identifier)
RemoveCookies	Remove cookies. (Default: No)
RemoveScripts	Remove Javascript/VBScript. (Default: No)
RemoveApplets	Remove Java applets. (Default: No)
RemoveActiveX	Remove ActiveX objects (including Flash). (Default: No)
VerifyUTF8URL	Verify that URLs does not contain invalid UTF8 encoding. (Default: No)
BlackURLDisplayReason	Message to show when there is an attempt to access a black-listed site. (Optional)
MaxDownloadSize	The maximal allowed file size in kB. (Optional)
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 extentions 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 trigger 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)
WebContentFilteringMode	Disabled, Audit or Enable. (Default: Disabled)
FilteringCategories	Web content categories to block. (Optional)
NonManagedAction	Action to take for content that hasn't been classified. (Default: Allow)
AllowFilteringOverride	Allow the user to display a blocked site. (Default: No)
AllowFilteringReclassification	Allow reclassification of sites. (Default: No)
Comments	Text describing the current object. (Optional)

3.4.3.1. ALG_HTTP_URL

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
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 do 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 extentions 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 trigger 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)
Comments	Text describing the current object. (Optional)

3.4.5. 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 between registration requests. (Default: 3600)
SipReqRespTmout	Timeout value between a request and its response. (Default: 180)
SipSignalTmout	Timeout value for last seen SIP message. (Default: 43200)
DataChannelTmout	Timeout value for data channel. (Default: 120)
Comments	Text describing the current object. (Optional)

3.4.6. ALG_TFTP

Description

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

Properties

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)

3.5. ARP

Description

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

Properties

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

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

Properties

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

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

3.8. Client

This is a category that groups the following object types.

3.8.1. DynDnsClientCjbNet

Description

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

Properties

Username Username.

Password The password for the specified username. (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.

3.8.2. DynDnsClientDLink

Description

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

Properties

DNSName The DNS name excluding the .dlinkddns.com suffix.

Username Username.

Password The password for the specified username. (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.

3.8.3. DynDnsClientDLinkChina

Description

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

Properties

DNSName	The DNS name excluding the .dlinkddns.com suffix.
Username	Username.
Password	The password for the specified username. (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.

3.8.4. DynDnsClientDyndnsOrg

Description

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

Properties

DNSName	The DNS name excluding the .dyndns.org suffix.
Username	Username.
Password	The password for the specified username. (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.

3.8.5. DynDnsClientDynsCx

Description

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

Properties

DNSName	The DNS name excluding the .dyns.cx suffix.
Username	Username.
Password	The password for the specified username. (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.

3.8.6. DynDnsClientPeanutHull

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
DNSNames	Specifies the DNS names separated by ";".
Username	Username.
Password	The password for the specified username. (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.

3.8.7. LoginClientBigPond

Description

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

Properties

Username	Username.
Password	The password for the specified username. (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.

3.9. COMPortDevice

Description

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

Properties

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

3.10. ConfigModePool

Description

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

Properties

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 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

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

3.12. Device

Description

Global parameters for this device.

Properties

Name	Name of the device. (Default: Device)
ConfigVersion	Version number of the configuration. (Default: 1)
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.

3.13. DHCPRelay

Description

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

Properties

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

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.
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: No)
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

Index	The index of the object, starting at 1. (Identifier)
Host	IP Address of the host.
MACAddress	The hardware address of the host.
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.

3.14.2. DHCPServerCustomOption

Description

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

Properties

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

3.15. DNS

Description

Configure the DNS (Domain Name System) client settings.

Properties

DNSServer1 IP of the primary DNS Server. (Optional)

DNSServer2 IP of the secondary DNS Server. (Optional)

DNSServer3 IP of the tertiary DNS Server. (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.

3.16. Driver

This is a category that groups the following object types.

3.16.1. 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.

3.16.2. MarvellEthernetPCIDriver

Description

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

Properties

Comments Text describing the current object. (Optional)

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

3.16.3. R8139EthernetPCIDriver

Description

RealTek (8139) Fast Ethernet Adaptor.

Properties

Comments Text describing the current object. (Optional)

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

3.17. DynamicRoutingRule

Description

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

Properties

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: No)
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

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

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

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)

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: No)

Note

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

3.20. HTTPPoster

Description

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

Properties

URL1	The first URL that will be posted when the security gateway is loaded. (Optional)
URL2	The second URL that will be posted when the security gateway is loaded. (Optional)
URL3	The third URL that will be posted when the security gateway is loaded. (Optional)
RepDelay	Delay in seconds until all URLs are refetched. (Default: 1200)
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.

3.21. IDList

Description

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

Properties

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

3.21.1. ID

Description

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

Properties

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

3.22. IDPRule

Description

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

Properties

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

3.22.1. IDPRuleAction

Description

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

Properties

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

BlackList	Activate BlackList. (Default: No)
BlackListTimeToBlock	The number of seconds that the dynamic black list should remain. (Optional)
BlackListBlockOnlyService	Only block the service that triggered the blacklisting. (Default: No)
BlackListIgnoreEstablished	Do not drop existing connection. (Default: No)
LogEnabled	Enable logging. (Default: No)
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.

3.23. IKEAlgorithms

Description

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

Properties

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

3.24. Interface

This is a category that groups the following object types.

3.24.1. DefaultInterface

Description

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

Properties

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

3.24.2. Ethernet

Description

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Properties

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

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

3.24.3. GRETunnel

Description

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

Properties

Name	Specifies a symbolic name for the interface. (Identifier)
IP	Specifies the IP address of the GRE interface.
Network	Specifies the network address of the GRE interface.
RemoteEndpoint	Specifies the IP address of the remote endpoint.
EncapsulationChecksum	Add an extra level of checksum above the one provided by the IPv4 layer. (Default: No)
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	
SessionKey	
Comments	Text describing the current object. (Optional)

3.24.4. InterfaceGroup

Description

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

Properties

Name	Specifies a symbolic name for the interface. (Identifier)
Equivalent	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)
Members	Specifies the interfaces that are included in the interface group.
Comments	Text describing the current object. (Optional)

3.24.5. IPSecTunnel

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
Name	Specifies a symbolic name for the interface.
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. (Default: PSK)
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 vie IKE XAuth.
XAuthPassword	Specifies the password to pass to the remote gateway vie 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: 1424)
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.
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)
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.

3.24.6. L2TPClient

Description

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

Properties

Name	Specifies a symbolic name for the interface. (Identifier)
IP	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)
Network	The network from which traffic should be routed into the tunnel.
RemoteEndpoint	The IP address of the L2TP/PPTP server.
TunnelProtocol	Specifies if PPTP or L2TP should be used for this tunnel. (Default: PPTP)
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.
DNS1	IP of the primary DNS server. (Optional)
DNS2	IP of the secondary DNS server. (Optional)
Username	Specifies the username to use for this PPTP/L2TP interface.
Password	The password to use for this PPTP/L2TP interface.
PPPAuthNoAuth	Allow no authentication for this tunnel. (Default: No)
PPPAuthPAP	Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)
PPPAuthCHAP	Use CHAP authentication protocol for this tunnel. (Default: Yes)
PPPAuthMSCHAP	Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)

PPPAuthMSCHAPv2	Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)
MPPENone	Allow authentication without Microsoft Point-to-Point Encryption (MPPE). (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)
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)
AutoInterfaceNetworkRoute	Automatically add a route for this interface using the given remote network. (Default: Yes)
Comments	Text describing the current object. (Optional)

3.24.7. L2TPServer

Description

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

Properties

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)
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)

3.24.8. PPPoETunnel

Description

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

Properties

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

ServiceName	Specifies the PPPoE server service name used to distinguish between two or more PPPoE servers attached to the same network. (Optional)
PPPAuthNoAuth	Allow no authentication for this tunnel. (Default: No)
PPPAuthPAP	Use PAP authentication protocol for this tunnel. User name and password are sent in plaintext. (Default: Yes)
PPPAuthCHAP	Use CHAP authentication protocol for this tunnel. (Default: Yes)
PPPAuthMSCHAP	Use MS-CHAP authentication protocol for this tunnel. (Default: Yes)
PPPAuthMSCHAPv2	Use MS-CHAP v2 authentication protocol for this tunnel. (Default: Yes)
DialOnDemand	Enable Dial-on-demand which means that the PPPoE 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)
AutoInterfaceNetworkRoute	Automatically add a route for this interface using the given remote network. (Default: Yes)
Schedule	The schedule defines when the PPPoE tunnel should be active. (Optional)
Comments	Text describing the current object. (Optional)

3.24.9. VLAN

Description

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

Properties

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

Broadcast	Specifies the broadcast address 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 interface. (Default: No)
AutoInterfaceNetworkRoute	Automatically add a route for this virtual LAN interface using the given network. (Default: Yes)
AutoDefaultGatewayRoute	Automatically add a default route for this virtual LAN interface using the given default gateway. (Default: Yes)
Comments	Text describing the current object. (Optional)

3.25. IPPool

Description

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

Properties

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

3.26. IPRule

Description

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

Properties

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

SLBMonitorPing	Enable monitoring using ICMP Ping packets. (Default: No)
SLBMonitorTCP	Enable monitoring using TCP packets. (Default: No)
SLBPingUseSharedIP	Use the shared IP of a HA cluster instead of the private IP of the node. (Default: Yes)
SLBTCPUseSharedIP	Use the shared IP of a HA cluster instead of the private IP of the node. (Default: Yes)
SLBPingInterval	Ping interval in milliseconds. (Default: 10000)
SLBPingMaxLoss	Ping maximum packet loss. (Default: 5)
SLBTCPInterval	TCP interval in milliseconds. (Default: 10000)
SLBTCPMaxLoss	TCP maximum packet loss. (Default: 5)
SLBTCPPorts	Specifies which ports will be monitored.
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)
SLBAddresses	The IP addresses of the servers in the server farm.
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: No)
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.

3.27. IPRuleFolder

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
Name	Specifies the name of the folder.
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.

3.27.1. IPRule

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

3.28. IPSecAlgorithms

Description

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

Properties

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

3.29. LDAPServer

Description

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

Properties

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

3.30. LocalUserDatabase

Description

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

Properties

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

3.30.1. User

Description

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

Properties

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

3.31. LogReceiver

This is a category that groups the following object types.

3.31.1. EventReceiverSNMP2c

Description

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

Properties

Name	Specifies a symbolic name for the log receiver. (Identifier)
IPAddress	
Port	(Default: 162)
Community	
RepeatCount	
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)

3.31.1.1. LogReceiverMessageException

Description

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

Properties

LogID	The ID number of the log message. (Identifier)
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)

3.31.2. LogReceiverMemory

Description

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

Properties

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

3.31.3. LogReceiverSMTP

Description

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

Properties

Name	Specifies a symbolic name for the log receiver. (Identifier)
IPAddress	The IP address of the SMTP server.
Port	Specifies the which port to use to connect to the SMTP server. (Default: 25)
Receiver1	The email address that the event information is sent to.
Receiver2	Alternate email receiver. (Optional)
Receiver3	Alternate email receiver. (Optional)
Sender	Specifies which sender the email will have. (Default: hostmaster)
Identity	Specifies which identity to write in the email header. (Default: hostmaster)
XMailer	Specifies the X-mailer information to write in the email header. (Optional)
Subject	The subject of the email. (Default: "Log event from D-Link DFL Firewall")
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)

3.31.4. 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)

3.31.4.1. LogReceiverMessageException

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

3.32. NATPool

Description

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

Properties

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

3.33. OSPFProcess

Description

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

Properties

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

3.33.1. OSPFArea

Description

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

Properties

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)

3.33.1.1. 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 OS-

	PF interface. (Identifier)
Type	Auto, Broadcast, Point-to-point or Point-to-multipoint. (Default: Auto)
MetricType	Metric value or Bandwidth. (Default: MetricValue)
Metric	Specifies the routing metric for this OSPF interface.
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. (Default: 5)
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 trough 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)

3.33.1.2. 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. (Identifier)
IPAddress	IP Address of the neighbor.
Metric	Specifies the metric of the neighbor. (Optional)
Comments	Text describing the current object. (Optional)

3.33.1.3. OSPFAggregate

Description

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

Properties

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

3.33.1.4. OSPFVLink

Description

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

Properties

Name	Specifies a symbolic name for the virtual link. (Identifier)
RouterID	The ID of the router on the other side of the virtual link.
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)
Comments	Text describing the current object. (Optional)

3.34. Pipe

Description

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

Properties

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 (the highest precedence). (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 destination network, the size of the network has to be specified by this setting. (Default: 0)
Dynamic	Enable dynamic balancing of groups. (Default: No)
PrecedenceMin	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)
PrecedenceDefault	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)
PrecedenceMax	Specifies the highest allowed precedence for traffic in this pipe. If a packet with a higher precedence enters, its precedence is lowered to this value. Should be higher than or equal to the default precedence. (Default: 7)

Comments	Text describing the current object. (Optional)

3.35. PipeRule

Description

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

Properties

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

3.36. PSK

Description

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

Properties

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

3.37. 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)

3.38. RemoteManagement

This is a category that groups the following object types.

3.38.1. RemoteMgmtHTTP

Description

HTTP/HTTPS management.

Properties

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

3.38.2. RemoteMgmtSNMP

Description

SNMP management.

Properties

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

3.38.3. RemoteMgmtSSH

Description

Secure Shell (SSH) Server.

Properties

Name	Specifies a symbolic name for the SSH server. (Identifier)
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 1 key exchange algorithm. (Default: Yes)
AllowKexDH1	Allow Diffie-Hellman Group 14 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)
LoginGraceTime	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)
AuthenticationRetries	The number of retires allowed before the session is closed. (Default: 5)
AccessLevel	The access level to grant the user that logs in. (Default: Admin)
LocalUserDatabase	Specifies the local user database to use for login.
Interface	Specifies the interface for which remote access is granted.
Network	Specifies the network for which remote access is granted.
Comments	Text describing the current object. (Optional)

3.39. RoutingRule

Description

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

Properties

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

3.40. RoutingTable

Description

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

Properties

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

3.40.1. Route

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
Name	Specifies a symbolic name for the object. (Optional)
Interface	Specifies which interface packets destined for this route shall be sent through.
Gateway	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)
LocalIP	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)
RouteMonitor	Specifies if this route should be monitored for route changes for route failover purposes. (Default: No)
MonitorLinkStatus	Mark the route as down if the interface link status changes to down. (Default: No)
MonitorGateway	Mark the route as down if the next hop does not answer on ARP lookups during a specified time. (Default: No)
MonitorGatewayManualARP	Enable a manually specified ARP lookup interval. (Default: No)
MonitorGatewayARPInterval	Specifies the ARP lookup interval in milliseconds. (Default:

	1000)
Network	Specifies the network address for this route.
Metric	Specifies the metric for this route. (Default: 0)
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)

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

3.40.2. SwitchRoute

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
Name	Specifies a symbolic name for the object. (Optional)
Interface	Specifies which interface packets destined for this route shall be sent through.
Network	Specifies the network address for this route.
Metric	Specifies the metric for this route. (Default: 0)
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)

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

3.41. ScheduleProfile

Description

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

Properties

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

3.42. Service

This is a category that groups the following object types.

3.42.1. ServiceGroup

Description

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

Properties

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

3.42.2. ServiceICMP

Description

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

Properties

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

3.42.3. 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)

3.42.4. ServiceTCPUDP

Description

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

Properties

Name	Specifies a symbolic name for the service. (Identifier)
DestinationPorts	Specifies the destination port or the port ranges applicable to this service.
Type	Specifies whether this service uses the TCP or UDP protocol or both. (Default: TCP)
SourcePorts	Specifies the source port or the port ranges applicable to this service. (Default: 0-65535)
SYNRelay	Enable SYN flood protection (SYN Relay). (Default: No)
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)

3.43. Settings

This is a category that groups the following object types.

3.43.1. ARPTableSettings

Description

Advanced ARP-table settings.

Properties

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

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

3.43.2. ConnTimeoutSettings

Description

Timeout settings for various protocols.

Properties

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.

3.43.3. 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)
MaxPPMPerIface	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.

3.43.4. 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.

3.43.5. 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	Illegaly 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 dups). (Default: 20)
ReassIllegalLinger	How long to remember an illegal reassembly (watching for more fragments). (Default: 60)

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

3.43.6. ICMPSettings

Description

Settings related to the ICMP protocol.

Properties

ICMPSendPerSecLimit	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.

3.43.7. 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)
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)

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

3.43.8. IPSettings

Description

Settings related to the IP protocol.

Properties

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

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

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

3.43.9. L2TPServerSettings

Description

PPTP/L2TP server settings.

Properties

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.

3.43.10. 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)
MaxGRELen	Encapsulated (tunneled transport), used by PPTP. (Default: 2000)
MaxESPLen	IPsec ESP; Encrypted communication. (Default: 2000)
MaxAHLen	IPsec AH; Authenticated communication. (Default: 2000)
MaxSKIPLen	SKIP; Simple Key management for IP, VPN protocol. (Default: 2000)
MaxOSPFLen	OSPF; Open Shortest Path First, routing protocol. (Default: 1480)
MaxIPIPLen	IPIP/FWZ; Encapsulated (tunneled) transport, used by VPN-1. (Default: 2000)
MaxIPCompLen	IPsec IPComp; Compressed communication. (Default: 2000)
MaxL2TPLen	L2TP; Layer 2 Tunneling Protocol. (Default: 2000)
MaxOtherSubIPLen	Others; sometimes has to be increased if unknown tunneling protocols are used. (Default: 1480)
LogOversizedPackets	Log occurrences of oversized packets. (Default: Yes)

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

3.43.11. LocalReassSettings

Description

Parameters use for local fragment reassembly.

Properties

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

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

3.43.12. LogSettings

Description

Advanced log settings.

Properties

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.

3.43.13. 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)

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

3.43.14. RemoteMgmtSettings

Description

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

Properties

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)
WWWSrv_HTTPPort	Specifies the HTTP port for the web user interface. (Default: 80)
WWWSrv_HTTPSPort	Specifies the HTTP(S) port for the web user interface. (Default: 443)
SSHBeforeRules	Enable SSH traffic to the security gateway regardless of configured IP Rules. (Default: Yes)
HTTPSCertificate	Specifies which certificate to use for HTTPS traffic. (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)
SNMPIfAlias	What to display in the SNMP ifMIB ifAlias variables. (Default: Hardware)
LocalConsoleIdleTimeout	Number of seconds of inactivity until the local console user is automatically logged out. (Default: 900)
WebUIIdleTimeout	Number of seconds of inactivity until the HTTP(S) session is closed. (Default: 900)

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

3.43.15. RoutingSettings

Description

Configure the routing capabilities of the system.

Properties

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

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

3.43.16. SSLSettings

Description

Settings related to SSL (Secure Sockets Layer).

Properties

SSL_ProcessingPriority	The amount of 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_EXPORT1024_WITH_RC4_40_MD5. (Default: No)
TLS_RSA_EXPORT512_WITH_RC2_40_MD5	Enable cipher TLS_RSA_EXPORT1024_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.

3.43.17. 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)

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

3.43.18. TCPSettings

Description

Settings related to the TCP protocol.

Properties

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

3.43.19. VLANSettings

Description

Settings for IEEE 802.1Q based Virtual LAN interfaces.

Properties

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

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

3.44. SSHClientKey

Description

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

Properties

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

3.45. ThresholdRule

Description

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

Properties

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

3.45.1. ThresholdAction

Description

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

Properties

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

ThresholdUnit	Specifies the threshold unit. (Default: ConnsSec)
ZoneDefense	Activate ZoneDefense. (Default: No)
BlackList	Activate BlackList. (Default: No)
BlackListTimeToBlock	The number of seconds that the dynamic black list should remain. (Optional)
BlackListBlockOnlyService	Only block the service that triggered the blacklisting. (Default: No)
BlackListIgnoreEstablished	Do not drop existing connection. (Default: No)
LogEnabled	Enable logging. (Default: No)
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.

3.46. 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	Specififes 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.

3.47. UserAuthRule

Description

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

Properties

Index	The index of the object, starting at 1. (Identifier)
Name	Specifies a symbolic name for the rule.
Agent	HTTP, HTTPS, XAUTH, PPP or EAP. (Default: HTTP)
AuthSource	Disallow, Radius or Local.
Interface	The interface on which the connection was received.
OriginatorIP	The network object that the incoming IP address must be a part of.
TerminatorIP	Specifies the destination IP configured on the PPTP/L2TP server configuration. Only used when agent is PPP.
RadiusServers	Specifies the authentication servers that will be used to authenticate users matching this rule.
RadiusMethod	Specifies the authentication method used for encrypting the user password. (Default: PAP)
LocalUserDB	Specifies the local user database that will be used to authenticate users matching this rule.
LoginType	HTML form or Basic authentication. (Default: HTMLForm)
RealmString	The string that is presented as a part of the 401 - Authentication Required message.
HostCertificate	Specifies the host certificate that the security gateway sends to the client.
RootCertificate	Specifies the root certificate that was used to sign the host certificate. (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 auto-

	matically 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: Yes)
InterimValue	The interval in seconds in which interim accounting events should be sent. (Default: 600)
LogEnabled	Enable logging. (Default: No)
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.

3.48. ZoneDefenseBlock

Description

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

Properties

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

3.49. ZoneDefenseExcludeList

Description

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

Properties

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

Comments Text describing the current object. (Optional)

Note

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

3.50. ZoneDefenseSwitch

Description

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

Properties

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

Index

Commands

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

B
bigpond, 32
blacklist, 33
buffers, 34

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

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

F
frags, 41

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

I
ifstat, 43
igmp, 44
ikesnoop, 44
ippool, 45
ipsecglobalstats, 46
ipseckeepalive, 46
ipsecstats, 46

K
killsa, 47

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

M
memory, 49

N
natpool, 49

O
ospf, 50

P
ping, 62
pipes, 51
pskgen, 23

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

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

T
time, 58

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

V
vlan, 61
vpnstats, 61
(see also ipsecstats)

Z
zonedefense, 61

Object types

A
Access, 66
AddressFolder, 68
AdvancedScheduleOccurrence, 71
AdvancedScheduleProfile, 71
ALG_FTP, 72
ALG_H323, 73
ALG_HTTP, 73
ALG_HTTP_URL, 74
ALG_POP3, 74
ALG_SIP, 75
ALG_TFTP, 75
ARP, 77
ARPTableSettings, 141

B
BlacklistWhiteHost, 78

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

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

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

F
FragSettings, 143

G
GRETunnel, 103

H
HighAvailability, 96
HTTPPoster, 97

I
ICMPSettings, 144
ID, 98
IDList, 98
IDPRule, 99
IDPRuleAction, 99
IKEAlgorithms, 101
InterfaceGroup, 103
IP4Address, 69, 70
IP4Group, 69, 70
IP4HAAddress, 70, 70
IPPool, 111
IPRule, 112, 114
IPRuleFolder, 114
IPSecAlgorithms, 115
IPSecTunnel, 104
IPSecTunnelSettings, 144
IPSettings, 145
IXP4NPEEthernetDriver, 91

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

M
MarvellEthernetPCIDriver, 91
MiscSettings, 148

N
NATPool, 121

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

OSPFProcess, 122
OSPFVLink, 125

P

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

R

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

S

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

T

TCPSettings, 152
ThresholdAction, 155
ThresholdRule, 155

U

UpdateCenter, 157
User, 117
UserAuthRule, 158

V

VLAN, 109
VLANSettings, 153

Z

ZoneDefenseBlock, 160
ZoneDefenseExcludeList, 161
ZoneDefenseSwitch, 162