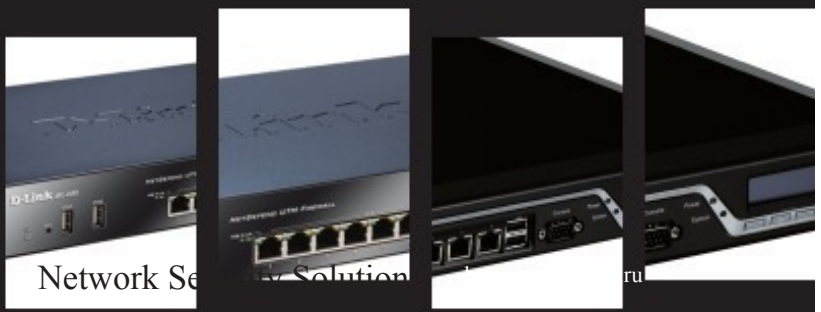
D-Link®

Building Networks for People



Network Se Solution ru

NetDefendOS

Версия 2.27

Руководство по использованию командной строки (CLI)

DFL-260E/860E/1660/2500/2560
NetDefendOS Версия 2.27

D-Link Corporation
http://www.dlink.ru

Опубликовано 26-02-2012

Руководство по использованию интерфейса командной строки (CLI)
DFL-260E/860E/1660/2500/2560
NetDefendOS Версия 2.27

Опубликовано 26-02-2012

Уведомление об авторском праве

Отказ от прав

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления. Компания D-Link не дает никаких заверений или гарантий в отношении содержания настоящего документа и отказывается от любых косвенных гарантий, касающихся товарного качества или пригодности товаров к использованию по назначению. Компания D-Link оставляет за собой право пересмотреть данный документ и периодически вносить изменения в содержание документа без предварительного уведомления лица или сторон об изменениях.

Ограничение ответственности

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОМПАНИЯ D-LINK ИЛИ ЕЕ ПОСТАВЩИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА УБЫТКИ ЛЮБОГО ХАРАКТЕРА (НАПРИМЕР, УЩЕРБ ОТ ПОТЕРИ ПРИБЫЛИ, ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОСТАНОВКИ РАБОТЫ, ПОТЕРИ СОХРАНЕННЫХ ДАННЫХ ИЛИ ЛЮБЫЕ ДРУГИЕ КОММЕРЧЕСКИЕ УБЫТКИ ИЛИ ПОТЕРИ), ВОЗНИКАЮЩИЕ В РЕЗУЛЬТАТЕ ПРИМЕНЕНИЯ ИЛИ НЕПРАВИЛЬНОГО ИСПОЛЬЗОВАНИЯ ПРОДУКТА D-LINK ИЛИ НЕИСПРАВНОСТИ ПРОДУКТА, ДАЖЕ ЕСЛИ КОМПАНИЯ D-LINK БЫЛА ПРОИНФОРМИРОВАНА О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ. КРОМЕ ТОГО, КОМПАНИЯ D-LINK НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ, ЕСЛИ ТРЕТЬЯ СТОРОНА ПРЕДЪЯВЛЯЕТ ТРЕБОВАНИЯ КЛИЕНТУ ИЗ-ЗА ПОТЕРЬ ИЛИ ПОВРЕЖДЕНИЙ. КОМПАНИЯ D-LINK НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА УЩЕРБ, ПРЕВЫШАЮЩИЙ СУММУ, ПОЛУЧЕННУЮ КОМПАНИЕЙ ОТ КОНЕЧНОГО ПОЛЬЗОВАТЕЛЯ ПРОДУКТА.

Содержание

Предисловие....9
Глава 1. Введение....10
1.1. Запуск команды....10
1.2. Справка....10
1.2.1. Справка по командам....10
1.2.2. Справка по типам объекта....11
1.3. Функциональные клавиши....11
1.4. История командной строки....11
1.5. Функция Tab completion....12
Глава 2. Справочная информация по командам....15
2.1. Настройка....15
2.1.1. activate....15
2.1.2. add....15
2.1.3. cancel....16
2.1.4. cc....17
2.1.5. commit....18
2.1.6. delete....18
2.1.7. pskgen....19
2.1.8. reject....20
2.1.9. reset....21
2.1.10. set....22
2.1.11. show....23
2.1.12. undelete....24
2.2. Работа системы....25
2.2.1. Информация об устройстве....25
2.2.2. alarm....25
2.2.3. arp....26
2.2.4. arpsnoop....27
2.2.5. ats....27
2.2.6. blacklist....27
2.2.7. buffers....29
2.2.8. cam....29
2.2.9. certcache....30
2.2.10. cfglog....30
2.2.11. connections....30
2.2.12. cpuid....31
2.2.13. crashdump....32
2.2.14. cryptostat....32
2.2.15. dconsole....32
2.2.16. dhcp....33
2.2.17. dhcprelay....33
2.2.18. dhcpserver....34
2.2.19. dns....35
2.2.20. dnsbl....36
2.2.21. dynroute....36
2.2.22. frags....36
2.2.23. ha....37
2.2.24. hostmon....38
2.2.25. httpalg....38
2.2.26. httpposter....39
2.2.27. hwaccel....39
2.2.28. hwm....39
2.2.29. idppipes....40

2.2.30. ifstat....40
2.2.31. igmp....41
2.2.32. ikesnoop....42
2.2.33. ippool....42
2.2.34. ipsecglobalstats....43
2.2.35. ipseckeepalive....43
2.2.36. ipsecstats....44
2.2.37. ipsectunnels....44
2.2.38. killsa....45
2.2.39. languagefiles....45
2.2.40. ldap....46
2.2.41. license....46
2.2.42. linkmon....47
2.2.43. lockdown....47
2.2.44. logout....48
2.2.45. memory....48
2.2.46. natpool....48
2.2.47. netcon....49
2.2.48. netobjects....49
2.2.49. ospf....50
2.2.50. pcapdump....51
2.2.51. pciscan....53
2.2.52. pipes....54
2.2.53. pptpalg....55
2.2.54. reconfigure....55
2.2.55. routemon....56
2.2.56. routes....56
2.2.57. rtmonitor....57
2.2.58. rules....58
2.2.59. selftest....58
2.2.60. services....60
2.2.61. sessionmanager....61
2.2.62. settings....62
2.2.63. shutdown....63
2.2.64. sipalg....63
2.2.65. sshserver....65
2.2.66. stats....66
2.2.67. sysmsgs....66
2.2.68. techsupport....66
2.2.69. time....67
2.2.70. uarules....67
2.2.71. updatecenter....68
2.2.72. userauth....69
2.2.73. vlan....70
2.2.74. vpnstats....70
2.3. Утилита....71
2.3.1. ping....71
2.4. Прочее....71
2.4.1. echo....71
2.4.2. help....72
2.4.3. history....73
2.4.4. ls....73
2.4.5. script....74
Глава 3. Справочная информация по настройкам....76
3.1. Access....77
3.2. Address....78
3.2.1. AddressFolder....78

3.2.1.1. IP4HAAddress....79
3.2.1.2. IP4Group....79
3.2.1.3. EthernetAddress....80
3.2.1.4. EthernetAddressGroup....80
3.2.1.5. IP4Address....80
3.2.2. EthernetAddress....81
3.2.3. EthernetAddressGroup....81
3.2.4. IP4Address....81
3.2.5. IP4Group....81
3.2.6. IP4HAAddress....81
3.3. AdvancedScheduleProfile....82
3.3.1. AdvancedScheduleOccurence....82
3.4. ALG....83
3.4.1. ALG_FTP....83
3.4.2. ALG_H323....84
3.4.3. ALG_HTTP....85
3.4.3.1. ALG_HTTP_URL....86
3.4.4. ALG_POP3....87
3.4.5. ALG_PPTP....88
3.4.6. ALG_SIP....88
3.4.7. ALG_SMTP....89
3.4.7.1. ALG_SMTP_Email....90
3.4.8. ALG_TFTP....91
3.4.9. ALG_TLS....91
3.5. ARP....92
3.6. BlacklistWhiteHost....92
3.7. Certificate....93
3.8. Client....93
3.8.1. DynDnsClientCjbNet....94
3.8.2. DynDnsClientDyndnsOrg....94
3.8.3. DynDnsClientDynsCx....95
3.8.4. DynDnsClientPeanutHull....95
3.9. CommentGroup....96
3.10. COMPortDevice....96
3.11. ConfigModePool....97
3.12. DateTime....97
3.13. Device....98
3.14. DHCPRelay....99
3.15. DHCPServer....100
3.15.1 DHCPServerPoolStaticHost....102
3.15.2 DHCPServerCustomOption....102
3.16. DNS....103
3.17. Driver....103
3.17.1. BNE2EthernetPCIDriver....103
3.17.2. BNE2EthernetPCIDriver....104
3.17.3. E1000EthernetPCIDriver....104
3.17.4. E100EthernetPCIDriver....105
3.17.5. IXP4NPEEthernetPCIDriver....105
3.17.6. MarvellEthernetPCIDriver....105
3.17.7. R8139EthernetPCIDriver....106
3.17.8. R8169EthernetPCIDriver....106
3.17.9. ST201EthernetPCIDriver....106
3.17.10. ST201EthernetPCIDriver....107
3.17.11. X3C905EthernetPCIDriver....107
3.18. DynamicRoutingRule....108
3.18.1. DynamicRoutingRuleExportOSPF....109

3.18.2. DynamicRoutingRuleAddRoute....109
3.19. EthernetDevice....110
3.20. HighAvailibiliy....111
3.21. HTTPALGBanners....112
3.22. HTTPAuthBanners....112
3.23. HTTPPoster....113
3.24. HWM....114
3.25. IDList....114
3.25.1. ID....114
3.26. IDPRule....115
3.26.1. IDPRuleAction....116
3.27. IGMPRule....117
3.28. IGMPSetting....119
3.29. IKEAlgorithms....120
3.30. Interface....120
3.30.1. DefaultInterface....120
3.30.2. Ethernet....121
3.30.3. GRETunnel....122
3.30.4. InterfaceGroup....123
3.30.5. IPsecTunnel....124
3.30.6. L2TPClient....126
3.30.7. L2TPServer....128
3.30.8. LoopbackInterface....129
3.30.9. PPPoETunnel....130
3.30.10. VLAN....132
3.31. IPPool....133
3.32. IPRuleSet....134
3.32.1. IPRule....134
3.32.2. IPRuleFolder....137
3.32.2.1. IPRule....137
3.33. IPsecAlgorithms....137
3.34. LDAPDatabase....138
3.35. LDAPServer....139
3.36. LinkMonitor....139
3.37. LocalUserDatabase....140
3.37.1. Пользователь....140
3.38. Получатель журнала....141
3.38.1. EventReceiverSNMP2c....141
3.38.1.1. EventReceiverSNMP2c....142
3.38.2. LogReceiverMemory....142
3.38.2.1. LogReceiverMessageException....143
3.38.3. LogReceiverSMTP....143
3.38.4. LogReceiverSyslog....144
3.38.4.1. LogReceiverMessageException....144
3.39. NATPool....145
3.40. OSPFProcess....145
3.40.1. OSPFArea....147
3.40.1.1. OSPFInterface....148
3.40.1.2. OSPFNeighbor....149
3.40.1.3. OSPFAggregate....150
3.40.1.4. OSPFVLink....150
3.41. Pipe....151
3.42. PipeRule....153
3.43. PSK....154
3.44. RadiusAccounting....154
3.45. RadiusServer....155

3.46. RealTimeMonitorAlert....155
3.47. RemoteIDList....156
3.48. RemoteManagement....157
3.48.1. RemoteMgmtHTTP....157
3.48.2. RemoteMgmtNetcon....157
3.48.3. RemoteMgmtSNMP....158
3.48.4. RemoteMgmtSSH....158
3.49. RouteBalancingInstance....160
3.50. RouteBalancingSpilloverSettings....160
3.51. RoutingRule....160
3.52. RoutingTable....161
3.52.1. Route....162
3.52.1.1. MonitoredHost....163
3.52.2. SwitchRoute....164
3.53. ScheduleProfile....164
3.54. Service....165
3.54.1. ServiceGroup....165
3.54.2. ScheduleProfile....166
3.54.3. ServiceIPProto....167
3.54.4. ServiceTCPUDP....167
3.55. Settings....168
3.55.1. ARPTableSettings....168
3.55.2. AuthenticationSettings....169
3.55.3. ConnTimeoutSettings....170
3.55.4. DHCPRelaySettings....170
3.55.5. DHCPServerSettings....171
3.55.6. EthernetSettings....172
3.55.7. FragSettings....173
3.55.8. HWMSettings....174
3.55.9. ICMPSettings....175
3.55.10. IPsecTunnelSettings....175
3.55.11. IPSettings....176
3.55.12. L2TPServerSettings....178
3.55.13. LengthLimSettings....179
3.55.14. LocalReassSettings....180
3.55.15. LogSettings....180
3.55.16. MiscSettings....181
3.55.17. MulticastSettings....182
3.55.18. RemoteMgmtSettings....183
3.55.19. RoutingSettings....184
3.55.20. SSLSettings....185
3.55.21. StateSettings....186
3.55.22. TCPSettings....187
3.55.23. VLANSettings....189
3.56. SSHClientKey....189
3.57. ThresholdRule....190
3.57.1. ThresholdAction....190
3.58. UpdateCenter....191
3.59. UserAuthRule....192

Предисловие

Целевая аудитория

Данное руководство предназначено для:

- администраторов, ответственных за настройку и управление межсетевыми экранами D-Link
- администраторов, ответственных за поиск и устранение неисправностей в межсетевых экранах D-Link

При разработке данного руководства предполагалось, что пользователь уже обладает знаниями в области межсетевых экранов D-Link и обеспечения безопасности сети.

Условные обозначения

Для определения опций команды используются следующие условные обозначения:

Угловые скобки <имя> или -опция=<описание>	Используется для *имени* опции или описания значения.
Квадратные скобки <имя> или -опция=<описание>	Указывает на то, что опция или ее значение является *дополнительным* и может быть пропущено.
Фигурные скобки {значение 1 | значение 2 | значение 3}	Указывает на *доступные значения* опции.
Многоточие …	Указывает на то, что для данной опции можно задать *несколько* значений.

Пример 1. Обозначение опций команд

Один из примеров использования команды **справка** выглядит следующим образом:

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

Это означает, что у справки есть опция `category (категория)`, поддерживающая два значения *`COMMANDS КОМАНДЫ`*) и *`TYPES (ТИПЫ)`*. Также существует дополнительная опция `Topic (Тема)`, которая в данном случае является строкой поиска, отображающей тему для справки. Так как данная опция является дополнительной, при выполнении команды ее можно пропустить.

Оба следующих примера являются корректными для использования, описанного выше:

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

Использование команды **routes**:

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

Ни одна из опций команды не является обязательной. У опции `flushl3cache` также есть дополнительное значение. Если значение не указано, будет использоваться значение по умолчанию – *100*.

У следующих двух примеров будет тот же результат:

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

Так как после опции `table` следует многоточие, это означает, что можно указать более одной таблицы маршрутизации. `Table name` является дполнительным, поэтому для таблиц маршрутизации на основе политики можно задать значение «ноль» или более.

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

Глава 1. Введение

- Запуск команды
- Справка
- Функциональные клавиши
- История командной строки
- Функция Tab completion
- Права пользователей

Руководство содержит инструкции по использованию всех команд и типов объектов настройки, доступных в интерфейсе командной строки для NetDefendOS.

1.1. Запуск команды

Команды, описанные в данном руководстве, можно выполнить с помощью ввода имени команды и нажатия клавиши **Return**. Для запуска некоторых команд требуется установить опции. Если необходимая опция пропущена, появится краткая справка.

1.2. Справка

1.2.1. Справка по командам

Существует два способа получения справки. Краткая справка по команде отображается, если после введенного имени команды следует символ «`-?`» или «`-h`». Это применяется ко всем командам, и по этой причине не отображается в списке опций для каждой команды. Использование команды **help** предоставляет более подробную информацию. В большинстве случаев для получения справки можно просто ввести **help**, за которой идет имя команды. Подробная информация о справке содержится в Разделе 2.4.2. Для того чтобы получить список доступных команд, просто введите **help** и нажмите **Return**.

Пример 1.1. Справка по команде

Краткая справка для **активации** команды:

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

Подробная справка для **активации**:

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

Справка по команде **arp**. Arp также является именем объекта настройки, таким образом, необходимо, чтобы отображался текст справки:

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

Список доступных команд:

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

1.2.2. Справка по типам объекта

Для получения справки по типам объекта используйте команду **help**. Также можно получить информацию о каждом параметре типа объекта (например, тип данных, значение по умолчанию и т.д.) с помощью ввода символа «?» после ввода значения параметра и нажатия **tab**. Подробная информация содержится в Разделе 1.5.1, «Справка онлайн».

Пример 1.2. Справка по типам объекта

Подробная справка для `IP4Address`:

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

Справка по типу объекта настройки `ARP`, который совпадает с командой **arp**:

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

1.3. Функциональные клавиши

Помимо клавиши **Return** в CLI используются и другие функциональные клавиши.

Backspace	Удаляет символ слева от курсора.
Tab	Автоматически завершает текущее слово.
Ctrl-A или Home	Перемещает курсор в начало строки.
Ctrl-B или Стрелка влево	Перемещает курсор на символ влево.
Ctrl-C	Удаляет содержимое строки или закрывает страницу, если отображаются несколько страниц.
Ctrl-D или Delete	Удаляет символ справа от курсора.
Ctrl-E или End	Перемещает курсор в конец строки.
Ctrl-F или Стрелка вправо	Перемещает курсор на один символ вправо.
Ctrl-K	Удаляет текст от курсора до конца строки.
Ctrl-N или Стрелка вниз	Отображает следующую запись в истории команды.
Ctrl-P или Стрелка вверх	Отображает предыдущую запись в истории команды.
Ctrl-T	Меняет текущий символ на предыдущий.
Ctrl-U	Удаляет текст от курсора до начала строки.
Ctrl-W	Удаляет слово в обратном направлении.

1.4. История командной строки

Каждый раз после запуска команды в историю добавляется новая запись о командной строке. Клавиши со стрелками вверх и вниз используются для доступа к предыдущим командным строкам (используйте клавишу со стрелкой вверх для перехода к прдедыдущим командным строкам и клавишу со стрелкой вниз для перехода к новой командной строке). Для получения подробной

информации обратитесь в Раздел 2.4.3., «История».

Пример 1.3. История командной строки

Использование клавиш со стрелками:

```
gw-world:/> show Address
gw-world:/> (стрелка вверх)
gw-world:/> show Address (отображается предыдущая командная строка)
```

1.5. Функция Tab completion

Благдаря использованию клавиши **tab** выполняется автоматическое завершение имен команд, опций, объектов, параметров объектов в CLI. Если текст, вводимый до нажатия клавиши **tab**, соответствует возможному термину, например, вводимое “acti” соответствует команде “activate”, которая должна быть выполнена, имя будет автоматически завершено. Для выполнения завершения слова необходимо несколько соответствий. В этом случае пользователь может ввести больше символов и снова нажать клавишу **tab**, при этом отобразится список возможных завершений. Кроме того, завершение можно выполнить без ввода каких-либо символов, но в этом случае список возможных результатов будет слишком большим, например, будет включать все команды.

Пример 1.4. Tab completion

Пример функции tab completion при использовании команды **add**:

```
gw-world:/> add Add (tab)
gw-world:/> add Address ("ress" добавлено автоматически)
gw-world:/> add Address i (tab)
gw-world:/> add Address IP4 ("IP4" добавлено автоматически)
gw-world:/> add Address IP4
        (tab, или двойное нажатие tab, если IP4 вводится вручную)
Отображается список всех типов, начинающихся с IP4.
gw-world:/> add Address IP4a (tab)
gw-world:/> add Address IP4Address ("Address" добавлено автоматически)
gw-world:/> add Address IP4Address example_ip a (tab)
gw-world:/> add Address IP4Address example_ip Address=
        ("Address=" добавлено автоматически)
gw-world:/> add Address IP4Address example_ip Address=1.2.3.4
```

Справка по Tab completion:

```
gw-world:/> set Address IP4Group examplegroup Members= (tab, tab)
Отображается список действующих объектов.
gw-world:/> set Address IP4Group examplegroup Members=e (tab)
gw-world:/> set Address IP4Group examplegroup Members=example_ip
("example_ip" добавлено автоматически)
```

1.5.1. Справка онлайн

Можно получить справку о доступных параметрах объектов настройки, если в командной строке вводится символ «?». Введите «?» вместо имени параметра и нажмите **tab**, появится справка о необходимых параметрах. Если ввести «?» вместо значения параметра и нажать **tab**, появится справка для данного параметра, которая содержит более подробную информацию, включая тип данных, значение по умолчанию и т.д.

Пример 1.5. Справка онлайн

Получение справки онлайн по всем параметрам IP4Address:

```
gw-world:/> set IP4Address example_ip ? (tab)
```

```
Отображается текст справки с описанием всех доступных параметров.
```

Получение справки онлайн для параметра Адрес:

```
gw-world:/> set IP4Address example_ip Address=? (tab)
Отображается подробная информация о параметре Адрес.
```

1.5.2. Автоматическое заполненеие параметров текущими значениями и значениями по умолчанию

При применении функции tab completion также используется символ «.»

Если символ «.» вводится вместо значения свойства, то после нажатия клавиши **tab** произойдет замена данного символа на текущее значение свойства. Данная функция является полезной при редактировании существующего списка объектов или при большом текстовом объеме значения.

Если значения еще не заданы, для автоматического заполнения параметров значениями по умолчанию можно нажать клавишу «<», а затем **tab**. Если используется символ «.», отображаются все возможные значения, которые можно редактировать, используя клавиши со стрелкой назад и backspace.

Пример 1.6. Изменение текущего значения параметра

Изменение текущего значения:

```
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
        (вставленное значение)
Теперь можно изменить значение с помощью клавиш со стрелками или клавиши 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
        (вставленное значение)
Теперь можно добавить или удалить пользователя из списка без ввода всех остальных
участников списка.
```

Изменение значения по умолчанию:

```
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
```

Теперь можно легко удалить уровень важности события для регистрации в журнале.

1.5.3. Настройка категорий типов объектов

Некоторые объекты объединены в категорию в CLI. Это имеет значение только при использовании функции tab completion, так как объекты используются для ограничения числа возможных завершений типов объектов. Если имя типа вводится вручную, при выполнении команды категорию можно пропустить.

Пример 1.7. Использование категорий с функцией tab completion

Доступ к объекту IP4Address с использованием категорий:

```
gw-world:/> show ad (tab)
gw-world:/> show Address (категория добавлена автоматически)
gw-world:/> show Address ip4a (tab)
gw-world:/> show Address IP4Address (тип добавлен автоматически)
```

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

Доступ к объекту IP4Address без использования категорий:

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

1.6. Права пользователей

Пользователь не может выполнять некоторые команды или воспользоваться некоторыми функциями до тех пор, пока не будут получены права Администратора. На необходимость прав Администратора указывает примечание, следующее за командой, или надпись «Только с правами Администратора» рядом с опцией.

Глава 2. Справочная информация по командам

- Настройка
- Работа системы
- Утилита
- Прочее

2.1. Настройка

2.1.1. activate

Активация изменений.

Описание

Активация последних изменений.

Будет выполнено изменение настроек с использованием новой конфигурации. Если изменение настроек прошло успешно, в течение заданного интервала времени появится команда **commit (подтвердить)** для сохранения изменений. Если этого не произойдет, система вернется к предыдущим настройкам.

Использование

```
activate
```

Примечание
Требуются права Администратора

2.1.2. add

Добавление нового объекта.

Описание

Создание нового объекта и его добавление в конфигурацию.

Укажите тип объекта, который необходимо создать, и идентификатор типа, если имеется, кроме случаев, когда объект идентифицируется по индексу. Задайте параметры объекта с помощью ввода имени параметра, знака равенства (=) и значения. При использовании функции tab completion можно указать дополнительную категорию для некоторых типов объектов.

Если обязательный параметр не указан, после создания объекта появится список ошибок. Если

указан некорректный параметр или значение, или пропущен идентификатор, команда не будет выполнена и объект не будет добавлен.

После создания объекта можно внести коррективы, используя команду **set.**

Пример 2.1. Создание нового объекта

```
Добавление объектов с идентификатором (не индексом):
  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

Добавление объекта с индексом:
  gw-world:/main> add Route Interface=lan

Добавление объекта без идентификатора:
  gw-world:/> add DynDnsClientDyndnsOrg DNSName=example Username=example
```

Использование

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

Опции

-force Добавить объект, даже если он содержит ошибки.

-silent Не отображать ошибки.

<Category> Категория, в которую объединены типы объектов.

<Identifier> Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.

<key-value pair> Одна пара или несколько пар «параметр-значение», например, <имя параметра>=<значение> или <имя параметра>= "<значение>".

<Type> Тип объекта настройки для выполнения операции.

Примечание
Требуются права Администратора

2.1.3. cancel

Отмена подтверждения.

Описание

Немедленная отмена подтверждения операции без ожидания истечения таймаута.

Использование

```
cancel
```

Примечание
Требуются права Администратора

2.1.4. cc

Изменение текущего контекста.

Описание

Изменение текущего контекста настройки.

Контекст представляет собой группу объектов, которые зависят от родительского объекта (parent object) и группируются им. Некоторые объекты относятся к «корневому» контексту и у них нет определенного родительского объекта. Другие объекты, например, Объекты пользователей (User objects) относятся к подконтексту (или дочернему контексту (child context)) корня – в данном случае в локальной базе данных пользователя (LocalUserDatabase). Для того чтобы добавить или изменить учетные записи пользователей, необходим корректный контекст, например, локальная база данных пользователя (LocalUserDatabase) под названием "exampledb". Доступ открыт только к объектам текущего контекста.

Пример 2.2. Изменение контекста

Изменение дочернего контекста:
```
  gw-world:/> cc LocalUserDatabase exampledb
  gw-world:/exampledb>
```

Возврат к родительскому контексту:
```
  gw-world:/ospf1/area1> cc ..
  gw-world:/ospf1> cc ..
  gw-world:/>
```

Возвращение к корневому контексту:
```
  gw-world:/ospf1/area1> cc
  gw-world:/>
```
или
```
  gw-world:/ospf1/area1> cc /
  gw-world:/>
```

Использование

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

Изменение текущего контекста.

```
cc -print
```

Печать текущего контекста.

```
cc
```

Замена на корневой контекст.

Опции

-print	Печать текущего контекста.
<Category>	Категория, в которую объединены типы объектов.
<Identifier>	Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.
<Type>	Тип объекта настройки для выполнения операции.

2.1.5. commit

Сохранение новых настроек.

Описание

Сохранение новых настроек. Данная команда выполняется только после успешного завершения команды «активировать».

Использование

```
commit
```

Примечание
Требуются права Администратора

2.1.6. delete

Удаление определенных объектов.

Описание

Удаление определенного объекта из конфигурации.

Добавление флага **force** для удаления объекта, даже если он связан с другими объектами или находится в контексте, у которого есть неудаленные дочерние объекты. Это может привести к тому, что объекты будут ссылаться на определенный объект или на один из дочерних объектов, вследствие чего появятся ошибки, которые необходимо исправить перед активацией настроек.

См. также: **undelete**

Пример 2.3. Удаление объекта

Удаление объекта без связей:
```
gw-world:/> delete Address IP4Address example_ip
```

Удаление объекта со связями:
(вызовет ошибку в examplerule)

```
gw-world:/> set IPRule examplerule SourceNetwork=examplenet
gw-world:/> delete Address IP4Address examplenet -force
```

Использование

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

Опции

-force Удаление объекта даже в случае, если он используется другими объектами или у него есть дочерние объекты.

<Category> Категория, в которую объединены типы объектов.

<Identifier> Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.

<Type> Тип объекта настройки для выполнения операции.

Примечание
Требуются права Администратора

2.1.7. pskgen

Генерирование общего ключа методом случайного выбора.

Описание

Генерирование общего ключа определенного размера, содержащего данные, выбранные в случайном порядке. Если ключ с указанным именем уже существует, он будет изменен. В противном случае будет создан новый ключ.

Использование

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

Опции

-comments=<String> Комментарии для данного ключа.

-size={64 | 128 | 256 | 512 | 1024 | 2048 | 4096} Количество бит данных в сгенерированном ключе (по умолчанию: 64).

<Name> Имя ключа.

Примечание
Требуются права Администратора

2.1.8. reject

Отказ от изменений.

Описание

Отказ от изменений, выполненных на определенном объекте, путем возврата к значениям последней подтвержденной конфигурации.

Все выполненные изменения будут утеряны. Если объект добавлен после последнего подтверждения, он будет удален.

Для отказа от изменений, выполненных на нескольких объектах, используйте либо флаг `-recursive` (для рекурсивного удаления контекста и всех его дочерних объектов) или флаг `-all` (для отказа от изменений, выполненных на *всех* объектах).

См. также: **activate, commit**

Пример 2.4. Отказ от изменений

Отказ от изменений, выполненных на отдельных объектах:

```
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
```

Отказ от изменений рекурсивным методом:
(будет выполнен отказ от изменений в базе данных пользователя и других пользователей)

```
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
```

Отказ от всех изменений:

```
gw-world:/anycontext> reject -all
```

Будет выполнен отказ от всех изменений, выполненных с момента последнего подтверждения:
(example_ip будет удален, так как добавлен недавно)

```
gw-world:/> add IP4Address example_ip Address=1.2.3.4
gw-world:/> delete IP4Address example_ip
gw-world:/> reject IP4Address example_ip
```

Использование

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

Отказ от изменений, выполненных на определенном объекте.

```
reject -all
```

Отказ от всех изменений в настройках.

Опции

-all	Отказ от всех изменений в настройках.
-recursive	Рекурсивный отказ от изменений.
<Category>	Категория, в которую объединены типы объектов.
<Identifier>	Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.
<Type>	Тип объекта настройки для выполнения операции.

Примечание
Требуются права Администратора

2.1.9. reset

Сброс настроек устройства и/или бинарное сообщение.

Описание

Сброс к общим настройкам или использование бинарного сообщения для сброса настроек к заводским по умолчанию.

Использование

```
reset –configuration
```

Сброс настроек к заводским по умолчанию.

```
reset -unit
```

Сброс устройства к заводским настройкам по умолчанию.

Опции

-configuration	Сброс к настройкам по умолчанию.
-unit	Сброс устройства к заводским настройкам по умолчанию.

Примечание
Требуются права Администратора

2.1.10. set

Установка значений свойств.

Описание

Установка значений свойств объектов настройки.

Определение типа объекта, который необходимо изменить, и идентификатора, если имеется. Установите свойства объекта путем ввода символа (=), а затем значения. При использовании функции tab completion можно указать дополнительную категорию для некоторых типов объектов.

Если обязательное свойство не было указано или если в свойстве есть ошибка, после указания свойств появится список ошибок. Если указано некорректное свойство или тип значения, команда не будет выполнена и объект не будет изменен.

См. также: **add**

Пример 2.5. Установка значений свойств

Установка свойств для объекта с идентификатором:

```
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
```

Установка свойства для объекта без идентификатора:

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

Использование

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

Опции

-disable Выключить объект. Эта опция недоступна, если объект уже выключен.

-enable Включить объект. Опция недоступна, если объект уже включен.

<Category> Категория, в которую объединены типы объектов.

<Identifier> Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.

<key-value pair> Одна пара или несколько пар «параметр-значение», например, <имя параметра>=<значение> или <имя параметра>= "<значение>".

<Type> Тип объекта настройки для выполнения операции.

Примечание
Требуются права Администратора

2.1.11. show

Отображение объектов.

Описание

Отображение объектов.

Отображение свойств определенного объекта. Существует несколько флагов, которые необходимо установить, в противном случае, свойства буду скрыты. Для отображения категорий и типов объектов, доступных в текущем контексте, просто введите show. При указании типа или категории будет отображаться таблица всех объектов типа. Используйте флаги `-errors` или `-changes` для отображения объектов, которые были изменены или у которых есть ошибки в конфигурации.

В таблице объектов определенного типа указывается статус каждого объекта последнего подтверждения конфигурации, при этом используются следующие флаги:

- **-** Объект удален.
- **o** Объект выключен.
- **!** У объекта есть ошибки.
- **+** Недавно созданный объект.
- ***** Объект изменен.

Дополнительные флаги:

D В списке категорий и типов объекта категрии обозначаются с помощью [], а типы – /.

Пример 2.6. Отображение объектов

Отображение совойств отдельного объекта:
```
gw-world:/> show Address IP4Address example_ip
gw-world:/main> show Route 1
gw-world:/> show Client DynDnsClientDyndnsOrg
```

Отображение таблицы всех типов объектов и выбор их свойств, а также статуса:
```
 gw-world:/> show Address IP4Address
gw-world:/> show IP4Address
```

Отображение таблицы всех объектов для каждого типа в категории:
```
gw-world:/> show Address
```

Отображение объектов с изменениями и с ошибками:
```
gw-world:/> show -changes
gw-world:/> show -errors
```

Отображение объектов, которые ссылаются на определенный объект:
```
gw-world:/> show Address IP4Address example_ip -references
```

Использование

```
show
```

Отображение типов и категорий, доступных в текущем контексте.

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

Отображение объекта или списка типа или категории.

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

Отображение всех ошибок.

```
show -changes
```

Отображение всех изменений.

Опции

-changes	Отображение всех изменений в текущей конфигурации.
-disabled	Отображение выключенных свойств.
-errors	Отображение всех ошибок в текущей конфигурации.
-references	Отображение всех связей с другими объектами.
-verbose	Подробная информация.
<Category>	Категория, в которую объединены типы объектов.
<Identifier>	Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.
<Type>	Тип объекта настройки для выполнения операции.

2.1.12. undelete

Восстановление удаленных объектов.

Описание

Восстановление удаленных объектов.

Восстановление объектов возможно до момента включения команды «activate».

См. также: **delete**

Пример 2.7. Восстановление объекта

Восстановление объекта без связей:

```
gw-world:/> delete Address IP4Address example_ip
gw-world:/> undelete Address IP4Address example_ip
```

Восстанволение объекта со связями:
(удалит ошибку в examplerule)

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

Использование

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

Опции

<Category> Категория, в которую объединены типы объектов.

<Identifier> Параметр, определяющий объект конфигурации. Применение зависит от указанного <Типа>.

<Type> Тип объекта настройки для выполнения операции.

Примечание
Требуются права Администратора

2.2. Работа системы

2.2.1. Информация об устройстве

Отображение авторских прав/информации о сборке.

Описание

Отображение авторских прав и информации о сборке.

Использование

```
about
```

2.2.2. alarm

Отображение информации о предупреждениях об опасности.

Описание

Отображение списка текущих активных предупреждений об опасности.

Использование

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

Опции

-active Отображает текущие активные предупреждения об опасности.

-history Отображает 20 последних предупреждений об опасности.

2.2.3. arp

Отображение записей ARP для данного интерфейса.

Описание

Список записей кэша ARP для определенных интерфейсов.

Если нет интерфейса, будут представлены записи кэша ARP для всех интерфейсов.

Можно выполнить фильтрацию представленного списка, используя опции *ip* и *hw*.

Использование

```
arp
```

Отображение всех записей ARP.

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

Отображение записей ARP.

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

Отображение информации о состоянии в хеш-таблице.

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

Очистка кэша ARP на определенном интерфейсе.

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

Отправка самообращенных ARP (gratuitous ARP) для IP-адреса.

Опции

-flush	Очистка кэша ARP на определенных интерфейсах.
-hashinfo	Отображение информации о состоянии в хеш-таблице.
-hw=<pattern>	Отображение только соответствующих образцу адресов устройства.
-hwsender=<Ethernet Address>	Ethernet-адрес отправителя.
-ip=<pattern>	Отображение только соответствующих образцу IP-адресов.
-notify=<ip>	Отправка самообращенных ARP (gratuitous ARP) для <ip>
-num=<n>	Отображение только первых записей <n> на один интефейс. По умолчанию: 20.
-show	Отображение записей ARP для данного интерфейса (-ов).
<Interface>	Имя интерфейса.

2.2.4. arpsnoop

Включение snooping и отображение запросов ARP.

Описание

Включение snooping и отображение запросов ARP и ответов на экране.

Отобранные (snooped) сообщения отображаются до того, как в отделе доступа будут подтверждены IP-адреса отправителя в данных ARP.

Использование

```
arpsnoop
```

Отображение интерфейсов, на которых запущен snoop.

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

Запустить snoop на определенном интерфейсе.

Опции

-verbose	Подробная информация.
{ALL | NONE | <interface>}	Имя интерфейса.

2.2.5. ats

Отображение активных ARP-транзакций.

Описание

Отображение активных ARP-транзакций.

Использование

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

Опции

-num=<n>	Ограничение списка до <n> записей. По умолчанию: 20.

2.2.6. blacklist

«Черный» список.

Описание

Блокировка и отмена блокировки узлов из «черного» и «белого» списков.

Примечание: Невозможно разблокировать статические IP-адреса узлов из «черного» списка.

Если опция `-force` не задана, можно разблокировать только узел с определенным сервисом, протоколом/портом и назначением.

Пример 2.8. Блокировка узлов

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

Использование

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

Отображение информации об узлах, занесенных в «черный» список.

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

Блокировка определенного сетевого объекта.

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

Отмена блокировки определенного сетевого объекта.

Опции

-all	Отображение всей информации.
-black	Отображение только узлов из «черного» списка.
-block	Блокировка определенного сетевого объекта (Только с правами Администратора).
-creationtime	Отображение времени создания.
-dest=<ip address>	Адрес назначения, который необходимо заблокировать/разблокировать (установка флага ExceptExtablished).
-dynamic	Отображение только динамических IP-адресов узлов.
-force	Отмена блокировки всех сервисов для узла, соответствующих опциям.
-info	Отображение подробной информации.
-listtime	Время в списке (для динамических IP-адресов узлов).
-port=<port number>	Номер порта для блокировки/отмены блокировки.
-prot={TCP | UDP | ICMP | OTHER | TCPUDP | ALL}	Протокол для блокировки/отмены блокировки.
-serv=<service>	Сервис для блокировки/отмены блокировки.
-show	Отображение информации об узлах, занесенных в «черный» список.

-time=<seconds>	Время, в течение которого узел будет оставаться заблокированным.
-unblock	Отмена блокировки определенного сетевого объекта (Только с правами Администратора).
-white	Отображение только узлов из «белого» списка.
<host>	Диапазон IP-адресов.

2.2.7. buffers

Список буферов пакетов или содержимого буферов.

Описание

Список, состоящий из 20 наиболее часто используемых буферов, или подробная информация об определенном буфере.

Использование

```
buffers
```

Список из 20 наиболее часто используемых буферов.

```
buffers -recent
```

Наиболее часто используемых буферов.

```
buffers <Num>
```

Номер буфера.

Опции

-recent	Наиболее часто используемые буферы.
<Num>	Номер буфера.

2.2.8. cam

Информация о таблице CAM.

Описание

Отображение информации о таблице (-ах) CAM и содержащихся в ней записях.

Использование

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

Отображение информации о таблице CAM.

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

Отображение информации о таблице CAM для указанного интерфейса.

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

Очистка таблицы CAM для указанного интерфейса.

```
cam -flush
```

Очистка таблицы CAM.

Опции

-flush	Очистка таблицы CAM. Если указан интерфейс, будут удалены только записи для данного интерфейса (Только с правами Администратора).
-num=<n>	Ограничение списка до <n> записей на таблицу CAM. По умолчанию: 20.
<Interface>	Интерфейс.

2.2.9. certcache

Отображение содержимого кэша сертификатов.

Описание

Отображение всех сертификатов из кэша.

Использование

```
certcache
```

2.2.10. cfglog

Отображение журнала настроек.

Описание

Отображение журнала с момента последней попытки чтения настроек.

Использование

```
cfglog
```

2.2.11. connections

Список соединений с отслеживаемым состоянием.

Описание

Список соединений с отслеживаемым состоянием.

Использование

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

Список соединений.

```
connections
```

Отображение соединений.

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

Завершение соединений.

Опции

-all	Отметить все соединения.
-close	Завершить все соединения, соответствующие FilterExpression (Только с правами Администратора).
-destiface=<interface>	Фильтрация на интерфейсе назначения.
-destip=<ip addr>	Фильтрация IP-адреса назначения.
-destport=<port>	Отображение только указанного TCP/UDP-порта назначения.
-num=<n>	Ограничение списка до <n> соединений. По умолчанию: 20.
-protocol=<name/num>	Отображение только указанного IP-протокола.
-show	Отображение соединений.
-srciface=<interface>	Фильтрация на интерфейсе источника.
-srcip=<ip addr>	Фильтрация IP-адреса источника.
-srcport=<port>	Отображение только указанного TCP/UDP-порта источника.
-verbose	Подробная информация.

2.2.12. cpuid

Отображение информации о CPU.

Описание

Отображение модели и производителя CPU компьютера.

Использование

```
cpuid
```

2.2.13. crashdump

Отображение содержимого файла crash.dmp.

Описание

Отображение содержимого файла crash.dmp, если есть.

Использование

```
crashdump
```

2.2.14. cryptostat

Отображение информации о крипто-акселераторах.

Описание

Отображение информации об установленных крипто-акселераторах.

Использование

```
cryptostat
```

2.2.15. dconsole

Отображение содержимого консоли диагностики.

Описание

Консоль диагностики используется для поиска и устранения внутренних неисправностей шлюза безопасности.

Использование

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

Опции

-clean Удаление всех записей диагностики (Только с правами Администратора).

-date=<date>	ДД-ММ-ГГ. Отображение записей только от данного числа и далее.
-flush	Удаление всех записей диагностики на диске (Только с правами Администратора).
-onlyhigh	Отображение записей только с высоким уровнем важности (Только с правами Администратора).

2.2.16. dhcp

Отображение информации об интерфейсах, на которых запущен DHCP, или информации об изменении/обновлении сроков аренды IP-адресов.

Описание

Отображение информации об интерфейсах, на которых запущен DHCP.

Использование

```
dhcp
```

Список интерфейсов, на которых запущен DHCP.

```
dhcp -list
```

Список интерфейсов, на которых запущен DHCP.

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

Отображение информации об интерфейсе, на котором запущен DHCP.

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

Изменение сроков аренды интерфейса.

Опции

-lease={RENEW | RELEASE}	Изменение сроков аренды интерфейса.
-list	Список всех интерфейсов, на которых запущен DHCP.
-show	Отображение информации о всех интерфейсах, на которых запущен DHCP.
<interface>	Интерфейс DHCP.

2.2.17. dhcprelay

Отображение набора правил DHCP/BOOTP relayer.

Описание

Отображение содержимого набора правил DHCP/BOOTP relayer и DHCP relay, маршрутизируемый в

настоящее время.

Отображаемый фильтр выполняет фильтрацию рентрансляторов на основе IP-адреса/интерфейса (например: адрес интерфейса 1: 192.168.*)

Использование

```
dhcprelay
```

Отображение текущих ретранслируемых DHCP-сессий.

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

Отображение набора правил DHCP/BOOTP relayer.

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

Завершение ретранслируемой сессии.

Опции

-interface=<Interface>	Интерфейс.
-release	Завершение ретранслируемой сессии <[interface:]ip>. (Только с правами Администратора).
-routes	Отображение текущих ретранслируемых DHCP-сессий.
-rules	Отображение набора правил DHCP/BOOTP relayer.
-show	Отображение набора правил.
<display filter>	Отображение фильтра, выполняющего фильтрацию рентрансляторов на основе IP-адреса/интерфейса.
<ip address>	IP-адрес.

2.2.18. dhcpserver

Отображение набора правил DHCP-сервера.

Описание

Отображение содержимого набора правил DHCP-сервера, а также различной информации об активных/неактивных сроках арендах.

Отображаемый фильтр выполняет фильтрацию рентрансляторов на основе IP-адреса/интерфейса (например: адрес интерфейса 1: 192.168.*)

Использование

```
dhcpserver
```

Отображение срока аренды адресов, выдаваемых DHCP-сервером.

```
dhcpserver -show [-rules] [-leases] [-num=<Integer>]
           [-fromentry=<Integer>] [-mappings] [<display filter>]...
```

Отображение набора правил DHCP-сервера.

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

Отказ от определенных типов IP-адресов.

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

Откза от активного IP-адреса.

Опции

-fromentry=<Integer>	Список сроков аренды IP-адресов, выдаваемых DHCP-сервером, <n>.
-leases	Отображение сроков аренды IP-адресов, выдаваемых DHCP-сервером.
-mappings	Отображение текущих ретранслируемых DHCP-сессий.
-num=<Integer>	Ограничение списка до <n>.
-release={BLACKLIST}	Отказ от определенных типов IP-адресов (Только с правами Администратора).
-releaseip	Отказ от активного IP-адреса (Только с правами Администратора).
-rules	Отбражение правил DHCP-сервера.
-show	Отображение набора правил.
<display filter>	Фильтры для фильтрации сроков аренды на основе IP/MAC/интерфейса (например, адрес интерфейса 1: 192.168.*)
<interface>	Интерфейс.
<ip address>	IP-адрес.

2.2.19. dns

DNS-клиент и запросы.

Описание

Отображение статуса DNS-клиента и управление текущими DNS-запросами.

Использование

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

Опции

-list	Список текущих DNS-запросов.
-query=<domain name>	Преобразование доменного имени.
-remove	Удаление всех текущих DNS-запросов.

2.2.20. dnsbl

DNSBL.

Описание

Отображение статуса DNSBL.

Использование

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

Опции

-clean	Очистка статистики DNSBL для ALG.
-show	Отображение статистики DNSBL для ALG.
<SMTP ALG>	Имя SMTP ALG.

2.2.21. dynroute

Отображение политики динамической маршрутизации.

Описание

Отображение набора правил фильтрации политики динамической маршрутизации и текущего экспорта.

В поле «Флаги» экспорта динамической маршрутизации используются следующие буквы:

o Оптимальный маршрут к сети

u Маршрут не экспортирован

Использование

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

Опции

-exports	Отображение текущего экспорта.
-rules	Отображение динамической маршрутизации, набора правил фильтрации.

2.2.22. frags

Отображение активной сборки фрагментов.

Описание

Список активных повторных сборок фрагментов.

Можно получить более подробную информацию о повторной сборке:

NEW Последняя сборка

ALL Все сборки

0..1023 Сборка 'N'

Пример 2.9. frags

```
frags NEW
frags 254
```

Использование

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

Опции

-done	Список выполненных повторных сборок.
-free	Список выключенных вместо активных.
-num=<n>	Количество записей в списке <n>. По умолчанию: 20.
{NEW | ALL | <reassembly id>}	Подробная информация о сборке <n>. По умолчанию: all (все).

2.2.23. ha

Текущий статус HA.

Описание

Отображение текущего статуса HA.

Использование

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

Опции

-activate	Активировать
-deactivate	Отменить активацию

2.2.24. hostmon

Отображение статистики по мониторингу узла.

Описание

Отображение активных сессий мониторинга узла.

Использование

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

Опции

-num=<n>	Ограничение списка до <n> записей. По умолчанию: 20.
-verbose	Подробная информация.

2.2.25. httpalg

Команды, связанные с HTTP Application Layer Gateway.

Описание

Отображение информации о кэше WCF или списка узлов, прошедших фильтрацию WCF.

Использование

```
httpalg -override [-flush]
```

Список узлов, прошедших фильтрацию wcf.

```
httpalg -wcfcache [-show] [-url=<String>] [-flush] [-verbose]
         [-count] [-server[={STATUS | CONNECT | DISCONNECT}]]
         [-num=<n>]
```

Отображение информации о кэше URL.

Опции

-count	Количество кэш-файлов.
-flush	Удаление всех записей.
-num=<n>	Ограничение списка до <n> записей. По умолчанию: 20.
-override	Список узлов, прошедших фильтрацию wcf.
-server[={STATUS | CONNECT | DISCONNECT}]	Опции сервера фильтрации Web-содержимого. По умолчанию: status (статус).

-show	Отображение данных кэша фильтрации Web-содержимого.
-url=<String>	Ограничение выходных данных команды «show» до данных, соответствующих определенным символам.
-verbose	Подробная информация.
-wcfcache	Отображение статистики по функционалу WCF.

2.2.26. httpposter

Отображение статуса HTTPPoster_URLx.

Описание

Отображение настроек и статуса настроенных целевых объектов HTTPPoster_URLx.

Использование

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

Опции

-display	Отображение статуса.
-repost	Повторная запись всех URL-адресов (Только с правами Администратора).

2.2.27. hwaccel

Список настроенных аппаратных ускорителей (Hardware Accelerators).

Описание

Отображение информации о настроенных аппаратных ускорителях (Hardware Accelerators).

Использование

```
hwaccel
```

2.2.28. hwm

Отображение статуса датчика.

Описание

Отображение статуса датчика.

Использование

```
hwm [-all] [-verbose]
```

Опции

-all	Отображение ВСЕХ датчиков. ПРЕДУПРЕЖДЕНИЕ: Обратите внимание на то, что копирование высокоскоростных интерфейсов может занять длительное время.
-verbose	Подробная информация: отображение типа номера, типа и ограничений датчика.

2.2.29. idppipes

Отображение и удаление узлов, подключенных к провайдеру.

Описание

Отображение списка узлов, подключенных в настоящее время.

Использование

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

Список узлов, для которых провайдер устанавливает новые соединения.

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

Прекращение отправки соединений в канал для определенного узла.

Опции

-all	Отметить все узлы.
-host=<ip addr>	Фильтрация IP-адреса источника.
-show	Список узлов, для которых провайдер устанавливает новые соединения.
-unpipe	Прекращение отправки соединений в канал для определенного узла (Только с правами Администратора).

2.2.30. ifstat

Отображение статистики по интерфейсу.

Описание

Отображение списка подключенных интерфейсов или подробной информации об определенном интерфейсе.

Использование

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

Опции

-allindepth	Отображение подробной информации обо всех интерфейсах.
-filter=<expr>	Список фильтрации интерфейсов.
-num=<n>	Ограничение списка до <n> строк. По умолчанию: 20.
-pbr=<table name>	Список только участников PBR-таблицы (таблиц).
-restart	Остановка и перезапуск интерфейса (Только с правами Администратора).
<Interface>	Имя интерфейса.

2.2.31. igmp

Интерфейсы IGMP.

Описание

Отображение информации о текущем состоянии интерфейсов IGMP.

Отправка на интерфейс ложных сообщений для проверки настроек.

Использование

```
igmp
```

Печать текущего состояния IGMP.

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

Печать текущего состояния IGMP. Если указан интерфейс, отображается более подробная информация.

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

Ложное входящее сообщение IGMP query.

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

Ложное входящее сообщение IGMP join для присоединения.

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

Ложное входящее сообщение IGMP leave для отключения.

Опции

-join	Ложное входящее сообщение IGMP join для присоединения.
-leave	Ложное входящее сообщение IGMP leave для отключения.

-query	Ложное входящее сообщение IGMP query.
-state	Отображение текущего состояния IGMP.
<host address>	IP-адрес узла.
<Interface>	Интерфейс.
<MC address>	Адрес многоадресной рассылки.
<router address>	IP-адрес маршрутизатора.

2.2.32. ikesnoop

Включение или выключение IKE-snooping.

Описание

Включение/выключение IKE-snooping. Используется для поиска и устранения неисправностей IPsec-соединений.

Использование

```
ikesnoop
```

Отображение статуса IKE snooping.

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

Включение IKE snooping.

```
ikesnoop -off
```

Выключение IKE snooping.

Опции

-off	Выключение IKE snooping.
-on	Включение IKE snooping.
-verbose	Включение IKE snooping с подробными выходными данными.
<ip address>	IP-адрес для отслеживания.

2.2.33. ippool

Отображение информации о пуле IP-адресов.

Описание

Отображение информации о текущем состоянии пулов IP-адресов.

Использование

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

Принудительное освобождение IP-адреса, назначенного подсистеме.

```
ippool -show [-verbose] [-max=<n>]
```

Отображение информации о пуле IP-адресов.

Опции

-all	Освободить все IP-адреса.
-max=<n>	Ограничение списка до <n> записей. По умолчанию: 10.
-release	Принудительное освобождение IP-адреса, назначенного подсистеме (Только с правами Администратора).
-show	Отображение информации о пуле IP-адресов.
-verbose	Подробная информация.
<ip address>	IP-адрес, который необходимо освободить.

2.2.34. ipsecglobalstats

Отображение общей статистики ipsec.

Описание

Отображение информации о текущем состоянии пулов IP-адресов.

Использование

```
ipsecglobalstats [-verbose]
```

Опции

-verbose	Подробная информация.

2.2.35. ipseckeepalive

Отображение статуса механизма keepalives IPsec ping.

Описание

Отображение статуса механизма keepalives IPsec ping.

Использование

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

Опции

-num=<n>	Максимальное количество отображаемых записей (по умолчанию: 48).

2.2.36. ipsecstats

Отображение используемых безопасных ассоциаций (Security Associations, SA).

Описание

Список текущих активных IKE и IPsec SA, дополнительно отображается только SA соответствующая образцу, предоставленному для параметра «tunnel».

Использование

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

Опции

-force	Обход подтверждения.
-ike	Отображение IKE SA.
-ipsec	Отображение IPsec SA.
-num={ALL | <Integer>}	Максимальное количество отображаемых записей. По умолчанию: 40/8.
-usage	Отображение подробной информации о статистике SA.
-verbose	Подробная информация.
<tunnel>	Отображение только SA, соответствующей образцу.

2.2.37. ipsectunnels

Список текущих настроек IPsec.

Описание

Список текущих настроек IPsec.

Использование

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

Отображение определенного интерфейса.

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

Отображение определенного номера.

```
ipsectunnels
```

Отображение интерфейсов.

Опции

-force	Обход подтверждения.
-iface=<recv iface>	Интерфейс IPsec, информацию о котором необходимо отобразить.
-num={ALL | <Integer>}	Максимальное количество отображаемых записей. По умолчанию: 40.

2.2.38. killsa

Удаление всех SA, принадлежащих указанному удаленному SG/узлу.

Описание

Удаление всех SA (IPsec и IKE), связанных с указанным удаленным узлом, или дополнительно всех SA в системе. Отправлены IKE-сообщения об удалении.

Использование

```
killsa <ip address>
```

Удаление SA, принадлежащих указанному/удаленному SG/узлу.

```
killsa -all
```

Удаление всех SA.

Опции

-all	Удаление всех SA.
<ip address>	IP-адрес удаленного SG/узла.

Примечание
Требуются права Администратора

2.2.39. languagefiles

Управление языковыми файлами на диске.

Описание

Управление языковыми файлами на диске.

Использование

```
languagefiles
```

Отображение всех языковых файлов на диске.

```
languagefiles -remove=<String>
```

Удаление языкового файла с диска.

Опции

-remove=<String>	Укажите языковой файл для удаления.

2.2.40. ldap

Информация о LDAP.

Описание

Статистика и статус настроенных баз данных LDAP.

Использование

```
ldap
```

Список всех баз данных LDAP.

```
ldap -list
```

Список всех баз данных LDAP.

```
ldap -show [<LDAP Server>]
```

Отображение статистики и статуса базы данных LDAP.

```
ldap -reset [<LDAP Server>]
```

Сброс базы данных LDAP.

Опции

-list	Список всех баз данных LDAP.
-reset	Статус сброса базы данных LDAP.
-show	Отображение статуса и статистики.
<LDAP Server>	База данных LDAP.

2.2.41. license

Отображение содержимого файла лицензии.

Описание

Отображение содержимого файла лицензии.

Использование

```
license [-remove]
```

Опции

-remove	Удаление файла лицензии со шлюза безопасности (Только с правами Администратора).

2.2.42. linkmon

Отображение статистики мониторинга соединения.

Описание

Если настроены узлы для мониторинга соединения, linkmon позволит выполнить мониторинг доступности узла для того, чтобы обнаружить проблемы соединения/ NIC.

Использование

```
linkmon
```

2.2.43. lockdown

Включить/выключить блокировку.

Описание

При локальной блокировке разрешена передача только трафика от администратора. Весь остальной трафик будет отброшен.

Блокировка не повлияет на трафик, который согласно набору правил не будет передаваться, например, трафик, разрешенный правилами IPsecBeforeRules, NetconBeforeRules, SNMPBeforeRules, если данные настройки включены.

Примечание: Если локальная блокировка установлена на уровне ядра по причине проблем, связанных с лицензией/настройками, данная команда НЕ удалит подобную блокировку.

Использование

```
lockdown
```

Отображение статуса блокировки.

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

Включить/выключить блокировку.

Опции

{ON | OFF}	Включить/Выключить блокировку.

Примечание
Требуются права Администратора

2.2.44. logout

Выход пользователя.

Описание

Выход текущего пользователя.

Использование

```
logout
```

2.2.45. memory

Отображение информации о состоянии памяти.

Описание

Отображение занятости оперативной памяти. Также отображается подробная информация о количестве памяти, занимаемом списками и компонентами.

Использование

```
memory
```

2.2.46. natpool

Отображение текущих пулов NAT.

Описание

Отображение текущих пулов NAT и подробной информации.

Использование

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

Опции

-num=<Integer>	Максимальное количество объектов в списке. По умолчанию: 20.
-verbose	Подробная информация.
<IP4 Address>	Преобразованный IP-адрес.
<pool name>	Имя пула NAT.

2.2.47. netcon

Список всех пользователей NetCon.

Описание

Отображение списка всех подключенных пользователей NetCon.

Использование

```
netcon
```

2.2.48. netobjects

Отображение значений сетевых объектов для рабочего использования.

Описание

Отображение сетевых объектов с именами и их содержимого.

Пример 2.10. Список сетевых объектов, содержащих в имени «net».

```
netobjects *net*
```

Использование

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

Опции

-num=<num>	Количество отображаемых записей. По умолчанию: 20.
<String>	Имя или шаблон.

2.2.49. ospf

Отображение информации о OSPF.

Описание

Отображение информации о процессе (-ax) маршрутизатора OSPF.

Примечание: `-process` требуется только при наличии более одного процесса маршрутизатора OSPF.

Использование

```
ospf
```

Отображение информации о выполнении.

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

Отображение информации об интерфейсе.

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

Отображение информации об области OSPF Area.

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

Отображение информации о соседних устройствах.

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

Отображение таблицы маршрутизации (routingtable) внутренних процессов OSPF.

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

Отображение базы данных LSA.

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

Отображение подробной информации об определенном LSA.

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

Отображение сообщений поиска и устранения неисправностей в консоли.

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

Отключение определенного интерфейса.

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

Включение определенного интерфейса.

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

Запуск/остановка/перезапуск процесса OSPF.

Опции

-area	Отображение информации области OSPF Area.
-database	Отображение базы данных LSA.

-execute={STOP | START | RE-START}	Запуск/остановка/перезапуск процесса OSPF (Только с правами Администратора).
-iface	Отображение информации об интерфейсе.
-ifacedown	Отключение определенного интерфейса (Только с правами Администратора).
-ifaceup	Включение определенного интерфейса (Только с правами Администратора).
-lsa	Отображение подробной информации об определенном LSA.
-neighbor	Отображение информации о соседних устройствах.
-process=<OSPF Router Process>	Требуется только при наличии более одного процесса маршрутизатора OSPF.
-route	Отображение таблицы маршрутизации (routingtable) внутренних процессов OSPF.
-snoop={ON | OFF}	Отображение сообщений поиска и устранения неисправностей в консоли.
-verbose	Подробная информация.
<interface>	Интерфейс, на котором включен OSPF.
<lsaID>	LSA ID.
<OSPF Area>	OSPF Area.
<OSPF Neighbor>	Соседнее устройство.
{HA | ALT}	Отображение таблицы маршрутизации HA.

2.2.50. pcapdump

Захват пакетов.

Описание

Механизм захвата пакетов.

Использование

```
pcapdump
```

Отображение статуса захвата.

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

Запуск захвата.

```
pcapdump -stop [<interface(s)>]
```

Остановка захвата.

```
pcapdump -status
```

Отображение статуса захвата.

```
pcapdump -show [<interface(s)>]
```

Отображение краткой информации о захваченных пакетах.

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

Запись захваченных пакетов на диск.

```
pcapdump -wipe
```

Удаление всех захваченных пакетов из памяти.

```
pcapdump -cleanup
```

Удаление всех захваченных пакетов, отключение режима захвата и удаление всех записанных файлов с диска.

Опции

-cleanup	Удаление всех захваченных пакетов, отключение режима захвата и удаление всех записанных файлов с диска.
-count=<value>	Количество пакетов для захвата.
-destport=<0...65535>	Фильтрация по TCP/UDP-порту назначения.
-eth=<Ethernet Address>	Фильтрация по Ethernet-адресу.
-ethdest=<Ethernet Address>	Фильтрация по Ethernet-адресу назначения.
-ethsrc=<Ethernet Address>	Фильтрация по Ethernet-адресу источника.
-filename=<String>	Имя файла для захвата.
-icmp	Фильтр ICMP.
-ip=<IP4 Address>	Фильтрация по IP-адресу.
-ipdest=<IP4 Address>	Фильтрация по IP-адресу назначения.
-ipsrc=<IP4 Address>	Фильтрация по IP-адресу источника.
-out	Краткая информация о пакете в реальном времени, выгруженная в консоль.
-out-nocap	Краткая информация о пакете, не помещенная в буфер (не хранящаяся в памяти) и выгруженная в консоль.
-port=<0...65535>	Фильтрация по TCP/UDP-порту.
-promisc	Задать интерфейс в неизбирательном режиме.
-proto=<0...255>	Фильтрация по IP-протоколу.

-show	Отображение краткой информации о захваченных пакетах.
-size=<value>	Размер (кб) буфера для хранения захваченных пакетов (по умолчанию: 512 кб).
-snaplen=<value>	Максимальная длина каждого пакета для захвата.
-srcport=<0...65535>	Фильтрация по TCP/UDP-порту источника.
-start	Запуск захвата.
-status	Отображение статуса захвата.
-stop	Остановка захвата.
-tcp	Фильтр TCP.
-udp	Фильтр UDP.
-wipe	Удаление всех захваченных пакетов из памяти.
-write	Запись захваченных пакетов на диск.
<interface(s)>	Имя интерфейса (-ов).

Примечание
Требуются права Администратора.

2.2.51. pciscan

Отображение обнаруженных устройств PCI.

Описание

Отображение обнаруженных устройств.

Использование

```
pciscan
```

Отображение идентифицированных устройств ethernet.

```
pciscan -all
```

Отображение всех обнаруженных устройств.

```
pciscan -ethernet
```

Отображение всех обнаруженных устройств ethernet.

```
pciscan -cfgupdate
```

Обновление конфигурационного файла при обнаружении устройств.

```
pciscan -force_driver <Integer> {BROADCOM | BNE2 | E100 | E1000 |
       R8139 | MARVELL | NITROXII | ST201 | TULIP | X3C905}
```

Установить определенный драйвер на устройство.

Опции

-all	Отображение всех обнаруженных устройств.
-cfgupdate	Обновление конфигурационного файла при обнаружении устройств (Только с правами Администартора).
-ethernet	Отображение всех обнаруженных устройств ethernet.
-force_driver	Установить определенный драйвер на устройство (Только с правами Администартора).
<Integer>	Индекс устройства для обновления.
{BROADCOM | BNE2 | E100 | E1000 | R8139 | MARVELL | NITROXII | ST201 | TULIP | X3C905}	Используемый драйвер.

2.2.52. pipes

Отображение информации о каналах.

Описание

Отображение списка установленных каналов/подробной информации о каналах/пользователях каналов.

Примечание: Команда «pipes» не выполняется сразу, она помещается в очередь до момента завершения расчетов значений канала.

Использование

```
pipes
```

Список всех каналов.

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

Список пользователей указанного канала.

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

Отображение подробной информации о канале.

Опции

-expr=<String>	Метод подстановки wildcard (*).
-show	Отображение подробной информации о канале.

-users	Список пользователей указанного канала.
<Pipe>	Отображение подробной информации о канале.

2.2.53. pptpalg

Отображение информации PPTP ALG.

Описание

Отображение информации и статисики PPTP ALG.

Использование

```
pptpalg
```

Отображение всех настроенных PPTP ALG.

```
pptpalg -sessions <PPTP ALG> [-verbose] [-num=<Integer>]
```

Список всех сессий PPTP.

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

Список всех сервисов, закрепленных за PPTP ALG.

Опции

-num=<Integer>	Количество записей в списке.
-services	Список всех сервисов, закрепленных за PPTP ALG.
-sessions	Список всех сессий с использованием PPTP-туннеля.
-verbose	Подробные выходные данные.
<PPTP ALG>	PPTP ALG.

2.2.54. reconfigure

Инициация изменения настроек.

Описание

Запуск шлюза безопасности с использованием текущих активных настроек.

Использование

```
reconfigure
```

Примечание
Требуются права Администратора.

2.2.55. routemon

Список шлюзов и интерфейсов, контролируемых на данный момент.

Описание

Список шлюзов /или интерфейсов, контролируемых на данный момент.

Использование

```
routemon
```

2.2.56. routes

Отображение списков маршрутизации.

Описание

Отображение информации о таблице (-ах) маршрутизации.

- Содержимое таблицы маршрутизации (имя).

- Список таблиц маршрутизации, включая общее количество записей маршрутов в каждой таблице и количество записей маршрутов к отдельным узлам.

Помните, что маршруты «core» не отображаются корректным образом. Для корректного отображения необходимо использовать `-all`.

Используйте `-switched` для отображения только коммутируемых маршрутов.

Значение поля с флагами таблицы маршрутизации:

O Изучено через OSPF

X Маршрут выключен

M Маршрут контролируется

A Опубликовано через Proxy ARP

D Динамический (например, DHCP relay, IPsec, L2TP/PPP-серверы и т.д.)

H Выполнена синхронизация HA с узла кластера

Использование

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

Опции

-all	Отображение маршрутов для интерфейса.
-flushl3cache	Flush Layer 3 Cache.
-lookup=<ip address>	Поиск маршрута для указанного IP-адреса.
-nonhost	Не отображать маршруты к отдельному узлу.
-num=<n>	Ограничение количества отображаемых записей до <n>. По умолчанию: 20.
-switched	Отображение только коммутируемых маршрутов и записей L3C.
-tables	Отображение списка таблиц маршрутизации (PBR)
-verbose	Подробная информация.
<table name>	Имя таблицы маршрутизации.

2.2.57. rtmonitor

Информация о мониторинге, выполняемом в реальном времени.

Описание

Отображение информации об объектах, за которыми ведется наблюдение в реальном времени, а также сигналах тревоги.

Отображаются все объекты, прошедшие фильтрацию. Фильтрация может выполняться по имени объекта или началу имени. Если фильтр не указан, отображаются все объекты.

Если указана опция «monitored», отображаются только объекты, с которых поступил сигнал тревоги при выполнении мониторинга в реальном времени.

Пример 2.11. Отображение всех объектов, за которыми ведется наблюдение в категории alg/http

```
gw-world:/> rtmonitor alg/http -m
```

Использование

```
rtmonitor [<filter>] [-terse] [-monitored]
```

Опции

-monitored	Отображение только объектов, за которыми ведется наблюдение.

-terse	Отображение только имени объекта.
<filter>	Фильтрация.

2.2.58. rules

Отображение списков правил.

Описание

Отображение содержимого правил различных типов, например, основного набора правил, набора правил канала и т.д.

Пример 2.12. Отображение диапазона правил

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

Использование

```
rules -type=IP [-ruleset={* | <IP Rule Set>}] [-verbose]
      [-schedule] [<rules>]...
```

Отображение IP-правил.

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

Отображение правил определенного типа.

Опции

-ruleset={* | <IP Rule Set>}	Отображение определенного набора IP-правил.
-schedule	Фильтрация правил, выполнение которых не разрешено согласно выбранному расписанию.
-type={IP | ROUTING | PIPE | IDP | THRESHOLD | IGMP}	Тип отображаемых правил. По умолчанию: IP.
-verbose	Подробная информация: отображение всех параметров правил.
<rules>	Диапазон правил, которые необходимо отобразить (по умолчанию: все правила).

2.2.59. selftest

Запуск самопроверки.

Описание

Самопроверка выполняется для проверки работы компонентов аппаратного обеспечения.

Во время выполнения проверки (-ок) стандартные операции SGW могут быть прерваны.

Результаты проверки крипто-акселератора зависят от значений конфигурации. Небольшое количество буферов большого размера (LocalReassSettings->LocalReass_NumLarge) может снизить результат пропускной способности. В поле «Drop/Fail» колонка Drop содержит количество пакетов, которые были отброшены до того, как они досигли крипто-акселератор, а колонка Fail содержит количество пакетов, которые по какой-либо причине не удалось зашифровать. Поле Pkt In/Out отображает общее количество входящих и исходящих пакетов акселератора.

Выполняемая проверка трафика и пропускной способности зависит от настроек размеров «кольца» NIC и, возможно, ограничений лицензии. Содержимое каждого полученного пакета проверяется. Для выполнения проверки пропускной способности используются только пакеты большого размера, при этом содержимое полученных пакетов не проверяется.

Пример 2.13. Тест ping, выполняемый между всеми интерфейсами

```
selftest -ping
```

Пример 2.14. Тест ping, выполняемый между интерфейсами 'if1' и 'if2'

```
selftest -ping -interfaces=if1,if2
```

Пример 2.15. Запуск функционального тестирования длительностью 30 минут для проверки оперативной памяти, среды хранения данных и крипто-акселератора

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

Использование

```
selftest -memory [-num=<Integer>]
```

Проверка оперативной памяти.

```
selftest -media [-size=<Integer>]
```

Проверка исправности дисковода.

```
selftest -mac
```

Проверка на наличие коллизий из-за одинаковых MAC-адресов.

```
selftest -ping [-interfaces=<Interface>]
```

Запуск теста ping.

```
selftest -throughput [-interfaces=<Interface>]
```

Запуск проверки пропускной способности.

```
selftest -traffic [-interfaces=<Interface>]
```

Запуск проверки трафика.

```
selftest -cryptoaccel
```

Проверка корректной работы карт крипто-акселераторов.

```
selftest -burnin [-hours[=<Integer>]] [-minutes[=<Integer>]]
         [-memory] [-media] [-ping] [-throughput] [-traffic]
```

```
          [-cryptoaccel]
```

Запуск функционального тестирования для набора субтестов. Если субтесты не указаны, используется следующее: -memory, -ping, -traffic, -cryptoaccel.

```
selftest -abort
```

Прерывание самопроверки.

```
selftest
```

Отображение статуса проверки.

Опции

-abort	Прерывание самопроверки.
-burnin	Запуск функционального тестирования для набора субтестов.
-cryptoaccel	Проверка корректной работы карт крипто-акселератора.
-hours[=<Integer>]	Длительность проверки в часах. По умолчанию: 48.
-interfaces=<Interface>	Интерфейс (-ы) Ethernet.
-mac	Проверка на наличие коллизий из-за одинаковых MAC-адресов.
-media	Проверка исправности дисковода.
-memory	Проверка оперативной памяти.
-minutes[=<Integer>]	Длительность проверки в минутах. По умолчанию: 0.
-num=<Integer>	Количество раз выполнения проверки. По умолчанию: 1.
-ping	Запуск теста ping.
-size=<Integer>	Количество места на носителе для выполнения проверки (МБ). (По умолчанию: 1).
-throughput	Запуск проверки пропускной способности. Отображает максимальную пропускную способность.
-traffic	Запуск проверки трафика. При проверке трафика используются фреймы различных размеров, при этом выполняется проверка содержимого каждого полученного фрейма.

Примечание
Требуются права Администратора.

2.2.60. services

Отображение выполнения настроенных сервисов.

Описание

Отображение выполнения всех настроенных сервисов.

Пример 2.16. Список всех сервисов, имя которых начинается с «http»

```
services http*
```

Использование

```
services [<String>]
```

Опции

<String> Имя или шаблон.

2.2.61. sessionmanager

Менеджер сессии.

Описание

Отбражение информации о менеджере сессии и списка текущих активных пользователей.

Значение флагов Timeout для сессии:

D Сессия выключена

S В подсистеме сессии используется таймаут

- Таймаут не используется

Использование

```
sessionmanager
```

Отображение статуса Менеджера сессии.

```
sessionmanager -status
```

Отображение статуса Менеджера сессии.

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

Список активных сессий.

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

Отображение подробной информации о сессии (-ях).

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

Отправка сообщения в сессию.

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

Принудительное завершение сессии (-ий).

Опции

-disconnect	Принудительное завершение сессии (-ий) (Только с правами Администратора).
-info	Отображение подробной информации о сессии.
-list	Список активных сессий.
-message	Отправка сообщения в сессию.
-num=<n>	Список <n> сессий.
-status	Отображение статуса менеджера сессии.
<database>	Имя базы данных пользователя.
<IP Address>	IP-адрес.
<message text>	Сообщение для отправки.
<session name>	Имя сессии.
{LOCAL | SSH | NETCON | HTTP | HTTPS}	Тип сессии.

2.2.62. settings

Отображение настроек.

Описание

Отбражение содержимого раздела настроек, категория за категорией.

Использование

```
settings
```

Отображение списка категорий.

```
settings <category>
```

Отображение настроек в категории.

Опции

<category>	Отображение настроек в категории.

2.2.63. shutdown

Выключение системы.

Описание

Перезапуск системы.

Использование

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

Опции

-normal Выключение системы.

-reboot Перезагрузка системы.

<seconds> Количество секунд до выключения (по умолчанию: 5)

Примечание
Требуются права Администратора.

2.2.64. sipalg

SIP ALG.

Описание

Список запущенных настроек SIP-ALG, информации о регистрации SIP и звонках.

Использование опции -flags совместно с -snoop обеспечивает любую комбинацию следующих значений:

- 0x00000001 GENERAL
- 0x00000002 ERRORS
- 0x00000004 OPTIONS
- 0x00000008 PARSE
- 0x00000010 VALIDATE
- 0x00000020 SDP
- 0x00000040 ALLOW_CHANGES
- 0x00000080 SUPPORTED_CHANGES

- 0x00000100 2543COMPLIANCE
- 0x00000200 RECEPTION
- 0x00000400 SESSION
- 0x00000800 REQUEST
- 0x00001000 RESPONSE
- 0x00002000 TOPO_CHANGES
- 0x00004000 MEDIA
- 0x00008000 CONTACT
- 0x00010000 CONN
- 0x00020000 PING
- 0x00040000 TRANSACTION
- 0x00080000 CALLLEG

Флаги можно добавить обычным способом. Значение по умолчанию: 0x00000003 (GENERAL и ERRORS).

ПРИМЕЧАНИЕ: Опция 'verbose' выводит на консоль большое количество информации, что может привести к нестабильной работе системы. Будьте внимательны.

Использование

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

Отображение запущенных параметров конфигурации ALG.

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

Отображение текущей таблицы регистрации.

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

Отображение таблицы активных звонков.

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

Отображение активных сессий SIP.

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

Отображение SIP-соединений.

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

Отображение счетчиков SIP.

```
sipalg -snoop={ON | OFF | VERBOSE} [<ipaddr>] [-flags=<String>]
```

Управление SIP snooping. Используется для поиска и устранения неисправностей транзакций SIP. ПРИМЕЧАНИЕ: Опция 'verbose' выводит на консоль большое количество информации, что может привести к нестабильной работе системы. Будьте внимательны.

Опции

-calls	Отображение таблицы активных звонков.
-connection	Отображение SIP-соединений.
-definition	Отображение запущенных параметров конфигурации ALG.
-flags=<String>	SIP snooping для некоторых уровней. Предполагаемое число в шестнадцатеричном виде.
-registration[={SHOW | FLUSH}]	Отображение таблицы регистрации. По умолчанию: show.
-session	Отображение активных SIP-сессий.
-snoop={ON | OFF | VERBOSE}	Включить или выключить SIP snooping. ПРИМЕЧАНИЕ: Опция 'verbose' выводит на консоль большое количество информации, что может привести к нестабильной работе системы. Будьте внимательны.
-statistics[={SHOW | FLUSH}]	Отображение счетчиков SIP. По умолчанию: show.
<alg>	Имя SIP-ALG.
<ipaddr>	IP-адрес для отслеживания.

2.2.65. sshserver

SSH-сервер.

Описание

Отображение статуса SSH-сервера или запуск/остановка/перезапуск SSH-сервера.

Использование

```
sshserver
```

Отображение статуса сервера и списка всех подключенных клиентов.

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

Отображение статуса сервера и списка всех подключенных клиентов.

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

Генерирование приватных ключей SSH-сервера.

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

Перезапуск SSH-сервера.

Опции

-b=<bits>	Размер в битах (по умолчанию: 1024).
-keygen	Генерирование приватных ключей SSH-сервера. Данная

	операция может продолжаться длительное время, около нескольких минут!
-restart	Остановка и запуск SSH-сервера.
-status	Отображение статуса сервера и списка всех подключенных клиентов.
-t={RSA | DSA}	Тип, (по умолчанию: будут созданы ключи RSA и DSA).
-verbose	Подробная информация.
<ssh server>	SSH-сервер.

Примечание
Требуются права Администратора.

2.2.66. stats

Отображение общей статистики по межсетевому экрану.

Описание

Отображение общей статистики по межсетевому экрану, включая продолжительность работы, загрузку CPU, потребление ресурсов и другую информацию о производительности.

Использование

```
stats
```

2.2.67. sysmsgs

Системные сообщения.

Описание

Отображение содержимого буфера FWLoader sysmsg.

Использование

```
sysmsgs
```

2.2.68. techsupport

Информация для технической поддержки.

Описание

Генерирование информации, полезной для технической поддержки.

Из-за большого количества выходных данных при выполнении с локальной консоли данная команда может отображать краткую информацию.

Использование

```
techsupport
```

2.2.69. time

Отображение текущего системного времени.

Описание

Отображение/настройка системного времени и даты.

Использование

```
time
```

Отображение текущего системного времени.

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

Настройка локального системного времени: <ДД-ММ-ГГГГ> <ЧЧ:ММ:СС>.

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

Синхронизация с сервером (-ами) времени (указано в настройках).

Опции

-force	Принудительная синхронизация независимо от настройки MaxAdjust.
-set	Настройка локального системного времени: <ДД-ММ-ГГГГ> <ЧЧ:ММ:СС>.
-sync	Синхронизация с сервером (-ами) времени (указано в настройках).
<date>	Дата ДД-ММ-ГГГГ.
<time>	Время ЧЧ:ММ:СС.

2.2.70. uarules

Отображение правил аутентификации пользователя.

Описание

Отображение содержимого правил аутентификации пользователя.

Пример 2.17. Отображение диапазона правил

```
uarules -v 1-2,4-5
```

Использование

```
uarules [-verbose] [<Integer Range>]
```

Опции

-verbose	Подробная информация.
<Integer Range>	Диапазон правил.

2.2.71. updatecenter

Отображение информации о статусе и контроле автоматического обновления.

Описание

Отображение статуса механизма автоматического обновления или принудительное обновление.

Использование

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

Инициация проверки обновлений определенной базы данных.

```
updatecenter -removedb={ANTIVIRUS | IDP}
```

Удаление определенной базы данных сигнатур.

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

Отображение информации о статусе обновления и базе данных.

```
updatecenter -servers
```

Отображение статуса серверов обновлений.

Опции

-removedb={ANTIVIRUS | IDP}	Удаление базы данных для определенного сервиса.
-servers	Отображение информации о сервере автоматического обновления.
-status[={ANTIVIRUS | IDP | ALL}]	Отображение информации о сервисе и статусе обновления (только с правами Администратора; По умолчанию: все).
-update[={ANTIVIRUS | IDP | ALL}]	Принудительное обновление определенного сервиса, выполняемое немедленно (только с правами Администратора;

По умолчанию: все).

2.2.72. userauth

Отображение информации о статусе и контроле автоматического обновления.

Описание

Отображение текущих регистрирующихся пользователей и другой информации, а также обеспечение принудительного вывода пользователей из системы.

Примечание: В списке пользователей `-list` отображаются только права доступа, используемые политикой.

Использование

```
userauth
```

Список всех аутентифицированных пользователей.

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

Список всех аутентифицированных пользователей.

```
userauth -privilege
```

Список всех известных прав доступа (имена пользователей и группы).

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

Отображение всей информации для пользователя (-ей) с данным IP-адресом.

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

Принудительный вывод аутентифицированного пользователя.

Опции

-list	Список всех аутентифицированных пользователей.
-num=<n>	Ограничение списка всех аутентифицированных пользователей. По умолчанию: 20.
-privilege	Список всех известных прав доступа (имена пользователей и группы).
-remove	Принудительный вывод аутентифицированного пользователя (Только с правами Администратора).
-user	Отображение всей информации для пользователя (-ей) с данным IP-адресом.
<Interface>	Интерфейс
<user ip>	IP-адрес для пользователя (-ей).

2.2.73. vlan

Отображение информации о VLAN.

Описание

Отображение списка подключенных виртуальных интерфейсов LAN или подробной информации об определенном VLAN.

Использование

```
vlan
```

Список подключенных VLAN.

```
vlan <Interface>
```

Отображение VLAN, подключенных к физическому интерфейсу <iface>.

Опции

<Interface>	Отображение информации о VLAN интерфейсе

2.2.74. vpnstats

Alias для **ipsecstats**.

2.3. Утилита

2.3.1. ping

Отображение авторских прав/информации о сборке.

Описание

Отправка одной или более дейтаграмм ICMP ECHO, TCP SYN или UDP на определенный IP-адрес узла. Все дейтаграммы отправляются одновременно.

Размер данных `-length` – это размер данных ICMP или UDP. 1472 байт данных ICMP дают в результате 1500-байт IP дейтаграммы (1514 байт в ethernet).

Использование

```
ping <host> [-recvif=<interface>] [-srcip=<ip address>]
     [-pbr=<table>] [-count=<1...10>] [-length=<4...8192>]
     [-port=<0...65535>] [-udp] [-tcp] [-tos=<0...255>] [-verbose]
```

Опции

-count=<1...10>	Количество пакетов для отправки. По умолчанию:1.
-length=<4...8192>	Размер пакета. По умолчанию: 4.
-pbr=<table>	Маршрут, использующий таблицу PBR.
-port=<0...65535>	Порт назначения UDP или TCP ping.
-recvif=<interface>	Прохождение пакета согласно набору правил с имитацией того, что пакет получен <recvif>.
-srcip=<ip address>	Используйте данный IP-адрес источника.
-tcp	Отправка TCP ping.
-tos=<0...255>	Тип сервиса.
-udp	Отправка UDP ping.
-verbose	Подробная информация.
<host>	IP-адрес узла, на который необходимо отправить ping

2.4. Прочее

2.4.1. echo

Печать текста.

Описание

Печать текста в консоли.

Пример 2.18. Hello World

```
echo Hello World
```

Использование

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

Опции

<String>	Текст для печати.

2.4.2. help

Отображение справки на определенную тему.

Описание

Система справки содержит информацию о командах и типах объекта конфигурации.

Наиболее быстрым способом получения справки является ввод **help**, за которым следует интересующая пользователя тема. Тема может представлять собой имя команды (например, **set**) или имя типа объекта конфигурации (например, **User**).

Если название неизвестно, можно указать категорию необходимой темы с помощью опции `-category`, и использовать функцию «Tab-completion» для отображения списка соответствующих тем.

Использование

```
help
```

Список команд в алфавитном порядке.

```
help <Topic>
```

Отображение справки на тему, выбранную из категории.

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

Отображение справки из категории определенной темы.

Опции

-category={COMMANDS | TYPES}	Категория темы.
<Topic>	Тема.

2.4.3. history

Вывод истории на экран.

Описание

Список недавно вводимых команд, хранящихся в истории.

Использование

```
history
```

2.4.4. ls

Список данных устройства, доступных через SCP.

Описание

Список данных устройства, доступных через SCP.

Пример 2.19. Передача скрипт-файлов на устройство и с устройства

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

Также можно загрузить файлы с лицензией, сертификатами и открытым ключом ssh.

Пример 2.20. Загрузка данных лицензии

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

Если сертификаты и ключ клиента ssh не существуют, их необходимо создать.

Пример 2.21. Загрузка данных сертификата

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

Пример 2.22. Загрузка данных открытого ключа ssh

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

Использование

Опции

-long	Включить формат списка большого размера.
<File>	Файл в списке.

2.4.5. script

Обработка файл-скриптов CLI.

Описание

Запуск, создание, отображение, хранение или удаление файл-скриптов.

Передача файлов-скриптов на устройство и с устройства выполняется с помощью протокола SCP. На устройстве файлы хранятся в папке "/script".

Пример 2.23. Выполнение файл-скрипта

```
"script.sgs":
add IP4Address Name=$1 Address=$2 Comment="$0: \$100".
:/> script -execute -name=script.sgs ip_test 127.0.0.1
is executed as line:
add IP4Address Name=ip_test Address=127.0.0.1 Comment="script.sgs: $100"
```

Использование

```
script -create [[<Category>] <Type> [<Identifier>]] [-name=<Name>]
```

Создание файл-скрипта конфигурации из определенного объекта, класса или категории.

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

Выполнение файл-скрипта.

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

Отображение файл-скрипта в окне консоли.

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

Отправка файл-скрипта на долгосрочное хранение.

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

Удаление файл-скрипта.

```
script
```

Список файл-скриптов.

Опции

-all	Применить ко всем файл-скриптам.
-create	Создание файл-скрипта конфигурации из определенного

	объекта, класса или категории.
-execute	Выполнение файл-скрипта.
-force	Принудительное выполнение файл-скрипта.
-name=<Name>	Имя файл-скрипта.
-quiet	Выполнение файл-скрипта без вывода на экран.
-remove	Удаление файл-скрипта.
-show	Отображение файл-скрипта в окне консоли.
-store	Отправка файл-скрипта на долгосрочное хранение.
-verbose	Подробная информация.
<Category>	Категория, в которую группируются типы объектов.
<Identifier>	Параметр, идентифицирующий объект конфигурации. Применение зависит от указанного <Типа>.
<Parameters>	Список вводимых параметров.
<Type>	Тип объекта конфигурации для выполнения операции.

Примечание
Требуются права Администратора.

Глава 3. Справочная информация по настройкам

- Access
- Address
- AdvancedScheduleProfile
- ALG
- ARP
- BlacklistWhiteHost
- Certificate
- Client
- CommentGroup
- COMPortDevice
- ConfigModePool
- DateTime
- Device
- DHCPRelay
- DHCPServer
- DNS
- Driver
- DynamicRoutingRule
- EthernetDevice
- HighAvailability
- HTTPALGBanners
- HTTPAuthBanners
- HTTPPoster
- HWM
- IDList
- IDPRule
- IGMPRule
- IGMPSetting
- IKEAlgorithms
- Interface
- IPPool

- IPRuleSet
- IPsecAlgorithms
- LDAPDatabase
- LDAPServer
- LinkMonitor
- LocalUserDatabase
- LogReceiver
- NATPool
- OSPFProcess
- Pipe
- PipeRule
- PSK
- RadiusAccounting
- RadiusServer
- RealTimeMonitorAlert
- RemoteIDList
- RemoteManagement
- RouteBalancingInstance
- RouteBalancingSpilloverSettings
- RoutingRule
- RoutingTable
- ScheduleProfile
- Service
- Settings
- SSHClientKey
- ThresholdRule
- UpdateCenter
- UserAuthRule

3.1. Access

Описание

Создание правила доступа позволяет разрешить или заблокировать указанные IP-адреса источника на определенном интерфейсе.

Свойства

Index	Индекс объекта, начинается с 1 (идентификатор).
Name	Символьное имя объекта.
Action	Accept (Принять), Expect (Ожидать) или Drop (Отклонить). По умолчанию: Drop.
Interface	Интерфейс, на который должен прийти пакет, чтобы данное правило могло быть выполнено. Исключение: в правиле задано действие Expect (Ожидать).
Network	Диапазон IP-адресов, которому должен принадлежать IP-адрес отправителя, чтобы данное правило могло быть выполнено.
LogEnabled	Включить регистрацию событий в журнале. По умолчанию: Yes (Вкл).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.2. Address

В данной категории представлены следующие типы объектов.

3.2.1. AddressFolder

Описание

Адресная папка предназначена для наглядного распределения по группам сходных адресных объектов.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Comments	Описание текущего объекта (опционально).

3.2.1.1. IP4HAAddress

Описание

Используйте объект IP4 HA Address, чтобы задать имя определенного IP4 узла, сети или диапазона для каждого узла в кластере высокой отказоустойчивости.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Address	IP-адрес с одним правилом для каждого узла в кластере высокой отказоустойчивости.
UserAuthGroups	Группы и имена пользователей, принадлежащие данному объекту. Объекты, осуществляющие фильтрацию на основе учетных данных, могут использоваться в правилах в качестве сети-источника или сети-назначения (опционально).
NoDefinedCredentials	Если данная опция включена, объекту требуется аутентификация пользователя, но учетные данные (имена пользователей или группы) при этом не заданы. Значит, объекту необходимо, чтобы пользователь аутентифицировался, но игнорирует при этом данные о принадлежности к какой-либо группе. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.2.1.2. IP4Group

Описание

Объект IP4 Address Group используется для объединения нескольких адресных объектов IP4 с целью упрощения управления.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Members	Участники группы.
UserAuthGroups	Группы и имена пользователей, принадлежащие данному объекту. Объекты, осуществляющие фильтрацию на основе учетных данных, могут использоваться в правилах в качестве сети-источника или сети-назначения (опционально).

NoDefinedCredentials	Если данное свойство включено, объекту требуется аутентификация пользователя, но учетные данные (имена пользователей или группы) при этом не определены. Значит, объекту необходимо, чтобы пользователь аутентифицировался, но игнорирует при этом данные о принадлежности к какой-либо группе. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.2.1.3. EthernetAddress

Описание

Используйте объект Ethernet Address, чтобы задать символьное имя для MAC-адреса Ethernet.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Address	MAC-адрес Ethernet. Например: “12-34-56-78-ab-cd”.
Comments	Описание текущего объекта (опционально).

3.2.1.4. EthernetAddressGroup

Описание

Объект Ethernet Address Group используется для объединения нескольких адресных объектов Ethernet с целью упрощения управления.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Members	Участники группы.
Comments	Описание текущего объекта (опционально).

3.2.1.5. IP4Address

Описание

Используйте объект IP4 Address, чтобы задать имя определенного IP4 узла, сети или диапазона.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Address	IP-адрес. Например: “172.16.50.8”, “192.168.30.7, 192.168.30.11”, “192.168.7.0/24” или “172.16.25.10-172.16.25.50”.
ActiveAddress	Динамически заданный адрес, используемый, например, Ethernet-интерфейсами с включенным DHCP-сервером.
UserAuthGroups	Группы и имена пользователей, принадлежащие данному объекту. Объекты, осуществляющие фильтрацию на основе учетных данных, могут использоваться в правилах в качестве сети-источника или сети-назначения (опционально).
NoDefinedCredentials	Если данное свойство включено, объекту требуется аутентификация пользователя, но учетные данные (имена пользователей или группы) при этом не заданы. Значит, объект требует, чтобы пользователь аутентифицировался, но игнорирует при этом данные о принадлежности к какой-либо группе. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.2.2. EthernetAddress

Описание данного объекта совпадает с определениями, представленными в Разделе 3.2.1.3 “EthernetAddress”.

3.2.3. EthernetAddressGroup

Описание данного объекта совпадает с определениями, представленными в Разделе 3.2.1.4 “EthernetAddressGroup”.

3.2.4. IP4Address

Описание данного объекта совпадает с определениями, представленными в Разделе 3.2.1.5 “IP4Address”.

3.2.5. IP4Group

Описание данного объекта совпадает с определениями, представленными в Разделе 3.2.1.2 “IP4Group”.

3.2.6. IP4HAAddress

Описание данного объекта совпадает с определениями, представленными в Разделе 3.2.1.1 “IP4HAAddress”.

3.3. AdvancedScheduleProfile

Описание

Объект Advanced Schedule Profile (Расширенный профиль расписания) позволяет задать расписание, используемое различными политиками системы.

Свойства

Name	Символьное имя сетевого объекта (идентификатор).
Comments	Описание текущего объекта (опционально).

3.3.1. AdvancedScheduleOccurence

Описание

Объект Advanced Schedule Occurrence (График работы расписания) позволяет задать расписание, срабатывающее в заданное время определенных дней недели/месяца.

Свойства

StartTime	Время включения расписания в формате ЧЧ:ММ. Например:13:30.
EndTime	Время выключения расписания в формате ЧЧ:ММ. Например:14:15.
Occurrence	График работы. По умолчанию: Weekly (На неделю).
Weekly	Позволяет задать дни недели, когда срабатывает расписание. Понедельник соответствует значению 1, воскресенье – 7. По умолчанию: 1 – 7.
Monthly	Позволяет задать дни месяца, когда должно срабатывать расписание. Расписание срабатывает, только если заданные дни в данном месяце действительно существуют. По умолчанию: 1 – 31.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.4. ALG

В данной категории представлены следующие виды объектов.

3.4.1. ALG_FTP

Описание

FTP ALG (Application Layer Gateway) предназначен для управления FTP-трафиком в системе.

Свойства

Name (Имя)	Символьное имя ALG (идентификатор).
AllowServerPassive	Разрешить серверу использовать пассивный режим (небезопасно для сервера). По умолчанию: No (Нет).
ServerPorts	Порты сервера для передачи данных. По умолчанию: 1024-65535.
AllowClientActive	Разрешить клиенту использовать активный режим (небезопасно для клиента). По умолчанию: No (Нет).
ClientPorts	Порты клиента для передачи данных. По умолчанию: 1024-65535.
AllowUnknownCommands	Разрешить неизвестные команды. По умолчанию: No (Нет).
AllowSITEEXEC	Разрешить команду SITE EXEC. По умолчанию: No (Нет).
MaxLineLength	Максимальная длина строки в канале управления. По умолчанию: 256.
MaxCommandRate	Максимальное количество команд в секунду. По умолчанию: 20.
Allow8BitStrings	Разрешить использование 8-битных строк в канале управления. По умолчанию: Yes (Да).
AllowResumeTransfer	Разрешить команду RESUME даже в случае сканирования содержимого. По умолчанию: No (Нет).
Antivirus	Режимы Disabled (Отключен), Audit (Сканирование) или Protect (Защита включена).
ScanExclude	Список типов файлов, которые необходимо исключить из антивирусного сканирования (опционально).

CompressionRatio	В случае превышения установленного значения для коэффициента сжатия будет предпринято заданное для такого события действие. При установке значения 0 все проверки сжатия будут отключены (по умолчанию: 20).
CompressionRatioAction	Действие, предпринимаемое в случае превышения верхнего порогового значения для коэффициента сжатия. Все действия заносятся в журнал.
AllowEncryptedZip	Разрешить зашифрованные файлы в формате zip, даже если их содержимое нельзя просканировать. По умолчанию: No (Нет).
ZDEnabled	Включить функцию блокировки с помощью технологии ZoneDefense. По умолчанию: No (Нет).
ZDNetwork	При обнаружении вируса узлы текущей сети будут заблокированы на коммутаторах.
FileListType	Указывается, содержит ли список файлов запрещенные или удаленные файлы.
FailModeBehavior	Стандартное поведение при ошибке: Allow (Разрешить) или Deny (Запретить). По умолчанию: Deny.
File	Список типов файлов, которые необходимо разрешить или запретить (опционально).
VerifyContentMimeType	Проверить расширение файла на соответствие типам MIME. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.4.2. ALG_H323

Описание

H.323 ALG (Application Layer Gateway) предназначен для управления мультимедийным трафиком с использованием стандарта H.323.

Свойства

Name	Символьное имя ALG (идентификатор).
AllowTCPDataChannels	Разрешить каналы передачи данных по протоколу TCP (T.120). По умолчанию: Yes (Да).
MaxTCPDataChannels	Максимальное количество каналов передачи данных по протоколу TCP для одного вызова. По умолчанию: 10.
TranslateAddresses	Преобразование адресов: Автоматически или Вручную. По умолчанию: Automatic (Автоматически).
TranslateLogicalChannelAddresses	Преобразовывать адреса логических каналов. По умолчанию: Yes (Да).

MaxGKRegLifeTime	Максимальный срок действия регистрации привратников. По умолчанию: 1800.
Comments	Описание текущего объекта (опционально).

3.4.3. ALG_HTTP

Описание

HTTP ALG (Application Layer Gateway) предназначен для фильтрации HTTP-трафика.

Свойства

Name	Символьное имя ALG (идентификатор).
RemoveCookies	Удалить файлы cookies.
RemoveScripts	Удалить Javascript/VBScript. По умолчанию: No (Нет).
RemoveApplets	Удалить JAVA-приложения. По умолчанию: No (Нет).
RemoveActiveX	Удалить объекты ActiveX (включая Flash). По умолчанию: No (Нет).
VerifyUTF8URL	Убедиться в том, что URL-адреса не содержат некорректную кодировку UTF-8. По умолчанию: No (Нет).
BlackURLDisplayReason	Сообщения о попытке получить доступ к сайту из «черного» списка (опционально).
HTTPBanners	HTML-страница баннера HTTP ALG. По умолчанию: Default (По умолчанию).
MaxDownloadSize	Максимально допустимый размер файла в килобайтах (опционально).
FileListType	Указывается, содержит ли список файлов запрещенные или удаленные файлы. По умолчанию: Block (Блокировать).
FailModeBehavior	Стандартное поведение при ошибке: Allow (Разрешить) или Deny (Запретить). По умолчанию: Deny.
File	Список типов файлов, которые необходимо разрешить или запретить (опционально).
VerifyContentMimeType	Проверить расширение файлов на соответствие типам MIME. По умолчанию: No (Нет).
Antivirus	Режимы Disabled (Отключен), Audit (Сканирование) или Protect (Защита включена).
ScanExclude	Список типов файлов, которые необходимо исключить из антивирусного сканирования (опционально).

CompressionRatio	В случае превышения установленного значения для коэффициента сжатия будет предпринято заданное для такого события действие. При установке значения 0 все проверки сжатия будут отключены. По умолчанию: 20.
CompressionRatioAction	Действие, предпринимаемое в случае превышения верхнего порогового значения для коэффициента сжатия. Все действия заносятся в журнал. По умолчанию: Drop (Отклонить).
AllowEncryptedZip	Разрешить зашифрованные файлы в формате zip, даже если их содержимое нельзя просканировать. По умолчанию: No (Нет).
ZDEnabled	Включить функцию блокировки с помощью технологии ZoneDefense. По умолчанию: No (Нет).
ZDNetwork	При обнаружении вируса узлы текущей сети будут заблокированы на коммутаторах.
WebContentFilteringMode	Режимы Disabled (Отключен), Audit (Сканирование) или Enable (Включить). По умолчанию: Disable.
FilteringCategories	Категории Web-контента, подлежащие блокировке (опционально).
NonManagedAction	Действие, которое необходимо предпринять в отношении неклассифицированных данных. По умолчанию: Allow (Разрешить).
AllowFilteringOverride	Разрешить пользователю просматривать заблокированный сайт. По умолчанию: No (Нет).
AllowFilteringReclassification	Разрешить повторную классификацию сайтов. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.4.3.1. ALG_HTTP_URL

Описание

Данный объект позволяет заносить в «черный» список URL-адреса и запрещать, таким образом, доступ к сайтам, файлам с указанным типом расширения или URL-адресам с определенными словами в составе.

Свойства

Action	Whitelist (Внести в белый список) или Blacklist (Внести в «черный» список). По умолчанию: Blacklist.
URL	Отображается URL-адрес, который необходимо занести в «белый» или «черный» список.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.4.4. ALG_POP3

Описание

POP3 ALG (Application Layer Gateway) предназначен для управления POP3-трафиком в системе.

Свойства

Name	Символьное имя ALG (идентификатор).
BlockUserPass	Блокировать клиентам отправку команд USER и PASS. По умолчанию: No (Нет).
HideUser	Не позволяет серверу распознать, что имя пользователя не существует. По умолчанию: No (Нет).
AllowUnknownCommands	Разрешить неизвестные команды. По умолчанию: No (Нет).
FileListType	Указывается, содержит ли список файлов запрещенные или удаленные файлы. По умолчанию: Block (Блокировать).
FailModeBehavior	Стандартное поведение при ошибке: Allow (Разрешить) или Deny (Запретить). По умолчанию: Deny.
File	Список типов файлов, которые необходимо разрешить или запретить (опционально).
VerifyContentMimeType	Проверить расширение файлов на соответствие типам MIME. По умолчанию: No (Нет).
Antivirus	Режимы Disabled (Отключен), Audit (Сканирование) или Protect (Защита включена).
ScanExclude	Список типов файлов, которые необходимо исключить из антивирусного сканирования (опционально).
CompressionRatio	В случае превышения установленного значения для коэффициента сжатия будет предпринято заданное для такого события действие. При установке значения 0 все проверки сжатия будут отключены. По умолчанию: 20.
CompressionRatioAction	Действие, предпринимаемое в случае превышения верхнего порогового значения для коэффициента сжатия. Все действия заносятся в журнал. По умолчанию: Drop (Отклонить).
AllowEncryptedZip	Разрешить зашифрованные файлы в формате zip, даже если их содержимое нельзя просканировать. По умолчанию: No (Нет).

ZDEnabled	Включить функцию блокировки с помощью технологии ZoneDefense. По умолчанию: No (Нет).
ZDNetwork	При обнаружении вируса узлы текущей сети будут заблокированы на коммутаторах.
Comments	Описание текущего объекта (опционально).

3.4.5. ALG_PPTP

Описание

PPTP ALG (Application Layer Gateway) предназначен для управления PPTP-трафиком в системе.

Свойства

Name	Символьное имя ALG (идентификатор).
EchoTimeout	Таймаут простоя для сообщений Echo в PPTP-туннеле (по умолчанию: 0).
IdleTimeout	Таймаут простоя для сообщений трафика пользователя в PPTP-туннеле (по умолчанию: 0).
Comments	Описание текущего объекта (опционально).

3.4.6. ALG_SIP

Описание

SIP ALG (Application Layer Gateway) предназначен для управления мультимедийными сессиями на основе протокола SIP.

Свойства

Name	Символьное имя ALG (идентификатор).
MaxSessionsPerId	Максимальное количество сессий для одного идентификатора SIP (по умолчанию: 5).
MaxRegistrationTime	Максимально допустимый период времени между запросами на регистрацию (по умолчанию: 3600).
SipSignalTmeout	Значение таймаута для последнего сообщения SIP (по умолчанию: 43200).
DataChannelTmout	Значение таймаута для канала передачи данных (по умолчанию: 120).
AllowMediaByPass	Разрешить клиентам при возможности обмениваться медиа-данными напрямую без участия межсетевого экрана. По умолчанию: Yes (Да).

AllowTCPDataChannels	Разрешить каналы передачи данных по протоколу TCP. По умолчанию: Yes (Да).
MaxTCPDataChannels	Максимальное количество каналов передачи данных по протоколу TCP для одного вызова (по умолчанию: 5).
Comments	Описание текущего объекта (опционально).

3.4.7. ALG_SMTP

Описание

SMTP ALG (Application Layer Gateway) предназначен для управления SMTP-трафиком в системе.

Свойства

Name	Символьное имя ALG (идентификатор).
VerifySenderEmailAction	Проверить сообщения электронной почты на наличие несоответствия адреса «От кого» в команде SMTP-протокола с адресом «От кого» заголовка сообщения.
VerifySenderEmailDomainOnly	TODO (по умолчанию: Deny (Запретить)).
MaxEmailPerMinute	Проверять только доменное имя в адресах электронной почты «От кого». По умолчанию: No (Нет).
MaxEmailSize	Максимальный размер электронного сообщения в килобайтах (опционально).
FileListType	Указывается, содержит ли список файлов запрещенные или удаленные файлы. По умолчанию: Block (Блокировать).
FailModeBehavior	Стандартное поведение при ошибке: Allow (Разрешить) или Deny (Запретить). По умолчанию: Deny.
File	Список типов файлов, которые необходимо разрешить или запретить (опционально).
VerifyContentMimeType	Проверить расширение файлов на соответствие типам MIME (по умолчанию: No (Нет)).
Antivirus	Режимы Disabled (Отключен), Audit (Сканирование) или Protect (Защита включена).
ScanExclude	Список типов файлов, которые необходимо исключить из антивирусного сканирования (опционально).
CompressionRatio	В случае превышения установленного значения для коэффициента сжатия будет предпринято заданное для такого события действие. При установке значения 0 все проверки сжатия будут отключены. По умолчанию: 20.
CompressionRatioAction	Действие, предпринимаемое в случае превышения

	верхнего порогового значения для коэффициента сжатия. Все действия заносятся в журнал. По умолчанию: Drop (Отклонить).
AllowEncryptedZip	Разрешить зашифрованные файлы в формате zip, даже если их содержимое нельзя просканировать. По умолчанию: No (Нет).
ZDEnabled	Включить функцию блокировки с помощью технологии ZoneDefense. По умолчанию: No (Нет).
ZDNetwork	При обнаружении вируса узлы текущей сети будут заблокированы на коммутаторах.
DNSBL	Disable (Отключить) или Enable (Включить) DNSBL-сервер. По умолчанию: No (Нет).
SpamThreshold	Опция Spam Threshold определяет условия, при которых сообщение электронной почты будет считаться спамом (по умолчанию: 10).
DropThreshold	Опция Drop Threshold определяет условия, при которых сообщение электронной почты считается вредоносным и отбрасывается (по умолчанию: 10).
SpamTag	Метка Spam вставляется в тему сообщения, которое было классифицировано как спам или вредоносное сообщение (по умолчанию: “***SPAM***”).
ForwardBlockedMail	Направлять заблокированные сообщения в объект DropAddress (Отбросить адрес). По умолчанию: No (Нет).
DropAddress	Адрес электронной почты, на который будут перенаправляться сообщения с пороговым значением для отбрасывания.
AppendTXT	Использовать запись TXT (используется только по достижении порогового значения для отбрасывания). По умолчанию: No (Нет).
CacheSize	Размер кэша IP-адресов проверенного отправителя (по умолчанию: 0).
CacheTimeout	Таймаут в секундах, перед тем как сохраненный в кэше IP-адрес будет удален.
DNSBlackLists	Позволяет задать имя домена из «черного» списка и определить размер самого списка.
Comments	Описание текущего объекта (опционально).

3.4.7.1. ALG_SMTP_Email

Описание

Данный объект позволяет заносить в «черный» или «белый» список отправителя/получателя сообщения электронной почты.

Свойства

Type	Отображается тип адреса электронной почты: отправитель или получатель. По умолчанию: Sender (Отправитель).
Action	Отображаются возможные варианты действий: внести в белый список (разрешить) или «черный» список (запретить). По умолчанию: Blacklist (Занести в «черный» список).
Email	Отображается электронный адрес получателя, который необходимо внести в «черный» или «белый» список.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.4.8. ALG_TFTP

Описание

TFTP ALG (Application Layer Gateway) предназначен для управления TFTP-трафиком в системе.

Свойства

Name	Символьное имя ALG (идентификатор).
AllowedCommands	Разрешенные команды (по умолчанию: ReadWrite).
RemoveOptions	Удалить опции из пакета запроса. По умолчанию: No (Нет).
AllowUnknownOptions	Разрешить неизвестные опции в пакете запроса. По умолчанию: No (Нет).
MaxBlockSize	Максимальное значение для размера блока (опционально).
MaxFileTransferSize	Максимальный размер для передаваемого файла (опционально).
BlockDirectoryTraversal	Запретить обход каталога (последовательные точки в именах файлов). По умолчанию: No (Нет)
Comments	Описание текущего объекта (опционально).

3.4.9. ALG_TLS

Описание

TLS ALG

Свойства

Name	Символьное имя ALG (идентификатор).
HostCert	Сертификат узла.
RootCert	Корневой сертификат (опционально).
Comments	Описание текущего объекта (опционально).

3.5. ARP

Описание

Используйте запись ARP для публикации дополнительных IP-адресов и/или MAC-адресов на указанном интерфейсе.

Свойства

Mode	Static, Publish или XPublish (по умолчанию: Publish).
Interface	Отображается интерфейс, для которого применяется ARP-запись. Например: интерфейс, на котором будет опубликован адрес.
IP	IP-адрес, который необходимо опубликовать или статически назначить аппаратному адресу.
MACAddress	Аппаратный адрес, связанный с IP-адресом (по умолчанию: 00-00-00-00-00-00).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.6. BlacklistWhiteHost

Описание

Узлы и сети, добавленные в белый список, не могут быть занесены в «черный» список по правилам пороговых значений (Threshold Rules) или правилам обнаружения и предотвращения вторжений (IDP Rules).

Свойства

Addresses	Отображается адрес для занесения в белый список.
Service	Отображается сервис для занесения в белый список.
Schedule	Расписание для работы белого списка (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.7. Certificate

Описание

Сертификат X. 509 используется для аутентификации клиента или шлюза VPN при создании IPSec-туннеля.

Свойства

Name	Символьное имя сертификата (идентификатор).
Type	Local (Локальный), Remote (Удаленный) или Request (По запросу).
CertificateData	Информация о сертификате.
PrivateKey	Личный ключ.
NoCRLs	Отключить CRL (Списки отозванных сертификатов). По умолчанию: No (Нет).
PKAType	Алгоритм шифрования с открытым ключом. По умолчанию: Unknown (Неизвестно).
Comments	Описание текущего объекта (опционально).

3.8. Client

Описание

В данной категории представлены следующие типы объектов.

3.8.1. DynDnsClientCjbNet

Описание

Данный объект предназначен для настройки параметров, используемых для подключения к сервису Cjb.net DynDNS.

Свойства

Username	Имя пользователя.
Password	Пароль для заданного имени пользователя (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.8.2. DynDnsClientDyndnsOrg

Описание

Данный объект предназначен для настройки параметров, используемых для подключения к сервису dyndns.org DynDNS.

Свойства

DNSName	Имя DNS без суффикса “.dyndns.org”.
Username	Имя пользователя.
Password	Пароль для заданного имени пользователя (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.8.3. DynDnsClientDynsCx

Описание

Данный объект предназначен для настройки параметров, используемых для подключения к сервису dyns.cx DynDNS.

Свойства

DNSName	Имя DNS без суффикса “.dyns.cx”.
Username	Имя пользователя.
Password	Пароль для заданного имени пользователя (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.8.4. DynDnsClientPeanutHull

Описание

Данный объект предназначен для настройки параметров, используемых для подключения к сервису Peanut Hull DynDNS.

Свойства

DNSName	Имена DNS, разделенных “,”.
Username	Имя пользователя.
Password	Пароль для заданного имени пользователя (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.9. CommentGroup

Описание

Данный объект предназначен для объединения одного или более объектов конфигурации.

Свойства

Description	TODO. По умолчанию: “(New Group)”/”(Новая группа)”.
Color	TODO. По умолчанию: 9EBEE7.
Password	Пароль для заданного имени пользователя (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.10. COMPortDevice

Описание

Последовательный порт используется для доступа к командной строке интерфейса (CLI).

Свойства

Port	Порт (идентификатор).
BitsPerSecond	Бит в секунду (по умолчанию: 9600).
DataBits	Бит данных (по умолчанию: 8).
Parity	Контроль четности. По умолчанию: None (Нет).
StopBits	Стоповые биты (по умолчанию: 1).
FlowControl	Управление потоком данных. По умолчанию: None (Нет).
Comments	Описание текущего объекта (опционально).

3.11. ConfigModePool

Описание

Объект IKE Config Mode Pool позволяет динамически назначить IP-адрес, DNS-сервер, WINS-сервер и т. п. клиенту VPN, подключившемуся к данному шлюзу.

Свойства

IPPoolType	Позволяет задать тип источника IP-адресов: предопределенный пул IP-адресов или статическая группа IP-адресов.
IPPool	Пул IP-адресов, используемый для назначения IP-адресов клиентам VPN.
IPPoolAddress	Диапазон IP-адресов, используемый для назначения IP-адресов клиентам VPN.
IPPoolNetmask	Маска сети, назначаемая клиентам VPN.
DNS	IP-адрес DNS-сервера, к которому клиент VPN должен подключиться (опционально).
NBNSIP	IP-адрес NBNS/WINS-сервера, к которому клиент VPN должен подключиться (опционально).
DHCP	IP-адрес DHCP-сервера, к которому клиент VPN должен подключиться (опционально).
Subnets	Дополнительные маски подсети для данного шлюза (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.12. DateTime

Описание

Данный объект позволяет выполнить настройку даты, времени и часового пояса.

Свойства

TimeZone	Часовой пояс. По умолчанию: GMT.

DSTEnabled	Включить переход на летнее время. По умолчанию: Yes (Да).
DSTOffset	Сдвиг при переходе на летнее время в минутах. По умолчанию: 60.
DSTStartMonth	Месяц, с которого начинает действовать летнее время. По умолчанию: March (Март).
DSTStartDay	День месяца, когда начинает действовать летнее время По умолчанию: 1.
DSTEndMonth	Месяц, когда прекращает действовать летнее время. По умолчанию: October (Октябрь).
DSTEndDay	День месяца, когда прекращает действовать летнее время. По умолчанию: 1.
TimeSyncEnable	Включить синхронизацию времени. По умолчанию: No (Нет).
TimeSyncServerType	Тип сервера, используемого для синхронизации времени: UDPTime или SNTP (Simple Network Time Protocol). По умолчанию: SNTP.
TimeSyncServer1	DNS-имя узла или IP-адрес Сервера времени 1.
TimeSyncServer2	DNS-имя узла или IP-адрес Сервера времени 2 (опционально).
TimeSyncServer3	DNS-имя узла или IP-адрес Сервера времени 3 (опционально).
TimeSyncInterval	Промежуток времени между каждой повторной синхронизацией. По умолчанию: 86400.
TimeSyncMaxAdjust	Максимальное смещение времени в секундах, предоставленное серверу для корректировки. По умолчанию: 600.
TimeSyncGroupIntervalSize	Интервал, в соответствии с которым группируются ответы сервера. По умолчанию: 10.
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.13. Device

Описание

Общие параметры данного устройства.

Свойства

Name	Имя устройства. По умолчанию: Device (Устройство).
LocalCfgVersion	Номер локальной версии конфигурации. По умолчанию: 1.
RemoteCfgVersion	Номер удаленной версии конфигурации. По умолчанию: 0.
ConfigUser	Имя пользователя, выполнившего настройку текущей конфигурации. По умолчанию: BaseConfiguration.
ConfigSession	Тип сессии, используемый при подтверждении текущей конфигурации. По умолчанию: BaseConfiguration.
ConfigIP	IP-адрес пользователя, выполнившего настройку текущей конфигурации.
ConfigDate	Дата выполнения текущей конфигурации (опционально).
DeviceID	Идентификатор устройства (опционально).
HWModel	Модель аппаратного обеспечения системы. По умолчанию: SOFTWARE.
RegistrationKey	Ключ регистрации системы (опционально).
ProductionDate	Дата изготовления устройства (опционально).
HWSerial	Серийный номер аппаратного обеспечения устройства (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.14. DHCPRelay

Описание

Применение DHCP Relay позволяет динамически изменять таблицу маршрутизации в соответствии со сроками аренды ретранслируемого DHCP.

Свойства

Name	Символьное имя для правила ретрансляции (идентификатор).
Action	Ignore (Игнорировать), Relay (Ретранслировать) или

	BootpFwd. По умолчанию: Ignore.
SourceInterface	Интерфейс источника DHCP-пакета.
TargetDHCPServer	IP-адрес сервера для отправки ему ретранслируемых DHCP-пакетов.
IPOffer	Диапазон IP-адресов, которые могут быть ретранслированы с DHCP-сервера. По умолчанию: 1.
AddRoute	Включить динамическое добавление маршрутов с учетом добавлений и удаления сроков аренды. По умолчанию: No (Нет).
AddRouteLocalIP	Данный IP-адрес будет автоматически опубликован на интерфейсах, куда добавляется маршрут (опционально).
AddRouteGatewayIP	IP-адрес, используемый в качестве шлюза для связи с узлами на данном маршруте (опционально).
RoutingTable	Позволяет задать таблицу маршрутизации, в которую должен быть добавлен маршрут клиентов к узлу. По умолчанию: main (основная).
MaxRelaysPerInterface	Позволяет задать количество ретрансляций, разрешенных для каждого интерфейса, т. е. количество DHCP-клиентов, которым разрешено ретранслироваться через каждый интерфейс (опционально).
AgentIP	Позволяет определить IP-адрес, который в ходе ретрансляции должен использоваться в качестве IP-адреса шлюза при передаче запросов на DHCP-сервер. По умолчанию: Recv.
AllowNULLOffers	Принять ответы сервера с предложенным IP-адресом "0.0.0.0" (IP-адрес не предложен). По умолчанию: No (Нет).
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов, предназначенных для ретрансляции через Proxy ARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейс/интерфейсы, на которых шлюз безопасности должен опубликовать маршруты, необходимые для ретрансляции через Proxy ARP (опционально).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Позволяет определить, события журнала с каким уровнем важности будут отправлены указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

3.15. DHCPServer

Описание

DHCP-сервер позволяет определить группу IP-адресов и параметры настройки узла для предоставления DHCP-клиентам, привязанным к данному интерфейсу.

Свойства

Index	Индекс объекта, начиная с 1 (идентификатор).
Name	Символьное имя для правила DHCP-сервера (идентификатор).
Interface	Интерфейс источника для прослушивания DHCP-запросов. Может использоваться как один, так и несколько интерфейсов.
RelayerFilter	Диапазон, группа или сеть, которые разрешат указанным ретрансляторам DHCP получить доступ к DHCP-серверу. По умолчанию: 0/0.
IPAddressPool	Диапазон, группа или сеть, которые DHCP-сервер будет использовать в качестве пула IP-адресов для предоставления сроков аренды адресов DHCP.
Netmask	Маска сети, отправляемая DHCP-клиенту.
DefaultGateway	Позволяет определить, какой IP-адрес должен быть отправлен клиенту для использования в качестве основного шлюза. Если IP-адрес не определен или определен как 0.0.0.0, выданный клиенту IP-адрес будет отправлен в качестве шлюза (опционально).
Domain	Доменное имя, используемое для разрешения DNS (опционально).
LeaseTime	Время в секундах, на которое узлу предоставляется аренда DHCP-адреса. По завершении срока аренды клиенту необходимо возобновить аренду. По умолчанию: 86400.
DNS1	IP-адрес предпочитаемого DNS-сервера (опционально).
DNS2	IP-адрес альтернативного DNS-сервера (опционально).
NBNS1	IP-адрес предпочитаемого WINS-сервера (Windows Internet Name Service), применяемого в среде Microsoft, который использует серверы имен NetBIOS (NBNS) для назначения IP-адресов именам NetBIOS (опционально).
NBNS2	IP-адрес предпочитаемого WINS-сервера (Windows Internet Name Service), применяемого в среде Microsoft, который использует серверы имен NetBIOS (NBNS) для назначения IP-адресов именам NetBIOS (опционально).
NextServer	IP-адрес следующего сервера в процессе загрузки (опционально).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Позволяет определить, события журнала с каким уровнем важности будут отправлены указанным получателям журнала. По умолчанию: Default (По умолчанию).

Comments	Описание текущего объекта (опционально).

3.15.1 DHCPServerPoolStaticHost

Описание

Запись статического узла DHCP-сервера

Свойства

Host	IP-адрес узла.
Static HostType	Идентификатор узла. По умолчанию: MACAddress.
MACAddress	Аппаратный адрес узла.
ClientIdentType	Заданный тип идентификатора клиента. По умолчанию: Ascii.
ClientIdent	Идентификатор клиента для узла.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.15.2 DHCPServerCustomOption

Описание

Данный объект позволяет расширить функциональные возможности DHCP-сервера благодаря добавлению пользовательских опций, которые будут предоставлены DHCP-клиентам.

Свойства

Code	Код опции DHCP (идентификатор).
Type	Тип опции, т. е. STRING, IP4 и другие. По умолчанию: UINT8.
Param	Параметры, отправляемые с кодом. Может отправляться как один параметр, так и целый список параметров, разделенных запятыми (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.16. DNS

Описание

Данный объект предназначен для настройки параметров клиентов DNS.

Свойства

DNSServer1	IP-адрес предпочтительного DNS-сервера (опционально).
DNSServer2	IP-адрес альтернативного DNS-сервера (опционально).
DNSServer3	IP-адрес третичного DNS-сервера (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17. Driver

В данной категории представлены следующие типы объектов.

3.17.1. BNE2EthernetPCIDriver

Описание

Broadcom NE2 Gigabit Ethernet.

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.2. BNE2EthernetPCIDriver

Описание

Broadcom NE Gigabit Ethernet.

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.3. E1000EthernetPCIDriver

Описание

Адаптер Gigabit Ethernet Intel (E1000).

Свойства

RxRingsize	Размер «кольца» Rx (по умолчанию: 64).
TxRingsize	Размер «кольца» Tx (по умолчанию: 256).
EnableMonitoring	Включить мониторинг. По умолчанию: No (Нет).
BelowCPULoad	Ниже уровня нагрузки CPU.
BelowInterfaceLoad	Ниже уровня нагрузки на интерфейс.
MinInterval	Минимальный интервал (по умолчанию: 30).
RxErrorPercentage	Процент ошибок Rx (по умолчанию: 20).
TxErrorPercentage	Процент ошибок Tx (по умолчанию:7).
ErrorTime	Время ошибки (по умолчанию: 10).
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.4. E100EthernetPCIDriver

Описание

Адаптер Gigabit Ethernet Intel (E100).

Свойства

RxRingsize	Размер «кольца» Rx (по умолчанию: 32)
TxRingsize	Размер «кольца» Tx (по умолчанию: 128)
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.5. IXP4NPEEthernetPCIDriver

Описание

Адаптер Fast Ethernet Intel (IXP4xxNPE).

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.6. MarvellEthernetPCIDriver

Описание

Адаптер Fast и Gigabit Ethernet Marvell (88E8001, 88E8053, 88E8062).

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.7. R8139EthernetPCIDriver

Описание

Адаптер Fast Ethernet RealTek (8139).

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.8. R8169EthernetPCIDriver

Описание

Адаптер Gigabit Ethernet RealTek (8169, 8110).

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.9. ST201EthernetPCIDriver

Описание

Адаптер Fast Ethernet D-Link (ST201).

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.10. ST201EthernetPCIDriver

Описание

Адаптер Fast Ethernet с тюльпановидным разъемом.

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.17.11. X3C905EthernetPCIDriver

Описание

Адаптер Fast Ethernet 3com.

Свойства

Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило

данного типа.

3.18. DynamicRoutingRule

Описание

Правило политики динамической маршрутизации позволяет осуществлять фильтрацию статически настроенных или изученных OSPF маршрутов. Для маршрутов, подпадающих под правила, могут быть заданы такие действия, как экспорт в OSPF-процессы или добавление в одну или несколько таблиц маршрутизации.

Свойства

Index	Индекс объекта, начиная с 1 (идентификатор).
Name	Символьное имя правила (опционально).
From	OSPF или Routing Table (Таблица маршрутизации). По умолчанию: Routing Table.
OSPFProcess	Позволяет определить из какого процесса OSPF следует импортировать маршрут в таблицу маршрутизации или в другой процесс OSPF.
RoutingTable	Позволяет определить из какой таблицы маршрутизации следует импортировать маршрут в OSPF AS или в другую таблицу маршрутизации.
DestinationInterface	Интерфейс, которому должна соответствовать политика (опционально).
DestinationNetworkExactly	Позволяет определить, требуется ли маршруту точное соответствие определенной сети.
DestinationNetworkIn	Позволяет определить, должен ли маршрут находиться в определенной сети (опционально).
NextHop	Адрес следующей пересылки (адрес маршрутизатора), которому должна соответствовать данная политика.
MetricRange	Определяет диапазон, в который должна попадать метрика маршрутов (опционально).
RouterID	Позволяет определить, должна ли политика осуществлять фильтрацию по идентификатору маршрутизатора. (опционально)
OSPFRouteType	Позволяет определить, должна ли политика осуществлять фильтрацию по типу OSPF маршрутизатора (опционально).
OSPFTagRange	Определяет диапазон допустимых значений для метки (tag) маршрутизаторов.
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default

(По умолчанию).

Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.18.1. DynamicRoutingRuleExportOSPF

Описание

Действие OSPF позволяет осуществлять управление и экспорт новых или измененных маршрутов в процесс OSPF маршрутизатора.

Свойства

ExportToProcess	Позволяет определить, в какой процесс OSPF должно быть экспортировано изменение маршрута.
SetTag	Позволяет определить метку для данного маршрута, которая может использоваться в других маршрутизаторах для фильтрации (опционально).
SetRouteType	Тип внешнего маршрута (опционально).
Offset Metric	Позволяет увеличить метрику импортируемого маршрута на данное значение (опционально).
LimitMetricRange	Позволяет назначить минимальное и максимальное значение для метрики данных маршрутов. Если значение маршрута выше или ниже заданного, такому маршруту будут присвоены заданные значения (опционально).
SetForward	IP-адрес, через который осуществляется маршрутизация (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.18.2. DynamicRoutingRuleAddRoute

Описание

Действие маршрутизации позволяет осуществлять управление и добавлять новые или измененные маршруты в одну или несколько локальных таблиц маршрутизации.

Свойства

Destination	Позволяет определить, в какую таблицу маршрутизации должно быть экспортировано изменение маршрута в процесс OSPF.
OverrideStatic	Разрешить замену статических маршрутов. По умолчанию: No (Нет).
OverwriteDefault	Разрешить перезапись основного маршрута. По умолчанию: No (Нет).
OffsetMetric	Позволяет увеличить метрику на данное значение (опционально).
OffsetMetricType2	Позволяет увеличить метрику маршрутов с типом Type2 на данное значение (опционально).
LimitMetricRange	Позволяет назначить минимальное и максимальное значение для метрики данных маршрутов. Если значение маршрута выше или ниже заданного, такому маршруту будут присвоены заданные значения (опционально).
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов через ProxyARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Позволяет определить интерфейсы, на которых шлюз безопасности должен опубликовать маршруты через ARP Proxy (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.19. EthernetDevice

Описание

Аппаратные настройки Ethernet-интерфейса.

Свойства

Name	Символьное имя устройства (идентификатор).
EthernetDriver	Драйвер Ethernet для шины PCI, который должен использоваться интерфейсом.
PCIBus	Номер шины PCI, в которую установлен Ethernet-адаптер.
PCISlot	Номер слота PCI, используемый Ethernet-адаптером.
PCIPort	Некоторые Ethernet-адаптеры оснащены несколькими портами, совместно использующими один и тот же номер шины и слота. Данный параметр позволяет задать необходимый порт.
Media	Позволяет определить, должна ли скорость соединения быть согласована автоматически или установлена статически. По умолчанию: Auto (Автоматически).
Duplex	Позволяет определить, должна ли дуплексная передача быть согласована автоматически или установлена в полный дуплекс или полудуплекс. По умолчанию: Auto (Автоматически).
MACAddress	Аппаратный адрес интерфейса (опционально).
Comments	Описание текущего объекта (опционально).

3.20. HighAvailibiliy

Описание

Настройка параметров кластера высокой отказоустойчивости.

Свойства

Enabled	Включить режим высокой отказоустойчивости. По умолчанию: No (Нет).
Sync	Позволяет определить, существуют ли участники кластера для параметров синхронизации конфигурации. По умолчанию: Yes (Да).
ClusterID	(Локально) уникальный идентификатор кластера для идентификации данной группы шлюзов безопасности HA. По умолчанию: 0.
SyncIface	Интерфейс, используемый для синхронизации состояния.
NodeID	Master (Главный узел) или Slave (Подчиненный узел). По умолчанию: Master.
HASyncBufSize	Объем данных синхронизации в Кб, которые можно поместить в буфер во время ожидания подтверждения от узла кластера. По умолчанию: 1024.

HASyncMaxPktBurst	Максимальное количество пакетов синхронизации состояния, отправляемых одновременно. По умолчанию: 20.
HAInitialSilence	Период времени в секундах, в течение которого устройство не будет отправлять пакеты обнаружения при запуске или после повторной конфигурации. По умолчанию: 5.
UseUniqueSharedMAC	Используйте уникальный совместно используемый MAC-адрес для каждого интерфейса. По умолчанию: Yes (Да).
HADeactivateBeforeReconf	Выключить (передать управление) перед повторной настройкой, если узел активен. По умолчанию: Да.
ReconfFailoverTime	Количество секунд без отклика перед отказом при повторной настройке HA (0=немедленный отказ). По умолчанию: 0.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.21. HTTPALGBanners

Описание

Файлы баннера HTTP определяют внешний вид Web-страниц с ограничением HTTP ALG.

Свойства

Name	Символьное имя для файлов баннера HTTP (идентификатор).
CompressionForbidden	HTML для Web-страницы CompressionForbidden.html.
ContentForbidden	HTML для Web-страницы ContentForbidden.html.
URLForbidden	HTML для Web-страницы URLForbidden.html.
RestrictedSiteNotice	HTML для Web-страницы RestrictedSiteNotice.html.
ReclassifyURL	HTML для Web-страницы ReclassifyURL.html.
Comments	Описание текущего объекта (опционально).

3.22. HTTPAuthBanners

Описание

Файлы баннера HTTP определяют внешний вид Web-страниц аутентификации HTML.

Свойства

Name	Символьное имя для файлов баннера HTTP (идентификатор).
FormLogin	HTML для Web-страницы FormLogin.html.
LoginSuccess	HTML для Web-страницы LoginSuccess.html.
LoginFailure	HTML для Web-страницы LoginFailure.html.
LoginalreadyDone	HTML для Web-страницы LoginAlreadyDone.html.
LoginChallenge	HTML для Web-страницы LoginChallenge.html.
LoginChallengeTimeout	HTML для Web-страницы LoginChallenge.html Timeout
LogoutSucces	HTML для Web-страницы LogoutSuccess.html.
LogoutSuccessBasicAuth	HTML для Web-страницы LogoutSuccessBasicAuth.html.
FileNotFound	HTML для Web-страницы FileNotFound.html.
Comments	Описание текущего объекта (опционально).

3.23. HTTPPoster

Описание

Используйте HTTP Poster для динамического DNS или автоматического входа в сервисы с использованием аутентификации через Web-интерфейс.

Свойства

URL1	Первый URL-адрес, который будет опубликован, когда шлюз безопасности будет загружен (опционально).
URL2	Второй URL-адрес, который будет опубликован, когда шлюз безопасности будет загружен (опционально).
URL3	Третий URL-адрес, который будет опубликован, когда шлюз безопасности будет загружен (опционально).
RepDelay	Задержка в секундах, пока все URL-адреса не будут повторно выбраны. По умолчанию: 1200.
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.24. HWM

Описание

Аппаратный мониторинг позволяет контролировать работу аппаратных датчиков.

Свойства

Name	Символьное имя для объекта.
Type	Тип мониторинга.
Sensor	Индекс датчика.
MinLimit	Нижний предел (опционально).
MaxLimit	Верхний предел (опционально).
EnableMonitoring	Включить/выключить мониторинг. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.25. IDList

Описание

Идентификационный список содержит идентификаторы, используемые в процессе аутентификации при установке IPsec-туннеля.

Свойства

Name	Символьное имя для списка идентификаторов (идентификатор).

Comments	Описание текущего объекта (опционально).

3.25.1. ID

Описание

Идентификатор позволяет задать параметры напротив поля объекта в сертификате X.509 при установке IPsec-туннеля.

Свойства

Name	Символьное имя для объекта.
Type	IP, DNS, E-Mail или Distinguished Name (Различаемое имя).
IP	IP-адрес.
Hostname	Имя узла.
CommonName	Стандартное имя владельца сертификата (опционально).
OrganizationName	Наименование организации, владеющей сертификатом (опционально).
OrganizationalUnit	Организационная единица, владеющая сертификатом (опционально).
Country	Определяет страну.
LocalityName	Местоположение.
EMailAddress	Адрес электронной почты.
DNTuples	Введите выше наиболее общие типы DN, или ниже - в виде разделенного запятыми списка типов. Т.е. 'SN=12345, S=Smith' для серийного номера и фамилии. (опционально).
Comments	Описание текущего объекта (опционально).

3.26. IDPRule

Описание

Правило IDP определяет фильтр для соответствующего специального сетевого трафика. При совпадении с критерием фильтра действия правила IDP оцениваются и принимаются возможные меры.

Свойства

Index	Индекс объекта, начиная с 1 (идентификатор).
Name	Символьное имя для правила (опционально).
SourceInterface	Определяет имя принимающего интерфейса для сравнения с полученным пакетом.
SourceNetwork	Определяет диапазон IP-адресов отправителя для сравнения с полученным пакетом.
DestinationInterface	Определяет интерфейс назначения для сравнения с полученным пакетом.
DestinationNetwork	Определяет диапазон IP-адресов для сравнения с IP-адресом назначения полученного пакета.
Service	Определяет службу, которая будет использоваться в качестве параметра фильтра при сопоставлении трафика с данным правилом.
Schedule	При добавлении расписания для правила шлюз безопасности разрешит включение этого правила только в назначенное время (опционально).
InsertionEvasion	Защитить от вредоносных атак. По умолчанию: Yes (Да).
URIIllegalUTF8	Позволяет задать действие, которое необходимо предпринять в случае, если в HTTP URI отображены некорректные символы UTF-8. По умолчанию: Log (Занести в журнал).
URIIllegalHex	Позволяет задать действие, которое необходимо предпринять в случае, если в HTTP URI отображено некорректное шестнадцатеричное кодирование (%xx). По умолчанию: DropLog.
URIDoubleEncode	Позволяет задать действие, которое необходимо предпринять в случае, если в HTTP URI отображены дважды закодированные символы. По умолчанию: Ignore (Игнорировать).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.26.1. IDPRuleAction

Описание

Объект IDP Rule Action (Действие IDP правила) позволяет определить, какие сигнатуры искать в сетевом трафике, и какое действие предпринять в случае обнаружения таких сигнатур.

Свойства

Action	Действие, предпринимаемое при обнаружении данной сигнатуры. По умолчанию: Protect (Включить защиту).
Signatures	Позволяет определить какую сигнатуру(-ы) искать в сетевом трафике (опционально).
BlackList	Активировать «черный» список. По умолчанию: No (Нет).
BlackListTimeToBlock	Количество секунд, в течение которых должен действовать динамический «черный» список (опционально).
BlackListBlockOnlyService	Блокировать только службу, которая активировала «черный» список. По умолчанию: No (Нет).
BlackListIgnoreEstablished	Не прерывать существующее соединение. По умолчанию: No (Нет).
PipeLimit	Позволяет определить предельное значение полосы пропускания в Кбит/с для узлов, активируемых данным действием.
PipeNetwork	Функция управления пропускной способностью трафика будет применяться только к узлам, находящимся в пределах данной сети. По умолчанию: 0/0.
PipeNewConnections	Включить передачу через Pipe-канал новых соединений к одному и тому же узлу и от него. По умолчанию: No (Нет).
PipeTimeWindow	Регулирование новых соединений к запущенному узлу и от него завершится по истечении заданного времени. По умолчанию: 10.
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.27. IGMPRule

Описание

Правило IGMP позволяет определить, как обращаться с входящими отчетами IGMP и исходящими

запросами IGMP.

Свойства

Index	Индекс объекта, начиная с 1 (идентификатор).
Name	Символьное имя для правила (опционально).
Type	Тип сообщений IGMP, к которому применяется правило. По умолчанию: Report (Отчет).
Action	Drop (Отклонить), Snoop (Отследить), Proxy или PIM. По умолчанию: Drop.
SourceInterface	Позволяет определить имя принимающего интерфейса для сравнения с полученным пакетом.
SourceNetwork	Определяет диапазон IP-адресов отправителя для сравнения с полученным пакетом.
DestinationInterface	Позволяет определить интерфейс назначения для сравнения с полученным пакетом. По умолчанию: core (Центральный).
MulticastGroup	Позволяет определить группу многоадресной рассылки для сравнения с полученным пакетом.
MulticastSource	Позволяет определить источник многоадресной рассылки для пакетов, соответствующих данному правилу.
RelayInterface	Позволяет задать интерфейс, через который будет осуществляться ретрансляция IGMP-сообщений.
TranslateMGroup	Преобразовать группу многоадресной рассылки для пакетов, соответствующих данному правилу. По умолчанию: No (Нет).
GrpAllToOne	Перезаписать все группы многоадресной рассылки в один IP-адрес. По умолчанию: No (Нет).
NewGrpIP	Преобразовать группу многоадресной рассылки в данный адрес.
TranslateMSource	Пропустить данные IGMP, не соответствующие данному правилу, к следующему правилу. По умолчанию: No (Нет).
SrcAllToOne	Перезаписать все источники многоадресной рассылки в один IP-адрес. По умолчанию: No (Нет).
NewSrcIP	Преобразовать источник многоадресной рассылки в данный адрес.
Filter	Пропустить данные IGMP, не соответствующие данному правилу, к следующему правилу. По умолчанию: Yes (Да).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).

Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.28. IGMPSetting

Описание

Параметры IGMP можно настроить как для одного, так и для группы интерфейсов с тем, чтобы они соответствовали характеристикам сети.

Свойства

Name	Символьное имя правила (идентификатор).
Interface	Интерфейсы, к которым данные настройки будут применяться.
RobustnessVariable	IGMP устойчив к (Переменная устойчивости - 1) потерям пакетов. По умолчанию: 2.
MaxRequestPerSecond	Максимальное количество IGMP-запросов для обработки в секунду. По умолчанию: 100.
RouterVersion	Группа маршрутизаторов, отправляющих в сеть IGMP-запросы, должна использовать одинаковую версию протокола IGMP. По умолчанию: IGMPv3.
LowestCompatibleVersion	Минимальная поддерживаемая версия IGMP для разрешения входящих запросов По умолчанию: IGMPv1.
QueryInterval	Интервал между общими запросами, отправляемыми шлюзом безопасности. По умолчанию: 125000.
QueryResponseInterval	Максимальное время, в течение которого узел (клиент) должен отправить ответ на запрос. По умолчанию: 10000.
LastMemberQueryInterval	Максимальное время, в течение которого узел (клиент) должен отправить ответ на специальный запрос группы или группы и источника. По умолчанию: 10000.
LastMemberQueryCount	Количество отправленных специальных запросов группы или группы и источника, прежде чем шлюз безопасности решит, что больше нет подписчиков на группу специальной многоадресной рассылки. По умолчанию: 2.
StartupQueryInterval	Интервал между общими запросами, отправляемыми на этапе запуска. По умолчанию: 30000.
StartupQueryCount	Количество запросов, отправляемых на этапе запуска. По

	умолчанию: 2.
UnsolicitedReportInterval	Время между повторными отправлениями отчетов о начальной подписке узла в группе. По умолчанию: 1000.
ReactToOwnQueries	Должна ли система отвечать на запросы отчетов учасника группы, отправленных самой системой. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.29. IKEAlgorithms

Описание

Данный объект позволяет выполнить настройку алгоритмов, используемых на этапе IKE IPsec-сессии.

Свойства

Name	Символьное имя объекта (идентификатор).
NULLEnabled	Включить открытый текст. По умолчанию: No (Нет).
DESEnabled	Включить алгоритм шифрования DES. По умолчанию No (Нет).
MD5Enabled	Включить алгоритм контроля целостности MD5. По умолчанию: No (Нет)
SHA1Enabled	Включить алгоритм контроля целостности SHA1. По умолчанию: No (Нет)
XCBCEnabled	Включить алгоритм контроля целостности XCBC-AES. По умолчанию: No (Нет)
Comments	Описание текущего объекта (опционально).

3.30. Interface

Описание

В данной категории представлены следующие типа объектов.

3.30.1. DefaultInterface

Описание

Специальный интерфейс, используемый для представления внутренних механизмов в системе, а также абстрактного «any» интерфейса.

Свойства

Name	Символьное имя объекта (идентификатор).
Comments	Описание текущего объекта (опционально).

3.30.2. Ethernet

Описание

Ethernet-интерфейс представляет собой логическую конечную точку для Ethernet-трафика.

Свойства

Name	Символьное имя интерфейса (идентификатор).
IP	IP-адрес интерфейса.
Network	Сеть интерфейса.
DefaultGateway	Основной шлюз интерфейса (опционально).
Broadcast	Широковещательный адрес подключенной сети (опционально).
PrivateIP	Частный IP-адрес данного узла высокой отказоустойчивости (опционально).
NOCHB	Данная опция позволяет отключить отправку периодических пакетов обнаружения кластеров для данного интерфейса (используется HA, чтобы определить, находится ли узел в режиме online, и работает ли он). (Опционально).
MTU	Размер самого большого пакета (в байтах), который может быть пропущен дальше. По умолчанию: 1500.
Metric	Метрика для автоматически созданного маршрута. По умолчанию: 100.
DHCPEnabled	Включить DHCP-клиента на данном интерфейсе. По умолчанию: No (Нет).
DHCPHostName	Дополнительное имя DHCP-узла. Оставьте поле незаполненным для использования имени по умолчанию (опционально).
EthernetDevice	Аппаратные настройки Ethernet-интерфейса.
AutoSwitchRoute	Включить режим transparent, который означает, что маршрут переключения добавляется для данного интерфейса автоматически. По умолчанию: No (Нет).
AutoInterfaceNetworkRoute	Автоматически добавить маршрут для данного интерфейса, используя данную сеть. По умолчанию: Yes (Да).
AutoDefaultGatewayRoute	Автоматически добавить маршрут по умолчанию для данного интерфейса, используя указанный основной шлюз. По умолчанию: Yes (Да).

DHCPDNS1	IP-адрес предпочитаемого DNS-сервера (опционально).
DHCPDNS2	IP-адрес альтернативного DNS-сервера (опционально).
ReceiveMulticastTraffic	Позволяет установить режим получения многоадресного трафика на интерфейсе. По умолчанию: Auto (Автоматически).
DHCPPreferredIP	Установить предпочитаемый IP-адрес, который будет включен в запрос к DHCP-серверу (опционально).
DHCPAllowStaticRoutes	Разрешить использование статических маршрутов, отправляемых от DHCP-сервера. По умолчанию: No (Нет).
DHCPPreferedLeaseTime	Установить предпочитаемое время аренды, которое будет включено в запрос к DHCP-серверу (опционально).
DHCPLeaseFilter	Разрешенные диапазоны IP-адресов для DHCP-аренды (опционально).
DHCPServerFilter	Диапазоны IP-адресов для DHCP-серверов, от которых принимаются сроки аренды. (Опционально).
DHCPDisallowIPConflict	Не допускать коллизии IP-адресов со статическими маршрутами. По умолчанию: Yes (Да).
DHCPDisallowNetConflicts	Не допускать коллизии сети со статическими маршрутами. По умолчанию: Yes (Да).
VLanQoSInherit	Установить, должны ли VLAN, использующие интерфейс, наследовать биты IP QoS. По умолчанию: No (Нет).
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.30.3. GRETunnel

Описание

GRE-интерфейс – это туннель общей инкапсуляции маршрутов (Generic Routing Encapsulation) в существующей IP-сети (нет шифрования, нет аутентификации, только инкапсуляция).

Свойства

Name	Символьное имя интерфейса (идентификатор).
IP	IP-адрес GRE-интерфейса.

Network	Сетевой адрес GRE-интерфейса.
RemoteEndpoint	IP-адрес удаленной конечной точки.
EncapsulationChecksum	Добавить дополнительный уровень контрольной суммы над уровнем протокола IPv4. По умолчанию: No (Нет).
OriginatorIPType	IP-адрес, используемый в качестве источника IP, например, в NAT. По умолчанию: LocalInterface.
OriginatorIP	Заданный вручную IP-адрес отправителя для использования в качестве IP-источника, например, в NAT.
Metric	Метрика для автоматически созданного маршрута. По умолчанию: 90.
AutoInterfaceNetworkRoute	Автоматически добавить маршрут для данного интерфейса, используя данную удаленную сеть. По умолчанию: Yes (Да).
OuterPBRTable	Внешняя таблица маршрутизации на основе правил. По умолчанию: main (основная).
UseSessionKey	Позволяет определить, использовать ключ сессии или нет. По умолчанию: No (Нет).
SessionKey	Ключ сессии. По умолчанию: 0.
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.30.4. InterfaceGroup

Описание

Группа интерфейсов позволяет объединить нескольких интерфейсов для упрощения настройки политики безопасности.

Свойства

Name	Символьное имя интерфейса (идентификатор).
Equivalent	Позволяет определить, должны ли интерфейсы считаться эквивалентом безопасности. Т.е. при включении данной опции группа интерфейсов может использоваться в качестве интерфейса назначения в правилах, где может потребоваться перемещение соединений между двумя

	интерфейсами. По умолчанию: No (Нет).
Members	Интерфейсы, входящие в группу.
Comments	Описание текущего объекта (опционально).

3.30.5. IPsecTunnel

Описание

Данный объект позволяет задать конечную точку IPsec-туннеля, которая будет использоваться в качестве логического интерфейса в системе.

Свойства

Index	Индекс объекта, начиная с 1 (идентификатор).
Name	Символьное имя интерфейса (идентификатор).
LocalNetwork	Сеть по "эту сторону" IPsec-туннеля. IPsec-туннель будет установлен между данной сетью и удаленной сетью.
RemoteNetwork	Сеть, подключенная к удаленному шлюзу. IPsec-туннель будет установлен между локальной сетью и данной сетью.
RemoteEndpoint	IP-адрес удаленной конечной точки. Это адрес, с которым шлюз безопасности установит IPsec-туннель. Данная опция также позволяет определить, откуда разрешены входящие IPsec-туннели (опционально).
IKEConfigModePool	Позволяет выбрать IKE Config Mode Pool для туннеля (опционально).
IKEAlgorithms	Список IKE Proposal, используемый с туннелем.
IPsecAlgorithms	Список IPsec Proposal, используемый с туннелем.
IKELifeTimeSeconds	Продолжительность IKE-соединения в секундах. Каждый раз по истечении продолжительности соединения, выполняется новая фаза-1. По умолчанию: 28800.
IPsecLifeTimeSeconds	Продолжительность IPsec-соединения в секундах. Каждый раз при превышении заданного значения будет инициирована смена ключей с предоставлением нового шифрования IPsec и аутентификационных ключей сессии. По умолчанию: 3600.
IPsecLifetimeKilobytes	Продолжительность IPsec-соединения в килобайтах. По умолчанию: 0.
EncapsulationMode	Позволяет задать режим работы IPsec-туннеля: Tunnel или Transport. По умолчанию: Tunnel.
AuthMethod	Метод аутентификации: Сертификат или Общий ключ.

PSK	Позволяет выбрать Общий ключ для работы с IPsec-туннелем.
LocalIDType	Позволяет выбрать тип используемого локального идентификатора. По умолчанию: Auto (Автоматически).
LocalIDValue	Определить идентификационный номер идентификатора туннеля.
GatewayCertificate	Позволяет выбрать сертификат, используемый шлюзом безопасности для собственной аутентификации к другому узлу IPsec.
RootCertificate	Позволяет выбрать один или несколько корневых сертификатов для использования с данным IPsec-туннелем.
IDList	Позволяет выбрать список идентификации для использования с данным IPsec-туннелем. Список идентификации – это список идентификаторов, которым разрешено устанавливать IPsec-туннель (опционально).
XAuth	Off (Выключено), Required for inbound (Аутентификация обязательна для входящих туннелей) или Pass to peer gateway (Пропустить к узлу шлюза).
XAuthUsername	Имя пользователя для перехода к удаленному шлюзу с использованием аутентификации IKE XAuth.
XAuthPassword	Пароль для перехода к удаленному шлюзу с использованием аутентификации IKE XAuth.
DHCPOverIPsec	Разрешить DHCP over IPsec от клиентов с одним узлом. По умолчанию: No (Нет).
AddRouteToRemoteNet	Динамически добавлять маршрут к удаленным сетям при установке туннеля. По умолчанию: No (Нет).
PlaintextMTU	Размер в байтах для фрагментации пакетов с незашифрованным текстом (вместо того, чтобы фрагментировать IPsec). По умолчанию: 1420.
OriginatorIPType	IP-адрес, используемый в качестве источника IP-адреса источника, например, в NAT. По умолчанию: LocalInterface.
OriginatorIP	Заданный вручную IP-адрес отправителя, используемый в HA.
OriginatorHAIP	Заданный вручную частный IP-адрес отправителя, используемый в HA (опционально).
IKEMode	Позволяет выбрать режим работы IKE: main или aggressive. По умолчанию: Main.
DHGroup	Группа Диффи-Хеллмана, используемая при обмене ключами в IKE. По умолчанию: 2.
PFS	Позволяет определить, должно ли использоваться PFS или нет. По умолчанию: No (Нет).
PFSDHGroup	Позволяет определить, какую группу Диффи-Хеллмана использовать с PFS. По умолчанию: 2.

SetupSAPer	Установить SA (Security Association) для сети, узла или порта. По умолчанию: Net (Сеть).
DeadPeerDetection	Включить Обнаружение недействующего узла. По умолчанию: Yes (Да).
NATTraversal	Включить или выключить NAT traversal. По умолчанию: OnIfNeeded (Включается при необходимости).
KeepAlive	Disable (Выключен), Auto (Автоматически) или Manual (Вручную). По умолчанию: Disable.
KeepAliveSourceIP	IP-адрес источника, используемый при отправке ping-запросов ICMP keep-alive.
KeepAliveDestinationIP	IP-адрес назначения, используемый при отправке ping-запросов ICMP keep-alive.
Metric	Метрика для автоматически созданного маршрута. По умолчанию: 90.
AutoInterfaceNetworkRoute	Автоматически добавить маршрут для данного интерфейса, используя указанную удаленную сеть. По умолчанию: Yes (Да).
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.30.6. L2TPClient

Описание

Интерфейс PPTP/L2TP-клиента - это туннель PPP (Point-to-Point Protocol) в существующей IP-сети. IP-адрес и DNS-серверы для данного интерфейса назначаются динамически.

Свойства

Name	Символьное имя интерфейса (идентификатор).
IP	Имя узла для хранения заданного IP-адреса. Если данный объект сети существует, и его значение отличается от 0.0.0.0, PPTP/L2TP-клиент попытается получить IP-адрес от PPTP/L2TP-сервера в качестве предпочитаемого IP-адреса (опционально).
Network	Сеть, трафик которой должен маршрутизироваться в туннель.

RemoteEndpoint	IP-адрес L2TP/PPTP-сервера. .
TunnelProtocol	Позволяет задать для данного туннеля протокол: PPTP или L2TP. По умолчанию: PPTP.
OriginatorIPType	IP-адрес, используемый в качестве IP-адреса источника, например, в NAT. По умолчанию: LocalInterface.
OriginatorIP	Заданный вручную IP-адрес отправителя, используемый в качестве IP-адреса источника, например, в NAT.
DNS1	IP-адрес предпочитаемого DNS-сервера (опционально).
DNS2	IP-адрес альтернативного DNS-сервера (опционально).
Username	Имя пользователя, применяемое для данного PPTP/L2TP-интерфейса.
Password	Пароль, используемый для данного PPTP/L2TP интерфейса.
PPPAuthNoAuth	Разрешить отсутствие аутентификации для данного туннеля. По умолчанию: No (Нет).
PPPAuthPAP	Использовать протокол аутентификации PAP для данного туннеля. Имя пользователя и пароль отправляются открытым текстом. По умолчанию: Yes (Да).
PPPAuthCHAP	Использовать протокол аутентификации CHAP для данного туннеля. По умолчанию: Yes (Да).
PPPAuthMSCHAP	Использовать протокол аутентификации MS-CHAP для данного туннеля. По умолчанию: Yes (Да).
PPPAuthMSCHAPv2	Использовать протокол аутентификации MS-CHAP v2 для данного туннеля. По умолчанию: Yes (Да).
MPPENone	Разрешить аутентификацию без использования шифрования MPPE (Microsoft Point-to-Point Encryption). По умолчанию: Yes (Да).
MPPERC440	Использовать 40-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
MPPERC456	Использовать 56-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
MPPERC4128	Использовать 128-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
DialOnDemand	Включить функцию Dial-on-demand (Соединение по требованию). Таким образом, L2TP/PPTP-туннель не будет установлен, пока трафик не отправлен на интерфейс. По умолчанию: No (Нет).
ActivitySensing	Позволяет определить в каких случаях должно срабатывать соединение по требованию: для входящего или исходящего трафика, или в обоих случаях. По умолчанию: BiDirectional (Двунаправленное).

IdleTimeout	Таймаут простоя в секундах для соединения по требованию. По умолчанию: 3600.
Metric	Метрика для автоматически созданного маршрута. По умолчанию: 90.
MTU	Размер (в байтах) самого большого пакета, который может быть пропущен дальше. По умолчанию: 1456.
AutoInterfaceNetworkRoute	Автоматически добавить маршрут для данного интерфейса, используя указанную удаленную сеть.
MPPEAllowStateful	Разрешить использование шифрования MPPE с контролем состояния (менее защищенное, использовать только для совместимости). По умолчанию: No (Нет).
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.30.7. L2TPServer

Описание

Интерфейс PPTP/L2TP-сервера позволяет прервать PPP-туннели (Point-to-Point Protocol), установленные в существующих IP-сетях.

Свойства

Name	Символьное имя интерфейса (идентификатор).
IP	IP-адрес интерфейса PPTP/L2TP-сервера.
TunnelProtocol	Позволяет задать для данного туннеля протокол: PPTP или L2TP. По умолчанию: PPTP.
Interface	Интерфейс, на котором должен прослушиваться PPTP/L2TP-сервер.
ServerIP	IP-адрес, который должен прослушиваться PPTP/L2TP-сервером. Это может быть IP-адрес интерфейса или, например, IP-адрес, опубликованный ARP.
UseUserAuth	Включить использование правил аутентификации пользователя на данном сервере. По умолчанию: Yes (Да).
MPPENone	Разрешить отсутствие аутентификации для данного туннеля. По умолчанию: Yes (Да).

MPPERC440	Использовать 40-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
MPPERC456	Использовать 56-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
MPPERC4128	Использовать 128-битный ключ RC4 сессии MPPE с протоколом аутентификации MS-CHAP или MS-CHAP v2. По умолчанию: Yes (Да).
IPPool	Диапазон, группа или сеть, которую PPTP/L2TP-сервер будет использовать в качестве пула IP-адресов для последующего предоставления клиентам.
DNS1	IP-адрес предпочитаемого DNS-сервера (опционально).
DNS2	IP-адрес альтернативного DNS-сервера (опционально).
NBNS1	IP-адрес предпочитаемого WINS-сервера (Windows Internet Name Service), применяемого в среде Microsoft, который использует серверы имен NetBIOS (NBNS) для назначения IP-адресов именам NetBIOS (опционально).
NBNS2	IP-адрес предпочитаемого WINS-сервера (Windows Internet Name Service), применяемого в среде Microsoft, который использует серверы имен NetBIOS (NBNS) для назначения IP-адресов именам NetBIOS (опционально).
AllowedRoutes	Позволяет ограничить сети, для которых маршруты могут быть добавлены автоматически. По умолчанию: all-nets (все сети).
MPPEAllowStateful	Разрешить использование шифрования MPPE с контролем состояния (менее защищенное, использовать только для совместимости). По умолчанию: No (Нет).
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main.
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов, предназначенных для ретрансляции через Proxy ARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейс/интерфейсы, на которых шлюз безопасности должен опубликовать маршруты, необходимые для ретрансляции через Proxy ARP (опционально).
Comments	Описание текущего объекта (опционально).

3.30.8. LoopbackInterface

Описание

Интерфейсы «обратной петли» примут все отправляемые через них пакеты и передадут их обратно другому интерфейсу, как заново полученные пакеты.

Свойства

Name	Символьное имя интерфейса (идентификатор).
LoopTo	Интерфейс «обратной петли» (опционально).
IP	IP-адрес интерфейса.
Network	Сеть интерфейса.
Broadcast	Широковещательный адрес подключенной сети (опционально).
Metric	Метрика для автоматически созданного маршрута. По умолчанию: 100.
AutoInterfaceNetworkRoute	Автоматически добавить маршрут для данного интерфейса, используя указанную удаленную сеть.
MemberOfRoutingTable	All (Все) или Specific (Определенные). По умолчанию: All.
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов, предназначенных для ретрансляции через Proxy ARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейс/интерфейсы, на которых шлюз безопасности должен опубликовать маршруты, необходимые для ретрансляции через Proxy ARP (опционально).
Comments	Описание текущего объекта (опционально).

3.30.9. PPPoETunnel

Описание

Интерфейс PPPoE представляет собой туннель PPP (point-to-point protocol) поверх существующего физического Ethernet-интерфейса. IP-адрес назначается динамически.

Свойства

Name	Символьное имя интерфейса (идентификатор).
EthernetInterface	Физический Ethernet-интерфейс, подключенный к сети PPPoE-сервера.
IP	Имя узла для хранения назначенного IP-адреса.
Network	Сеть, из которой трафик должен быть смаршрутизирован в туннель.
DNS1	IP-адрес предпочитаемого DNS-сервера (опционально).
DNS2	IP-адрес альтернативного DNS-сервера (опционально).
Username	Имя пользователя, используемое для данного PPPoE-туннеля.
Password	Пароль, используемый для данного PPPoE-туннеля.
ServiceName	Имя службы PPPoE-сервера, используемое для того, чтобы различать два (или более) PPPoE-сервера, подключенных к одной и той же сети (опционально).
PPPAuthNoAuth	Отмена аутентификации для данного туннеля. По умолчанию: No (Нет).
PPPAuthPAP	Используйте протокол аутентификации PAP для данного туннеля. Имя пользователя и пароль будут отправлены в незашифрованном виде. По умолчанию: Yes (Да).
PPPAuthCHAP	Используйте протокол аутентификации CHAP для данного туннеля. По умолчанию: Yes (Да).
PPPAuthMSCHAP	Используйте протокол аутентификации MS-CHAP для данного туннеля. По умолчанию: Yes (Да).
PPPAuthMSCHAPv2	Используйте протокол аутентификации MS-CHAP v2 для данного туннеля. По умолчанию: Yes (Да).
DialOnDemand	После включения опции **Dial-on-demand** (Соединение по запросу) PPPoE-туннель не будет установлен до тех пор, пока трафик не отправлен на интерфейс. По умолчанию: No (Нет).
ActivitySensing	С помощью данной опции можно указать, для какого типа трафика необходимо запустить опцию **Dial-on-demand** (Соединение по запросу): входящего, исходящего или для трафика в обоих направлениях. По умолчанию: BiDirectional.
IdleTimeout	Таймаут простоя (в секундах) для опции **Dial-on-demand** (по умолчанию: 3600).
Metric	Метрика для автоматически создаваемого маршрута (по умолчанию: 90).
AutoInterfaceNetworkRoute	Автоматическое добавление марушрута на данный интерфейс с использованием предоставленной сети. По умолчанию: Yes (Да).
Schedule	Расписание, в котором указано время активности PPPoE-

	туннеля (по умолчанию: опционально).
ForceUnnumbered	Отмена назначения номера PPPoE-туннелю. По умолчанию: No (Нет).
SpecifyManually	Указание объекта IP-адрес вручную. По умолчанию: No (Нет).
MTU	Максимальный размер передаваемого пакета (в байтах). По умолчанию: 1492.
MemberOfRoutingTable	All (Все) или Specific (Определенный). По умолчанию: All (Все).
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.30.10. VLAN

Описание

Используйте VLAN для указания виртуального интерфейса, совместимого со стандартом IEEE 802.1Q Virtual LAN.

Свойства

Name	Символьное имя интерфейса (идентификатор).
Ethernet	Ethernet-интерфейс для виртуальной локальной сети.
VLANID	Идентификатор (ID) виртуальной локальной сети, используемый для интерфейса данной сети. Если две виртуальные LAN указаны на одном и том же Ethernet-интерфейсе, у них не может быть один и тот же идентификатор. По умолчанию: 0.
IP	IP-адрес виртуальной локальной сети, если необходимо задать адрес, отличающийся от IP-адреса Ethernet-интерфейса.
Network	Адрес интерфейса виртуальной LAN.
DefaultGateway	Основной шлюз интерфейса виртуальной LAN (опционально).
Broadcast	Широковещательный адрес виртуальной LAN (опционально).
PrivateIP	Приватный IP-адрес данного узла с высокой отказоустойчивостью (опционально).

Metric	Метрика для автоматически создаваемого маршрута. По умолчанию: 100.
AutoSwitchRoute	Включить прозрачный режим, означающий, что маршрут автоматически добавлен на данный интерфейс виртуальной LAN. По умолчанию: No (Нет).
AutoInterfaceNetworkRoute	Автоматическое добавление марушрута на данный интерфейс виртуальной LAN с использованием предоставленной сети. По умолчанию: Yes (Да).
AutoDefaultGatewayRoute	Автоматическое добавление марушрута по умолчанию на данный интерфейс виртуальной LAN с использованием предоставленного основного шлюза. По умолчанию: Yes (Да).
PrioCopyPolicy	Задайте QoS в качестве политики копирования приоритета VLAN. По умолчанию: InheritFromPhys.
MemberOfRoutingTable	All (Все) или Specific (Определенный). По умолчанию: All (Все).
RoutingTable	Таблица PBR для добавления IP-маршрута интерфейса. Указанная таблица маршрутизации будет использоваться при любом поиске маршрутов, кроме случаев, заранее определенных правилом маршрутизации. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.31. IPPool

Описание

Пул IP-адресов – это динамический объект, содержащий сроки аренды IP-адресов, назначаемых DHCP-сервером. Пул IP-адресов используется в качестве источника адресов для подсистем, которым может потребоваться распределение адресов, например, IPsec в режиме Configuration.

Свойства

Name	Символьное имя пула IP-адресов (идентификатор).
DHCPServerType	Указать адрес сервера или использовать на интерфейсе широковещательную рассылку. По умолчанию: Interface.
ServerIP	Адрес DHCP-сервера.
ServerFilter	DHCP-сервер, который назначает сроки аренды (опционально).
Interface	Интерфейс DHCP-сервера, назначаемого сроки аренды.
IPFilter	IP-адрес, полученный от DHCP-сервера (опционально).
ReceiveInterface	Интерфейс, используемый при обмене данными с DHCP-

	сервером (опционально).
PrefetchLeases	Количество предварительно выбранных сроков аренды в пуле IP-адресов. По умолчанию: 3.
MaxFree	Максимальное количество свободных IP-адресов в пуле адресов, остальные адреса будут возвращены на DCHP-сервер (опционально).
MaxClients	Максимальное количество клиентов в пуле IP-адресов (опционально).
MacRangeStart	Начальный адрес диапазона MAC-адресов, используемого DCHP-клиентами при обмене данными с сервером (опционально).
MacRangeEnd	Конечный адрес диапазона MAC-адресов, используемого DCHP-клиентами при обмене данными с сервером (опционально).
SenderIP	Локальный IP-адрес, используемый при обмене данными с DCHP-сервером (опционально).
AscendingFreeList	После включения данной опции IP-адреса выдаются в обычном порядке из списка свободных адресов. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.32. IPRuleSet

Описание

IP Rule Set – это независимый набор IP-правил. Действие по умолчанию: Drop (Отклонить).

Свойства

Name	Имя, идентифицирующее данный IPRuleSet (идентификатор).
Comments	Описание текущего объекта (опционально).

3.32.1. IPRule

Описание

IP-правило определяет действие, выполняемое над сетевым трафиком, прошедшим определенную фильтрацию.

Свойства

Name	Символьное имя правила (опционально).

Action	Reject, Drop, FwdFast, Allow, NAT, SAT ,SLB_SAT, GOTO или RETURN.
SourceInterface	Имя принимающего интерфейса для сравнения с полученным пакетом.
SourceNetwork	Диапазон IP-адресов отправителя для сравнения с полученным пакетом.
DestinationInterface	Интерфейс назначения для сравнения с полученным пакетом.
DestinationNetwork	Диапазон IP-адресов для сравнения с полученным пакетом.
Service	Сервис, который будет использоваться в качестве параметра фильтра в случае соответствия трафика данному правилу.
Schedule	Если в правило добавлено расписание, шлюз безопасности разрешает запуск правила только в указанное время (опционально).
NATAction	Адрес отправителя или адрес интерфейса. По умолчанию: UseInterfaceAddress.
NATSenderAddress	Адрес отправителя, который необходимо использовать.
NATPool	Адрес отправителя, который необходимо использовать.
SATTranslate	Преобразование IP-адреса источника или назначения. По умолчанию: DestinationIP.
SATTranslateToIP	Преобразование в данный IP-адрес.
SATTranslateToPort	Преобразование в данный порт (опционально).
SATAllToOne	Замена всех IP-адресов назначения одним IP-адресом. По умолчанию: No (Нет).
SLBAddresses	IP-адреса серверов в кластере серверов.
SLBStickiness	Режим привязки. По умолчанию: None (Нет).
SLBIdleTimeOut	Новые соединения, устанавливаемые в период таймаута простоя, назначаются тому же серверу, что и предыдущие соединения с данного адреса. После каждой установки нового соединения таймаут обновляется По умолчанию: 30
SLBMaxSlots	Максимальное количество слотов для IP и привязки. По умолчанию: 2048.
SLBNetSize	Диапазон IP-адресов сети для привязки. По умолчанию: 24.
SLBNewPort	Замена порта назначения данным портом (опционально).
SLBMonitorRoutingTable	Таблица маршрутизации, используемая для мониторинга сервера. По умолчанию: main (основная).
SLBMonitorPing	Включить мониторинг сервера с использованием пакетов

	ICMP Ping. По умолчанию: No (Нет).
SLBPingPollingInterval	Интервал (в миллисекундах) между запросами ping (по умолчанию: 5000).
SLBPingSamples	Количество попыток для статистики (по умолчанию: 10).
SLBPingMaxPollFails	Максимальное количество неудачных попыток запросов ping , свидетельствующих о недоступности узла. По умолчанию: 2.
SLBPingMaxAverageLatency	Максимальное время ожидания для совершения попыток. По умолчанию: 800.
SLBMonitorTCP	Мониторинг с использованием TCP handshakes. По умолчанию: No (Нет).
SLBTCPPorts	Порты, за которыми будет идти наблюдение.
SLBTCPPollingInterval	Интервал (в миллисекундах) между TCP handshake. По умолчанию: 10000.
SLBTCPSamples	Количество попыток для статистики. По умолчанию: 10.
SLBTCPMaxPollFails	Максимальное количество неудачных попыток TCP, свидетельствующих о недоступности узла. По умолчанию: 2.
SLBTCPMaxAverageLatency	Максимальное время ожидания для совершения попыток. По умолчанию: 800.
SLBMonitorHTTP	Включить мониторинг с использованием запросов HTTP. По умолчанию: No (Нет).
SLBHTTPPorts	Порты, за которыми будет идти наблюдение. По умолчанию: 80.
SLBHTTPPollingInterval	Интервал (в миллисекундах) между опросами при мониторинге. По умолчанию: 10000.
SLBHTTPSamples	Количество попыток для статистики (по умолчанию: 10).
SLBHTTPMaxPollFails	Максимальное количество неудачных попыток HTTP, свидетельствующих о недоступности узла. По умолчанию: 2.
SLBHTTPMaxAverageLatency	Максимальное время ожидания ответа для совершения попыток (по умолчанию: 800).
SLBHTTPURLType	Транслируемый URL-адрес. По умолчанию: FQDN.
SLBHTTPRequestURL	HTTP URL для мониторинга.
SLBHTTPExpectedResponse	Ожидаемый ответ HTTP.
SLBDistribution	Алгоритм, используемый для распределения нагрузки. По умолчанию: RoundRobin.
SLBWindowTime	Период времени, используемый для ретроспективного подсчета количества секунд, чтобы резюмировать количество новых соединенией для алгоритма connection-rate. По умолчанию: 10.

RequireIGMP	Перед перенаправлением трафика многоадресной рассылки необходимо выполнить запрос с использованием IGMP. По умолчанию: Yes (Да).
MultiplexArgument	Способ перенаправления и трансляции трафика.
MultiplexAllToOne	Замена всех IP-адресов назначения одним IP-адресом. По умолчанию: No (Нет).
RuleSet	Предполагаемое действие – Goto, точка, в которую перенаправляется поиск правила.
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.32.2. IPRuleFolder

Описание

Папка IP-правила (IP Rule Folder) используется для объединения IP-правил в логические группы, что значительно упрощает управление и обзор.

Свойства

Name	Имя папки (идентификатор).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.32.2.1. IPRule

В данном пункте используются определения, указанные в разделе 3.32.1, «IPRule».

3.33. IPsecAlgorithms

Описание

Настройка алгоритмов, используемых в фазе IPsec сессии IPsec.

Свойства

Name	Символьное имя объекта (идентификатор).
NULLEnabled	Включить незашифрованный текст. По умолчанию: No (Нет).
DESEnabled	Включить алгорим шифрования DES. По умолчанию: No (Нет).
MD5Enabled	Включить алгорим целостности MD5. По умолчанию: No (Нет).
SHA1Enabled	Включить алгорим целостности SHA1. По умолчанию: No (Нет).
XCBCEnabled	Включить алгорим целостности XCBC-AES. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.34. LDAPDatabase

Описание

Внешний LDAP-сервер используется для подтверждения имен пользователей и паролей.

Свойства

Name	Символьное имя сервера (идентификатор).
IP	IP-адрес сервера.
Port	TCP-порт сервера. По умолчанию: 389.
Timeout	Таймаут (в миллисекундах), используемый для обработки запросов. По умолчанию: 5.
NameAttr	Атрибут «имя» в базе данных LDAP. По умолчанию: uid.
PassAttr	Атрибут «пароль» в базе данных LDAP. По умолчанию: userPassword.
GroupsAttr	Атрибут «принадлежность к группам», используемый в базе данных LDAP. По умолчанию: memberOf.
GetGroups	Стать участником группы. По умолчанию: Yes (Да).
DomainName	Доменное имя сервера (опционально).

BaseObject	Объект, который необходимо найти в базе (опционально).
UserName	Имя пользователя (опционально).
Password	Пароль (опционально).
Type	Добавление доменного имени к имени пользователя. По умолчанию: 0.
RoutingTable	Таблица маршрутизации, в которую добавляется маршрут к узлу клиента. По умолчанию: main.
Comments	Описание текущего объекта (опционально).

3.35. LDAPServer

Описание

LDAP-сервер используется в качестве центрального хранилища сертификатов и CRL, которые при необходимости загружаются шлюзом безопасности.

Свойства

Host	IP-адрес или имя узла, используемого в качестве LDAP-сервера.
Username	Имя пользователя, используемое для доступа к LDAP-серверу (опционально).
Password	Пароль, используемый для доступа к LDAP-серверу (опционально).
Port	Номер порта, используемый для LDAP. По умолчанию: 389.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.36. LinkMonitor

Описание

Мониторинг соединения позволяет системе вести наблюдение за одним или несколькими узлами и предпринимать необходимые меры в случае их недоступности.

Свойства

Name	Действие, которое необходимо предпринять.
Addresses	IP-адреса, за которыми надо вести наблюдение.
MaxLoss	Узел считается недоступным, если он не ответил на данное количество последовательных запросов ping. По умолчанию: 7.
PingInterval	Количество миллисекунд между попытками мониторинга. По умолчанию: 250.
InitGracePeriod	После изменения настроек в течение данного количества секунд не запускайте мониторинг трафика. По умолчанию: 45.
RoutingTable	Таблица маршрутизации, используемая для мониторинга соединения. По умолчанию: main (основная).
UseSharedIP	Используйте общий IP-адрес кластера HA вместо приватного IP-адреса узла По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.37. LocalUserDatabase

Описание

Локальная база данных содержит учетные записи, использующиеся для аутентификации.

Свойства

Name	Символьное имя объекта (идентификатор).
Comments	Описание текущего объекта (опционально).

3.37.1. Пользователь

Описание

Учетные данные пользователя могут использоваться в Правилах аутентификации пользователя, которые, в свою очередь, также используются, например, PPP, IPsec XAuth, Web-аутентификация и т.д.

Свойства

Name	Имя пользователя для добавления в базу данных (идентификатор).
Password	Пароль пользователя.
Groups	Группа, участником которой является пользователь, например, Administrators (опционально).
IPPool	Если пользователь подключается по PPTP/L2TP, назначается данный статический IP-адрес (опционально).
AutoAddRouteNet	PPTP/L2TP позади пользователя (опционально).
AutoAddRouteMetric	Метрика для сети (опционально).
SSHKeys	Открытые ключи, использующиеся для авторизации через SSH (опционально).
Comments	Описание текущего объекта (опционально).

3.38. Получатель журнала

Категория, в которую сгруппированы следующие типы объектов.

3.38.1. EventReceiverSNMP2c

Описание

Получатель события SNMP2c используется для получения сообщений SNMP от системы.

Свойства

Name	Символьное имя получателя журнала (идентификатор).
IPAddress	IP-адрес назначения.
Port	Порт назначения. По умолчанию: 162.

Community	Строка community. По умолчанию: public.
RepeatCount	Счетчик повторений. По умолчанию: 0.
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. (Optional; Default: Emergency, Alert, Critical, Error, Warning, Notice, Info).
RoutingTable	Таблица маршрутизации, в которую должен быть добавлен маршрут узла клиентов. По умолчанию: main (основная).
Comments	Описание текущего объекта (опционально).

3.38.1.1. EventReceiverSNMP2c

Описание

Сообщение-исключение (LogReceiverMessageException) используется для прохождения фильтра важности событий в получателе журнала.

Свойства

LogCategory	Категория сообщения, регистрируемого в журнале.
LogID	Идентификатор сообщения, регистрируемого в журнале, если значение не указано, будут выбраны все сообщения в данной категории (опционально).
LogType	EXCLUDE или INCLUDE. По умолчанию: EXCLUDE.
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.38.2. LogReceiverMemory

Описание

Получаемые события журнала хранятся в памяти получателя (log receiver).

Свойства

Name	Символьное имя получателя журнала (идентификатор).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. (Optional; Default: Emergency, Alert, Critical, Error, Warning, Notice, Info).
Comments	Описание текущего объекта (опционально).

3.38.2.1. LogReceiverMessageException

В данном пункте используются определения, указанные в разделе 3.38.1.1, «LogReceiverMessageException».

3.38.3. LogReceiverSMTP

Описание

Получатель события SMTP, используемый для получения сообщений по электронной почте о событиях IDP.

Свойства

Name	Символьное имя получателя журнала (идентификатор).
IPAddress	IP-адрес SMTP-сервера.
Port	Номер порта, используемый для подключения к SMTP-серверу. По умолчанию: 25.
Receiver1	Адрес электронной почты, на который отправляется информация о событии.
Receiver2	Альтернативный адрес получателя (опционально).
Receiver3	Альтернативный адрес получателя (опционально).
Sender	Отправитель (по умолчанию: hostmaster).
Identity	Идентификация, указываемая в заголовке письма (по умолчанию: hostmaster).
XMailer	Информация о почтовой программе, использованной для написания письма (опционально).
Subject	TODO.
HoldTime	Период времени удержания в секундах, в течение которого должен быть достигнут порог для отправки письма. По умолчанию: 120.
MinRepeatDelay	Количество секунд, по истечении которых шлюз безопасности отправит следующее письмо. По

	умолчанию: 600.
LogThreshold	Количество событий, которые должны произойти в течение времени удержания для отправки письма. По умолчанию: 2.
Comments	Описание текущего объекта (опционально).

3.38.4. LogReceiverSyslog

Описание

Получатель системного журнала (LogReceiverSyslog) используется для получения журнала событий в стандартном формате.

Свойства

Name	Символьное имя получателя журнала (идентификатор).
IPAddress	IP-адрес получателя журнала.
Port	Номер порта, используемого для отправки журнала. По умолчанию: 514.
Facility	Тип программы (facility), используемый для ведения журнала. По умолчанию: local0.
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. (Optional; Default: Emergency, Alert, Critical, Error, Warning, Notice, Info).
RoutingTable	Таблица маршрутизации, в которую должен быть добавлен маршрут узла клиентов. По умолчанию: main.
Comments	Описание текущего объекта (опционально).

3.38.4.1. LogReceiverMessageException

В данном пункте используются определения, указанные в разделе 3.38.1.1, «LogReceiverMessageException».

3.39. NATPool

Описание

Пул NAT используется для преобразования IP-адресов источника при наличии нескольких одновременных соединений.

Свойства

Name	Символьное имя для пула NAT (идентификатор).
Type	Тип трансляции IP-адресов. По умолчанию: stateful (с сохранением состояний).
IPSource	IP-адрес источника, который необходимо использовать. По умолчанию: IPRange (Диапазон IP-адресов).
IPPool	Пул IP-адресов, используемых для трансляции.
IPPoolIPs	Количество IP-адресов в пуле.
IPRange	Диапазон IP-адресов, используемых для трансляции.
StateKeepAlive	Количество секунд без новых соединений. По умолчанию: 120.
MaxStates	Максимальное количество отслеженных состояний пула NAT с сохранением состояний (stateful). По умолчанию: 16384.
ProxyARPAllInterfaces	Постоянный выбор всех интерфейсов, включая новые, для опубликования маршрутов, необходимых для получения трафика на адресах пула NAT. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейс/интерфейсы, на которых шлюз безопасности должен опубликовать маршруты, необходимые для ретрансляции через Proxy ARP (опционально).
Comments	Описание текущего объекта (опционально).

3.40. OSPFProcess

Описание

OSPF Router Process определяет группу маршрутизаторов, обменивающихся информацией о

маршрутизации через протокол маршрутизации Open Shortest Path First.

Свойства

Name	Символьное имя процесса OSPF (идентификатор).
RouterID	IP-адрес, идентифиицирующий маршрутизатор. Если идентификатор маршрутизатора не указан, он будет вычислен автоматически на основе наибольшего IP-адреса любого интерфейса, участвующего в процессе OSPF (опционально).
PrivRouterID	Приватный идентификатор маршрутизатора данного узла с высокой отказоустойчивостью (опционально).
RFC1583	Включить эту опцию, если шлюз безопасности будет использоваться в среде, которая состоит из маршрутизаторов, поддерживающих стандарт RFC 1583. По умолчанию: No (Нет).
SPFHoldTime	Минимальное время в секундах между двумя вычислениями SPF. По умолчанию: 10.
SPFDelayTime	Интервал времени (в секундах) между принятием изменения топологии и запуском вычисления SPF. По умолчанию: 5.
LSAGroupPacing	Интервал времени (в секундах) между объединением в группу и обновлением LSA OSPF. По умолчанию: 10.
RoutesHoldtime	Период времени (в секундах), в течение которого таблица маршрутизации будет оставаться неизменной после повторной настройки записей OSPF или отказа HA. По умолчанию: 45.
RefBandwidthValue	Установка указателя полосы пропускания, используемого при подсчете стоимости интерфейса для маршрутов по умолчанию. По умолчанию: 1.
RefBandwidthUnit	Единица измерения полосы пропускания. По умолчанию: Gbps (Гбит/с).
MemoryMaxUsage	Максимальное количество оперативной памяти в килобайтах, которое разрешено использовать процессу OSPF. По умолчанию, это один процент заданной оперативной памяти. Значение 0 означает, что процессу OSPF разрешено использовать всю доступную оперативную память (опционально).
DebugPacket	Включение или выключение регистрации в журнале обрабатываемых событий, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugHello	Включение или выключение регистрации в журнале пакетов hello, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugDDesc	Включение или выключение регистрации в журнале пакетов описания базы данных, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugExchange	Включение или выключение регистрации в журнале

	пакетов обмена, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugLSA	Включение или выключение записи в журнал событий LSA, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugSPF	Включение или выключение регистрации в журнале событий вычисления OSPF, а также подробная информация о журнале. По умолчанию: Off (Выключено).
DebugRoute	Включение или выключение регистрации в журнале событий работы с таблицей маршрутизации, а также подробная информация о журнале. По умолчанию: Off (Выключено).
AuthType	Тип аутентификации для обмена OSPF-протоколами. По умолчанию: None (Нет).
AuthPassphrase	Парольная фраза, используемая для аутентификации (опционально).
AuthMD5ID	Идентификатор ключа MD5, используемый для аутентификации дайджеста MD5.
AuthMD5Key	128-битный ключ, используемый для создания дайджеста MD5 (опционально).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

3.40.1. OSPFArea

Описание

Область OSPF – это поддомен внутри процесса OSPF, включающий OSPF-интерфейсы, соседние устройства, составные данные и виртуальные соединения.

Свойства

Name	Символьное имя области (идентификатор).
AreaID	Идентификатор области, если задан 0.0.0.0, то это основная область.
Stub	Включите данную опцию для того, чтобы маршрутизатор автоматически объявлял маршрут по умолчанию, в результате чего маршрутизаторы в тупиковой области смогут достичь назначений за пределами области. По умолчанию: No (Нет).
StubSummarize	Преобразование в маршрут по умолчанию для тупиковой

	области (Суммировать). По умолчанию: Yes (Да).
StubMetric	Метрика маршрута для тупиковой области (опционально).
FilterExternal	Сетевые адреса, которые разрешено импортировать в данную область из внешних источников маршрутизации (опционально).
FilterInterArea	Сетевые адреса, которые разрешено импортировать из других маршрутизаторов внутри области (опционально).
Comments	Описание текущего объекта (опционально).

3.40.1.1. OSPFInterface

Описание

Выберите и определите свойства интерфейса, который необходимо сделать участником процесса маршрутизатора.

Свойства

Interface	Интерфейс шлюза безопасности, который будет использоваться для данного OSPF-интерфейса (идентификатор).
Type	Auto (Автоматический), Broadcast (Широковещательный), Point-to-point (Точка-точка) или Point-to-multipoint (Точка-много точек). По умолчанию: Auto (Автоматический).
Network	Сеть, относящаяся к настроенному OSPF-интерфейсу (опционально).
MetricType	Значение метрики или пропускная способность. По умолчанию: MetricValue.
Metric	Метрика маршрутизации для данного OSPF-интерфейса. По умолчанию: 10.
BandwidthValue	Пропускная способность для данного OSPF-интерфейса.
BandwidthUnit	Единица измерения полосы пропускания. По умолчанию: Mbps (Мбит/с).
UseDefaultAuth	Использовать настройку аутентификации, определенную в OSPF-процессе. По умолчанию: Yes (Да).
AuthType	Тип аутентификации для обмена OSPF-протоколами. По умолчанию: None (Нет).
AuthPassphrase	Парольная фраза, используемаю для аутентификации (опционально).
AuthMD5ID	Идентификатор ключа MD5, используемый для аутентификации дайджеста MD5.
AuthMD5Key	128-битный ключ, используемый для создания дайджеста

	MD5 (опционально).
HelloInterval	Количество секунд между получением HELLO-пакетов, отправленных с интерфейса. По умолчанию: 10.
RtrDeadInterval	Если HELLO-пакеты не будут получены от соседнего устройства в данном интервале (в секундах), соседний маршрутизатор будет объявлен недействующим. По умолчанию: 40.
RxmtInterval	Количество секунд между повторными передачами LSA соседним устройствам на данном интерфейсе. По умолчанию: 5.
RtrPrio	Приоритет маршрутизатора; чем выше число, тем больше вероятность, что данный маршрутизатор станет DR (выделенный маршрутизатор) или BDR (резервный выделенный маршрутизатор). Если задано значение 0, данный маршрутизатор не рассматривается в качестве DR/BDR. По умолчанию: 1.
InfTransDelay	Предположительная задержка передачи для интерфейса (в секундах). Данное значение представляет собой максимальное время, которое занимает передача LSA-пакета через маршрутизатор. По умолчанию: 1.
WaitInterval	Количество секунд между моментами загрузки интерфейса и выбора DR и BDR. Данное значение должно быть больше, чем hello-интервал. По умолчанию: 40.
Passive	Включите данную опцию для возможности участия сетей в процессе маршрутизации OSPF без запуска OSPF на интерфейсе, подключенном к сети. По умолчанию: No (Нет).
IgnoreMTU	Включите данную опцию, чтобы разрешить несоответствие MTU OSPF. По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.40.1.2. OSPFNeighbor

Описание

Укажите IP-адреса, подключенных напрямую маршрутизаторов для сетей с соединением Точка-точка и Точка-много точек.

Свойства

Interface	OSPF интерфейс соседнего устройства.
IP Address	IP-адрес соседнего устройства.
Metric	Метрика соседнего устройства (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.40.1.3. OSPFAggregate

Описание

Совокупность используется для замены любого количества небольших сетей, принадлежащих локальной (внутренней) области, одной смежной сетью, которая затем может быть объявлена или скрыта.

Свойства

Network	Совокупная сеть, используемая для объединения нескольких небольших маршрутов.
Advertise	Объявить совокупность. По умолчанию: Yes (Да).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.40.1.4. OSPFVLink

Описание

У области, которая не имеет прямого подключения к основной сети, должен быть хотя бы один пограничный маршрутизатор с виртуальным подключением к маршрутизатору из основной сети.

Свойства

Name	Символьное имя виртуального соединения (идентификатор).
RouterID	Идентификатор маршрутизатора в противоположной точке виртуального соединения.
UseDefaultAuth	Используйте настройку аутентификации, определенную в OSPF-процессе. По умолчанию: Yes (Да).
AuthType	Тип аутентификации для обмена OSPF-протоколами. По умолчанию: None (Нет).
AuthPassphrase	Парольная фраза, используемая для аутентификации (опционально).

AuthMD5ID	Идентификатор ключа MD5, используемый для аутентификации дайджеста MD5.
AuthMD5Key	128-битный ключ, используемый для создания дайджеста MD5 (опционально).
Comments	Описание текущего объекта (опционально).

3.41. Pipe

Описание

Pipe (канал) определяет основные параметры формирования трафика. Правила канала определяют тип трафика и каналы, через которые он будет проходить.

Свойства

Name	Символьное имя канала (идентификатор).
LimitKbpsTotal	Общее ограничение полосы пропускания для данного канала в Кбит/с (опционально).
LimitPPSTotal	Общее количество пакетов в секунду для данного канала (опционально).
LimitKbps0	Ограничение полосы пропускания в Кбит/с для приоритета 0 (самый низкий приоритет) (опционально).
LimitPPS0	Количество пакетов в секунду для приоритета 0 (самый низкий приоритет) (опционально).
LimitKbps1	Ограничение полосы пропускания в Кбит/с для приоритета 1 (опционально).
LimitPPS1	Количество пакетов в секунду для приоритета 1 (опционально).
LimitKbps2	Ограничение полосы пропускания в Кбит/с для приоритета 2 (опционально).
LimitPPS2	Количество пакетов в секунду для приоритета 2 (опционально).
LimitKbps3	Ограничение полосы пропускания в Кбит/с для приоритета 3 (опционально).
LimitPPS3	Количество пакетов в секунду для приоритета 3 (опционально).
LimitKbps4	Ограничение полосы пропускания в Кбит/с для приоритета 4 (опционально).
LimitPPS4	Количество пакетов в секунду для приоритета 4 (опционально).
LimitKbps5	Ограничение полосы пропускания в Кбит/с для

	приоритета 5 (опционально).
LimitPPS5	Количество пакетов в секунду для приоритета 5 (опционально).
LimitKbps6	Ограничение полосы пропускания в Кбит/с для приоритета 6 (опционально).
LimitPPS6	Количество пакетов в секунду для приоритета 6 (опционально).
LimitKbps7	Ограничение полосы пропускания в Кбит/с для приоритета 7 (самый высокий приоритет) (опционально).
LimitPPS7	Количество пакетов в секунду для приоритета 7 (самый высокий приоритет) (опционально).
UserLimitKbpsTotal	Общее ограничение полосы пропускания на группу в канале в Кбит/с (опционально).
UserLimitPPSTotal	Общее ограничение полосы пропускания на группу в канале в пакетах в секунду (опционально).
UserLimitKbps0	Ограничение полосы пропускания на группу в кбит/с для приоритета 0 (самый низкий приоритет) (опционально).
UserLimitPPS0	Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 0 (самый низкий приоритет) (опционально).
UserLimitKbps1	Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 1 (опционально).
UserLimitPPS1	Ограничение полосы пропускания на группу в PPS для приоритета 1 (опционально).
UserLimitKbps2	Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 2 (опционально).
UserLimitPPS2	Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 2 (опционально).
UserLimitKbps3	Общий предел полосы пропускания на группу в Кбит/с для приоритета 3 (опционально).
UserLimitPPS3	Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 3 (опционально).
UserLimitKbps4	Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 4 (опционально).
UserLimitPPS4	Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 4 (опционально).
UserLimitKbps5	Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 5 (опционально).
UserLimitPPS5	Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 5 (опционально).
UserLimitKbps6	Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 6 (опционально).

UserLimitPPS6 — Ограничение полосы пропускания на группу в PPS (пакетах в секунду) для приоритета 6 (опционально).

UserLimitKbps7 — Общее ограничение полосы пропускания на группу в Кбит/с для приоритета 7 (самый высокий приоритет) (опционально).

UserLimitPPS7 — Ограничение полосы пропускания на группу в PPS для приоритета 7 (самый высокий приоритет) (опционально).

Grouping — Группирование включает ограничение полосы пропускания на порт/IP-адрес/сеть, а также динамическую балансировку между группами. По умолчанию: None (Нет).

GroupingNetworkSize — Если пользователи объединены в группы по сети источника или назначения, размер сети указывается в данной настройке. По умолчанию: 0.

Dynamic — Включить динамическую балансировку групп. По умолчанию: No (Нет).

PrecendenceMin — Самый низкий разрешенный приоритет для трафика в этом канале. Если входящий пакет обладает меньшим приоритетом, то значение приоритета повышается до данного значения. По умолчанию: 0.

PrecendenceDefault — Приоритет по умолчанию для канала. Если для входящего пакета приоритет не установлен, назначается данное значение. Значение должно быть выше или равно минимальному приоритету. По умолчанию: 0.

PrecendenceMaX — Самый высокий разрешенный приоритет для трафика в этом канале. Если входящий пакет обладает более высоким приоритетом, то значение приоритета снижается до данного значения. Значение должно быть выше или равно приоритету по умолчанию. По умолчанию: 7.

Comments — Описание текущего объекта (опционально).

3.42. PipeRule

Описание

Правило канала определяет политику формирования трафика – выбор каналов (Pipes) – для одного или нескольких типов трафика с одинаковым шагом, так используется стандартный набор правил.

Свойства

Index — Индекс объекта, начинается с 1 (идентификатор).

Name — Символьное имя объекта (опционально).

SourceInterface — Имя принимающего интерфейса для сравнения с полученным пакетом.

SourceNetwork — Диапазон IP-адресов отправителя для сравнения с

полученным пакетом.

DestinationInterface	Интерфейс назначения для сравнения с полученным пакетом.
DestinationNetwork	Диапазон IP-адресов для сравнения с IP-адресом назначения полученного пакета.
Service	Служба, которая будет использоваться в качестве параметра фильтра при сопоставлении трафика с данным правилом.
Schedule	Если в правило добавлено расписание, шлюз безопасности разрешает запуск правила только в указанное время (опционально).
ForwardChain	Один или несколько каналов для передачи трафика (опционально).
ReturnChain	Один или несколько каналов для возврата трафика (опционально).
Precedence	Приоритет, который должен быть назначен пакетам перед отправкой их в канал. По умолчанию: FromPipe.
FixedPrecedence	Фиксированный приоритет.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.43. PSK

Описание

Аутентификация PSK (Pre-Shared Key) основана на использовании общего секретного ключа, известного только заинтересованным сторонам.

Свойства

Name	Символьное имя pre-shared key (идентификатор).
Type	Тип совместно используемого ключа.
PSKAscii	PSK в виде парольной фразы.
PSKHex	PSK в виде шестнадцатеричного ключа.
Comments	Описание текущего объекта (опционально).

3.44. RadiusAccounting

Описание

Внешний RADIUS-сервер, используемый для сбора статистики пользователей.

Свойства

Name	Символьное имя сервера (идентификатор).
IPAddress	IP-адрес сервера.
Port	UDP-порт сервера (по умолчанию: 1813).
RetryTimeout	Таймаут повтора в секундах, используемый при попытке установки связи с RADIUS-сервером учетных записей. Если ответ не был получен в течение, например, 2 секунд, шлюз безопасности попробует еще раз отправить новый пакет AccountingRequest. По умолчанию: 2.
SharedSecret	Общая секретная фраза для генерирования Аутентификатора.
RoutingTable	Таблица маршрутизации, в которую должен быть добавлен маршрут клиентов к узлу. По умолчанию: main.
Comments	Описание текущего объекта (опционально).

3.45. RadiusServer

Описание

Внешний RADIUS-сервер, используемый для проверки подлинности имен пользователей и паролей.

Свойства

Name	Символьное имя сервера (идентификатор).
IPAddress	IP-адрес сервера.
Port	UDP-порт сервера (по умолчанию: 1812).
RetryTimeout	Таймаут повтора в секундах, используемый при попытке установки связи с RADIUS-сервером учетных записей. Если ответ не был получен в течение, например, 2 секунд, шлюз безопасности попробует еще раз отправить новый пакет AccountingRequest. По умолчанию: 2.
SharedSecret	Общая секретная фраза для генерирования Аутентификатора.
RoutingTable	Таблица маршрутизации, в которую должен быть добавлен маршрут клиентов к узлу. По умолчанию: main.

Comments	Описание текущего объекта (опционально).

3.46. RealTimeMonitorAlert

Описание

Мониторинг статистического значения. Сообщения журнала формируются, если значение менее самого низкого значения порога или более самого высокого значения порога.

Свойства

Index	Индекс объекта, начинается 1 (идентификатор).
Monitor	Статистическое значение.
SampleTime	Интервал в секундах между проверкой статистики (опционально).
Low Threshold	Занести в журнал, если статистическое значение ниже данного порога (опционально).
High Threshold	Занести в журнал, если статистическое значение выше данного порога (опционально).
BackoffInterval	Минимальное количество секунд между следующими друг за другом сообщениями журнала. По умолчанию: 60.
Continuous	При выборе данной опции будет сгенерировано событие с возвратом в допустимое значение, если значение выходит за пределы порогов. По умолчанию: No (Нет).
LogMessageID	Идентификатор сгенерированных сообщений журнала (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.47. RemoteIDList

Описание

Список удаленных идентификаторов, которым разрешен доступ при использовании общих ключей для аутентификации.

Свойства

Type	Тип совместно используемого ключа.

PSKAscii	PSK в виде парольной фразы.
PSKHex	PSK в виде шестнадцатеричного ключа.
IDType	Выбор типа удаленной идентификации.
IDValue	Удаленное именование идентификатора туннеля.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.48. RemoteManagement

Это категория, которая распределяет по группам следующие типы объектов.

3.48.1. RemoteMgmtHTTP

Описание

Настройте управление HTTP/HTTPS, чтобы включить удаленное управление системой.

Свойства

Name	Символьное имя объекта (идентификатор).
Interface	Интерфейс, для которого предоставляется удаленный доступ.
AccessLevel	Уровень доступа для входящего пользователя. По умолчанию: Admin.
LocalUserDatabase	Локальная база данных пользователей с целью использования для авторизации.
HTTP	Включить удаленное управление через HTTP. По умолчанию: No (Нет).
HTTPS	Включить удаленное управление через HTTPS. По умолчанию: No (Нет).
Network	Сеть, для которой предоставляется удаленный доступ.
Comments	Описание текущего объекта (опционально).

3.48.2. RemoteMgmtNetcon

Описание

Настройте управление Netcon, чтобы включить удаленное управление системой.

Свойства

Name	Символьное имя объекта. По умолчанию: NetconMgmt.
Interface	Интерфейс, для которого предоставляется удаленный доступ.
Mode	Configure, Console или Uptimepoll. По умолчанию: Configure.
IdleTimeout	Количество секунд отсутствия активности до тех пор, пока работа пользователя консоли Netcon не будет завершена автоматически. По умолчанию: 900.
Key	64-байтный Netcon PSK.
Network	Сеть, для которой предоставляется удаленный доступ.
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.48.3. RemoteMgmtSNMP

Описание

Настройте управление SNMP, чтобы включить SNMP-опрос.

Свойства

Name	Символьное имя объекта (идентификатор).
Interface	Интерфейс, для которого предоставляется удаленный доступ.
SNMPGetCommunity	Имя сообщества для предоставления прав удаленного мониторинга шлюза безопасности.
Network	Сеть, для которой предоставляется удаленный доступ.
Comments	Описание текущего объекта (опционально).

3.48.4. RemoteMgmtSSH

Описание

Настройте Secure Shell (SSH) Server, чтобы включить удаленный доступ к управлению системой.

Свойства

Name	Символьное имя SSH-сервера (идентификатор).
Interface	Интерфейс, для которого предоставляется удаленный доступ.
Port	Порт прослушивания для SSH-сервера. По умолчанию: 22.
AllowAuthMethodPassword	Разрешить аутентификацию клиента по паролю. По умолчанию: Yes (Да).
AllowAuthMethodPublicKey	Разрешить аутентификацию клиента по открытому ключу. По умолчанию: Yes (Да).
AllowHostKeyDSA	Разрешить алгоритм открытого ключа DSA. По умолчанию: Yes (Да).
AllowHostKeyRSA	Разрешить алгоритм открытого ключа RSA. По умолчанию: Yes (Да).
AllowKexDH14	Разрешить алгоритм обмена ключами Group 1 Диффи-Хеллмана. По умолчанию: Yes (Да).
AllowKexDH1	Разрешить алгоритм обмена ключами Group 14 Диффи-Хеллмана. По умолчанию: Yes (Да).
AllowMACSHA1	Разрешить алгоритм целостности SHA1. По умолчанию: Yes (Да).
AllowMACMD5	Разрешить алгоритм целостности MD5. По умолчанию: Yes (Да).
AllowMACSHA196	Разрешить алгоритм целостности SHA1-96. По умолчанию: Yes (Да).
AllowMACMD596	Разрешить алгоритм целостности MD5-96. По умолчанию: Yes (Да).
Banner	Приветственное сообщение, отображающееся при входе пользователя (опционально).
MaxSessions	Максимальное число клиентов, которые могут быть подключены одновременно. По умолчанию: 5.
SessionIdleTime	Количество секунд, в течение которых пользователь может простаивать, прежде чем сессия будет закрыта. По умолчанию: 1800.
LoginGraceTime	При вводе имени пользователя необходимо предоставить пароль в течение данного количества секунд, в противном случае сессия будет закрыта. По умолчанию: 30
AuthenticationRetries	Количество разрешенных попыток, прежде чем сессия будет закрыта. По умолчанию: 3.
AccessLevel	Уровень доступа для предоставления входящему пользователю. По умолчанию: Admin.
LocalUserDatabase	Локальная база данных пользователей, используемая для авторизации.

Network	Сеть, для которой предоставляется удаленный доступ.
Comments	Описание текущего объекта (опционально).

3.49. RouteBalancingInstance

Описание

Правило балансировки маршрутов связано с таблицей маршрутизации и определяет способ использования маршрутов одного и того же назначения.

Свойства

RoutingTable	Таблица маршрутизации для размещения в ней балансировки нагрузки маршрута (идентификатор).
Algorithm	Алгоритм, используемый при балансировке маршрутов. По умолчанию: RoundRobin.
Comments	Описание текущего объекта (опционально).

3.50. RouteBalancingSpilloverSettings

Описание

Настройки, связанные с алгоритмом spillover.

Свойства

Interface	Интерфейс для предела порога (идентификатор).
HoldTime	Количество следующих друг за другом секунд над/под пределом порога для запуска изменения состояния для неисправных маршрутов. По умолчанию: 30
OutboundThreshold	Предел порога исходящего трафика (опционально).
OutboundUnit	TODO. По умолчанию: kbps (кбит/с).
InboundThreshold	Предел порога входящего трафика (опционально).
InboundUnit	TODO. По умолчанию: kbps (кбит/с).
Comments	Описание текущего объекта (опционально).

3.51. RoutingRule

Описание

Правило маршрутизации подразумевает использование таблицы маршрутизации в прямом и/или обратном направлении трафика в соединении. Параметр упорядочения таблицы маршрутизации

определяет, до или после главной таблицы маршрутизации он был учтен.

Свойства

Index	Индекс объекта, начинается 1 (идентификатор).
Name	Символьное имя правила (опционально).
ForwardRoutingTable	Прямая таблица маршрутизации будет использоваться для пакетов от инициатора соединения к конечной точке соединения.
ReturnRoutingTable	Обратная таблица маршрутизации будет использоваться для пакетов, перемещающихся в обратном направлении.
SourceInterface	Имя принимающего интерфейса для сравнения с полученным пакетом.
SourceNetwork	Диапазон IP-адресов отправителя для сравнения с полученным пакетом.
DestinationInterface	Интерфейс назначения для сравнения с полученным пакетом.
DestinationNetwork	Диапазон IP-адресов для сравнения с IP-адресом назначения полученного пакета.
Service	Служба, которая будет использоваться в качестве параметра фильтра при сопоставлении трафика с данным правилом.
Schedule	Если в правило добавлено расписание, шлюз безопасности разрешает запуск правила только в указанное время (опционально).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.52. RoutingTable

Описание

В системе есть предварительно указанная главная таблица маршрутизации. Альтернативные таблицы маршрутизации могут быть определены пользователем.

Свойства

Name	Символьное имя таблицы маршрутизации (идентификатор).
Ordering	Метод поиска маршрута в именованной таблице маршрутизации. По умолчанию: Only (Только).
RemoveInterfaceIPRoutes	Удаление маршрутов интерфейсов. Шлюз безопасности становится полностью «прозрачным». По умолчанию: No (Нет).
Comments	Описание текущего объекта (опционально).

3.52.1. Route

Описание

Маршрут определяет, какой интерфейс и шлюз использовать для достижения определенной сети.

Свойства

Name	Символьное имя объекта (опционально).
Interface	Интерфейс, через который должны быть переданы пакеты, предназначенные для данного маршрута.
Gateway	IP-адрес следующей пересылки маршрутизатора, используемой для того, чтобы достичь сети назначения. Если сеть подключена напрямую к интерфейсу шлюза безопасности, адрес шлюза не определен (опционально).
LocalIP	Определенный здесь IP-адрес будет автоматически опубликован на соответствующем интерфейсе. Данный адрес также будет использоваться в качестве адреса отправителя в ARP-запросах. Если адрес не определен, будет использоваться IP-адрес интерфейса шлюза безопасности (опционально).
RouteMonitor	Определяет, должен ли осуществляться мониторинг данного маршрута на предмет изменений маршрута с целью обнаружения отказа маршрута. По умолчанию: No (Нет).
MonitorLinkStatus	Пометить маршрут как недействующий, если статус соединения интерфейса меняется на неактивный. По умолчанию: No (Нет).
MonitorGateway	Пометить маршрут как неработающий, если следующая пересылка не отвечает на поиск ARP в течение определенного времени. По умолчанию: No (Нет).
MonitorGatewayManualARP	Включить заданный вручную интервал поиска ARP. По умолчанию: No (Нет).
MonitorGatewayARPInterval	Интервал поиска ARP в миллисекундах. По умолчанию: 1000.
EnableHostMonitoring	Включает функцию Мониторинг хостов. По умолчанию:

	No (Нет).
Reachability	Количество хостов, которое должно быть достигнуто для того чтобы маршрут считался действующим. По умолчанию: ALL (ВСЕ).
GracePeriod	Время ожидания после повторной настройки, прежде чем мониторинг будет запущен. По умолчанию: 5.
ReachabilityCount	Минимальное количество достижимых хостов для того, чтобы маршрут считался действующим.
Network	Сетевой адрес для данного маршрута.
Metric	Метрика для данного маршрута. По умолчанию: 0.
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов через Proxy ARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейсы, на которых шлюз безопасности должен опубликовать маршруты через Proxy ARP (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.52.1.1. MonitoredHost

Описание

Определите хост и метод мониторинга.

Свойства

Method	Метод мониторинга. По умолчанию: ICMP.
IP Address	IP-адрес узла для мониторинга.
Post	TCP-порт для мониторинга.
PollingInterval	Задержка (в миллисекундах) между каждой попыткой мониторинга. По умолчанию: 10000.
ReachabilityRequired	Определяет, должен ли хост быть достижимым для того, чтобы мониторинг был успешным. По умолчанию: No (Нет).
Samples	Количество попыток с целью использования для статистических расчетов. По умолчанию: 10.
MaxPollFails	Максимальное количество неудачных попыток, прежде чем хост будет считаться недостижимым. По умолчанию:

2.

MaxAverageLatency	Определяет макс. среднее время задержки для пробных попыток. По умолчанию: 800.
RequestURL	Определяет URL-адрес HTTP для мониторинга.
ExpectedResponse	Предположительный HTTP-ответ.
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.52.2. SwitchRoute

Описание

Маршрут переключения определяет, на каких интерфейсах сеть может быть достижимой. Proxy ARP определяет между какими интерфейсами разрешен ARP.

Свойства

Name	Символьное имя объекта (опционально).
Interface	Интерфейс, через который должны быть переданы пакеты, предназначенные для данного маршрута.
Network	Сетевой адрес для данного маршрута.
Metric	Метрика для данного маршрута. По умолчанию: 0.
ProxyARPAllInterfaces	Всегда выбирать все интерфейсы, включая новые, для опубликования маршрутов через Proxy ARP. По умолчанию: No (Нет).
ProxyARPInterfaces	Интерфейсы, на которых шлюз безопасности должен опубликовать маршруты через Proxy ARP (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.53. ScheduleProfile

Описание

Профиль расписания определяет дни и даты, которые используются различными политиками в системе.

Свойства

Name	Символьное имя службы (идентификатор).
Mon	Интервалы, в течение которых профиль расписания активен по понедельникам (опционально).
Tue	Интервалы, в течение которых профиль расписания активен по вторникам (опционально).
Wed	Интервалы, в течение которых профиль расписания активен по средам (опционально).
Thu	Интервалы, в течение которых профиль расписания активен по четвергам (опционально).
Fri	Интервалы, в течение которых профиль расписания активен по пятницам (опционально).
Sat	Интервалы, в течение которых профиль расписания активен по субботам (опционально).
Sun	Интервалы, в течение которых профиль расписания активен по воскресеньям (опционально).
StartDate	Дата, после которой данное расписание будет активным (опционально).
EndDate	Дата, после которой данное расписание больше не будет активным (опционально).
Comments	Описание текущего объекта (опционально).

3.54. Service

Это категория, которая распределяет по группам следующие типы объектов.

3.54.1. ServiceGroup

Описание

Служебная группа – это собрание служебных объектов, которые могут использоваться различными политиками в системе.

Свойства

Name	Символьное имя службы (идентификатор).
Members	Участники группы.
Comments	Описание текущего объекта (опционально).

3.54.2. ScheduleProfile

Описание

Служба ICMP – это определение объекта, представляющее ICMP-трафик со специальными параметрами.

Свойства

Name	Символьное имя службы (идентификатор).
MessageTypes	Типы ICMP-сообщений, которые применимы к данной службе. По умолчанию: All (Все).
EchoRequest	Включить сопоставление сообщений эхо-запросов. По умолчанию: No (Нет).
EchoRequestCodes	Сообщение эхо-запросов, которому должны соответствовать коды. По умолчанию: 0-255.
DestinationUnreachable	Включить сопоставление сообщений о недостижимости Назначения. По умолчанию: No (Нет).
DestinationUnreachableCodes	Определяет, какому сообщению о недостижимости назначения должны соответствовать коды. По умолчанию: 0-255.
Redirect	Включить сопоставление сообщений перенаправления. По умолчанию: No (Нет).
RedirectCodes	Определяет, какому сообщению перенаправления должны соответствовать коды. По умолчанию: 0-255.
ParameterProblem	Включить сопоставление сообщений о проблемах параметров. По умолчанию: No (Нет).
ParameterProblemCodes	Определяет, какому сообщению о проблемах параметра должны соответствовать коды. По умолчанию: 0-255.
EchoReply	Включить сопоставление сообщений эхо-ответов. По умолчанию: No (Нет).
EchoReplyCodes	Определяет, какому сообщению эхо-ответов должны соответствовать коды. По умолчанию: 0-255.
SourceQuenching	Включить сопоставление сообщений подавления источника. По умолчанию: No (Нет).
SourceQuenchingCodes	Определяет, какому сообщению подавления источника должны соответствовать коды. По умолчанию: 0-255.
TimeExceeded	Включить сопоставление сообщений превышения

	времени. По умолчанию: No (Нет).
TimeExceededCodes	Определяет, какому сообщению превышения времени должны соответствовать коды. По умолчанию: 0-255.
PassICMPReturn	Включить передачу ICMP-сообщения об ошибке только в том случае, если оно относится к существующему соединению при использовании данной службы. По умолчанию: No (Нет).
ALG	Шлюз прикладного уровня (ALG), способный управлять расширенными протоколами, может быть определен для данной службы (опционально).
MaxSessions	Определяет количество параллельных сессий, разрешенных при использовании данной службы. По умолчанию: 200.
Comments	Описание текущего объекта (опционально).

3.54.3. ServiceIPProto

Описание

Служба IP-протокола – это определение IP-протокола со специальными параметрами.

Свойства

Name	Символьное имя службы (идентификатор).
IPProto	Номер IP-протокола или диапазон, например, "1-4,7" будет соответствовать протоколам ICMP, IGMP, GGP, IP-in-IP и CBT. По умолчаниию: 0-255.
PassICMPReturn	Включить передачу ICMP-сообщения об ощибке только в том случае, если оно относится к существующему соединению при использовании данной службы. По умолчанию: No (Нет).
ALG	Шлюз прикладного уровня (ALG), способный управлять расширенными протоколами, может быть определен для данной службы (опционально).
MaxSessions	Количество параллельных сессий, разрешенных при использовании данной службы. По умолчанию: 200.
Comments	Описание текущего объекта (опционально).

3.54.4. ServiceTCPUDP

Описание

TCP/UDP-служба – это определение протокола TCP или UDP со специальными параметрами.

Свойства

Name	Символьное имя службы (идентификатор).
DestinationPorts	Порт или диапазоны портов назначения, применимые к данной службе.
Type	Какой тип протокола использует данная служба: TCP, UDP или оба. По умолчанию: TCP.
SourcePorts	Порт или диапазоны портов источника, применимые к данной службе. По умолчанию: 0-65535.
SYNRelay	Включить защиту от SYN-потока (SYN Relay). По умолчанию: No (Нет).
PassICMPReturn	Включить передачу ICMP-сообщения об ошибке только в том случае, если оно относится к существующему соединению при использовании данной службы. По умолчанию: No (Нет).
ALG	Шлюз прикладного уровня (ALG), способный управлять расширенными протоколами, может быть определен для данной службы (опционально).
MaxSessions	Количество параллельных сессий, разрешенных при использовании данной службы. По умолчанию: 200.
Comments	Описание текущего объекта (опционально).

3.55. Settings

Это категория, которая распределяет по группам следующие типы объектов.

3.55.1. ARPTableSettings

Описание

Расширенные настройки ARP-таблицы.

Свойства

ARPMatchEnetSender	Ethernet-адрес отправителя, совпадающий с аппаратным адресом в ARP-данных. По умолчанию: DropLog (Отклонить).
ARPQueryNoSenderIP	Если IP-адресом источника ARP-запроса (НЕТ ответа!) является «0.0.0.0». По умолчанию: DropLog (Отклонить).
ARPSenderIP	IP-адрес источника в ARP-пакетах. По умолчанию умолчанию: Validate (Проверить).
UnsolicitedARPReplies	Непредусмотренные ARP-ответы. По умолчанию: DropLog (Отклонить).
ARPRequests	Определяет, должны ли ARP-запросы быть добавлены автоматически в ARP-таблицу или нет. По умолчанию: DropLog (Отклонить).

ARPChanges	ARP-пакеты, которые вызовут изменение записи. По умолчанию: AcceptLog (Принять).
StaticARPChanges	ARP-пакеты, которые вызовут изменение статических записей. По умолчанию: DropLog (Отклонить).
ARPExpire	Время жизни ARP-записи в секундах. По умолчанию: 900.
ARPExpireUnknown	Время жизни «неизвестной» ARP-записи в секундах. По умолчанию: 3.
ARPMulticast	ARP-пакеты, претендующие на то, чтобы быть групповыми адресами; возможно, потребуется включить для некоторых балансировщиков нагрузки/решений избыточности. По умолчанию: DropLog (Отклонить).
ARPBroadcast	ARP-пакеты, претендующие на то, чтобы быть широковещательными адресами; никогда не требуется включать. По умолчанию: DropLog (Отклонить).
ARPCacheSize	Общее количество ARP-записей в КЭШе. По умолчанию: 4096.
ARPHashSize	Количество хэш-сегментов ARP на физический интерфейс. По умолчанию: 512.
ARPHashSizeVLAN	Количество хэш-сегментов ARP на VLAN-интерфейс. По умолчанию: 64.
ARPIPCollision	Поведение, когда принимается ARP-запрос с IP-адресом отправителя, сталкивающийся с используемым на принимающем интерфейсе. По умолчанию: DropLog (Отклонить).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.2. AuthenticationSettings

Описание

Настройки, связанные с аутентификацией и ведением учетных записей.

Свойства

LogoutAccUsersAtShutdown	Завершить работу аутентифицированных пользователей учетных записей и отправить стоп-пакеты ведения учетных записей до выключения. По умолчанию: Yes (Да).
AllowAuthIfNoAccountingResponse	Разрешить аутентифицированному пользователю иметь доступ даже в том случае, если сервером ведения учетных записей не получен ответ. По умолчанию: Yes (Да).

LogALGUser	Аутентифицированные пользователи журнала вместе с URL-адресом в сообщениях журнала ALG. По умолчанию: Yes (Да).
MaxRADIUSContexts	Максимальное количество контекстов связи RADIUS. По умолчанию: 1024.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.3. ConnTimeoutSettings

Описание

Настройки таймаута для различных протоколов.

Свойства

ConnLife_TCP_SYN	Время жизни простоя соединения для создающихся TCP-соединений. По умолчанию: 60.
ConnLife_TCP	Время жизни простоя соединения для TCP. По умолчанию: 262144.
ConnLife_TCP_FIN	Время жизни простоя соединения для закрывающихся TCP-соединений. По умолчанию: 80.
ConnLife_UDP	Время жизни простоя соединения для UDP. По умолчанию: 130.
AllowBothSidesToKeepConnAlive_UDP	Разрешить обеим сторонам поддерживать UDP-соединение в рабочем состоянии. По умолчанию: No (Нет).
ConnLife_Ping	Таймаут соединения для эхо-запроса. По умолчанию: 8.
ConnLife_Other	Время жизни простоя для остальных протоколов. По умолчанию: 130.
ConnLife_IGMP	Время жизни простоя соединения для IGMP. По умолчанию: 12.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.4. DHCPRelaySettings

Описание

Расширенные настройки DHCP relay.

Свойства

MaxTransactions	Максимальное количество параллельных BOOTP/DHCP-транзакций. По умолчанию: 32.
TransactionTimeout	Таймаут для каждой транзакции (в секундах). По умолчанию: 10.
MaxPPMPerIface	Максимальное количество пакетов в минуту на интерфейс, которые перенаправляются от клиентов к серверу. По умолчанию: 500.
MaxHops	Запросы/ответы, прошедшие через большее, чем данное, число пересылок, не будут перенаправлены. По умолчанию: 5.
MaxLeaseTime	Максимальное время аренды (секунды), получаемое от DHCP-сервера (слишком большое время будет понижено автоматически). По умолчанию: 10000.
MaxAutoRoutes	Максимальное количество IP-адресов DHCP-клиентов, добавляемых автоматически в таблицу маршрутизации. По умолчанию: 256.
AutoSaveRelayPolicy	Политика для сохранения списка перенаправления на диск. По умолчанию: ReconfShut.
AutoSaveRelayInterval	Секунды между автосохранением списка перенаправления на диск. По умолчанию: 86400.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.5. DHCPServerSettings

Описание

Расширенные настройки DHCP-сервера.

Свойства

AutoSaveLeasePolicy	Политика для сохранения базы данных сроков аренды на диск. По умолчанию: ReconfShut.

AutoSaveLeaseInterval — Секунды между автосохранением базы данных сроков аренды на диск. По умолчанию: 86400.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.6. EthernetSettings

Описание

Настройки для Ethernet-интерфейса.

Свойства

DHCP_MinimumLeaseTime — Минимальное время аренды (секунды), получаемое от DHCP-сервера. По умолчанию: 60.

DHCP_ValidateBcast — Потребовать, чтобы назначенный широковещательный адрес был наивысшим адресом в назначенной сети. По умолчанию: Yes (Да).

DHCP_AllowGlobalBcast — Разрешить DHCP-серверу назначить 255.255.255.255 в качестве широковещательного адреса (Нестандартный). По умолчанию: No (Нет).

DHCP_UseLinkLocalIP — Использовать IP-адрес 169.254.*.* во время ожидания срока аренды (вместо 0.0.0.0). По умолчанию: No (Нет).

DHCP_DisableArpOnOffer — Выключить arp-решение по предложениям (обычно используется, чтобы проверить, не занят ли IP-адрес). По умолчанию: No (Нет).

Ringsize_e1000_rx — Размер кольца получения e1000 (на интерфейс). По умолчанию: 64.

Ringsize_e1000_tx — Размер кольца отправления e1000 (на интерфейс). По умолчанию: 256.

Ringsize_e100_rx — Размер кольца получения e100 (на интерфейс). По умолчанию: 32.

Ringsize_e100_tx — Размер кольца отправления e100 (на интерфейс). По умолчанию: 128.

Ringsize_yukonii_rx — Размер кольца получения Yukon-II (на интерфейс). По умолчанию: 128.

Ringsize_yukonii_tx — Размер кольца отправления Yukon-II (на интерфейс). По умолчанию: 128.

Ringsize_yukon_rx — Размер кольца получения Yukon (на интерфейс). По умолчанию: 256.

Ringsize_yukon_tx — Размер кольца отправления Yukon (на интерфейс). По умолчанию: 256.

Ringsize_bne2_rx	Размер кольца получения bne2 (на интерфейс). По умолчанию: 1024.
Ringsize_bne2_tx	Размер кольца отправления bne2 (на интерфейс). По умолчанию: 512.
Ringsize_r8169_rx	Размер кольца получения r8169 (на интерфейс). По умолчанию: 256.
Ringsize_r8169_tx	Размер кольца отправления r8169 (на интерфейс). По умолчанию: 256.
Ringsize_pcnet32_rx	Размер кольца получения pcnet32 (на интерфейс). По умолчанию: 256.
Ringsize_pcnet32_tx	Размер кольца передачи pcnet32 (на интерфейс). По умолчанию: 256.
IfaceMon_e1000	Включить диспетчер интерфейсов для интерфейсов e1000. По умолчанию: Yes (Да).
IfaceMon_BelowCPULoad	Временно выключить диспетчер интерфейсов, если нагрузка центрального процессора превышает данную процентную норму. По умолчанию: 80.
IfaceMon_BelowIfaceLoad	Временно выключить диспетчер интерфейсов на интерфейсе, если нагрузка сети на интерфейсе превышает данную процентную норму. По умолчанию: 70.
IfaceMon_MinInterval	Минимальный интервал между двумя сбросами одного и того же интерфейса. По умолчанию: 30
IfaceMon_RxErrorPerc	По какому проценту ошибок полученных пакетов объявить о проблеме. По умолчанию: 20.
IfaceMon_TxErrorPerc	По какому проценту ошибок отправленных пакетов объявить о проблеме. По умолчанию: 7.
IfaceMon_ErrorTime	Как долго проблема может сохраняться, прежде чем интерфейс будет сброшен. По умолчанию: 10.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.7. FragSettings

Описание

Настройки, связанные с фрагментированными пакетами.

Свойства

PseudoReass_MaxConcurrent	Максимальное количество параллельных повторных

	сборок фрагментов. Установите 0, чтобы отбросить все фрагменты. По умолчанию: 1024.
IllegalFrags	Некорректно построенные фрагменты; неполные перекрытия, неверные размеры и т.д. По умолчанию: DropLog.
DuplicateFragData	При приеме дублирующих фрагментов проверить совпадающие данные… По умолчанию: Check8.
FragReassemblyFail	Неудачные попытки повторной сборки пакетов из-за таймаутов или потерь пакетов. По умолчанию: LogSuspectSubseq.
DroppedFrags	Фрагменты пакетов, отброшенные из-за базы правил. По умолчанию: LogSuspect.
DuplicatedFrags	Дублировать полученные фрагменты. По умолчанию: LogSuspect.
FragmentedICMP	Фрагментированные ICMP-сообщения, за исключением эхо-запросов; обычно некорректные. По умолчанию: DropLog.
MinimumFragLength	Минимальная разрешенная длина не последних фрагментов. По умолчанию: 8.
ReassTimeout	Таймаут повторной сборки с момента получения предыдущего фрагмента. По умолчанию: 65.
ReassTimeLimit	Максимальное время жизни повторной сборки с момента получения первого фрагмента. По умолчанию: 90.
ReassDoneLinger	Как долго хранить в памяти завершенную повторную сборку (отслеживание старых дубликатов). По умолчанию: 20.
ReassIllegalLinger	Период хранения в памяти некорректной повторной сборки (отслеживание большего числа фрагментов). По умолчанию: 60.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.8. HWMSettings

Описание

Общие настройки для мониторинга аппаратной части.

Свойства

EnableSensors	Включить/выключить все функциональные возможности HWM. По умолчанию: No (Нет).

SensorPollInterval	Интервал опроса сенсора. По умолчанию: 500.
MemoryPollInterval	Интервал опроса памяти в минутах. По умолчанию: 15.
MemoryUsePercent	Должен ли диспетчер памяти использовать долю в процентах в качестве единицы мониторинга, или же в мегабайтах. По умолчанию: Yes (Да).
MemoryLogRepetition	Следует ли отправлять сообщение журнала для каждого результата опроса, находящегося на уровне Аварийный, Критический или Предупреждающий, или следует отправлять только тогда, когда достигнут новый уровень. По умолчанию: No (Нет).
MemoryAlertLevel	Аварийное сообщение журнала, если количество свободной памяти менее данного значения, выключить, используя 0. По умолчанию: 0.
MemoryCriticalLevel	Критическое сообщение журнала, если количество свободной памяти меньше данного значения, выключить, используя 0. По умолчанию: 0.
MemoryWarningLevel	Предупреждающее сообщение журнала, если количество свободной памяти меньше данного значения, выключить, используя 0. По умолчанию: 0.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.9. ICMPSettings

Описание

Настройки, связанные с ICMP-протоколом.

Свойства

ICMPSendPerSecLimit	Максимальное число ICMP-ответов, которые будут отправляться каждую секунду (по умолчанию: 500).
SilentlyDropStateICMPErrors	Автоматически отбросить ICMP-ошибки относительно отслеживаемых с сохранением состояния открытых соединений. По умолчанию: Yes (Да).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.10. IPsecTunnelSettings

Описание

Настройки для интерфейсов IPsec-туннелей, используемых для установки VPN-соединений IPsec к данной системе и от нее.

Свойства

IPsecMaxTunnels	Количество разрешенных IPsec-туннелей (0 = автоматическое). По умолчанию: 0.
IPsecMaxRules	Количество разрешенных IPsec-правил (0 = автоматическое). По умолчанию: 0.
IKESendInitialContact	Отправить сообщения 'первоначальный контакт'. По умолчанию: Yes (Да).
IKESendCRLs	Отправить CRL в обмене IKE. По умолчанию: Yes (Да).
IKECRLValidityTime	Максимальное количество секунд, в течение которых CRL считается корректным (0=подчиняться полю 'следующее обновление' в CRL). По умолчанию: 86400.
IKEMaxCAPath	Максимальное количество сертификатов CA в пути сертификата. По умолчанию: 15.
IPsecCertCacheMaxCerts	Максимальное количество записей в кэше сертификата. По умолчанию: 1024.
IPsecBeforeRules	Пропустить трафик IKE и IPsec (ESP/AH), отправляемый на шлюз безопасности, напрямую к процессору IPsec без согласования с множеством правил. По умолчанию: Yes (Да).
IPsecGWNameCacheTime	Количество времени, в течение которого IPsec-туннель будет открыт, когда удаленное DNS-имя не удается исправить. По умолчанию: 14400.
DPDMetric	Метрика 10s секунд без трафика или других признаков жизни в туннеле, прежде чем SA будет удален. По умолчанию: 3.
DPDKeepTime	Количество 10s секунд, в течение которых SA будет оставаться в недействующем кэше после удаления. DPD не запустится, если узел уже помещен в кэш как недействующий. По умолчанию: 2.
DPDExpireTime	Количество секунд, в течение которых будут отправляться сообщения DPD-R-U-THERE. По умолчанию: 15.
IPsecHardwareAcceleration	Аппаратное ускорение IPsec. По умолчанию: Inline.
IPsecDisablePKAccel	Выключить аппаратное ускорение для операций с открытым ключом. По умолчанию: No (Нет).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.11. IPSettings

Описание

Настройки, связанные с IP-протоколом.

Свойства

LogCheckSumErrors	Занести в журнал IP-пакеты с неверными контрольными суммами. По умолчанию: Да.
LogNonIP4	Занести в журнал появления не-IPv4-пакетов. По умолчанию: Да.
LogReceivedTTL0	Занести в журнал полученные пакеты с TTL=0; этого никогда не должно произойти! По умолчанию: Да
Log0000Src	Занести в журнал некорректный адрес источника 0.0.0.0. По умолчанию: Drop (Отклонить).
Block0Net	Блокировать адреса источников 0.*. По умолчанию: DropLog (Отклонить).
Block127Net	Блокировать адреса источников 127.*. По умолчанию: DropLog (Отклонить).
BlockMulticastSrc	Блокировать многоадресные адреса источников (224.0.0.0--255.255.255.255). По умолчанию: DropLog (Отклонить).
TTLMin	Минимальное значение IP Time-To-Live на приеме. По умолчанию: 3.
TTLOnLow	Какое действие предпринять над слишком низкими значениями одноадресного TTL. По умолчанию: DropLog (Отклонить).
TTLMinMulticast	Минимальное значение многоадресного IP Time-To-Live на приеме. По умолчанию: 3.
TTLOnLowMulticast	Какое действие предпринять над слишком низкими значениями многоадресного TTL. По умолчанию: DropLog (Отклонить).
DefaultTTL	IP Time-To-Live пакетов, образованных шлюзом безопасности, по умолчанию (32-255). По умолчанию: 255.
LayerSizeConsistency	Данные уровня TCP/UDP/ICMP/и т.д. и размеры заголовков, соответствующие информации размером более низкого уровня. По умолчанию: ValidateLogBad.
SecuRemoteUDPEncapCompat	Разрешить IP-данным содержать на восемь байтов

	больше, чем определяет поле общей длины UDP -- Checkpoint SecuRemote нарушает NAT-T drafts. По умолчанию: No (Нет).
IPOptionSizes	Правильность размеров опций IP-заголовка. По умолчанию: ValidateLogBad.
IPOPT_SR	Способ обработки IP-пакетов с содержащимися маршрутами источника или возврата. По умолчанию: DropLog (Отклонить).
IPOPT_TS	Способ обработки IP-пакетов с содержащимися метками времени. По умолчанию: DropLog (Отклонить).
IPOPT_RTRALT	Способ обработки IP-пакетов с содержащимся маршрутом Оповещения. По умолчанию: ValidateLogBad.
IPOPT_OTHER	Способ обработки IP-опций, не указанных выше. По умолчанию: DropLog (Отклонить).
DirectedBroadcasts	Способ обработки прямых трансляций, пропускаемых с одного интерфейса на другой. По умолчанию: DropLog (Отклонить).
IPRF	Способ обработки зарезервированного флага IP, если он установлен; это недопустимо. По умолчанию: DropLog (Отклонить).
StripDFOnSmall	Убрать флаг "DontFragment" для пакетов данного или меньшего размера. По умолчанию: 65535.
MulticastIPEnetOnMismatch	Какое действие предпринять, когда Ethernet-адрес и групповой IP-адрес не совпадают. По умолчанию: DropLog (Отклонить).
TTLMinBroadcast	Значение самого короткого широковещательного IP Time-To-Live на приеме. По умолчанию: 1.
TTLOnLowBroadcast	Действие, которое необходимо предпринять над слишком низкими значениями широковещательного TTL. По умолчанию: DropLog (Отклонить).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.12. L2TPServerSettings

Описание

Настройки PPTP/L2TP-сервера.

Свойства

L2TPBeforeRules	Пропустить L2TP-соединения, отправляемые на шлюз безопасности, напрямую к процессору L2TP без

	согласования с множеством правил. По умолчанию: Да.
PPTPBeforeRules	Пропустить PPTP-соединения, отправляемые на шлюз безопасности, напрямую к процессору PPTP без согласования с множеством правил. По умолчанию: Да.
PPP_MaxResends	Максимальное количество повторных пересылок уровня PPP. По умолчанию: 10.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.13. LengthLimSettings

Описание

Ограничения длины для различных протоколов.

Свойства

MaxTCPLen	TCP; Иногда должно быть увеличено, если используются протоколы туннелирования. По умолчанию: 1480.
MaxUDPLen	UDP; Многие интерактивные приложения используют большие UDP-пакеты, иначе может быть понижено до 1480. По умолчанию: 60000.
MaxICMPLen	ICMP; Может быть понижено по желанию до 1480. По умолчанию: 10000.
MaxGRELen	Инкапсулированная (туннелированная передача), используемая PPTP. По умолчанию: 2000.
MaxESPLen	IPsec ESP; Зашифрованная передача данных. По умолчанию: 2000.
MaxAHLen	IPsec AH; Аутентифицированная передача данных. По умолчанию: 2000.
MaxSKIPLen	SKIP; простой протокол управления ключами в IP-сети, VPN-протокол. По умолчанию: 2000.
MaxOSPFLen	OSPF; открытый протокол предпочтения кратчайшего пути, протокол маршрутизации. По умолчанию: 1480.
MaxIPIPLen	IPIP/FWZ; Инкапсулированная (туннелированная) передача, используемая VPN-1. По умолчанию: 2000.
MaxIpCompLen	IPsec IPComp; Сжатая передача данных. По умолчанию: 2000.
MaxL2TPLen	L2TP; Протокол туннелирования 2 уровня. По умолчанию: 2000.
MaxOtherSubIPLen	Остальные; иногда должно быть увеличено, если

	используются неизвестные протоколы туннелирования. По умолчанию: 1480.
LogOversizedPackets	Занести в журнал появления слишком больших пакетов. По умолчанию: Yes (Да).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.14. LocalReassSettings

Описание

Использование параметров для локальной повторной сборки фрагмента.

Свойства

LocalReass_MaxConcurrent	Максимальное количество параллельных локальных повторных сборок. По умолчанию: 256.
LocalReass_MaxSize	Максимальный размер повторно собранного локально пакета. По умолчанию: 10000.
LocalReass_NumLarge	Количество больших (>2K) буферов локальной повторной сборки (из вышеуказанного размера). По умолчанию: 32.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.15. LogSettings

Описание

Расширенные настройки ведения журнала.

Свойства

LogSendPerSecLimit	Количество пакетов ведения журнала в секунду, отправляемые шлюзом безопасности. По умолчанию: 2000.
AlarmRepeatInterval	Интервал повторения для непрерывных аварийных сигналов (в секундах). По умолчанию: 60.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.16. MiscSettings

Описание

Дополнительные настройки

Свойства

UDPSrcPort0	Способ обработки UDP-пакетов с портом источника 0. По умолчанию: DropLog (Отклонить).
Port0	Способ обработки TCP/UDP-пакетов с портом назначения 0 и TCP-пакеты с портом источника 0. По умолчанию: DropLog (Отклонить).
WatchdogTimerTime	Количество секунд без отклика, прежде чем сработает «сторожевой» таймер (0=выключить). По умолчанию: 180.
BufFloodRebootTime	Период времени, в течение которого буферы будут оставаться заполненными до момента перезагрузки шлюза безопасности. По умолчанию: 3600.
ScrSave	Выбор режима сохранения экрана. По умолчанию: ScrSaveBlank.
StatusBar	Контроль строки состояния. По умолчанию: Auto (Автоматически).
ScrSaveTime	Секунды простоя, прежде чем режим сохранения экрана будет активирован автоматически (0=выключить). По умолчанию: 300.
HighBuffers_Dynamic	Определить значение HighBuffers динамически. По умолчанию: Yes (Да).
HighBuffers	Количество буферов пакетов для назначения в дополнение к ~200 исходным буферам. По умолчанию: 1024.
LocalUndelivered	Способ обработки (разрешенных) пакетов, отправленных на шлюз безопасности, которые не соответствуют открытым портам (snmp, scp, netcon и т.д.). По умолчанию: DropLog (Отклонить).
MaxPipeUsers	Максимальное количество одновременно отслеживаемых пользователей канала. По умолчанию: 1024.
Reassembly_MaxConnections	Максимальная доля в процентах разрешенных соединений, на которых может быть выполнена повторная сборка данных. По умолчанию: 80.
Reassembly_MaxProcessingMem	Максимальная доля в процентах памяти устройства,

	которая может использоваться для обработки данных на повторно собранных соединениях. По умолчанию: 3.
AVSW_Engine	Выбор подсистемы антивирусного программного обеспечения. По умолчанию: Auto (Автоматически).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.17. MulticastSettings

Описание

Расширенные настройки многоадресной передачи.

Свойства

AutoAddMulticastCoreRoute	Автоматически создать маршрут ядра для «224.0.0.1-239.255.255.255». По умолчанию: Yes (Да).
IGMPBeforeRules	Разрешает IGMP-трафику войти в шлюз безопасности по умолчанию. По умолчанию: Yes (Да).
IGMPMaxGlobalRequestsPerSecond	Максимальное количество запросов в секунду. По умолчанию: 1000.
IGMPMaxRequestsPerSecond	Максимальное количество запросов на интерфейс в секунду. По умолчанию: 100.
IGMPReactToOwnQueries	Шлюз безопасности должен всегда отвечать отчетами участников группы даже на запросы, исходящие от него самого. По умолчанию: No (Нет).
IGMPRobustnessVariable	IGMP является устойчивым к 'значению' – потери 1 пакета. По умолчанию: 2.
IGMPQueryInterval	Интервал (мс) между общими запросами, отправляемыми шлюзом безопасности. По умолчанию: 125000.
IGMPQueryResponseInterval	Максимальное время (мс) до тех пор, пока хост/клиент не будет вынужден отправить ответ на запрос. По умолчанию: 10000.
IGMPStartupQueryInterval	Интервал общих запросов (мс) для использования во время фазы загрузки (по умолчанию: 1/4 от параметра 'IGMP Query Interval'). По умолчанию: 30000.
IGMPStartupQueryCount	Количество запросов загрузки для отправки во время фазы загрузки. По умолчанию: 2.
IGMPLastMemberQueryInterval	Максимальное время (мс) до тех пор, пока хост/клиент не будет вынужден отправить ответ на специальный запрос группы, и группы и источника. По умолчанию: 5000.
IGMPUnsolicitatedReportInterval	Время между повторениями (мс) исходного отчета об

участии в группе. По умолчанию: 1000.

IGMPReportVersion — Многочисленные маршрутизаторы, запрашивающие IGMP, в сети должны использовать одинаковую версию IGMP. По умолчанию: IGMPv3.

IGMPLowestCompatibleVersion — Самый низкий режим совместимости IGMP. По умолчанию: IGMPv1.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.18. RemoteMgmtSettings

Описание

Установите и настройте методы и права доступа для удаленного управления данной системой.

Свойства

NetconBiDirTimeout — Количество секунд ожидания входа администратора, прежде чем вернуться к предыдущей конфигурации. По умолчанию: 30

WebUIBeforeRules — Включить HTTP(S)-трафик к шлюзу безопасности, независимо от настроенных IP-правил. По умолчанию: Да.

WWWSrv_HTTPPort — HTTP-порт для пользовательского Web-интерфейса. По умолчанию: 80.

WWWSrv_HTTPSPort — HTTP(S)-порт для пользовательского Web-Интерфейса. По умолчанию: 443.

SSHBeforeRules — Включить SSH-трафик к шлюзу безопасности, независимо от настроенных IP-правил. По умолчанию: Yes (Да).

HTTPSCertificate — Определяет, какой сертификат использовать для HTTPS-трафика. Поддерживаются только сертификаты RSA (опционально).

NetconBeforeRules — Включить netcon-трафик к шлюзу безопасности, независимо от настроенных IP-правил. По умолчанию: Yes (Да).

NetConMaxChannels — Максимальное количество параллельных Netcon-каналов. Netcon-каналы состоят из следующего: консоль, регистратор реального времени, статистический опрос или контекст файла отправления/получения. По умолчанию: 18.

SNMPBeforeRules — Включить SNMP-трафик к шлюзу безопасности, независимо от настроенных IP-правил. По умолчанию: Yes (Да).

SNMPRequestLimit	Максимальное количество SNMP-пакетов, которые будут обрабатываться каждую секунду. По умолчанию: 100.
SNMPSysContact	Контактное лицо для данного управляемого узла. По умолчанию: N/A (Нет данных).
SNMPSysName	Имя для данного управляемого узла. По умолчанию: N/A (Нет данных).
SNMPSysLocation	Физическое местоположение данного узла. По умолчанию: N/A (Нет данных).
SNMPIfDescription	Значение переменных SNMP MIB-II ifDescr. По умолчанию: Name (Имя).
SNMPIfAlias	Значение переменных SNMP ifMIB ifAlias. По умолчанию: Hardware (Аппаратная часть).
LocalConsoleIdleTimeout	Количество секунд отсутствия активности до тех пор, пока работа локального пользователя консоли не будет завершена автоматически. По умолчанию: 900.
WebUIIdleTimeout	Количество секунд отсутствия активности до тех пор, пока HTTP(S)-сессия не будет закрыта. По умолчанию: 900.
NetconIdleTimeout	Количество секунд отсутствия активности до тех пор, пока Netcon-сессия не будет закрыта. По умолчанию: 600.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.19. RoutingSettings

Описание

Настройте возможности маршрутизации системы.

Свойства

RouteFailOver_IfacePollInterval	Время (мс) между опросом на предмет отказа интерфейса. По умолчанию: 500.
RouteFailOver_ARPPollInterval	Время (мс) между ARP-поиском шлюзов. Может быть переопределено для каждого маршрута. По умолчанию: 1000.
RouteFailOver_PingPollInterval	Время (мс) между отправкой эхо-запросов на шлюзы. По умолчанию: 1000.
RouteFailOver_GraceTime	Время (мс) между запуском/повторной настройкой и запуском мониторинга. По умолчанию: 30
RouteFailOver_ConsecFails	Количество следующих друг за другом отказов, прежде

	чем маршрут будет помечен как недоступный. По умолчанию: 5.
RouteFailOver_ConsecSuccess	Количество следующих друг за другом успешных ответов, прежде чем маршрут будет помечен как доступный. По умолчанию: 5.
Transp_CAMToL3CDestLearning	Выполнить обучение L3 Cache на основе IP-адресов и MAC-адресов назначения в комбинации с содержимым таблицы CAM. По умолчанию: Yes (Да).
Transp_DecrementTTL	Уменьшить TTL на пакетах, перенаправляемых между «прозрачными» интерфейсами. По умолчанию: No (Нет).
Transp_CAMSizeDynamic	Определить значение CAM Size динамически. По умолчанию: Yes (Да).
Transp_CAMSize	Максимальное количество записей в каждой таблице CAM. По умолчанию: 8192.
Transp_L3CSize_Dynamic	Определить значение L3 Cache Size динамически. По умолчанию: Yes (Да).
Transp_L3CSize	Максимальное количество записей в каждом кэше 3 уровня. По умолчанию: 8192.
Transp_RelaySTP	Relay Spanning-Tree (STP, RSTP и MSTP) Bridge Protocol Data Units ко всем интерфейсам переключения. По умолчанию: Drop (Отклонить).
Transp_RelayMPLS	Перенаправить MPLS-пакеты на все интерфейсы переключения. По умолчанию: Drop (Отклонить).
RFO_GratuitousARPOnFail	Отправить свободный ARP на отказ для предупреждения хостов об изменении Ethernet-адресов и IP-адресов интерфейса. По умолчанию: Yes (Да).
Transparency_ATSExpire	Время жизни оставшейся без ответа ATS-записи в секундах. По умолчанию: 3.
Transparency_ATSSize	Общее количество ATS-записей. По умолчанию: 4096.
NullEnetSender	Предпринимаемое действие в случае, если MAC-адресом отправителя в Ethernet-заголовке является пустой адрес (0000:0000:0000). По умолчанию: DropLog (Отклонить).
BroadcastEnetSender	Предпринимаемое действие в случае, если MAC-адресом отправителя в Ethernet-заголовке является широковещательный Ethernet-адрес (FFFF:FFFF:FFFF). По умолчанию: DropLog (Отклонить).
MulticastEnetSender	Предпринимаемое действие в случае, если MAC-адресом отправителя в Ethernet-заголовке является групповой Ethernet-адрес. По умолчанию: DropLog (Отклонить).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.20. SSLSettings

Описание

Настройки, связанные с SSL (Secure Sockets Layer).

Свойства

SSL_ProcessingPriority	Количество времени центрального процессора, которое разрешено использовать SSL-обработке. По умолчанию: Normal (Стандартное).
TLS_RSA_WITH_RC4_128_SHA1	Включить шифрование RSA_WITH_RC4_128_SHA1. По умолчанию: Yes (Да).
TLS_RSA_WITH_RC4_128_MD5	Включить шифрование TLS_RSA_WITH_RC4_128_MD5. По умолчанию: Yes (Да).
_RC4_56_SHA1	Включить шифрование TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1. По умолчанию: Yes (Да).
TLS_RSA_EXPORT512_WITH_RC4_40_MD5	Включить шифрование TLS_RSA_EXPORT1024_WITH_RC4_40_MD5. По умолчанию: No (Нет).
TLS_RSA_EXPORT512_WITH_RC2_40_MD5	Включить шифрование TLS_RSA_EXPORT1024_WITH_RC2_40_MD5. По умолчанию: No (Нет).
TLS_RSA_EXPORT_WITH_NULL_SHA1	Включить шифрование TLS_RSA_EXPORT_WITH_NULL_SHA1 (нет кодирования, просто проверка правильности сообщений). По умолчанию: No (Нет).
TLS_RSA_EXPORT_WITH_NULL_MD5	Включить шифрование TLS_RSA_EXPORT_WITH_NULL_MD5 (нет кодирования, просто проверка правильности сообщений). По умолчанию: No (Нет).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.21. StateSettings

Описание

Параметры для процессора состояния в системе.

Свойства

ConnReplace	Действие, выполняемое при заполнении таблицы соединений. По умолчанию: ReplaceLog (Замена).
LogOpenFails	Занести в журнал пакеты, которые не являются ни частью открытых соединений, ни корректными новыми соединениями. По умолчанию: Yes (Да).
LogReverseOpens	Занести в журнал попытки обратного соединения через установленное соединение. По умолчанию: Yes (Да).
LogStateViolations	Занести в журнал пакеты, которые нарушают правила отслеживания с сохранением состояния; к примеру, последовательность TCP-соединений. По умолчанию: Yes (Да).
LogConnections	Занести в журнал открывающие и закрывающие соединения. По умолчанию: Log (Занести в журнал).
LogConnectionUsage	Занести в журнал для каждого пакета, который проходит через соединение. По умолчанию: No (Нет).
MaxConnections_Dynamic	Определить значение Max Connection динамически. По умолчанию: Yes (Да).
MaxConnections	Максимальное количество одновременных соединений. По умолчанию: 8192.

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.22. TCPSettings

Описание

Настройки, связанные с TCP-протоколом.

Свойства

TCPOptionSizes	Правильность размеров опций TCP-заголовка. По умолчанию: ValidateLogBad.
TCPMSSMin	Минимальный разрешенный TCP MSS (Максимальный размер сегмента). По умолчанию: 100.
TCPMSSOnLow	Способ обработки слишком низких значений MSS. По умолчанию: DropLog (Отклонить).
TCPMSSMax	Максимальный разрешенный TCP MSS (Максимальный размер сегмента). По умолчанию: 1460.
TCPMSSVPNMax	Ограничивает TCP MSS для VPN-соединений; минимизирует фрагментацию. По умолчанию: 1400.
TCPMSSOnHigh	Способ обработки слишком больших значений MSS. По

	умолчанию: Adjust (Регулировать).
TCPMSSLogLevel	Авторизация со слишком большим значением TCP MSS, если не занесено в журнал «TCP MSS on high». По умолчанию: 7000.
TCPMSSAutoClamping	Автоматически фиксировать TCP MSS в соответствии с MTU вовлеченных интерфейсов – в дополнение к «TCP MSS max». По умолчанию: Yes (Да).
TCPZeroUnusedACK	Установить неиспользуемые поля ACK в ноль; помогает предотвратить подделку соединений. По умолчанию: Yes (Да).
TCPZeroUnusedURG	Установить неиспользуемые поля URG в ноль; предотвращает небольшую утечку информации. По умолчанию: Yes (Да).
TCPOPT_WSOPT	Опция WSOPT (Масштабирование окна) (общая). По умолчанию: ValidateLogBad.
TCPOPT_SACK	Опции SACK/SACKPERMIT (Выборочный ACK) (общие). По умолчанию: ValidateLogBad.
TCPOPT_TSOPT	Опция TSOPT (Метка времени) (общая). По умолчанию: ValidateLogBad.
TCPOPT_ALTCHKREQ	Опция ALTCHKREQ (Запрос альтернативной контрольной суммы). По умолчанию: StripLog.
TCP-OPT_ALTCHKDATA	Опция ALTCHKDATA (Данные альтернативной контрольной суммы). По умолчанию: StripLog.
TCPOPT_CC	Серия опций CC (Счетчик соединений) (полуобщая). По умолчанию: StripLogBad.
TCPOPT_OTHER	Способ обработки опций TCP, не указанных выше. По умолчанию: StripLog.
TCPSynUrg	Флаг TCP URG вместе с SYN; обычно некорректный (strip=strip URG). По умолчанию: DropLog.
TCPSynPsh	Флаг TCP PSH вместе с SYN; обычно некорректный, но всегда используемый некоторыми IP-стэками (strip=strip PSH). По умолчанию: StripSilent.
TCPSynRst	Флаг TCP RST вместе с SYN; обычно некорректный (strip=strip RST). По умолчанию: DropLog.
TCPSynFin	Флаг TCP FIN вместе с SYN; обычно некорректный (strip=strip FIN). По умолчанию: DropLog.
TCPFinUrg	Флаг TCP URG вместе с FIN; обычно некорректный (strip=strip URG). По умолчанию: DropLog.
TCPUrg	Флаг TCP URG; многие операционные системы не могут обработать его корректно. По умолчанию: StripLog.
TCPECN	Флаги уведомления о явном переполнении (ECN). Ранее известные как флаги "XMAS"/"YMAS". Также используются в «OS fingerprinting» (удаленном определении ОС). По умолчанию: StripLog.

TCPRF	Поле TCP Reserved: должно быть нулем. Используется в в «OS fingerprinting» (удаленном определении ОС). Также является частью расширения ECN. По умолчанию: StripLog.
TCPNULL	Пакеты TCP "NULL" без SYN, ACK, FIN или RST; обычно некорректный, используется сканерами. По умолчанию: DropLog.
TCPSequenceNumbers	Проверка правильности номеров последовательностей TCP. По умолчанию: ValidateLogBad.
TCPAllowReopen	Разрешить клиентам повторно открыть TCP-соединения, которые находятся в закрытом состоянии. По умолчанию: No (Нет).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.55.23. VLANSettings

Описание

Настройки для интерфейсов Virtual LAN на основе IEEE 802.1Q.

Свойства

UnknownVLANTags	VLAN-пакеты, помеченные неизвестным идентификатором. По умолчанию: DropLog (Отклонить).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.56. SSHClientKey

Описание

Открытый ключ клиента, подключающегося к SSH-серверу.

Свойства

Name	Символьное имя ключа (идентификатор).
Type	DSA или RSA. По умолчанию: DSA.
Subject	Значение метки заголовка объекта файла открытого ключа (опционально).

PublicKey	Открытый ключ.
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.57. ThresholdRule

Описание

Правило порога определяет фильтр для установления соответствия специального сетевого трафика. При сопоставлении с критерием фильтра действия правила порога оцениваются, и выполняются возможные действия.

Свойства

Index	Индекс объекта, начинается с 1 (идентификатор).
Name	Символьное имя правила (опционально).
SourceInterface	Имя принимающего интерфейса для сравнения с полученным пакетом.
SourceNetwork	Диапазон IP-адресов отправителя для сравнения с полученным пакетом.
DestinationInterface	Интерфейс назначения для сравнения с полученным пакетом.
DestinationNetwork	Диапазон IP-адресов для сравнения с IP-адресом назначения полученного пакета.
Service	Служба, которая будет использоваться в качестве параметра фильтра при сопоставлении трафика с данным правилом.
Schedule	Если в правило добавлено расписание, шлюз безопасности разрешает запуск правила только в указанное время (опционально).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.57.1. ThresholdAction

Описание

Действие правила порога определяет, какие пороги измерять, и какое действие предпринять по достижении порогов.

Свойства

Action	Protect (Защитить) или Audit (Проверить). По умолчанию: Protect.
GroupBy	Указание значения порога в зависимости от узла или сети. По умолчанию: SourceIP.
Threshold	Значение порога.
ThresholdUnit	Единица порога. По умолчанию: ConnsSec.
BlackList	Активировать «черный» список. По умолчанию: No (Нет).
BlackListTimeToBlock	Количество секунд, в течение которых должен действовать динамический «черный» список (опционально).
BlackListBlockOnlyService	Блокировать только службу, запустившую занесение в «черный» список. По умолчанию: No (Нет).
BlackListIgnoreEstablished	Не сбрасывать текущее соединение. По умолчанию: No (Нет).
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

3.58. UpdateCenter

Описание

Настройка автоматических обновлений.

Свойства

AVEnabled	Автоматические обновления антивирусных определений

	и подсистемы. По умолчанию: No (Нет).
IDPEnabled	Автоматические обновления сигнатур технического обслуживания IDP. По умолчанию: No (Нет).
AdvancedIDPEnabled	Автоматические обновления расширенных сигнатур IDP. По умолчанию: No (Нет).
UpdateInterval	Интервал, с которым выполняется автоматическое обновление. По умолчанию: Daily (Ежедневно).
UpdateDate	День месяца выполнения автоматического обновления.
UpdateWeekday	День недели выполнения автоматического обновления. По умолчанию: mon (пн).
Hourly	Количество часов между периодическими обновлениями.
UpdateHour	Час выполнения автоматического обновления. По умолчанию: 0.
UpdateMinute	Минута выполнения автоматического обновления. По умолчанию: 0.
Comments	Описание текущего объекта (опционально).

Примечание
Для данного типа объекта идентификатор не предусмотрен. Объект идентифицируется только по названию типа. Существует только одно правило данного типа.

3.59. UserAuthRule

Описание

Набор правил аутентификации пользователей определяет, каким образом пользователям разрешено аутентифицироваться в системе.

Свойства

Index	Индекс объекта, начинается с 1 (идентификатор).
Name	Символьное имя правила (опционально).
Agent	HTTP, HTTPS, XAUTH, PPP или EAP. По умолчанию: HTTP.
ChallengeExpire	Период времени в секундах до момента истечения запроса RADIUS. По умолчанию: 160.
AuthSource	Disallow (Отказать), LDAP, RADIUS или Local (Локальный).
Interface	Интерфейс, на котором было принято соединение.
OriginatorIP	Объект сети, частью которого должен быть входящий IP-адрес.

TerminatorIP	IP-адрес назначения, настроенный на PPTP/L2TP-сервере. Используется только в случае, если агентом является PPP.
RadiusServers	Серверы аутентификации, которые будут использоваться для аутентификации пользователей, соответствующих данному правилу.
LDAPServers	Серверы аутентификации, которые будут использоваться для аутентификации пользователей, соответствующих данному правилу.
RadiusMethod	Метод аутентификации, используемый для шифрования пароля пользователя. По умолчанию: PAP.
LocalUserDB	Локальная база данных пользователей, которая будет использоваться для аутентификации пользователей, соответствующих данному правилу.
LoginType	HTML-форма или Базовая аутентификация. По умолчанию: HTMLForm.
HTTPBanners	HTML-баннеры HTTP-аутентификации. По умолчанию: Default.
RealmString	Строка, представляемая как часть сообщения 401 – Требуется аутентификация.
HostCertificate	Сертификат хоста, который шлюз безопасности отправляет клиенту. Поддерживаются только сертификаты RSA.
RootCertificate	Корневой сертификат, который использовался для подписания сертификата хоста. Поддерживаются только сертификаты RSA (опционально).
PPPAuthNoAuth	Отмена аутентификации. По умолчанию: No (Нет).
PPPAuthPAP	Использовать протокол аутентификации PAP. Имя пользователя и пароль отправляются в незашифрованном виде. По умолчанию: Yes (Да).
PPPAuthCHAP	Использовать протокол аутентификации CHAP. По умолчанию: Yes (Да).
PPPAuthMSCHAP	Использовать протокол аутентификации MS-CHAP. По умолчанию: Yes (Да).
PPPAuthMSCHAPv2	Использовать протокол аутентификации MS-CHAP v2. По умолчанию: Yes (Да).
IdleTimeout	Если пользователь был успешно аутентифицирован, и трафик с его IP-адреса не был обнаружен в течение данного количества секунд, работа пользователя будет автоматически завершена. По умолчанию: 1800.
SessionTimeout	Если пользователь был успешно аутентифицирован, его работа будет автоматически завершена по истечении данного количества секунд независимо от того, исходила от пользователя активность или нет (опционально).
UseServerTimeouts	Использовать таймауты, полученные от сервера аутентификации. Если значения не получены, будут

	использоваться значения, определенные вручную. По умолчанию: No (Нет).
MultipleUsernameLogins	Метод обработки нескольких имен регистрации пользователей. По умолчанию: AllowMultiple.
ReplaceIdleTime	Заменить существующего пользователя, если он простаивает большее количество секунд, чем данное. По умолчанию: 10.
AccountingServers	Серверы учетных записей, которые будут использоваться для уведомления о применении пользователей, соответствующих данному правилу (опционально).
BytesSent	Включить передачу отчетов о количестве байтов, отправленных пользователем. По умолчанию: Yes (Да).
PacketsSent	Включить передачу отчетов о количестве пакетов, отправленных пользователем. По умолчанию: Yes (Да).
BytesReceived	Включить передачу отчетов о количестве байтов, полученных пользователем. По умолчанию: Yes (Да).
PacketsReceived	Включить передачу отчетов о количестве пакетов, полученых пользователем. По умолчанию: Yes (Да).
SessionTime	Включить передачу отчетов о количестве секунд, в течение которых длилась сессия. По умолчанию: Yes (Да).
SupportInterimAccounting	Включить сообщения временного учета записей для обновления сервера учетных записей с текущим статусом аутентифицированного пользователя. По умолчанию: No (Нет).
ServerInterimControl	Разрешить RADIUS-серверу определить интервал, в котором должны отправляться события временного учета записей. По умолчанию: Yes (Да).
InterimValue	Интервал в секундах, в котором должны отправляться события временного учета запсией. По умолчанию: 600.
LogEnabled	Включить ведение журнала. По умолчанию: Yes (Да).
LogSeverity	Степень важности события, которое будет отправлено указанным получателям журнала. По умолчанию: Default (По умолчанию).
Comments	Описание текущего объекта (опционально).

Примечание
Если при создании правила данного типа `Индекс` не был указан, объект будет помещен на последнее место в списке, а его `Индекс` будет задан в соответствии с ранее присвоенными идентификаторами.

Адрес производителя:
Россия, 129626, г. Москва, Графский переулок, 14
Тел.: +7 (495) 744-0099
Круглосуточная тех. поддержка по телефону: 8-800-700-5465
www.dlink.ru