SonicWALL Global Management System Command Line Interface Guide

Standard Edition

Version 2.3

Copyright Information

Part Number: 232-000186-00 Rev D

Software License Agreement for SonicWALL Global Management System

To review the SonicWALL Global Management System Software License Agreement, see the *SonicWALL Global Management System Introduction Guide*.

Chapter 1 Introduction **15**

Chapter 2 Using the Command Line Interface **17**
Accessing the CLI **17**
CLI Commands **18**
Logging In **18**
Logging Out **19**
Executing a Command without Logging In **20**
Adding SonicWALL Appliances or Ravlin Devices **21**
Adding and Removing Activation Codes **25**
Using the Configure Command **28**
Preparing a Configuration File **29**

Chapter 3 Configuration Parameters **31**
Access/General **32**
nbt_dmzEnable **32**
nbt_enable **32**
randomizeIds **32**
enableStealthMode **33**
cacheTimeout **33**
Access/Management **34**
useRemoteMgtName **34**
useGlobalMgt **34**
enableIE **34**
globalMgtIpName **35**
globalMgtNatInterposeName **35**
globalMgtNatInterposeIpName **35**
globalMgtSgmsOnVpn **36**
globalMgtSecretTagName **36**
globalMgtAuthKeyTagName **36**
Access/RADIUS **38**
radiusUserRemoteAccess **38**
radiusUserBypassFilters **38**
radiusUserLimitedMgmt **38**
radiusUserVpnAccess **39**
radiusUserVpnXauthClient **39**
Radius_user **39**
Radius_passwd **40**
Radius_retries **40**
Radius_timeout **40**
Rad_prm_IP **41**
Rad_prm_port **41**
Rad_prm_secret **41**
Rad_sec_IP **42**
Rad_sec_port **42**

Rad_sec_secret 42
Access/Rules 44
prefs_svcName 44
serviceNameInRule 44
serviceInternalName 44
prefs_ruleAction 45
prefs_ruleSrcEnet 45
prefs_ruleSrcBegin 45
prefs_ruleSrcEnd 46
prefs_ruleDstEnet 46
prefs_ruleDstBegin 46
prefs_ruleDstEnd 47
prefs_ruleTimeConstraint 47
prefs_ruleTimeBegin 47
prefs_ruleTimeEnd 48
prefs_ruleTimeout 48
prefs_ruleEnabled 48
prefs_ruleAllowFrags 49
prefs_ruleBwMgmtEnabled 49
prefs_ruleBwMgmtGuaranteed 49
prefs_ruleBwMgmtMaximum 50
prefs_ruleBwMgmtPriority 50
Access/Services 51
prefs_svcPortNum 51
serviceInternalName 51
prefs_svcIPType 51
prefs_svcName 52
prefs_svcActionMask 52
prefs_svcPortEnd 52
known_svcName 53
Access/SNMP 54
snmp_Enable 54
snmp_Mib2SysName 54
snmp_Mib2SysContact 54
snmp_Mib2SysLocation 55
snmp_GetCommunity 55
snmp_TrapCommunity 55
snmp_HostIP0 56
snmp_HostIP1 56
snmp_HostIP2 56
snmp_HostIP3 57
Access/Users 58
userInactivity 58
users_loginName 58
users_password 58
userRemoteAccess 59
userBypassFilters 59
userMaxTime 59
userVpnAccess 60
userVpnXauthClient 60
userLimitedMgmt 60
userRadiusSelect 61

userNoAuthDNS 61
userRadiusCheckLocal 61
Advanced/DMZ Addresses 63
prefs_dmzBegin 63
prefs_dmzEnd 63
natOnDmz 63
dmzNetwork 64
dmzSubnetMask 64
dmzPublic 64
Advanced/Ethernet 66
wanBwMgmtEnabled 66
wanBwMgmtAvailable 66
wanLinkAbility 66
dmzLinkAbility 67
lanLinkAbility 67
proxyPcMacOnWan 68
fragmentPackets 68
wanMtu 68
Advanced/Intranet 70
rangeMode 70
prefs_intraBegin 70
prefs_intraEnd 70
Advanced/One-to-One NAT 72
nat_oneToOneOn 72
nat_121priv 72
nat_121pub 72
nat_121len 73
Advanced/Proxy Relay 74
webProxySrvrName 74
webProxyPort 74
bypassFailedProxy 74
Advanced/Routes 76
ipAddr 76
ipSubnetMask 76
wanSubnetMask 76
prefs_route_dstNet 77
prefs_route_dstMask 77
prefs_route_dstGw 77
prefs_route_link 78
Anti-Virus/Configure 79
avExcludeBegin 79
avExcludeEnd 79
highRiskAlert 79
avListMode 80
avEnable 80
policeDmz 80
avDisableLanToDmzPolicing 81
daysToForceUpdate 81
lowRiskAlert 81
mediumRiskAlert 82
avReduceTraffic 82
Anti-Virus/EMail Filter 83

MAFiAEnabled 83
smtpFilterEnabled 83
smtpFilterMode 83
smtpAttachmentStrip 84
extension_add 84
DHCP/DHCP over VPN 85
dhcprLocalIp 85
dhcprIpMac 85
localLanMac 85
centralDhcpIp 86
dhcpIpHelper 86
doTempLease 86
dhcprTempLease 87
vpnDhcpTunnel 87
dhcprStaticIp 87
dhcprSpoof 88
isRemoteGw 88
DHCP/Setup 89
prefs_dhstaticip 89
prefs_dhstatichw 89
dhcp_gateway 89
prefs_dhdynstart 90
prefs_dhdynend 90
prefs_dhdynbootp 90
dhcp_dns0 91
dhcp_dns1 91
dhcp_dns2 91
dhcp_wins0 92
dhcp_wins1 92
dhcp_lease 92
dhcp_domainname 93
dhcp_propagateSettingsToLan 93
enableDHCP 93
enablePassDHCP 94
dhcp_dmz_gateway 94
General/Network 95
L2tpdnsServer1 95
L2tpdnsServer2 95
L2tpGlobalSonicIp 95
L2TPClientPswd 96
L2TPTimeoutEnable 96
L2tpIdleTime 96
L2tpGlobalServerIp 97
PPPoE_Timeout_Enable 97
PPPoEIdleTime 97
PPPoEDynamicLocalIP 98
PPPOEStaticLocalIP 98
L2tpServerIP 98
L2TPClientEnabled 99
L2tpClientIslocalDynamicIP 99
L2TPClientHostName 99
L2TPClientUserName 100

nat_manyToOneOn **100**
dhClient_active **100**
PPPOEEnabled **101**
ipAddr **101**
ipSubnetMask **101**
lanSubnetGateway **102**
PPPOEUserName **102**
PPPOEPswd **102**
nat_mTo1PubAddr **103**
ipGateway **103**
wanSubnetMask **103**
dhClient_leaseDuration **104**
dhClient_hostName **104**
dnsSrvAddr **104**
dnsServer2 **105**
dnsServer3 **105**
General/Time **106**
timezone **106**
ntp_useNtp **106**
ntp_useDst **106**
ntp_utcLogs **107**
useInternational **107**
addCustomNTPServer **107**
ntp_updateInterval **108**
High Availability/Configure **109**
haPrimaryLanIp **109**
haPrimaryWanIp **109**
enableHA **109**
haBackupMacAddr **110**
haBackupLanIp **110**
haBackupWanIp **110**
enablePreemptMode **111**
heartbeatInterval **111**
maxHeartbeatWait **111**
electionDelayTime **112**
Log/Log Settings **113**
firewallName **113**
logPrefs_alertMask_2 **113**
logPrefs_alertMask_5 **113**
logPrefs_alertMask_1 **114**
logPrefs_logMask_7 **114**
logPrefs_logMask_8 **114**
logPrefs_logMask_9 **115**
logPrefs_logMask_11 **115**
logPrefs_logMask_0 **115**
logPrefs_logMask_1 **116**
logPrefs_logMask_2 **116**
logPrefs_logMask_3 **116**
logPrefs_logMask_4 **117**
logPrefs_logMask_14 **117**
logPrefs_logMask_5 **117**
logPrefs_logMask_6 **118**

smtpServerName 118
logPrefs_logEmailAddr 118
logPrefs_alertEmailAddr 119
logPrefs_logEmailFreq 119
logPrefs_dayOfWeek 119
logPrefs_timeOfDay 120
logPrefs_syslogFreqSecs 120
syslogStatusFreqSecs 120
logPrefs_disableWhenFull 121
syslogFormat 121
Modem/Configure 122
dialupProfileInUse_0 122
dialupProfileInUse_1 122
speakerSettings 122
atCommand 123
enableWanFailover 123
enableProbing 123
probeOnInterfaces 124
probeTarget 124
probeInterval 124
failoverThreshold 125
probesToActive 125
enableFailoverPreempt 125
Modem/Profile 127
dialConfigName 127
priPhone 127
secPhone 127
dupUserName 128
dupUserPass 128
dialIpAddrBool 128
dialupIP Address 129
dialDnsSrvBool 129
dialupDns1 129
dialupDns2 130
dialChatScript 130
connectOnData 130
ispInactivityTimeout 131
baudRate 131
maxConnectTime 132
ispReconnectDelay 132
modemDisableVpn 132
callWaitEnable 133
callWaitString 133
ispRetries 133
ispRetryDelay 134
Website Blocking/Consent 135
prefs_aupFilter 135
aupURL4 135
aupURL2 135
aupURL3 136
aupEnable 136
aupActivityTimeout 136

aupURL1 **137**
userInactivity **137**
Website Blocking/Customization **138**
sbi_blockCustom **138**
sbi_trustedOnly **138**
forbiddenURLs_add **138**
allowedURLs_add **139**
Website Blocking/General **140**
cf_method **140**
trustedURLs_add **140**
sbi_trustCode **140**
sbi_webBlockMsg **141**
CFLinkMask_0 **141**
CFLinkMask_1 **141**
Website Blocking/Filter List **143**
sbi_urlBlockMask_0 **143**
sbi_urlBlockMask_1 **143**
sbi_urlBlockMask_2 **143**
sbi_urlBlockMask_3 **144**
sbi_urlBlockMask_4 **144**
sbi_urlBlockMask_5 **144**
sbi_urlBlockMask_6 **145**
TOD_useTOD **145**
TOD_startHour **145**
TOD_startMin **146**
TOD_startDay **146**
TOD_endHour **146**
TOD_endMin **147**
TOD_endDay **147**
sbi_dontBlockOnlyLog **147**
filterListFallback **148**
sbi_urlBlockMask_7 **148**
sbi_urlBlockMask_8 **148**
sbi_urlBlockMask_9 **149**
sbi_urlBlockMask_10 **149**
sbi_urlBlockMask_11 **149**
LRI_autoDownload **150**
LRI_dayOfWeek **150**
LRI_timeOfDay **150**
Website Blocking/N2H2 **152**
n2h2UserName **152**
n2h2CacheSize **152**
n2h2FailedTimeout **152**
n2h2SrvAddr **153**
n2h2SrvPort **153**
n2h2LocalPort **153**
n2h2BlockOnFail **154**
n2h2BlockBlockedSites **154**
n2h2LogBlockedSites **154**
Website Blocking/URL Keywords **156**
keyword_add **156**
sbi_blockURLKeywords **156**

Website Blocking/Web Features **157**
sbi_blockActiveX **157**
sbi_blockJava **157**
sbi_blockCookies **157**
sbi_blockHTTPProxy **158**
scanForFakeMicrosoftCerts **158**
Website Blocking/Websense **159**
wseSrvAddr **159**
wseSrvPort **159**
wseUserName **159**
wseCacheSize **160**
wseFailedTimeout **160**
wseBlockOnFail **160**
VPN/CA Certs **162**
caCertHash **162**
caCertName **162**
caCertData **162**
pkiCaUrlForCrl **163**
pkiNextUpdateForCrl **163**
VPN/Configure **164**
ipsecpeerCertID **164**
pkiPrefNameThirdCert **164**
ipsecCertName **164**
ipsecPeerIdtype **165**
ipsecName **165**
ipsecInSPI **165**
ipsecApplyRules **166**
ipsecDefaultSa **166**
ipsecForwardPackets **166**
ipsecDefaultLanGw **167**
remoteUnit **167**
ipsecDstAddrBegin **167**
ipsecDstAddrEnd **168**
ipsecSubnetMask **168**
ipsecOutSPI **168**
ipsecRemoteClients **169**
ipsecAllowNetBIOS **169**
ipsecGwAddr **169**
ipsecAlgo **170**
ipsecESPKey **170**
ipsecAHKey **170**
ipsecRadiusAuth **171**
ipsecLifeSecs **171**
ipsecAllowSWPeerCert **171**
ipsecAllowSWClientCert **172**
ipsecSWPeerCertNum **172**
ipsecSWClientCertDN **172**
ipsecSaDisabled **173**
ipsecPFSEnablePFS **173**
ipsecKeepAlive **173**
ipsecAGMode **174**
ipsecP1DHGrp **174**

ipsecP2DHGrp **174**
ipsecAlgIdPh1 **175**
ipsecTermAt **175**
ipsecLocalUserAuth **176**
ipsecRemoteUserAuth **176**
ipsecDhcpTunnel **176**
VPN/Local Certs **178**
localCertData **178**
pkiAliasThirdCert **178**
localCertReqData **178**
pkiPrefNameThirdCert **179**
pkiValidThirdCert **179**
VPN/Summary **180**
firewallId **180**
remoteUnit **180**
ipsecInSPI **180**
ipsecOutSPI **181**
ipsecAlgo **181**
ipsecName **181**
ipsecSaDisabled **182**
ipsecGwAddr **182**
ipsecBwMgmtPriority **182**
ipsecBwMgmtEnabled **183**
ipsecBwMgmtGuaranteed **183**
ipsecBwMgmtMaximum **183**
ipsecP1DHGrp **184**
ipsecAlgIdPh1 **184**
ipsecP2DHGrp **185**
ipsecEnable **185**
nbt_vpnDisable **185**
ipsec_allowPmtuIcmpInClear **186**

Introduction

To provide flexibility to our customers, the SonicWALL Global Management System (SonicWALL GMS) includes a command-line interface (CLI).

The SonicWALL GMS CLI can make it easier to add new SonicWALL appliances or Ravlin devices and modify existing ones. However, it requires a strong familiarity with using a command-line interface and SonicWALL GMS. We recommend caution when using this tool.

Using the Command Line Interface

This chapter describes how to access the command line interface (CLI) and how to execute CLI commands.

Accessing the CLI

To access the CLI, follow these steps:

1. Open the command-line prompt.
2. Change to the following directory:

   sonicwall_directory\cli

   where *sonicwall_directory* is the location where SonicWALL GMS is installed.
3. Enter one of the following commands:
   - For Windows NT, enter:

     sgms
   - For Solaris, enter:

     ./sgms.sh

   The SGMS prompt appears:

   sgms>
4. Perform any of the commands described in "CLI Commands" on page 18.
5. To exit from the SonicWALL GMS CLI, enter the following command:

   sgms> **quit**

CLI Commands

This section describes each CLI command.

Logging In

To log in to the SonicWALL GMS CLI, use the **login** command.

```
sgms> login username password
```

Syntax

username	Admin user.
password	Password of the admin user.

Defaults

none

Usage Guidelines

When this command is entered, SonicWALL GMS does the following:

- Checks whether the command is entered with the correct parameters.
  - If the command is not entered correctly, it returns the correct form of the command.
- Checks the validity of the username and password.
- Executes the login command.
- Creates a new session with a randomly generated session ID.
- Returns any command output.

XML Command Output

SonicWALL GMS receives and returns all command input and output in XML format. The following is the actual XML output of this command:

```
<?xml version="1.0">
<SgmsApiResult><returnCode>error.getCode() </returnCode>;
<returnString>Just a test string</returnString>";
</sgmsApiResult>
```

Example

In the following example, the user admin logs in using the password “password.”

```
sgms> login admin password
```

Logging Out

To log out from the SonicWALL GMS CLI, use the **logout** command.

```
sgms> logout
```

Syntax

This command has no arguments.

Defaults

none

Usage Guidelines

When this command is entered, SonicWALL GMS does the following:

- Executes the logout command.
- Closes the session.
- Returns to the SGMS prompt from which you can login again.

XML Command Output

SonicWALL GMS receives and returns all command input and output in XML format. The following is the actual XML output of this command:

```
<?xml version="1.0">
<SgmsApiResult><returnCode>error.getCode() </returnCode>;
<returnString>Just a test string</returnString>";
</sgmsApiResult>
```

Example

In the following example, the SGMS user logs out:

```
sgms> logout
```

Executing a Command without Logging In

To execute a command without logging in to the SonicWALL GMS CLI, use the **login** command.

```
sgms> login -L "username password" -C "command parameter"
```

Syntax

username	Admin user.
password	Password of the admin user.
command	The command.
parameter	Any command parameters.

Defaults

none

Usage Guidelines

When this command is entered, SonicWALL GMS does the following:

- Checks whether the command is entered with the correct parameters.
  - If the command is not entered correctly, it returns the correct form of the command.
- Checks the validity of the username and password.
- Executes the login command.
- Creates a new session with a randomly generated session ID.
- Executes the command.
- Closes the session and exits.

XML Command Output

SonicWALL GMS receives and returns all command input and output in XML format. The following is the actual XML output of this command:

```
<?xml version="1.0">
<SgmsApiResult><returnCode>error.getCode() </returnCode>;
<returnString>Just a test string</returnString>";
</sgmsApiResult>
```

Example

In the following example, the user admin logs in using the password “password” and runs an **addunit** command.

```
sgms> login -L admin password -C addunit new_sonicwall.xml
```

Adding SonicWALL Appliances or Ravlin Devices

To add one or more SonicWALL appliances or Ravlin devices to SonicWALL GMS using the CLI, use the **addunit** command.

```
sgms> addunit xml_file
```

Syntax

xml_file	XML file that contains SonicWALL appliance or Ravlin device information.

Defaults

none

Usage Guidelines

The XML file should contain the following:

```
<?xml version ="1.0" ?>
<sgmscommand>
     <command>addUnit</command>
     <FirewallList>
          <FirewallInfo>
               <SonicwallName>sonicwall_name</sonicwallName>
               <SonicwallPassword>password</sonicwallPassword>
               <IpAddress>ip_address</ipAddress>
               <SerialNumber>serial_number</serialNumber>
               <SAencryptionKey>encrypt_key</SAencryptionKey>
               <SAAuthKey>auth_key</SAAuthKey>
               <AntivirusPassword>av_password</antivirusPassword>
               <SchedulerIPAddress>scheduler_ip</schedulerIPAddress>
               <StandbySchedulerIP>standby_ip</standbySchedulerIP>
               <UseVPN>use_vpn</useVPN>
               <supportRavlin>ravlin_bit</supportRavlin>
               <snmpRead>read_string</snmpRead>
               <snmpWrite>write_string</snmpWrite>
               <httpsMgmt>https_bit</httpsMgmt>
               <managedOnLanIP>managedon_lanip</managedOnLanIP>
               <StandbyManagedAtWan>standbymanaged_atwan</standbyManagedAtWan>
               <CustomInfo>
                    <Customfield01>field_01</Customfield01>
                    <Customfield02>field_02</Customfield02>
                    ...
                    <Customfield10>field_10</Customfield10>
               </CustomInfo>
               <userList>
                    <user>user_01</user>
                    <user>user_02</user>
                    ...
               </userList>
          </FirewallInfo>
          <FirewallInfo>
               (SonicWALL Configuration Information)
          </FirewallInfo>
          <FirewallInfo>
               (SonicWALL Configuration Information)
          </FirewallInfo>
     </FirewallList>
</sgmscommand>
```

sonicwall_name	Required. Descriptive name for the SonicWALL appliance or Ravlin device.
password	Required. Password used to access the SonicWALL appliance or Ravlin device.
ip_address	If the WAN IP address of the SonicWALL appliance is static, enter the IP address. If the WAN IP address of the SonicWALL appliance changes dynamically, leave this field blank. For a Ravlin device, leave this field blank.
serial_number	Required. Serial number of the SonicWALL appliance or Ravlin device.
encrypt_key	Required. Enter a 16-character encryption key. The key must be exactly 16 characters long and comprised of hexadecimal characters. Valid hexadecimal characters are “0” to “9”, and “a” to “f” (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be 1234567890abcdef. This key must match the encryption key of the SonicWALL appliance or Ravlin device.
auth_key	Required. Enter a 32-character authentication key. The key must be exactly 32 characters long and comprised of hexadecimal characters. For example, a valid key would be 1234567890abcdef1234567890abcdef. This key must match the authentication key of the SonicWALL appliance or Ravlin device.
av_password	If the SonicWALL appliance uses the Anti-Virus feature, enter the Anti-Virus password. Otherwise, leave the field blank. This field is not applicable to Ravlin devices.
scheduler_ip	Required. Enter the IP address of the SonicWALL GMS server that will manage the SonicWALL appliance or Ravlin device: • If SonicWALL GMS is configured in a two-tier distributed environment, you can select any Agent. However, the IP address must match the IP address that you specified when configuring the SonicWALL appliance for SonicWALL GMS management. • If SonicWALL GMS is in a single server environment, enter the IP address of the SonicWALL GMS server.
standby_ip	Enter the IP address of the standby SonicWALL GMS server. The standby SonicWALL GMS server will automatically manage the SonicWALL appliance in the event of a primary failure. Any Agent can be configured as the standby. If SonicWALL GMS is in a single server environment, leave this field blank. This field is not applicable to Ravlin devices.
use_vpn	Specifies whether SonicWALL GMS will need a VPN tunnel to reach the SonicWALL appliance or Ravlin device (default: yes). If yes, enter use_vpn. If no, leave it blank.
ravlin_bit	Specifies whether this is a Ravlin device (default: no). If yes, enter 1. If no, enter 0. If this entry does not appear in the file, SonicWALL GMS assumes it is SonicWALL appliance.
read_string	Specifies the SNMP read string for Ravlin devices.
write_string	Specifies the SNMP write string for Ravlin devices.
https_bit	Specifies whether this device uses HTTPS instead of a VPN tunnel (default: no). If yes, enter 1. If no, enter 0.
managedon_lanip	Specifies the device will be managed from the LAN interface. If you will use HTTPS, this setting must be enabled.
standbymanaged_atwan	Specifies whether the SonicWALL appliance or Ravlin device will establish a VPN tunnel to the standby scheduler (default: yes). If yes, standbymanaged_atwan. If no, leave it blank.
field_01...field_10	Specifies the values of each custom field.
user_01...	Specifies the usernames of non-administrator SonicWALL GMS users that have access to this SonicWALL appliance through the SonicWALL GMS UI.

XML Command Output

SonicWALL GMS receives and returns all command input and output in XML format. The following is the actual XML output of this command:

```
<?xml version="1.0">
<SgmsApiResult><returnCode>error.getCode() </returnCode>;
<returnString>Just a test string</returnString>";
</sgmsApiResult>
```

Example

In the following example, two new SonicWALL appliances are added to SonicWALL GMS:

```
sgms> addunit new_sonicwall.xml
```

The following is the content of new_sonicwall.xml.

```
<?xml version ="1.0" ?>
<sgmscommand>
     <command>addUnit</command>
     <FirewallList>
          <FirewallInfo>
               <sonicwallName>ABC14</sonicwallName>
               <sonicwallPassword>abc</sonicwallPassword>
               <ipAddress></ipAddress>
               <serialNumber>00F12211F114</serialNumber>
               <SAencryptionKey>1234567812345678</SAencryptionKey>
               <SAuthKey>12345678123456781234567812345678</SAuthKey>
               <antivirusPassword>avpass</antivirusPassword>
               <schedulerIPAddress>192.168.168.168</schedulerIPAddress>
               <useVPN>1</useVPN>
               <standbyManagedAtWan>1</standbyManagedAtWan>
               <standbySchedulerIP>192.168.168.23</standbySchedulerIP>
               <supportRavlin>1</supportRavlin>
               <snmpRead>abcdef12</snmpRead>
               <snmpWrite>abcdef12</snmpWrite>
               <httpsMgmt>0</httpsMgmt>
               <manageOnLanIP>0</manageOnLanIP>
               <CustomInfo>
                    <Company>SonicWAll</Company>
                    <Country>China</Country>
                    <State>California</State>
                    <Department>Engineering</Department>
               </CustomInfo>
               <userList>
                    <user>billb</user>
                    <user>dana</user>
                    <user>mgg</user>
                    <user>prasad</user>
               </userList>
          </FirewallInfo>
          <FirewallInfo>
               <sonicwallName>XYZ26</sonicwallName>
               <sonicwallPassword>abc</sonicwallPassword>
               <ipAddress></ipAddress>
               <serialNumber>00F1434CE265</serialNumber>
               <SAencryptionKey>1234567812345678</SAencryptionKey>
               <SAuthKey>12345678123456781234567812345678abcdef89</SAuthKey>
               <antivirusPassword></antivirusPassword>
               <schedulerIPAddress>192.168.168.168</schedulerIPAddress>
               <useVPN>1</useVPN>
```

```
            <standbyManagedAtWan>1</standbyManagedAtWan>
            <standbySchedulerIP>192.168.168.23</standbySchedulerIP>
            <httpsMgmt>0</httpsMgmt>
            <manageOnLanIP>0</manageOnLanIP>
            <CustomInfo>
                  <Company>SonicWAll</Company>
                  <Country>China</Country>
                  <State>California</State>
                  <Department>Engineering</Department>
            </CustomInfo>
         </FirewallInfo>
     </FirewallList>
</sgmscommand>
```

Note: *A sample of the file is available on the SonicWALL GMS CD-ROM. It is called sample_nodes.xml and is located in the Misc directory.*

Adding and Removing Activation Codes

To add or remove activation codes for SonicWALL appliances, use the **activationcode** command.

```
sgms> activationcode xml_file
```

Syntax

xml_file	XML file that contains activation code information.

Defaults

none

Usage Guidelines

The XML file should contain the following:

```
<? Xml version ="1.0" >
<Sgmscommand>
     <Activation>command_type</Activation>
     <Activation values>
          <Activation category>category</Activation _category >
          <Activation type>activation_type</Activation type>
     </Activation values>
     <Codes>
          <Code>code</code>
          <Code>code</code>
     </Codes>
</Sgmscommand>
```

command_type	Required. Specifies the action to perform. Options include: • add—adds the specified category and type. • delete—deletes the specified activation codes. • list—lists the activation codes for the specified category and type. To add activation codes, enter add. To remove codes, enter delete.
category	Required for add and list. Enter the category of upgrade. Options include: • Anti-Virus • Content Filter Subscription • PKI End User Certificate • Node Upgrade • PKI Administrator Certificate • VPN Upgrade • VPN Client Upgrade • HA Upgrade

activation_type	Required for add and list. Enter the type of upgrade for the selected category. Options include: Anti-Virus • 5 Nodes • 10 Nodes • 50 Nodes • 100 Nodes • 1000 Nodes Content Filter Subscription • 5 Nodes • 10 Nodes • 50 Nodes • Unlimited Nodes PKI EndUser Certificate • 1 Node • 10 Nodes • 50 Nodes • 100 Nodes Node Upgrade • 10->25 Nodes • 10->50 Nodes • 10->Unlimited Nodes • 25->50 Nodes • 50->Unlimited Nodes PKI Administrator Certificate • SOHO2/SOHO3 • GX 2500/GX 2500 HA Backup • GX 6500/GX6500 HA Backup • XPRS/XPRS2/PRO 100 • PRO/PRO-VX/RPO 200/PRO 300 • TELE2/TELE3 VPN Upgrade • 5/10/25/50 Nodes • Unlimited Nodes VPN Client Upgrade • Single VPN Client • 10 VPN Clients • 100 VPN Clients • 50 VPN Clients HA Upgrade • PRO/PRO 200
code	Required for add and delete. One or more code numbers. Each code number must appear on its own line.

XML Command Output

SonicWALL GMS receives and returns all command input and output in XML format. The following is the actual XML output of this command:

```
<?xml version="1.0">
<SgmsApiResult><returnCode>error.getCode() </returnCode>;
<returnString>Just a test string</returnString>";
```

```
</sgmsApiResult>
```

Example

In the following example, four 100 Node Anti-Virus activation codes are added to SonicWALL GMS:

```
sgms> activationcode new_virus_codes.xml
```

The following is the content of new_virus_codes.xml.

```
<? Xml version ="1.0" >
<Sgmscommand>
     <Activation>add</Activation>
     <Activation values>
          <Activation category>Anti-Virus</Activation _category >
          <Activation type>100 Nodes</Activation type>
     </Activation values>
     <Codes>
          <Code>12345678</code>
          <Code>23456780</code>
          <Code>34567890</code>
          <Code>45678901</code>
     </Codes>
</Sgmscommand>
```

Note: *A sample of the file is available on the SonicWALL GMS CD-ROM. It is called sample_activationcode.xml and is located in the Misc directory.*

Using the Configure Command

To execute a group of commands in an XML configuration file, use the **configure** command.

```
sgms> configure xml_file
```

Note: *For information on creating a configuration file, see "Preparing a Configuration File" on page 29.*

Syntax

xml_file	The XML file that contains configuration instructions.

Defaults

none

Usage Guidelines

When this command is entered, SonicWALL GMS does the following:

- Checks whether the command is entered with the correct parameters.
  - If the command is not entered correctly, it returns the correct form of the command.
- Checks the validity of the XML file.
- Executes the command.
- Closes the session and exits.

Example

In the following example, the user admin logs in using the password "password" and runs an **addunit** command.

```
sgms> configure configure.xml
```

Preparing a Configuration File

Configuration files can be used to set, add, or delete parameters that are normally only accessible from the SonicWALL GMS UI.

Note: *For detailed information on configuration parameteres, see Chapter 3, "Configuration Parameters."*

The following is the format of an XML configuration file:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!DOCTYPE Configure [

<!ELEMENT Configure (Task*)>

<!ELEMENT Task  (SetParam*,DelParam*,AddParam*)>
<!ATTLIST Task
                displayname      CDATA    #REQUIRED
                viewname         CDATA    #REQUIRED
                updatetype       CDATA    #REQUIRED
                tasktype         CDATA    #REQUIRED
                description      CDATA    #REQUIRED>

<!ELEMENT SetParam        EMPTY>
<!ATTLIST  SetParam
                setParamNameCDATA         #REQUIRED
                setParamValueCDATA        #REQUIRED>

<!ELEMENT DelParamEMPTY>
<!ATTLIST  DelParam
                delParamNameCDATA         #REQUIRED
                delParamValueCDATA        #REQUIRED>

<!ELEMENT AddParamEMPTY>
<!ATTLIST  AddParam
                addParamNameCDATA         #REQUIRED
                addParamValueCDATA        #REQUIRED>

]>
<Configure>
        <Task
displayname="firewall_parameters"
                viewname="view_name"
                updatetype="update_type"
                tasktype="task_type"
                description="description"
        >
<AddParam  addParamName="add_parameter_name"  addParamValue="add_parameter_value"/>

<AddParam  setParamName="set_parameter_name"  setParamValue="set_parameter_value"/>
        </Task>
</Configure>
```

firewall_parameters	Required. Specifies the firewall or parameters of the firewalls that will updated. To specify a single firewall, enter the firewall name. For example: displayname="Firewall_42" To specify more than one firewall, enter each group parameter that applies to the firwall. For example: `displayname="Country=USA:State=California:Department=Engineering"`
view_name	Specifies the view to which the firewall or group of firewalls belongs. This allows you to apply changes to firewalls within a specific view. For example, to apply the changes to firewalls that meet the parameters that you specified in the view "USA_west_coast," enter the following `viewname="USA_west_coast"`
task_type	Specifies the task type. Options include: • Configure_FW—used to configure SonicWALL firewalls • Configure_RC—used to configure Ravlin devices • Register—used to register SonicWALL appliances or Ravlin devices
description	Description of the tasks you are performing. This information will appear in the log files.
Parameter Settings	Used to add, delete, or set parameters. Change Fields Used to set independent firewall parameters. • *set_parameter_name*—specifies the name of the parameter. • *set_parameter_value*—specifies the new setting. Add Fields Used to add new firewall parameters. • *add_parameter_name*—specifies the name of the parameter. • *add_parameter_value*—specifies the new parameter setting. Delete Fields Used to delete firewall parameters. • *del_parameter_name*—specifies the name of the parameter. • *del_parameter_value*—specifies the setting to delete. Special Action Used to execute special actions such as a resetting a firewall. • *set_parameter_name*—specifies the name of the parameter. • *set_parameter_value*—specifies the action to execute.

Configuration Parameters

This chapter contains information on each parameter that can be used with the command-line interface (CLI) configure command.

This chapter is divided alpabetically by configuration tree. For example, Access/General appears before VPN/Configure.

Each command has a brief description plus guidelines and restrictions. These include:

- Configuration Command—specifies the command to use when setting the parameter.
- Group Configurable—specifies whether the command can be executed at the group or global level.
- Type—specifies the command type. It may be a simple text string or a Boolean operator that indicates whether the option is enabled.
- Control Type—specifies the type of user interface control that corresponds to this parameter. It might be a check box, radio button, or text field.
- Default Value—specifies the default value, if applicable.
- Minimum Value:—specifies the minimum value, if applicable.
- Maximum Value:—specifies the maximum value, if applicable.
- Requires Reboot—specifies whether the SonicWALL appliance(s) will require rebooting after the command is executed.

Note: *For information on using the configure command, see "Using the Configure Command" on page 28.*

Access/General

This section describes parameters that can be configured from the General page of the Access tree.

nbt_dmzEnable

Description

Computers running Microsoft Windows communicate with each other through NetBIOS broadcast packets. By default, SonicWALL appliances block these broadcasts. This parameter configures the SonicWALL appliance(s) to allow NetBIOS packets to pass from the LAN (WorkPort) to the DMZ (HomePort).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

nbt_enable

Description

Allows the SonicWALL appliance(s) to allow NetBIOS packets to pass from the LAN (WorkPort) to the WAN.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

randomizeIds

Description

Hackers can use various detection tools to “fingerprint” IP IDs and detect the presence of a SonicWALL appliance. This parameter configures the SonicWALL appliance(s) to generate random IP IDs.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enableStealthMode

Description

This parameter enables stealth mode. During normal operation, SonicWALL appliances respond to incoming connection requests as either “blocked” or “open.” During stealth operation, SonicWALL appliances do not respond to inbound requests, making the appliances “invisible” to potential hackers.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

cacheTimeout

Description

The Network Connection Inactivity Timeout option disables connections outside the LAN if they are idle for a specified period of time. Without this timeout, connections can stay open indefinitely and create potential security holes. Use this parameter to specify how long (in minutes) the SonicWALL appliance(s) wait before closing inactive connections outside the LAN.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 1

Maximum Value: 999

Requires Reboot: No

Access/Management

This section describes parameters that can be configured from the Management page of the Access tree.

useRemoteMgtName

Description

This parameter specifies how the SonicWALL appliance is managed. If it will be managed from the WAN, enter 1. If it will be managed from the SonicWALL GMS, enter 0.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

useGlobalMgt

Description

This parameter specifies how the SonicWALL appliance is managed. If it will be managed from the WAN, enter 0. If it will be managed from the SonicWALL GMS, enter 1.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enableIE

Description

Specifies whether the SonicWALL appliance(s) will be managed using Internet Explorer. If yes, enter 1. If no, enter 0.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

globalMgtIpName

Description

Specifies the hostname or IP address of the SonicWALL GMS agent that manages the SonicWALL appliance(s).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 39

Requires Reboot: No

globalMgtNatInterposeName

Description

Specifies whether the SonicWALL GMS agent is behind a NAT Device.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

globalMgtNatInterposeIpName

Description

Specifies the IP address of the NAT Device.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

globalMgtSgmsOnVpn

Description

Specifies that the SonicWALL appliance and the SGMS Gateway already communicate through a VPN tunnel and no management security association is necessary.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

globalMgtSecretTagName

Description

Specifies the encryption key. The DES and ARCFour Keys must be exactly 16 characters long and be composed of hexadecimal characters. Encryption keys less than 16 characters will not be accepted; keys longer than 16 characters will be truncated. If the **SGMS on VPN** option is enabled, this is not necessary.

Note: *Valid hexadecimal characters are "0" to "9", and "a" to "f" (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be "1234567890abcdef."*

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: (DefaultData)paramDefaultGlobalMgmtSecret

Minimum Value: None

Maximum Value: None

Requires Reboot: No

globalMgtAuthKeyTagName

Description

Specifies the authentication key. The authentication key must be exactly 32 characters long and be composed of hexadecimal characters. Authentication keys less than 32 characters will not be accepted; keys longer than 32 characters will be truncated. If the **SGMS on VPN** option is enabled, this is not necessary.

Note: *Valid hexadecimal characters are "0" to "9", and "a" to "f" (i.e., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f). For example, a valid key would be "1234567890abcdef1234567890abcdef."*

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: (DefaultData)paramDefaultGlobalMgtAuthKey

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Access/RADIUS

This section describes parameters that can be configured from the RADIUS page of the Access tree.

radiusUserRemoteAccess

Description

Enables users to access LAN (WorkPort) resources from the Internet.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0001

Maximum Value: 0x0001

Requires Reboot: No

radiusUserBypassFilters

Description

Enables Bypass Filters if the users can bypass Content Filtering settings.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0002

Maximum Value: 0x0002

Requires Reboot: No

radiusUserLimitedMgmt

Description

Allows authorized users limited local management access to the SonicWALL Management interface. This access is limited to the following pages:

- **General**—Status, Network, Time
- **Log**—View Log, Log Settings, Log Reports
- **Tools**—Restart, Diagnostics minus Tech Support Report

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0020

Maximum Value: 0x0020

Requires Reboot: No

radiusUserVpnAccess

Description

Enables the users to send information over VPN Security Associations.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0008

Maximum Value: 0x0008

Requires Reboot: No

radiusUserVpnXauthClient

Description

Enable this option if VPN clients are using XAUTH for authentication.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: (DefaultData)paramDfltRadUserXauth

Minimum Value: 0x0010

Maximum Value: 0x0010

Requires Reboot: No

Radius_user

Description

Defines the name of the RADIUS test user.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 32

Requires Reboot: No

Radius_passwd

Description

Defines the password of the RADIUS test user.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 32

Requires Reboot: No

Radius_retries

Description

Use this parameter to configure the number of retries. This parameter defines the number of times the SonicWALL will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection will be dropped. The RADIUS server retries can range from 0 to 30, but three retries is recommended.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 3

Minimum Value: 1

Maximum Value: 10

Requires Reboot: No

Radius_timeout

Description

Use this parameter to configure the amount of time that will elapse before the SonicWALL reattempts to contact the RADIUS server. The RADIUS server timeout can range from 1 to 60 seconds, but 5 seconds is recommended.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 1

Maximum Value: 60

Requires Reboot: No

Rad_prm_IP

Description

Configures the IP address or domain name of the primary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Rad_prm_port

Description

Configures the port of the primary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 1812

Minimum Value: 0

Maximum Value: 65535

Requires Reboot: No

Rad_prm_secret

Description

Configures the shared secret of the primary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 31

Requires Reboot: No

Rad_sec_IP

Description

Configures the IP address or domain name of the secondary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Rad_sec_port

Description

Configures the port of the secondary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 1812

Minimum Value: 0

Maximum Value: 65535

Requires Reboot: No

Rad_sec_secret

Description

Configures the shared secret of the secondary RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 31

Requires Reboot: No

Access/Rules

This section describes parameters that can be configured from the Rules page of the Access tree.

prefs_svcName

Description

Specifies the service name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

serviceNameInRule

Description

Key: equals SERVICES (svcInternalName)

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 0xFFFF

Requires Reboot: No

serviceInternalName

Description

Service Name - always in English - used as key for rules

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleAction

Description

Specifies whether the service is allowed or denied.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Radio button

Default Value: (DefaultData)paramDefaultRules

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

prefs_ruleSrcEnet

Description

Specifies the source SonicWALL interface to which this rule applies (0 => LAN; 1 => WAN; 2 => DMZ; 3 => *).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 3

Requires Reboot: No

prefs_ruleSrcBegin

Description

Specify the first IP address in the source IP address range. The rule will apply to requests originating from IP addresses within this range. For all IP addresses, enter an asterisk (*).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleSrcEnd

Description

Specify the last IP address in the source IP address range. The rule will apply to requests originating from IP addresses within this range. For all IP addresses, enter an asterisk (*).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleDstEnet

Description

Specifies the destination SonicWALL interface to which this rule applies (0 => LAN; 1 => WAN; 2 => DMZ; 3 => *).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 3

Requires Reboot: No

prefs_ruleDstBegin

Description

Specify the first IP address in the destination IP address range. The rule will apply to requests originating from IP addresses within this range. For all IP addresses, enter an asterisk (*).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleDstEnd

Description

Specify the last IP address in the destination IP address range. The rule will apply to requests originating from IP addresses within this range. For all IP addresses, enter an asterisk (*).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleTimeConstraint

Description

Specify when the rule will be applied.

0 => Apply Rule Always; 1 => Apply Rule At Specified Times

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleTimeBegin

Description

If the rule will be enforced during a specific time period, enter the start time in minutes:

0 = Sun 00:00; 10080 = Sat 24:00

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: ((6 * 1440) + (23 * 60) + 59)

Requires Reboot: No

prefs_ruleTimeEnd

Description

If the rule will be enforced during a specific time period, enter the end time in minutes:

0 = Sun 00:00; 10080 = Sat 24:00

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: ((6 * 1440) + (23 * 60) + 59)

Requires Reboot: No

prefs_ruleTimeout

Description

Specifies how long (in minutes) the connection may remain idle before the connection is terminated.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 60000

Requires Reboot: No

prefs_ruleEnabled

Description

To enable the rule, enter 1. To disable the rule, enter 0.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleAllowFrags

Description

Allows fragmented packets.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleBwMgmtEnabled

Description

Enables outbound bandwidth management.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleBwMgmtGuaranteed

Description

Specifies the amount of bandwidth that will always be available to this service. This bandwidth will be permanently assigned to this service and not available to other services, regardless of the amount of bandwidth this service does or does not use.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Float

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleBwMgmtMaximum

Description

Specifies the maximum amount of bandwidth that will be available to this service.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Float

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_ruleBwMgmtPriority

Description

Specifies the priority of this service.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Access/Services

This section describes parameters that can be configured from the Services page of the Access tree.

prefs_svcPortNum

Description

Specifies the beginning of the port range for the service.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 0xFFFF

Requires Reboot: No

serviceInternalName

Description

Specifies the service name. It is used as a key for the rule and must be in English.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_svcIPType

Description

Specifies the protocol:

1 => ICMP; 6 => TCP; 17 => UDP

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 255

Requires Reboot: No

prefs_svcName

Description

Specifies the service name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_svcActionMask

Description

Enables or disables logging:

1 => Enable Logging; 0 => Disable Logging

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_svcPortEnd

Description

Specifies the ending of the port range for the service.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 0xFFFF

Requires Reboot: No

known_svcName

Description

Specifies the name of a known service. This service name must exactly match the service name for the firewall.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

Access/SNMP

This section describes parameters that can be configured from the Simple Network Management Protocol (SNMP) page of the Access tree.

snmp_Enable

Description

Enables SNMP.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

snmp_Mib2SysName

Description

Specifies the SNMP system name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpMib2SysName) - 1

Requires Reboot: No

snmp_Mib2SysContact

Description

Specifies the SNMP system contact.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpMib2SysContact) - 1

Requires Reboot: No

snmp_Mib2SysLocation

Description

Specifies the SNMP system location.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpMib2SysLocation) - 1

Requires Reboot: No

snmp_GetCommunity

Description

Specifies the SNMP get community name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: strSnmpDefaultGetCommunity

Minimum Value: 0

Maximum Value: sizeof(gSnmpGetCommunity[0]) - 1

Requires Reboot: No

snmp_TrapCommunity

Description

Specifies the SNMP trap community name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpTrapCommunity[0]) - 1

Requires Reboot: No

snmp_HostIP0

Description

Specifies the IP address or hostname of Host 1.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpHost[0]) - 1

Requires Reboot: No

snmp_HostIP1

Description

Specifies the IP address or hostname of Host 2.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpHost[1]) - 1

Requires Reboot: No

snmp_HostIP2

Description

Specifies the IP address or hostname of Host 3.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpHost[2]) - 1

Requires Reboot: No

snmp_HostIP3

Description

Specifies the IP address or hostname of Host 4.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gSnmpHost[3]) - 1

Requires Reboot: No

Access/Users

This section describes parameters that can be configured from the Users page of the Access tree.

userInactivity

Description

Specifies the maximum amount of time (in minutes) a connection may remain idle before users are required to reestablish an authenticated session. The timeout applies to both Remote Access and Bypass Filters.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 5

Maximum Value: 99

Requires Reboot: No

users_loginName

Description

Specifies a username.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

users_password

Description

Specifies the user's password.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

userRemoteAccess

Description

Specifies whether the user can access LAN resources from the Internet.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0001

Maximum Value: 0x0001

Requires Reboot: No

userBypassFilters

Description

Specifies whether the user can bypass Content Filtering settings.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0002

Maximum Value: 0x0002

Requires Reboot: No

userMaxTime

Description

Specifies the maximum session time.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 30

Minimum Value: 0

Maximum Value: None

Requires Reboot: No

userVpnAccess

Description

Specifies whether the user can send information over the VPN Security Associations.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0008

Maximum Value: 0x0008

Requires Reboot: No

userVpnXauthClient

Description

Enable this option if the VPN client user will use XAUTH for authentication.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0010

Maximum Value: 0x0010

Requires Reboot: No

userLimitedMgmt

Description

Allows authorized users limited local management access to the SonicWALL interface. Access is limited to the General page (Status, Network, Time), the Log page (View Log, Log Settings, Log Reports), and the Tools page (Restart, Diagnostics minus Tech Support).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: BooleanInBitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0x0020

Maximum Value: 0x0020

Requires Reboot: No

userRadiusSelect

Description

Specifies whether manually entered users are authenticated by the SonicWALL appliance or whether the SonicWALL appliance will use RADIUS for authentication:

0 => Authenticate users listed below 1 => Use RADIUS

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: (DefaultData)paramDefaultUseRadius

Minimum Value: None

Maximum Value: None

Requires Reboot: No

userNoAuthDNS

Description

Specifies whether DNS access will be available for unauthenticated VPN users.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

userRadiusCheckLocal

Description

Allows only manually entered users to access the RADIUS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Advanced/DMZ Addresses

This section describes parameters that can be configured from the DMZ Addresses page of the Advanced tree.

prefs_dmzBegin

Description

If the devices on the DMZ will use fixed IP addresses, use this parameter to enter the starting IP address in the range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_dmzEnd

Description

If the devices on the DMZ will use fixed IP addresses, use this parameter to enter the ending IP address in the range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

natOnDmz

Description

Use this parameter to enable NAT on the DMZ. Select from the following:

1 => Enable DMZ in NAT Mode; 0 => DMZ in Standard Mode

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dmzNetwork

Description

Specifies the private internal IP address assigned to the DMZ or HomePort interface.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dmzSubnetMask

Description

Specifies the DMZ subnet mask.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0xffffff00

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dmzPublic

Description

Specifies the DMZ or HomePort public IP address that will be used to access devices on the DMZ interface.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Advanced/Ethernet

This section describes parameters that can be configured from the Ethernet page of the Advanced tree.

wanBwMgmtEnabled

Description

Enables bandwidth management.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

wanBwMgmtAvailable

Description

Specifies the amount of available bandwidth in kilobytes per second.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Float

Control Type: Text field

Default Value: 0

Minimum Value: 20

Maximum Value: 100000

Requires Reboot: No

wanLinkAbility

Description

Specifies whether the WAN link automatically negotiates Ethernet settings or is forced to a specific setting. Select from the following:

- Auto Negotiate => AutoNeg
- Forced Settigns => Force

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Special

Default Value: 0x40000000ul

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dmzLinkAbility

Description

Specifies whether the DMZ link automatically negotiates Ethernet settings or is forced to a specific setting. Select from the following:

- Auto Negotiate => AutoNeg
- Forced Settigns => Force

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Special

Default Value: 0x40000000ul

Minimum Value: None

Maximum Value: None

Requires Reboot: No

lanLinkAbility

Description

Specifies whether the LAN link automatically negotiates Ethernet settings or is forced to a specific setting. Select from the following:

- Auto Negotiate => AutoNeg
- Forced Settigns => Force

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Special

Default Value: 0x40000000ul

Minimum Value: None

Maximum Value: None

Requires Reboot: No

proxyPcMacOnWan

Description

If you are managing the Ethernet connection from the LAN (WorkPort) side of your network, use this option. The SonicWALL appliance will take the Ethernet address of the computer that is managing the SonicWALL appliance and will proxy the address on the WAN port of the SonicWALL. If you are not managing the SonicWALL appliance from the LAN side of your network, the firmware looks for a random computer on the LAN which can be a lengthy search process.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

fragmentPackets

Description

To limit the size of packets sent over the Ethernet WAN interface, use the Fragment Outbound Packets Larger than the WAN MTU option.

If the maximum transmission unit (MTU) size is too large for a remote router, it may require more transmissions. If the packet size is too small, this could result in more packet header overhead and more acknowledgements that have to be processed. The default size is 1,500 MTU.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

wanMtu

Description

Specifies the WAN MTU.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 1500

Minimum Value: 68

Maximum Value: 1500

Requires Reboot: No

Advanced/Intranet

This section describes parameters that can be configured from the Intranet page of the Advanced tree.

rangeMode

Description

Select from the following Intranet options:

- If the SonicWALL is not used to separate LAN segments on the intranet, select SonicWALL's WAN link is connected to the Internet Router (0).
- If the smaller network is connected to the LAN, select Specified addresses are attached to the LAN (WorkPort) link (1).
- If the smaller network is connected to the WAN, select Specified addresses are attached to the WAN link (2).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Radio button

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

prefs_intraBegin

Description

Specifies the beginning of the IP address range of a group of systems on the smaller network.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_intraEnd

Description

Specifies the ending of the IP address range of a group of systems on the smaller network.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Advanced/One-to-One NAT

This section describes parameters that can be configured from the One-to-One NAT page of the Advanced tree.

nat_oneToOneOn

Description

Enables One-to-One NAT.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

nat_121priv

Description

Specifies the first IP address of the internal IP address range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

nat_121pub

Description

Specifies the first IP address of the public IP address range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

nat_121len

Description

Specifies the range length.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 1

Maximum Value: 253

Requires Reboot: No

Advanced/Proxy Relay

This section describes parameters that can be configured from the Proxy Relay page of the Advanced tree.

webProxySrvrName

Description

Specifies the hostname or IP address of web proxy server

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 39

Requires Reboot: No

webProxyPort

Description

Specifies the Port of the web proxy server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 65535

Requires Reboot: No

bypassFailedProxy

Description

When enabled, the proxy server will be bypassed upon proxy server failure.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Advanced/Routes

This section describes parameters that can be configured from the Routes page of the Advanced tree.

ipAddr

Description

Specifies the SonicWALL LAN IP address.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: (DefaultData)paramDefaultMgmtAddr

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

ipSubnetMask

Description

Specifies the SonicWALL LAN subnet mask.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: (DefaultData)paramDefaultMgmtAddr

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

wanSubnetMask

Description

Specifies the SonicWALL WAN/DMZ subnet mask.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0xffffff00

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_route_dstNet

Description

Specifies the destination network.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_route_dstMask

Description

Specifies the destination subnet mask.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_route_dstGw

Description

Specifies the destination gateway.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_route_link

Description

Specifies the link to which the router is attached. Select from the following:

0 => LAN; 1 => WAN; 2 => DMZ; 3 => *

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Scrollbox

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

Anti-Virus/Configure

This section describes parameters that can be configured from the Configure page of the Anti-Virus tree.

avExcludeBegin

Description

Specifies the first IP address of a range that is included or excluded from anti-virus scanning. Whether the address range is included or excluded will depend on how you configured the avListMode option.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

avExcludeEnd

Description

Specifies the last IP address of a range that is included or excluded from anti-virus scanning. Whether the address range is included or excluded will depend on how you configured the avListMode option.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

highRiskAlert

Description

Significant virus events can occur without warning (e.g., Melissa, ILOVEYOU, and others). When these occur, SonicWALL GMS can be configured to block network traffic until the latest virus definition files are downloaded.

Use this parameter to configure SonicWALL GMS to block access when High Risk events occur.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

avListMode

Description

Selects whether the SonicWALL appliance will enforce virus scanning for specific IP address ranges, all IP address ranges, or all IP address ranges except for a specific list.

- To enforce anti-virus scanning for all IP addresses, enter 0.
- To scan only a list of IP address ranges, enter 1. To specify the list range, see “avExcludeBegin” on page 79 and “avExcludeBegin” on page 79.
- To scan all IP address ranges except for a list of ranges, enter 2. To specify the list range, see “avExcludeBegin” on page 79 and “avExcludeBegin” on page 79.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Radio button

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

avEnable

Description

Enables Anti-Virus.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

policeDmz

Description

Enables DMZ policing.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

avDisableLanToDmzPolicing

Description

Disables policing from LAN to DMZ.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

daysToForceUpdate

Description

Specifies the maximum days before an update is forced.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 5

Minimum Value: 0

Maximum Value: 10

Requires Reboot: No

lowRiskAlert

Description

Significant virus events can occur without warning (e.g., Melissa, ILOVEYOU, and others). When these occur, SonicWALL GMS can be configured to block network traffic until the latest virus definition files are downloaded.

Use this parameter to configure SonicWALL GMS to block access when Low Risk events occur.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

mediumRiskAlert

Description

Significant virus events can occur without warning (e.g., Melissa, ILOVEYOU, and others). When these occur, SonicWALL GMS can be configured to block network traffic until the latest virus definition files are downloaded.

Use this parameter to configure SonicWALL GMS to block access when Medium Risk events occur.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

avReduceTraffic

Description

Configure the SonicWALL appliance(s) to only check for updates once a day. This reduces the amount of network activity for low-speed connections such as ISDN.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

Anti-Virus/EMail Filter

This section describes parameters that can be configured from the Email Filter page of the Anti-Virus tree.

MAFiAEnabled

Description

Enables the E-Mail Attachment Filtering Alert service.

Note: *Never go against the family.*

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

smtpFilterEnabled

Description

Enables e-mail attachment filtering.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

smtpFilterMode

Description

Configures how infected files are handled. If the file extension will be changed so the file cannot be executed, enter 0. If infected files will be deleted, enter 1.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

smtpAttachmentStrip

Description

Defines the warning message text that will be sent to users who receive infected e-mail messages.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: strAttachmentStripMessage

Minimum Value: 0

Maximum Value: 304 - 1

Requires Reboot: No

extension_add

Description

Adds a file extension to scan.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: SearchList

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

DHCP/DHCP over VPN

This section describes parameters that can be configured from the DHCP over VPN page of the VPN tree.

dhcprLocalIp

Description

Defines a static IP address on the LAN. This option is used with dhcprIpMac.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: 1

Maximum Value: 0xFFFFFFFE

Requires Reboot: No

dhcprIpMac

Description

Defines the MAC address for the static IP address on the LAN. This option is used with dhcprLocalIp (xx:xx:xx:xx:xx:xx).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

localLanMac

Description

Specifies a LAN MAC address that is not allowed to obtain an IP address through the SA (xx:xx:xx:xx:xx:xx).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

centralDhcpIp

Description

If using a central gateway, specifies the IP address of the central gateway server.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: 1

Maximum Value: 0xFFFFFFFE

Requires Reboot: No

dhcpIpHelper

Description

Sends DHCP requests to the listed server addresses.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

doTempLease

Description

Allows users to obtain temporary leases from the local DHCP server if the tunnel is down.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcprTempLease

Description

Specifies the length of the temporary lease in minutes.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 120

Minimum Value: 60

Maximum Value: 3600

Requires Reboot: No

vpnDhcpTunnel

Description

Obtains IP addresses using DHCP through the specified SA. This must exactly match the SA name specified in the SonicWALL GMS UI.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcprStaticIp

Description

Specifies the DHCP relay IP address.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcprSpoof

Description

Blocks traffic through tunnel when an IP spoof detected.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

isRemoteGw

Description

Not configurable - used to distinguish which screen is displayed.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

DHCP/Setup

This section describes parameters that can be configured from the Setup page of the DHCP tree.

prefs_dhstaticip

Description

Specifies a static IP address. Used in conjunction with prefs_dhstatichw.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_dhstatichw

Description

Specifies a MAC address for the IP address. Used in conjunction with prefs_dhstaticip.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_gateway

Description

Specifies the IP address of the gateway used by LAN (WorkPort) clients to access the Internet. If NAT is enabled, use the SonicWALL LAN (WorkPort) IP address.DHCP Gateway (dhcp_dmz_gateway).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_dhdynstart

Description

Specifies the first address in a dynamic address range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_dhdynend

Description

Specifies the last address in a dynamic address range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

prefs_dhdynbootp

Description

Use this option to allow BootP clients to use the IP address range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

dhcp_dns0

Description

Specifies the IP address of the first DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_dns1

Description

Specifies the IP address of the second DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_dns2

Description

Specifies the IP address of the third DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_wins0

Description

Specifies the IP address of the first WINS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_wins1

Description

Specifies the IP address of the second WINS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_lease

Description

Specifies the DHCP Lease Time in minutes.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 599940

Minimum Value: 60

Maximum Value: 599940

Requires Reboot: No

dhcp_domainname

Description

Specifies the registered domain name for the DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 255

Requires Reboot: No

dhcp_propagateSettingsToLan

Description

Specifies whether the DNS servers will use the SonicWALL appliance's network settings or the manually entered DNS servers:

- 0 => Use SonicWALL Network settings
- 1 => Specify manually

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enableDHCP

Description

Enables the DHCP Server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enablePassDHCP

Description

The Allow DHCP Pass Through option disables the DHCP server and configure computers on the LAN (WorkPort) to use a DHCP server outside the firewall.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhcp_dmz_gateway

Description

Specifies the IP address of the gateway used by LAN (WorkPort) clients if NAT is enabled.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

General/Network

This section describes parameters that can be configured from the Network page of the General tree.

L2tpdnsServer1

Description

Specifies the IP address of the first DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

L2tpdnsServer2

Description

Specifies the IP address of the second DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

L2tpGlobalSonicIp

Description

Specifies the L2TP SonicWALL IP address.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

L2TPClientPswd

Description

Specifies the L2TP user password.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: L2TP_MAX_PASSWORD

Requires Reboot: No

L2TPTimeoutEnable

Description

Enables L2TP disconnect after inactivity.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

L2tpIdleTime

Description

Specifies how long the SonicWALL appliance waits before disconnecting from an L2TP session.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 10

Minimum Value: 1

Maximum Value: 999

Requires Reboot: No

L2tpGlobalServerIp

Description

IP address of the L2TP Server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

PPPoE_Timeout_Enable

Description

Enables PPPoE disconnect after inactivity.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

PPPoEIdleTime

Description

Specifies how long the SonicWALL appliance waits before disconnecting from a PPPoE session.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 10

Minimum Value: 1

Maximum Value: 999

Requires Reboot: No

PPPoEDynamicLocalIP

Description

Configures the SonicWALL appliance to obtain a PPPoE IP Address automatically.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

PPPOEStaticLocalIP

Description

Specifies a static PPPoE IP address.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

L2tpServerIP

Description

IP address of the L2TP Server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

L2TPClientEnabled

Description

Sets L2TP Client mode.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

L2tpClientIslocalDynamicIP

Description

Specifies a static L2TP IP address (use DHCP if this is null).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

L2TPClientHostName

Description

Specifies the L2TP hostname.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: L2TP_MAX_HOST_NAME

Requires Reboot: No

L2TPClientUserName

Description

Specifies the L2TP user name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: L2TP_MAX_USER_NAME

Requires Reboot: No

nat_manyToOneOn

Description

Enables NAT mode.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

dhClient_active

Description

Enables DHCP mode.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

PPPOEEnabled

Description

Enables PPPoE mode.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

ipAddr

Description

Specifies the SonicWALL LAN IP Address.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: (DefaultData)paramDefaultMgmtAddr

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

ipSubnetMask

Description

Specifies the LAN Subnet Mask.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: (DefaultData)paramDefaultMgmtAddr

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

lanSubnetGateway

Description

Specifies the subnet mask of the Network Gateway.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

PPPOEUserName

Description

Specifies the PPPoE user name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 64

Requires Reboot: No

PPPOEPswd

Description

Specifies the PPPoE user password.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 64

Requires Reboot: No

nat_mTo1PubAddr

Description

Specifies the SonicWALL WAN IP address (NAT Public).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipGateway

Description

Specifies the IP address of WAN Gateway.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

wanSubnetMask

Description

Specifies the subnet mask of WAN Gateway.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0xffffff00

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhClient_leaseDuration

Description

Specifies the DHCP lease duration.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dhClient_hostName

Description

Specifies the hostname of the DHCP server (if applicable).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 64

Requires Reboot: No

dnsSrvAddr

Description

Specifies the IP address of the first DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dnsServer2

Description

Specifies the IP address of the second DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dnsServer3

Description

Specifies the IP address of the third DNS server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

General/Time

This section describes parameters that can be configured from the Time page of the General tree.

timezone

Description

Sets the time zone.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 829

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ntp_useNtp

Description

Configures the SonicWALL appliance(s) to use Network Time Protocol (NTP).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ntp_useDst

Description

Configures the SonicWALL appliance(s) to automatically adjust the clock for Daylight Savings Time changes.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ntp_utcLogs

Description

Configures the SonicWALL appliance(s) to display UTC in the logs instead of local time.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

useInternational

Description

Configures the SonicWALL appliance(s) to display time in the International Format.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

addCustomNTPServer

Description

Specifies the hostname or IP address of an NTP server.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: VLA

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ntp_updateInterval

Description

Specifies how often (in minutes) the SonicWALL appliance will synchronize its time settings with the NTP server.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 60

Minimum Value: 5

Maximum Value: 100080

Requires Reboot: No

High Availability/Configure

This section describes parameters that can be configured from the Configure page of the High Availability tree.

haPrimaryLanIp

Description

Specifies the LAN IP address of the primary SonicWALL appliance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0x00000000

Minimum Value: None

Maximum Value: None

Requires Reboot: No

haPrimaryWanIp

Description

Specifies the WAN IP address of the primary SonicWALL appliance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0x00000000

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enableHA

Description

Enables High Availability.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

haBackupMacAddr

Description

Specifies the MAC address of the backup SonicWALL appliance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: (DefaultData)paramDefaultHaBackupMac

Minimum Value: None

Maximum Value: None

Requires Reboot: No

haBackupLanIp

Description

Specifies the LAN IP address of the backup SonicWALL appliance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0x00000000

Minimum Value: None

Maximum Value: None

Requires Reboot: No

haBackupWanIp

Description

Specifies the WAN IP address of the backup SonicWALL appliance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0x00000000

Minimum Value: None

Maximum Value: None

Requires Reboot: No

enablePreemptMode

Description

Configures the primary SonicWALL appliance to take over from the backup SonicWALL appliance when it becomes available. Otherwise, the backup SonicWALL appliance will remain active.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

heartbeatInterval

Description

Specifies the heartbeat interval (in seconds).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 3

Maximum Value: 255

Requires Reboot: No

maxHeartbeatWait

Description

Specifies how long the backup waits before replacing the primary (in seconds).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 3

Minimum Value: 2

Maximum Value: 99

Requires Reboot: No

electionDelayTime

Description

Specifies the length of the SonicWALL detection time.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 300

Requires Reboot: No

Log/Log Settings

This section describes parameters that can be configured from the Log Settings page of the Log tree.

firewallName

Description

Specifies the name of the SonicWALL appliance. The firewall name appears in the subject of email sent by the SonicWALL appliance. By default, the firewall name is the same as the SonicWALL appliance serial number

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: (DefaultData)paramDefaultFirewallName

Minimum Value: 0

Maximum Value: 63

Requires Reboot: No

logPrefs_alertMask_2

Description

Configures the SonicWALL appliance to log Blocked Web Sites (Alerts/SNMP Traps).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (logCatAttack | logCatSysErr)

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_alertMask_5

Description

Configures the SonicWALL appliance to log Attacks (Alerts/SNMP Traps).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (logCatAttack | logCatSysErr)

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_alertMask_1

Description

Configures the SonicWALL appliance to log System Errors (Alerts/SNMP Traps).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (logCatAttack | logCatSysErr)

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_7

Description

Configures the SonicWALL appliance to log Dropped UDP.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_8

Description

Configures the SonicWALL appliance to log Dropped ICMP.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_9

Description

Configures the SonicWALL appliance to log Network Debugging.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_11

Description

Configures the SonicWALL appliance to log blocked LAN IP connections.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_0

Description

Configures the SonicWALL appliance to log System Maintenance.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_1

Description

Configures the SonicWALL appliance to log System Errors.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_2

Description

Configures the SonicWALL appliance to log Blocked Web Sites.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_3

Description

Configures the SonicWALL appliance to log Blocked Java, ActiveX, and Cookies.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_4

Description

Configures the SonicWALL appliance to log User Activity.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_14

Description

Configures the SonicWALL appliance to log VPN TCP Statistics.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_5

Description

Configures the SonicWALL appliance to log Attacks.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

logPrefs_logMask_6

Description

Configures the SonicWALL appliance to log Dropped TCP.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: (~(logCatDebug|logCatLanTCP|logCatLanUDP|logCatLanICMP|logCatVPNStat))

Minimum Value: 0

Maximum Value: 15

Requires Reboot: No

smtpServerName

Description

Configures the SonicWALL appliance to log Mail Server errors.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 40 - 1

Requires Reboot: No

logPrefs_logEmailAddr

Description

Specifies the e-mail address where the log file will be sent.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 63

Requires Reboot: No

logPrefs_alertEmailAddr

Description

Specifies the e-mail address where alerts will be sent.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 63

Requires Reboot: No

logPrefs_logEmailFreq

Description

Specifies how frequently the log is mailed:

- 0 => When Full
- 1 => Daily
- 2 => Weekly

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

logPrefs_dayOfWeek

Description

If the log is mailed weekly, specifies the day of week (0 = Sunday).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

logPrefs_timeOfDay

Description

If the log is mailed daily or weekly, specifies the hour of day (24 hour format).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 23

Requires Reboot: No

logPrefs_syslogFreqSecs

Description

Specifies the syslog event rate in seconds.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 86400

Requires Reboot: No

syslogStatusFreqSecs

Description

Specifies the heartbeat interval in seconds.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 60

Minimum Value: 0

Maximum Value: 86400

Requires Reboot: No

logPrefs_disableWhenFull

Description

Specifies what will happen when the log is full:

- 0 => Overwrite Log
- 1 => Shutdown SonicWALL

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

syslogFormat

Description

Specifies the syslog format:

- 0 => Default
- 1 => Webtrends

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Modem/Configure

This section describes parameters that can be configured from the Configure page of the Modem tree.

Note: *These parameters only apply to the SonicWALL Tele3 SP.*

dialupProfileInUse_0

Description

Specifies the primary dialing profile.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: PN_LEN+1

Requires Reboot: No

dialupProfileInUse_1

Description

Specifies the secondary dialing profile.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: PN_LEN+1

Requires Reboot: No

speakerSettings

Description

Specifies the speaker volume:

- 0 = Off
- 1 = Low
- 2 = Medium
- 3 = High

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Popup

Default Value:

Minimum Value: 0

Maximum Value: 3

Requires Reboot: No

atCommand

Description

Specifies the AT command string for dialing.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: MODEMSTR_LEN+1

Requires Reboot: No

enableWanFailover

Description

Enables WAN Failover.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

enableProbing

Description

Enables probing on primary and/or secondary interfaces.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

probeOnInterfaces

Description

Probes primary and/or secondary interfaces.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Popup

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot: No

probeTarget

Description

Specifies the IP address that the SonicWALL appliance will use to test Internet connectivity. We recommend using the IP address of the WAN Gateway.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

probeInterval

Description

Specifies how often the SonicWALL appliance tests the broadband interface (in seconds).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot: No

failoverThreshold

Description

Specifies how many times the probe target must be unavailable before the SonicWALL appliance fails over to the modem.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot: No

probesToActive

Description

Specifies how many times the SonicWALL appliance must successfully reach the probe target to reactivate the broadband connection.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot: No

enableFailoverPreempt

Description

Enables Preempt mode.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

Modem/Profile

This section describes parameters that can be configured from the Profile page of the Modem tree.

Note: *These parameters only apply to the SonicWALL Tele3 SP.*

dialConfigName

Description

Sets the modem profile name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 1

Maximum Value: PN_LEN+1

Requires Reboot: No

priPhone

Description

Specifies the primary phone number for a profile.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value:

Requires Reboot: No

secPhone

Description

Specifies the secondary phone number for a profile.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value:

Requires Reboot: No

dupUserName

Description

Specifies the ISP user name for a profile.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: GTH32

Requires Reboot: No

dupUserPass

Description

Specifies the user password.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value:

Requires Reboot: No

dialIpAddrBool

Description

Specifies whether the account uses a static or dynamic IP address:

- 0 = Specify an IP Address
- 1 = Obtain automatically

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

dialupIP Address

Description

Specifies the IP Address for the firewall.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dialDnsSrvBool

Description

Specifies whether the account uses a specific DNS server:

- 0 = Specify an DNS Address
- 1 = Obtain automatically

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

dialupDns1

Description

Specifies the first DNS Address for the firewall.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dialupDns2

Description

Specifies the second DNS Address for the firewall.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

dialChatScript

Description

Specifies the dial chat script for the ISP.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 1024 characters

Requires Reboot: No

connectOnData

Description

Select from the following connection options:

- If the SonicWALL appliance(s) will remain connected to the Internet until the broadband connection is restored, enter 0 (persistent connection).
- If the SonicWALL appliance(s) will only connect to the Internet when data is being sent, enter 1 (dial on data).
- If the SonicWALL appliance(s) will connect to the Internet manually, enter 2 (manual dial).

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Radio button

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot: No

ispInactivityTimeout

Description

Specifies the connection inactivity timeout.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value:

Minimum Value: 0

Maximum Value: 1440

Requires Reboot: No

baudRate

Description

Specifies the baud rate:

- 0 = Auto
- 1 = 2440
- 2 = 4800
- 3 = 9600
- 4 = 14400
- 5 = 19200
- 6 = 38400
- 7 = 57600

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Special

Default Value: 0

Minimum Value:

Maximum Value: DU_SPEED_57600

Requires Reboot: No

maxConnectTime

Description

Specifies the maximum connection time. The SonicWALL appliance will reattempt to connect based on the connectOnData parameter.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0 (no maximum time)

Maximum Value: 1440

Requires Reboot: No

ispReconnectDelay

Description

Specifies how long (in minutes) the SonicWALL appliance waits before reconnecting after the maximum connection time expires

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0 (no delay)

Maximum Value: 1440

Requires Reboot: No

modemDisableVpn

Description

Disables VPN for a profile.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value:

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

callWaitEnable

Description

Enables or disables call waiting for the profile.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

callWaitString

Description

Specifies the string that disables call waiting. For example, “*70.”

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value:

Requires Reboot: No

ispRetries

Description

Specifies the number of dial retries per phone number.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 3

Minimum Value: 0

Maximum Value: 3

Requires Reboot: No

ispRetryDelay

Description

Specifies the delay (in minutes) between retries.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 0

Maximum Value: 60

Requires Reboot: No

Website Blocking/Consent

This section describes parameters that can be configured from the Consent page of the Website Blocking tree.

prefs_aupFilter

Description

Specifies a mandatory filtered IP address.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IP Address

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

aupURL4

Description

Specifies the consent accepted URL (Filtering On).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 99

Requires Reboot: No

aupURL2

Description

Specifies the consent page URL (Mandatory Filtering).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 99

Requires Reboot: No

aupURL3

Description

Specifies the consent accepted URL (Filtering Off).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 99

Requires Reboot: No

aupEnable

Description

Enables the Consent feature.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

aupActivityTimeout

Description

Specifies the maximum web usage time (in minutes).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 9999

Requires Reboot: No

aupURL1

Description

Specifies the consent page URL (Optional Filtering).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 99

Requires Reboot: No

userInactivity

Description

Specifies how long (in minutes) the SonicWALL appliance(s) wait before logging out inactive users.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 5

Maximum Value: 99

Requires Reboot: No

Website Blocking/Customization

This section describes parameters that can be configured from the Customization page of the Website Blocking tree.

sbi_blockCustom

Description

Enables filter list customization.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_trustedOnly

Description

Disables all web traffic except for Trusted Domains.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

forbiddenURLs_add

Description

Specifies a forbidden domain.

Note: *Enter the domain name only. For example, "bad-site.com." Do not include "http://."*
Entering "bad-site.com" will also block access to www.bad-site.com, really.bad-site.com, amazingly.bad-site.com, and so on.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: SearchList

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

allowedURLs_add

Description

Specifies allowed domains.

Note: *Enter the domain name only. For example, "yahoo.com." Do not include "http://."*
Entering "yahoo.com" will also allow access to www.yahoo.com, my.yahoo.com, sports.yahoo.com, and so on.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: SearchList

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Website Blocking/General

This section describes parameters that can be configured from the General page of the Website Blocking tree.

cf_method

Description

Specifies the content filter type:

- 0 = SonicWALL
- 1 = N2H2
- 2 = Websense

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

trustedURLs_add

Description

Specifies a trusted domain.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: SearchList

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_trustCode

Description

Configures the SonicWALL appliance(s) to not block Java/ActiveX/Cookies/Web Proxy on Trusted Domains.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_webBlockMsg

Description

Specifies the message to display when a site is blocked.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: String

Control Type: Text field

Default Value: strWebBlockMessage

Minimum Value: 0

Maximum Value: 255

Requires Reboot: No

CFLinkMask_0

Description

Enables the content filter and restricts web features on the LAN.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

CFLinkMask_1

Description

Enables the content filter and restricts web features on the DMZ.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

Website Blocking/Filter List

This section describes parameters that can be configured from the Filter List page of the Website Blocking tree.

sbi_urlBlockMask_0

Description

Blocks the Violence/Profanity SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_1

Description

Blocks the Partial Nudity SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_2

Description

Blocks the Full Nudity SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_3

Description

Blocks the Sexual Acts SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_4

Description

Blocks the Gross Depictions SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_5

Description

Blocks the Intolerance SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_6

Description

Blocks the Satanic/Cult SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

TOD_useTOD

Description

Specifies when to block restricted content:

- 0 => Always block
- 1 => During a specific time of day

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

TOD_startHour

Description

Specifies the hour when SonicWALL appliance(s) start blocking restricted content in 24-hour time (0-24).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 8

Minimum Value: 0

Maximum Value: 23

Requires Reboot: No

TOD_startMin

Description

Specifies the minute of the hour when the SonicWALL appliance(s) start blocking restricted content (0 - 59).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 59

Requires Reboot: No

TOD_startDay

Description

Specifies the day when the SonicWALL appliance(s) start blocking restricted content (0 - 6; 0 = Sunday)

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 1

Minimum Value: 0

Maximum Value: 6

Requires Reboot: No

TOD_endHour

Description

Specifies the hour when SonicWALL appliance(s) stop blocking restricted content in 24-hour time (0-24).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 18

Minimum Value: 0

Maximum Value: 23

Requires Reboot: No

TOD_endMin

Description

Specifies the minute of the hour when the SonicWALL appliance(s) stop blocking restricted content (0 - 59).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 59

Requires Reboot: No

TOD_endDay

Description

Specifies the day when the SonicWALL appliance(s) stop blocking restricted content (0 - 6; 0 = Sunday)

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 5

Minimum Value: 0

Maximum Value: 6

Requires Reboot: No

sbi_dontBlockOnlyLog

Description

Specify how the SonicWALL appliance(s) will respond when a user attempts to access a restricted site:

- 0 => Log and Block Access
- 1 => Log Only

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Radio button

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

filterListFallback

Description

Specify how the SonicWALL appliance(s) will respond if the filter list expires:

- 0 => Block Traffic
- 1 => Allow Traffic

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Radio button

Default Value: 0

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

sbi_urlBlockMask_7

Description

Blocks the Drug Culture SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_8

Description

Blocks the Militant/Extremist SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_9

Description

Blocks the Sex Education SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_10

Description

Blocks the Gambling/Questionable/Illegal SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

sbi_urlBlockMask_11

Description

Blocks the Alcohol/Tobacco SonicWALL Content Filtering category.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Bitmask

Control Type: Check box

Default Value: 0

Minimum Value: 0

Maximum Value: 13

Requires Reboot: No

LRI_autoDownload

Description

Configures the SonicWALL appliance(s) to automatically download and update the content filter list.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

LRI_dayOfWeek

Description

Specifies the day when the SonicWALL appliance(s) will automatically download the content filter list (0 = Sunday).

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Popup

Default Value: 0

Minimum Value: 0

Maximum Value: 6

Requires Reboot: No

LRI_timeOfDay

Description

Specifies the time when the SonicWALL appliance(s) will automatically download the content filter list (24 hour format)

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 23

Requires Reboot: No

Website Blocking/N2H2

This section describes parameters that can be configured from the N2H2 page of the Website Blocking tree.

n2h2UserName

Description

Specifies the N2H2 user name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gn2h2Param.userName) - 1

Requires Reboot: No

n2h2CacheSize

Description

Specifies the N2H2 cache size in kilobytes.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 50

Minimum Value: 0

Maximum Value: 0

Requires Reboot: No

n2h2FailedTimeout

Description

If N2H2 is unreachable for the specified period of time (in seconds), use the value in n2h2BlockOnFail

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 1

Maximum Value: 10

Requires Reboot: No

n2h2SrvAddr

Description

Specifies the N2H2 Server IP address or hostname.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gn2h2Param.serverAddr) - 1

Requires Reboot: No

n2h2SrvPort

Description

Specifies the N2H2 Server listening port.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 4005

Minimum Value: 1

Maximum Value: 65535

Requires Reboot: No

n2h2LocalPort

Description

Specifies the N2H2 Server reply port.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 4005

Minimum Value: 1

Maximum Value: 65535

Requires Reboot: No

n2h2BlockOnFail

Description

Specifies how the SonicWALL appliance(s) will respond when the N2H2 server cannot be reached:

- 0 = Allow traffic to all websites
- 1 = Block traffic to all websites

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Radio button

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

n2h2BlockBlockedSites

Description

Configure the SonicWALL appliance(s) to block access to restricted sites.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

n2h2LogBlockedSites

Description

Configure the SonicWALL appliance(s) to log access to restricted sites.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Website Blocking/URL Keywords

This section describes parameters that can be configured from the URL Keywords page of the Website Blocking tree.

keyword_add

Description

Specifies a URL keyword to block.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: SearchList

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_blockURLKeywords

Description

Enables keyword blocking.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Website Blocking/Web Features

This section describes parameters that can be configured from the Web Features page of the Website Blocking tree.

sbi_blockActiveX

Description

Blocks ActiveX controls. ActiveX is a programming language used to imbed small programs in web pages. It is generally considered insecure because it is possible for malicious programmers to write controls that can delete files, compromise security, or cause other damage.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_blockJava

Description

Blocks Java applets. Java applets are downloadable web applications that are used on many websites. Selecting this option will block all Java applets, regardless of their function.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_blockCookies

Description

Prevents websites from placing information on user hard drives. Cookies are used by Web servers to track Web usage and remember user identity. Cookies can compromise users' privacy by tracking Web activities.

Note: *Blocking cookies on the public Internet creates a large number of accessibility problems. Most sites make extensive use of cookies to generate web pages and blocking cookies will make most e-commerce applications unusable.*

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

sbi_blockHTTPProxy

Description

Blocks users from accessing web proxy servers on the Internet to circumvent content filtering by pointing their computers to the proxy servers.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

scanForFakeMicrosoftCerts

Description

Blocks access to web content that originated from a known fraudulent certificate. Digital certificates help verify that web content originated from an authorized party.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

Website Blocking/Websense

This section describes parameters that can be configured from the Websense page of the Website Blocking tree.

wseSrvAddr

Description

Specifies the Websense Server IP address or hostname.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gWseParam.serverAddr) - 1

Requires Reboot: No

wseSrvPort

Description

Specifies the Websense Server port.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 15868

Minimum Value: 1

Maximum Value: 65535

Requires Reboot: No

wseUserName

Description

Specifies the Websense user name.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: sizeof(gWseParam.userName) - 1

Requires Reboot: No

wseCacheSize

Description

Specifies the Websense cache size in kilobytes.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 50

Minimum Value: 0

Maximum Value: 0

Requires Reboot: No

wseFailedTimeout

Description

If Websense is unreachable for the specified period of time (in seconds), use the value in wseBlockOnFail

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 5

Minimum Value: 1

Maximum Value: 10

Requires Reboot: No

wseBlockOnFail

Description

Specify how the SonicWALL appliance(s) will respond when the Websense Server cannot be reached.

- 0 = Allow traffic to all websites
- 1 = Block traffic to all websites

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Radio button

Default Value: 1

Minimum Value: 0

Maximum Value: 1

Requires Reboot: No

VPN/CA Certs

This section describes parameters that can be configured from the CA Certs page of the VPN tree.

caCertHash

Description

Specifies the hash index for the CA certificate.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

caCertName

Description

Specifies the CA certificate name computed value.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

caCertData

Description

Specifies the encoded CA certificate contents.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

pkiCaUrlForCrl

Description

Specifies the URL for the Certificate Revocation List.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

pkiNextUpdateForCrl

Description

Specifies the validity of the Certificate Revocation List.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

VPN/Configure

This section describes parameters that can be configured from the Configure page of the VPN tree.

ipsecpeerCertID

Description

Specifies the peer certificate ID. This used with ipsecPeerIdtype.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

pkiPrefNameThirdCert

Description

Specifies the certificate name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 10

Requires Reboot: No

ipsecCertName

Description

Specifies the third Party Certificate name. This is used when the in/out SPI set to 5.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecPeerIdtype

Description

Specifies the peer certificate ID type:

- 1 => Distinguished Name
- 2 => Email ID
- 3 => Domain Name

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecName

Description

Specifies the SA name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 33

Requires Reboot: No

ipsecInSPI

Description

Specifies the incoming SPI

- 1 = IKE
- 2 = Certs
- 5 = 3rd party certificates

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IntegerAsHex

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecApplyRules

Description

Applies NAT and firewall rules to the SA.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0400

Maximum Value: 0x0400

Requires Reboot: No

ipsecDefaultSa

Description

Routes all Internet traffic through this SA.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x2000

Maximum Value: 0x2000

Requires Reboot: No

ipsecForwardPackets

Description

Forward packets to remote VPNs.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x1000

Maximum Value: 0x1000

Requires Reboot: No

ipsecDefaultLanGw

Description

Specifies the IP address of the Default LAN Gateway.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

remoteUnit

Description

Remote Units Serial Number in interconnected mode

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecDstAddrBegin

Description

Specifies the start of the destination network range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecDstAddrEnd

Description

Specifies the end of the destination network range.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecSubnetMask

Description

Specifies the destination subnet mask for NETBIOS Broadcast. This is not used for IKE.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecOutSPI

Description

Specifies the outgoing SPI:

- 1 = IKE
- 2 = Certs
- 5 = 3rd party certificates

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IntegerAsHex

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecRemoteClients

Description

Not used. Leave set to 0.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0001

Maximum Value: 0x0001

Requires Reboot: No

ipsecAllowNetBIOS

Description

Allows Windows Networking (NETBIOS) Broadcasting.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0004

Maximum Value: 0x0004

Requires Reboot: No

ipsecGwAddr

Description

Specifies the IPSec Gateway Address.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecAlgo

Description

Specifies the encryption method.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecESPKey

Description

Specifies the encryption key or IKE shared secret.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecAHKey

Description

Specifies the authentication key.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecRadiusAuth

Description

Forces inbound VPN clients to authenticate with the RADIUS server.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0002

Maximum Value: 0x0002

Requires Reboot: No

ipsecLifeSecs

Description

Specifies the SA lifetime in seconds.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecAllowSWPeerCert

Description

Used for third party certificate support. This option is not available at this time.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 1

Maximum Value: 1

Requires Reboot: No

ipsecAllowSWClientCert

Description

Used for third party certificate support. This option is not available at this time.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 2

Maximum Value: 2

Requires Reboot: No

ipsecSWPeerCertNum

Description

Specifies the peer SonicWALL serial number when using IKE with certificates.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecSWClientCertDN

Description

Used for third party certificate support. This option is not available at this time.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecSaDisabled

Description

Disables this SA.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0100

Maximum Value: 0x0100

Requires Reboot: No

ipsecPFSEnablePFS

Description

Enables Perfect Forward Secrecy, which prevents repeated compromises of the same security key when reestablishing a tunnel.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value:

Maximum Value:

Requires Reboot: No

ipsecKeepAlive

Description

Enables Keep Alive, which configures the VPN tunnel to remain open as long as there is network traffic on the SA.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x4000

Maximum Value: 0x4000

Requires Reboot: No

ipsecAGMode

Description

Enables Aggressive Mode. Aggressive mode improves the performance of IKE SA negotiation by only requiring three packet exchanges. However, it provides no identity protection.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value:

Maximum Value:

Requires Reboot: No

ipsecP1DHGrp

Description

Specifies the Phase 1 DH group.

- 0 = Group 1
- 1 = Group 2
- 2 = Group 5

Note: *Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.*

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

ipsecP2DHGrp

Description

Specifies the Phase 2 DH group:

- 0 = Group 1

- 1 = Group 2
- 2 = Group 5

Note: *Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.*

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

ipsecAlgIdPh1

Description

Specifies the Phase 1 encryption/authentication algorithm:

- 0 = None
- 1 = DES & MD5
- 2 = DES & SHA1
- 3 = 3DES & MD5
- 4 = 3DES & SHA1

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 4

Requires Reboot: No

ipsecTermAt

Description

Specifies where the VPN will terminate:

- 0 => LAN
- 1 => DMZ
- 2 => LAN/DMZ

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Integer

Control Type: Radio button

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

ipsecLocalUserAuth

Description

Requires authentication of local users.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x01

Maximum Value: 0x01

Requires Reboot: No

ipsecRemoteUserAuth

Description

Requires authentication of remote users.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x02

Maximum Value: 0x02

Requires Reboot: No

ipsecDhcpTunnel

Description

Specifies that the destination network obtains IP addresses using DHCP.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0800

Maximum Value: 0x0800

Requires Reboot: No

VPN/Local Certs

This section describes parameters that can be configured from the Local Certs page of the VPN tree.

localCertData

Description

Specifies the encoded local certificate contents.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

pkiAliasThirdCert

Description

Specifies the local certificate request name.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

localCertReqData

Description

Specifies the encoded certificate request contents.

Guidelines and Restrictions

Configuration Command:

Group Configurable:

Type:

Control Type:

Default Value:

Minimum Value:

Maximum Value:

Requires Reboot:

pkiPrefNameThirdCert

Description

Specifies the certificate name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 10

Requires Reboot: No

pkiValidThirdCert

Description

Specifies the verified certificate using a valid CA certificate.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

VPN/Summary

This section describes parameters that can be configured from the Summary page of the VPN tree.

firewallId

Description

Specifies the unique firewall identifier.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: String

Control Type: Text field

Default Value: (DefaultData)paramDefaultFirewallId

Minimum Value: 4

Maximum Value: 32

Requires Reboot: Yes

remoteUnit

Description

Specifies the remote unit serial number in interconnected mode.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecInSPI

Description

Specifies the incoming SPI

- 1 = IKE
- 2 = Certs
- 5 = 3rd party certs

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IntegerAsHex

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecOutSPI

Description

Specifies the outgoing SPI

- 1 = IKE
- 2 = Certs
- 5 = 3rd party certs

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: IntegerAsHex

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecAlgo

Description

Specifies the Encryption Method.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecName

Description

Specifies the SA name.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Hack

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 33

Requires Reboot: No

ipsecSaDisabled

Description

Disable this SA

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0x0100

Maximum Value: 0x0100

Requires Reboot: No

ipsecGwAddr

Description

Specifies the IPSec gateway address.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: No

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecBwMgmtPriority

Description

Specifies the VPN bandwidth priority.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Integer

Control Type: Text field

Default Value: 0

Minimum Value: 0

Maximum Value: 7

Requires Reboot: No

ipsecBwMgmtEnabled

Description

Enables VPN bandwidth management.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecBwMgmtGuaranteed

Description

Specifies the amount of bandwidth that will always be available to this SA. This bandwidth will be permanently assigned to this SA and not available to other SAs, regardless of the amount of bandwidth this SA does or does not use.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Float

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecBwMgmtMaximum

Description

Specifies the maximum amount of bandwidth that will be available to this SA.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: No

Type: Float

Control Type: Text field

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsecP1DHGrp

Description

Specifies the Phase 1 DH group.

- 0 = Group 1
- 1 = Group 2
- 2 = Group 5

Note: *Group 1 specifies a 768-bit Diffie-Hellman value, Group 2 specifies a more secure 1024-bit Diffie-Hellman value, and Group 5 specifies the currently most secure 1536-bit Diffie-Hellman value.*

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

ipsecAlgIdPh1

Description

Specifies the Phase 1 encryption/authentication algorithm:

- 0 = None
- 1 = DES & MD5
- 2 = DES & SHA1
- 3 = 3DES & MD5
- 4 = 3DES & SHA1

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 4

Requires Reboot: No

ipsecP2DHGrp

Description

Specifies the Phase 2 DH group.

Guidelines and Restrictions

Configuration Command: ADD_PARAM_NAMES

Group Configurable: Yes

Type: Special

Control Type: Special

Default Value: 0

Minimum Value: 0

Maximum Value: 2

Requires Reboot: No

ipsecEnable

Description

Enables VPN.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: Yes

nbt_vpnDisable

Description

Disables all VPN Windows Networking (NETBIOS) broadcasts.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 1

Minimum Value: None

Maximum Value: None

Requires Reboot: No

ipsec_allowPmtuIcmpInClear

Description

Enables fragmented packet handling.

Guidelines and Restrictions

Configuration Command: SET_PARAM_NAMES

Group Configurable: Yes

Type: Boolean

Control Type: Check box

Default Value: 0

Minimum Value: None

Maximum Value: None

Requires Reboot: No