ZyXEL

Firmware Release Note

ZyWALL 1050

Release 1.01(XL.1)

ZyXEL ZyWALL 1050

Release 1.01(XL.1)

Release Note

Date: Nov, 03, 2006

Supported Platforms:

ZyXEL ZyWALL 1050

Versions:

ZLD Version: 1.01(XL.1) | 11/03/2006
Bootbase: V1.08 | 05/05/2006

Read Me First

1. If user upgrades from 1.00(XL.1) or 1.01(XL.0) to this version, there is no need to restore to system default.

2. It is recommended that user backs up “startup-config.conf file” first before doing upgrade. The backup configuration file can be used later, if user wants to downgrade to an older firmware version or to archive the current configuration file.

3. The default device administration username is “admin”, password is “1234”.

4. The default LAN interface is ge1, which is located on the most left side. The default LAN subnet is 192.168.1.0/24.

5. By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.

6. The default WAN interface is ge2, and the secondary WAN interface is ge3. These two interfaces will automatically get IP address using DHCP by default.

7. User can upgrade this firmware by using GUI or ftp client.

8. The default NTP time server address is changed to “0.pool.ntp.org” starting from this release.

9. For more details of the feature enhancement list of this release, please refer to Appendix 2 through 6 of this document.

Known Issues:

System:

1. [SPR: 060208177]
   [Symptom] In some occasions, Outlook Express might be terminated if both ZW1050 force authentication and https force redirect features are enabled and access user does not login to ZyWALL first.
   [Work around] The access user must be authenticated first
2. [SPR: 060710491]
   [Symptom] When user configures PPTP interfaces as WAN interface and high volume traffic going through the interface, the CPU usage might stay high.
3. [SPR: 060831779]
   [Symptom] Long DNS domain zone forward will cause zysh daemon terminated.
   [Work around] Don't use DNS domain zone forward with more than 235 characters.
4. [SPR: 060831779]
   [Symptom] When user uses wizard to configure ZW1050 interface, wizard does not accept '\' as PPPoE password.
   [Work around] If user has to configure password with '\' character, please go to ZyWALL 1050 > Configuration > Network > ISP Account to configure the profile directly.
5. [SPR: 060830672]
   [Symptom] DNS Domain Zone and Domain Name don’t show warning message and constrain to input ”_” character.
   [Work around] Currently, ZyWALL 1050 doesn't support '_' in domain name field. Do not use '_' character in the domain name. Note that '_' character is also not a legal character in domain name.
6. [SPR: 060906284]
   [Symptom] GUI can not display log category “interface statistics” correctly.
   [Work around] Use CLI command to show “interface statistics” log category.

Certificate:

1. [SPR: 050523482]
   [Symptom] PKI does not interoperate with Windows CA server, when using SCEP.

Device HA:

1. [SPR: 060527709]
   [Symptom] In some occasions, backup device might fail to apply configuration after it synchronize configuration file from master device. However, the backup device might recover

itself in the next sync period.

2. [SPR: 060818195]
   [Symptom] When Auto Synchronize is enabled and a virtual server is created to map public IP to LAN side virtual server, PC from WAN side can't ping to LAN side virtual server, if master device is down.
3. [SPR: 060907317]
   [Symptom] When user configures IPSec VPN on master device and establishes tunnels with remote ZW1050 gateway, once master device goes down remote security gateway cannot dynamically rebuild tunnels with backup device.
   [Work around] Redial the tunnel again on remote ZW1050 gateway if master device goes down.

IPsec VPN:

1. [SPR: 051206484]
   [Symptom] ZW1050 does not support DNAT over IPSec with "Many one-to-one" case.
2. [SPR: 060703016]
   [Symptom] ZW1050 does not support domain zone forwarding within VPN tunnel.
3. [SPR: 060126368]
   [Symptom] VPN tunnel could not be established between ZW1050 and Fortinet products if IKE is configured as x-auth client or server.
4. [SPR: 060327208]
   [Symptom] VPN tunnel could not be established when 1) a non ZW1050 peer gateway reboot and 2) ZW1050 has a previous established Phase 1 with peer gateway, and the Phase 1 is not yet expired. Under those conditions, ZW1050 will continue to use the previous phase 1 SA to negotiate the Phase 2 SA. It would result in phase 2 negotiation to fail.
   [Work around] User could disable and re-enable phase 1 rule in ZW1050 or turn on DPD function to resolve problem.
5. [SPR: 060602172]
   [Symptom] IKE phase 1 certificate authentication would fail, if the key algorithms are different between initiator and responder. For example, initiator use RSA certificate and responder use DSA certificate.
   [Work around] Use same key algorithm in both initiator and responder.
6. [SPR: 060724520]
   [Symptom] When Device HA is turned on and Auto Synchronize is enabled, the backup device might create tunnel with peer gateway, if tunnel is configured with nail-up setting and peer gateway is configured to accept connection from any gateway IP address.

[Work around] Configure peer gateway to only accept connection from master device's gateway IP address.

7. [SPR: 060904101]

   [Symptom] ZW1050 might crash if using certificate as IKE authentication method.

8. [SPR: 060825495]

   [Symptom] When configuring IPSec VPN Authentication Method as Certificate user can't edit IP on Peer ID Type=IP.

   [Work around] User can use IPSec CLI to configure Peer ID value.

9. [SPR: 060908420]

   [Symptom] Use bridge interface to create tunnel with remote security gateway might cause device crash.

Firewall:

1. [SPR: 060821250]
   [Symptom] When adding a new member into a zone, intra-zone blocking for the newly added member will not work correctly.

Diagnostic Tools:

1. [SPR: 060823385]
   [Symptom] When user downloads a diagnostic report, the default downloaded filename would have extra square bracket. For example diaginfo-xxx[1].tar.bz2.

Interface:

1. [SPR: 060904116]
   [Symptom] When VLAN interface was disabled, there are many error logs (Connectivity Check) appear on log page.
   [Work around] Users could re-enable the VLAN interface and then disable it again to avoid the log messages from appearing.
2. [SPR: 060824406]
   [Symptom] If virtual server IP and virtual interface IP are on the same subnet, shutdown virtual interface will cause virtual server IP disappear.

Object:

1. [SPR: 060824416]
   [Symptom] Object Schedule "Recurring" can not be unchecked all of weekly days.
2. [SPR: 060829601]

[Symptom] When user creates a new Schedule object and edits it, there will be a warning message.

IDP:

1. [SPR: 060908395]

   [Symptom] IDP signature rule can not detect MS05-039 and MS06-040 attack.

2. [SPR: 060908396]

   [Symptom] IDP signature rule ID 8000773 and 8000759 can not correctly detect FTP user overflow attack.

Features:

Modifications in 1.01(XL.0)

First release.

Modifications in 1.01(XL.0)b1

1. [BUG FIX] 060703029

   Symptom:

   Voice sometimes can not pass through.

   Condition:

   Topology:

   P2002---(L) ZyWALL 70(W)---Server---(W) ZyWALL 1050(L)---P2302

   1. SIP Server is “VOCAL v1.50” and IP is 192.168.14.
   2. ZW1050 WAN is 192.168.14.100, ATA on LAN and IP is 192.168.123.28
   3. ZW70 WAN is 192.168.14.108.
   4. SIP data can not pass through from WAN to LAN via ZW1050.
   5. Attached files are sip package.

2. [BUG FIX] 060714812

   Symptom:

   Send log to server1 and server2 when log is daily. User can't receive log at correct time.

   Condition:

   1. Logs > Log Setting. modify system log
      - Fill in E-mail Server 1 necessary data. Sending Log daily/16:30.and enables E-mail Server 1.
      - Fill in E-mail Server 2 necessary data. Sending Log daily/16:30.and enables E-mail Server 2.
   2. User can't receive DUT log at 16:30, user receive log when log is full.

3. [Enhancement] VRPT 3.0 support

   Symptom:

   VRPT 3.0 supports, including IKE and traffic log.

4. [Enhancement] New Content filtering 60 Category support.

   Symptom:

   1. Content filter support new 60 categories.

5. [Enhancement] PPP username supports '#' character and character length up to 64.
   Symptom:
   ppp and aux support '#' character and character length to 64.

6. [Enhancement] Virtual server enhancement
   Symptom:
   1. The virtual server feature is to create NAT 1:1 mapping relationship between outside IP addresses and inside IP addresses. This enhancement eliminates the need to add virtual interface on incoming interface, when add virtual server.
   2. Increase maximum number of virtual server rule support from 32 to 1024.

7. [Enhancement] OpenSSH upgrade
   Symptom:
   Upgrade OpenSSH to version 4.3p2.

8. [Enhancement] Private mib support for CPU, Memory and VPN throughput.
   Symptom:
   Private mib supports CPU, MEM usage and VPN total throughput information in SNMP.

9. [Enhancement] Diagnostic Tool support
   Symptom:
   Add Diagnostic Information Collector to collect debug information.

10. [BUG FIX]
    Symptom:
    Solve the duplicate SA with the same policy when remote dial-in.
    Condition:
    N/A

11. [BUG FIX] 060707409
    Symptom:
    Compatible issue with P2000W or P2302
    Condition:
    Topology:

    (Proxy Server)
    |

P2000W--(LAN)zw1050A(WAN)----------(WAN)zw1050b--(LAN)—P2002.
Under this topology, when P2000W makes a call to P2002 can not heard any thing.
After sniffing the packet, it shows that the RTP traffic from P2000W to P2002 has destination IP with zw1050b LAN IP causing the traffic to be dropped.
However if we replace the P2002 with P2302, it works well. Perhaps this is a compatibility issue with P2000W or P2002.

12. [EXTERNAL][ENHANCEMENT]

Symptom:

Compatible with old ZyNOS ZyWALL firmware, which uses invalid vender ID.

Condition:

When zw1050 and old ZyNOS ZyWALL firmware negotiate to use DPD, ZyNOS use invalid vender ID of DPD, which is 14 bytes. If ZW1050 receives invalid vender ID of DPD, it will turn on the DPD.

13. [BUG FIX] 060713697

Symptom:

When create add two service objects and one service group into a group, GUI show error.

Condition:

1. Create a group with Object HTTP, Object HTTPS and Group SSH, and then save.
2. Go back and want to edit the group, now only Group SSH is there.

14. [BUG FIX] 060720304

Symptom:

NTP update packet will be matched by eDonkey signature.

Condition:

1. Enable App Patrol and reject eDonkey connection.
2. On LAN side PC, use NTP update agent to update PC local time.
3. We can find that the NTP update packet will be rejected by App Patrol due to coincidence with eDonkey signature.

15. [BUG FIX] 060726769

Symptom:

Use ftp to update custom signature will fail and no error log.

Condition:

1. Use GUI to export a custom signatures file.
2. Rename the file and use FTP to upload file to zw1050.

3. Import didn't work there was an error message that said to check the log. But log didn't appear to have anything about it.

16. [BUG FIX] 060719261

Symptom:

NTP update failed.

Condition:

Apply default configuration.

1. Use NTP to update system date.
   Go to System->Date/Time
2. Enable "Get from Time Server" and click "Synchronize Now".
3. Sometimes update process failed but there is no error displaying on GUI.
4. In Log, we can see that there is a log record "NTP update has failed."

17. [BUG FIX] 060720269

Symptom:

Install the same certificate into EMS and M110B, but the "Subject Name" of it is NOT the same.

Condition:

1. It happens when certificate is signed by CA.
2. One question: subject name in m70b is "CN=...." but in m110b is "...,CN=...", and z1050 is also the same with M110b.

18. [BUG FIX] 060718042

Symptom:

ping check display counter incorrectly

Condition:

Router(config)# show ping-check status
Interface Status Fail Count
==========
vlan0 Ok -9877
fail count should not be negative.

19. [BUG FIX] 060718041

Symptom:

While configuring in-use aaa object, the reference count could be reset to 0.

Condition:

1. By default configuration, the default aaa object is used by http service.

2. Configure default aaa object and show it again.
3. Since it is still used by http, the reference count should remain 1 but actually it has been reset to 0.

20. [BUG FIX] 060714823

Symptom:

Virtual server rules may not be deleted correctly and rename address object would cause virtual server rule applying failure

Condition:

1. Use the following script to reproduce the problem
   address-object SERVER_WAN_IP 61.1.1.1
   ip virtual-server test interface ge2 original-ip SERVER_WAN_IP map-to 192.168.4.2 map-type any
   address-object SERVER_WAN_IP 61.1.1.2
   ip virtual-server test interface ge2 original-ip 61.1.1.1 map-to 192.168.4.2 map-type port protocol tcp original-port 80 mapped-port 80

   There is only one virtual server rule but it appears two rules in internal ip tables

2. *address-object SERVER_WAN_IP 61.1.1.1*
   ip virtual-server test interface ge2 original-ip SERVER_WAN_IP map-to 192.168.4.2 map-type any
   address-object rename SERVER_WAN_IP abc

   After renaming the address object used by virtual server, it may cause virtual server applying failure at the next reboot

21. [BUG FIX] 060725661

Symptom:

IDP log exceeding 128 characters, VRPT can not parse log for getting information

Condition:

1. Trigger signature 3999. The log message will exceed 128 bytes, and severity information will not showing correctly.

<140>Jul 19 01:17:52 zw1050 src="192.168.1.34:1956" dst="172.25.5.1:445" msg="[type=Sig(3999)] NETBIOS SMB-DS umpnpmgr PNP_QueryResConfList unicode little endian attempt, Action: No Action, Severity: sever" note="ACCESS FORWARD" user="admin" devID="001349b4954d" cat="IDP" class="VirusWorm" act="No Action" sid=3999 ob="1" ob_mac="00111107C878".

22. [BUG FIX] 060227231

Symptom:

SPR 060105267 fails; the default certificate of Backup is deleted after sync.

Condition:

1. Verifying 060105267.
2. Add a self-signed cert in Master.
3. After sync, the default certificate in Backup disappears, but the added certificate exists in Backup.

23. [BUG FIX] 060705177

Symptom:

Packets cannot be dropped when matching PA rules under bridge scenario.

Condition:

1. Set a bridge br0 (ge4, ge5).
2. Client A is on ge5, server B is on ge5. We turn on the PA rules, log, drop packet.
3. Client A try to send packets to server B, in order to trigger some PA rule.
4. There will be logs, but packets are not dropped.

24. [EXTERNAL][ENHANCEMENT]

Symptom:

Support routing order change between policy routing and VPN dynamic rules.

Condition:

N/A

25. [EXTERNAL][ENHANCEMENT]

Symptom:

IKE rule swaps for ID in aggressive mode.

Condition:

Swap tunnel to the suitable one by the remote proposed ID.

26. [EXTERNAL][ENHANCEMENT]

Symptom:

When use VPN wizard, user can only select ge1~ge5 and aux interface for My Address.

Condition:

This minor enhancement removes this restriction from VPN wizard. User can select ge1~ge5, ppp, bridge, aux, vlan, and virtual interface as My Address, which is just like GUI's VPN gateway page configuration.

27. [BUG FIX] 060822318

Symptom:

Adding 1024 user objects to a user group would crash zyshd.

Condition:

1. Create 1024 user objects

   username harry0 nopassword user-type user
   username harry1 nopassword user-type user
   username harry2 nopassword user-type user
   ...
   username harry1022 nopassword user-type user
   username harry1023 nopassword user-type user

2. Join all the user objects to a user group

   groupname harrygroup
   user harry0
   user harry1
   user harry2
   ...
   ...
   user harry1023
   exit

   zyshd would crash at exit function

28. [BUG FIX] 060823343

Symptom:

Change VRRP interface on Backup device may cause Device HA Sync failed.

Condition:

1. Configuring A/P mode Device HA
2. Change VRRP interface on Bakcup
3. Perform Device HA Sync, but failed.

29. [BUG FIX] 060816985

Symptom:

Dial pptp may cause kernel crash.

Condition:

This problem can not always reproduce.

1. Import start-up-pptp-crash.conf.
2. Apply to ZW1050.
3. Run dial-pptp.zysh.
4. Then kernel crash.

30. [BUG FIX] 060823370

Symptom:

Virtual interface disappears after shutdown other virtual interface.

Condition:

1. set ge2:1 192.168.1.20
2. set ge2:2 192.168.1.21
3. set ge2:3 192.168.2.20
4. set ge2:4 192.168.2.21
5. shutdown ge2:1
6. no shutdown ge2:1
7. shutdown ge2:3
8. Use show interface all then see ge2:1 ip address is disappear

No. Name Status IP Address Mask IP Assignment

1 ge1 100M/Full 192.168.1.1 255.255.255.0 Static
2 ge2 Down 0.0.0.0 0.0.0.0 DHCP client
3 ge2:1 Down 0.0.0.0 0.0.0.0 Static
4 ge2:2 Down 1.1.1.21 255.255.255.0 Static
5 ge2:4 Down 1.1.2.21 255.255.255.0 Static
6 ge3 Down 0.0.0.0 0.0.0.0 DHCP client
7 ge4 Down 0.0.0.0 0.0.0.0 Static
8 ge5 Down 0.0.0.0 0.0.0.0 Static
9 aux Inactive 0.0.0.0 0.0.0.0 Dynamic

Appendix 1. Firmware downgrade procedure

The following is the firmware downgrade procedure:

1. If user has already backup the configuration file before firmware upgrade, please follow the procedures below:
    1. Use Console/Telnet /SSH to login into ZW1050.
    2. Router>**enable**
    3. Router#**configure terminal**
    4. Router(config)#**setenv-startup stop-on-error off**
    5. Router(config)#**write**
    6. Load the older firmware to ZW1050 using standard firmware upload procedure.
    7. After system uploads and boot-up successfully, login into ZW1050 via GUI.
    8. Go to GUI → "File Manager" menu, select the backup configuration filename, for example, statup-config-backup.conf and press "Apply" button.
    9. After several minutes, the system is successfully downgraded to older version.

2. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
    1. Use Console/Telnet /SSH to login into ZW1050.
    2. Router>**enable**
    3. Router#**configure terminal**
    4. Router(config)#**setenv-startup stop-on-error off**
    5. Router(config)#**write**
    6. Load the older firmware to ZW1050 using standard firmware upload procedure.
    7. After system upload and boot-up successfully, login into ZW1050 via Console/Telnet/SSH.
    8. Router>**enable**
    9. Router#**write**
    10. Now the system is successfully downgraded to older version.
        Note: ZW1050 might lose some configuration settings during this downgrade procedure. It is caused by configuration conflict between older and newer firmware version. If this situation happens, user needs to configure these settings again.

Appendix 2. Diagnostic Information Collector

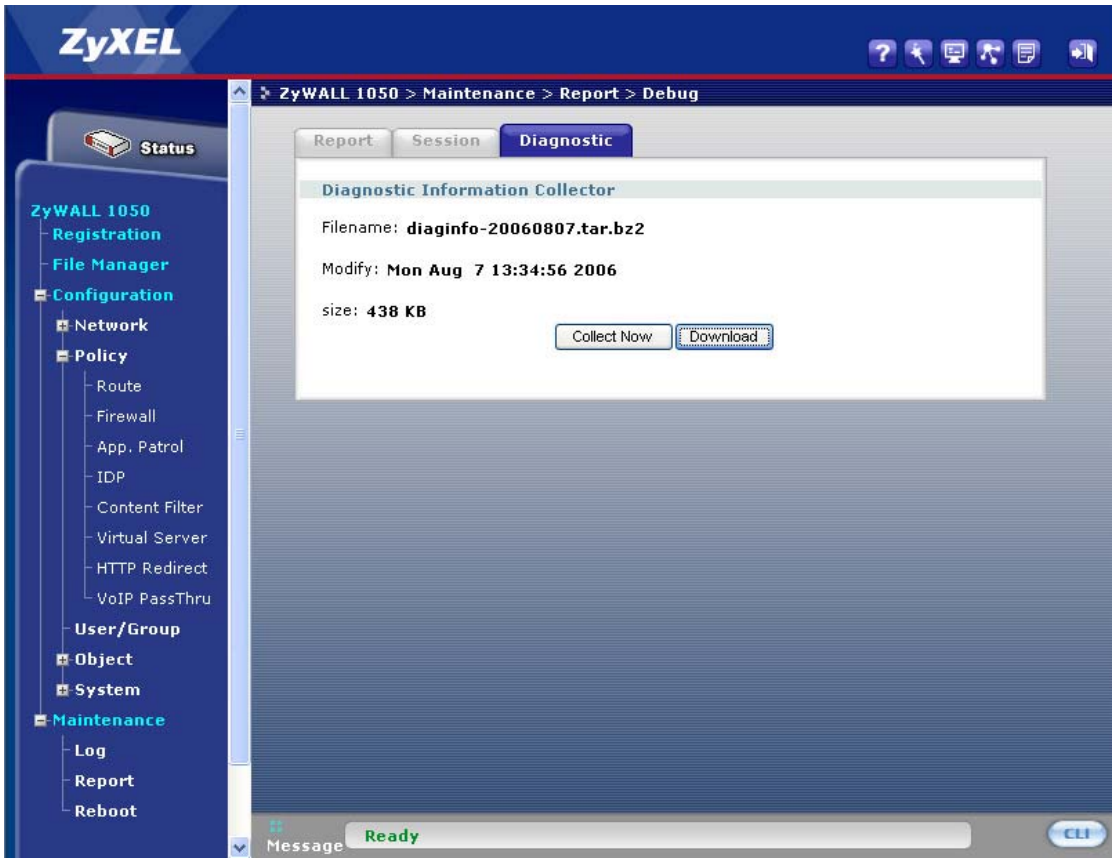
The Diagnostic Information Collector is designed to collect the configuration and diagnostic information on ZW1050. When the product is deployed in the field it is not so easy to gather all diagnostic information for developers to fix the problem at once, if a problem occurs and no matter what is the root cause of problem. Most of the time, fixing the problem depends on the skills of the engineer who is responsible for that device and configuration. He/she must have the ability to gather crucial information to figure out the root cause; furthermore, if that problem is a feature defect, the field engineer is always instructed to gather all other information for the develop engineer. However, not all companies have a job position dedicated for the network device and the network configuration. Sometimes the field engineer does not know that they put invalid configurations on the equipments and experiences difficulty on troubleshooting. The Diagnostic Information Collector is designed to avoid these situations.

The purpose of Diagnostic Information Collector's to use a very simple command and GUI that can help the field engineers get the diagnostic information for problem solving. It is designed very easy; even an office employee can gather the diagnostic information and send it to others. For example, on the web configuration interface, it does not need complicate setup steps to activate this feature, only a simple click and download it.

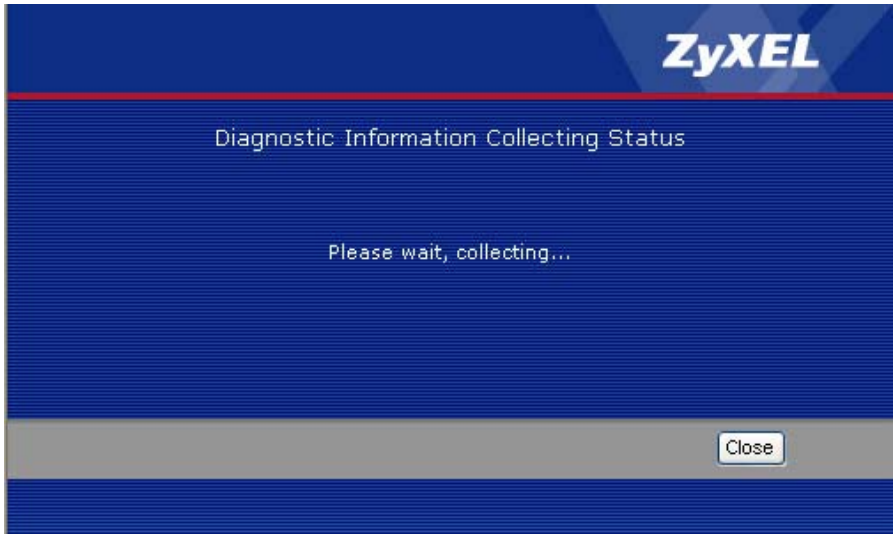
The Diagnostic Information Collector will generate a package contains all diagnostic information. It contains the configurations, system status information and hardware status. By analyzing the diagnostic information, it can save a tremendous amount of turn around time on communication, and solve the problem in a short time. The Diagnostic Information Collector is indeed a tool to gather information for problem solving.

How to use it

Collect information CLI command:
Router > diag-info collect
GUI: the page is located in **Maintenance > Report > Diagnostic**
Click "Collect Now" button will activate the function to collect.



After the “Collect Now” is clicked, a new collection window will pop up. This window indicates the status of the collection, and during its operation, you can feel free to switch between different configuration pages.



Show collected package file information CLI command:

Router > show diag-info

Filename : diaginfo-20060803.tar.bz2

File size : 1026 KB

Date : 2006-08-04 06:52:51

When using the CLI command to collect information, once it is done, the package file is available on **FTP, /debug directory.** If using the web interface, once the action is done, the package can be downloaded from the web interface.

Appendix 3. SNMPv2 private MIBS support

SNMPv2 private MIBs provides user to monitor ZW1050 platform status. If user wants to use this feature, you must prepare the following step:

1. Have zw1050 mib files (zywall.mib and zyxel-zywall-ZLD-Common.mib) and install to your MIBs application (like MIB-browser). You can see zywallZLDCommon (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZW1050 SNMP is enabled.
3. Using your MIBs application connects to ZW1050.
4. SNMPv2 private MIBs support three kinds of status in ZW1050:
   (A) CPU usage: Device CPU loading (%)
   (B) Memery usage: Device RAM usage (%)
   (C) VPNIpsecTotalThroughput: The VPN total throughput (Bytes/s), Total means all packets(Tx + Rx) through VPN.

Appendix 4. Virtual Server Enhancement

The virtual server feature is to create NAT mapping relationship between outside IP addresses and inside IP addresses. The conventional way of using this feature consists of four steps of action:

1. Create a virtual server map setting which uses that just created virtual interface.
2. Create a virtual interface on a designated interface if the virtual server traffic needs ARP reply in order to route the traffic to correct interface.
3. Create firewall rule to allow virtual server traffic.
4. Create policy route if virtual server needs to establish connection to clients.

The limitation of previous design is that each interface can create maximum of 4 virtual interfaces. Therefore, if customer needs to create more than 4 virtual servers in an interface, it can't be done.

The revised virtual server feature will take care about the virtual interface setting for the user, it is no longer need to create a virtual interface on a designated interface; the virtual server has the ability to handle the configuration itself internally without operator's care.

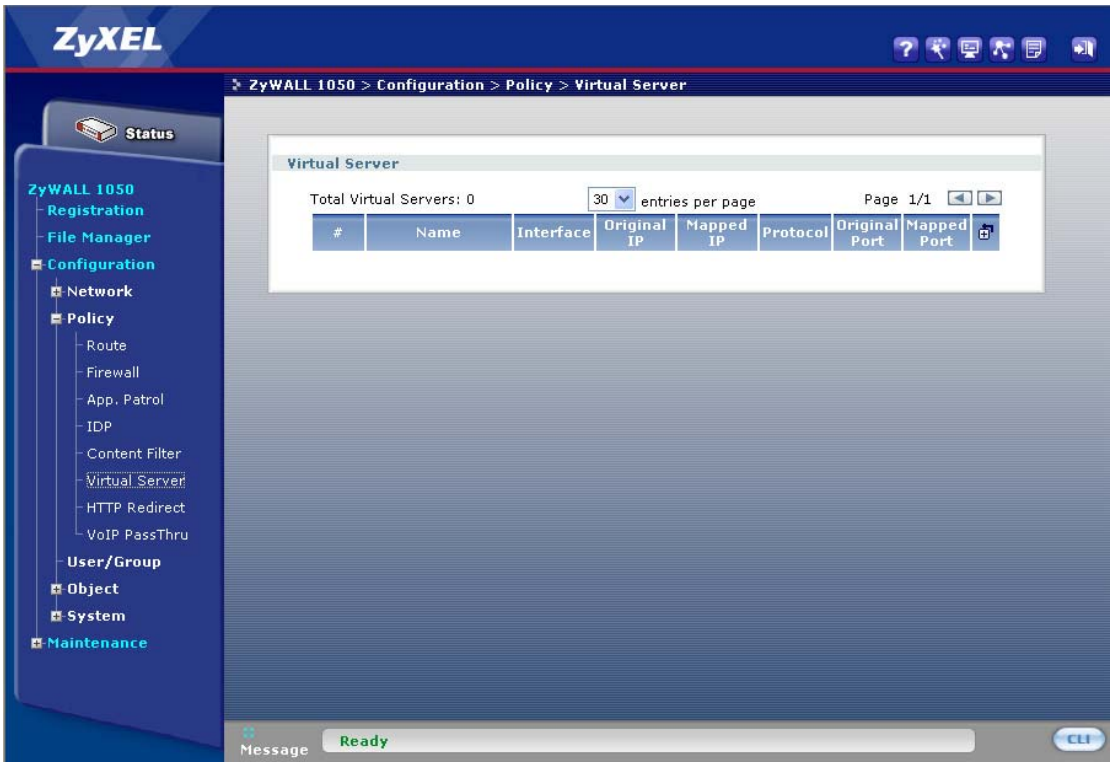
Major change

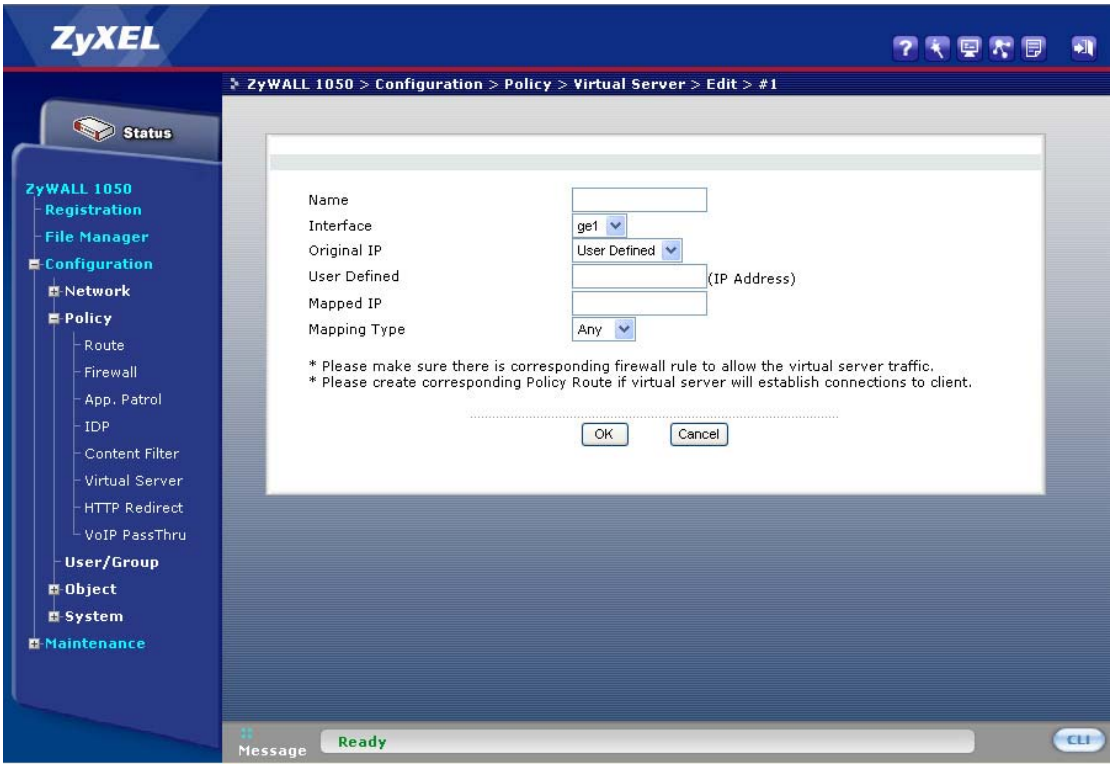
1. User no longer needs to create a virtual interface when creating virtual server.
2. Original IP Netmask needs to be supported in virtual server setting since it needs to create a corresponding virtual interface. This setting is an optional setting and only supported in CLI command. If user does not specify it, the default Netmask is 255.255.255.255. GUI configuration will use default Netmask.
3. Increase maximum Virtual Server rule support from 32 to 1024.

How to use it

On GUI:

1. Click Policy > Virtual Server
2. Click new entry icon to create a new virtual server setting.





In CLI configuration, the following two examples of commands is supported:

Router(config)# ip virtual-server VR1 interface ge2 original-ip any map-to 192.168.3.2 map-type any

Router(config)# show ip virtual-server

virtual server: VR1
  active: yes
  interface: ge2
  original IP: any, netmask 255.255.255.255 mapped IP: 192.168.3.2
  mapping type: any, protocol type: any
  original start port: none, original end port: none
  mapped start port: none, mapped end port: none

Router(config)# ip virtual-server VR1 interface ge2 original-ip 1.1.1.1 netmask 255.255.255.0 map-to 192.168.3.2 map-type any

Router(config)# show ip virtual-server

virtual server: VR1
  active: yes
  interface: ge2
  original IP: 1.1.1.1, netmask 255.255.255.0 mapped IP: 192.168.3.2
  mapping type: any, protocol type: any
  original start port: none, original end port: none
  mapped start port: none, mapped end port: none

Appendix 5. Content Filter Support 60 Categories

Introduction

Content Filter is a function to help administrators manage or control the accesses of web browsing. It could classify websites into 52 categories which provide administrators a convenient and efficient way to block unwanted web materials for internal users. With evolution and diversity of the web contents nowadays, original web categories may not be able to meet the needs to classify and block websites accurately. That is why 60 categories support is introduced. With this support, administrators are allowed to perform even more fine-grained control over websites which provide better internal users browsing experiences. Note that it is possible that an URL could be classified into more than 1 category in new design. If either one category is matched in a filtering profile, the web access is blocked.

Category Modifications

In new design, some categories are divided into several categories to provide fine-grained control while some are obsolete. There are also newly-added or renamed categories. Here comes the table to summarize the change.

New category	Old category	Note
"Adult/Mature Content"	"Adult/Mature Content"	
"Pornography"	"Pornography"	
"Sex Education"	"Sex Education"	
"Intimate Apparel/Swimsuit"	"Intimate Apparel/Swimsuit"	
"Nudity"	"Nudity"	
"Alcohol/Tobacco"	"Alcohol/Tobacco"	
"Illegal/Questionable"	"Illegal/Questionable"	
"Gambling"	"Gambling"	
"Violence/Hate/Racism"	"Violence/Hate/Racism"	
"Weapons"	"Weapons"	
"Abortion"	"Abortion"	
"Hacking"		New category
"Phishing"		New category
"Arts/Entertainment"	"Arts/Entertainment"	
"Business/Economy"	"Business/Economy"	
"Alternative Spirituality/Occult"	"Cult/Occult"	Rename
"Illegal Drugs"	"Illegal Drugs"	
"Education"	"Education"	
"Cultural/Charitable Organization"	"Cultural Institutions"	Rename
"Financial Services"	"Financial Services"	
"Brokerage/Trading"	"Brokerage/Trading"	
"Online Games"	"Games"	Rename
"Government/Legal"	"Government/Legal"	
"Military"	"Military"	
"Political/Activist Groups"	"Political/Activist Groups"	
"Health"	"Health"	
"Computers/Internet"	"Computers/Internet"	
	"Hacking/Proxy Avoidance"	Obsolete but if the old category is selected, convert it to "Hacking" and "Proxy Avoidance"

"Search Engines/Portals"	"Search Engines/Portals"	
	"Web Communications"	Obsolete
"Spyware/Malware Sources"		New category
"Spyware Effects/Privacy Concerns"		New category
"Job Search/Careers"	"Job Search/Careers"	
"News/Media"	"News/Media"	
"Personals/Dating"	"Personals/Dating"	
"Reference"	"Reference"	
"Open Image/Media Search"		New category
"Chat/Instant Messaging"	"Chat/Instant Messaging"	
"Email"	"Email"	
"Blogs/Newsgroups"	"Newsgroups"	Rename
"Religion"	"Religion"	
"Social Networking"		New category
"Online Storage"		New category
"Remote Access Tools"		New category
"Shopping"	"Shopping"	
"Auctions"	"Auctions"	
"Real Estate"	"Real Estate"	
"Society/Lifestyle"	"Society/Lifestyle"	Rename
"Sexuality/Alternative Lifestyles"	"Gay/Lesbian"	Rename
"Restaurants/Dining/Food"	"Restaurants/Dining/Food"	
"Sports/Recreation/Hobbies"	"Sports/Recreation/Hobbies"	
"Travel"	"Travel"	
"Vehicles"	"Vehicles"	
"Humor/Jokes"	"Humor/Jokes"	
	"Streaming Media/MP3"	Obsolete but if the old category is selected convert it to "Peer-to-Peer" and "Streaming Media/MP3s"
"Software Downloads"	"Software Downloads"	
"Pay to Surf"	"Pay to Surf"	
"Peer-to-Peer"		New category
"Streaming Media/MP3s"		New category
"Proxy Avoidance"		New category
"For Kids"	"For Kids"	
"Web Advertisements"	"Web Advertisements"	
"Web Hosting"	"Web Hosting"	

CLI Modifications

```
CATEGORY_NUMBER =
  <0..51>
CATEGORY_SET =
  {adult-mature-content| pornography| sexeducation| intimate-apparel-swimsuit| nudity|
  alcohol-tobacco| illegal-questionable| gambling| violence-hate-racism| weapons|
  abortion| hacking| phishing| arts-entertainment| business-economy| alternative-
  spirituality-occult| illegal-drugs| education| cultural-charitable-organization|
  financial-services| brokerage-trading| online-games| government-legal| military|
  political-activist-groups| health| computers-internet| search-engines-portals|
  spyware-malware-sources| spyware-effects-privacy-concerns| job-search-careers| news-
  media| personals-dating| reference| open-image-media-search| chat-instant-messaging|
  email| blogs-newsgroups| religion| social-networking| online-storage| remote-access-
  tools| shopping| auctions| real-estate| society-lifestyle| sexuality-alternative-
  lifestyles| restaurants-dining-food| sports-recreation-hobbies| travel| vehicles|
  humor-jokes| software-downloads| pay-to-surf| peer-to-peer| streaming-media-mp3s|
  proxy-avoidance| for-kids| web-advertisements| web-hosting}
BACKWARD_COMPATIBLE_CATEGORY_SET =
  {cult-occult| cultural-institutions| games| hacking-proxy-avoidance| web-
  communications| newsgroups| gay-lesbian| streaming-media-mp3}
```

The following CLI commands have been obsolete:

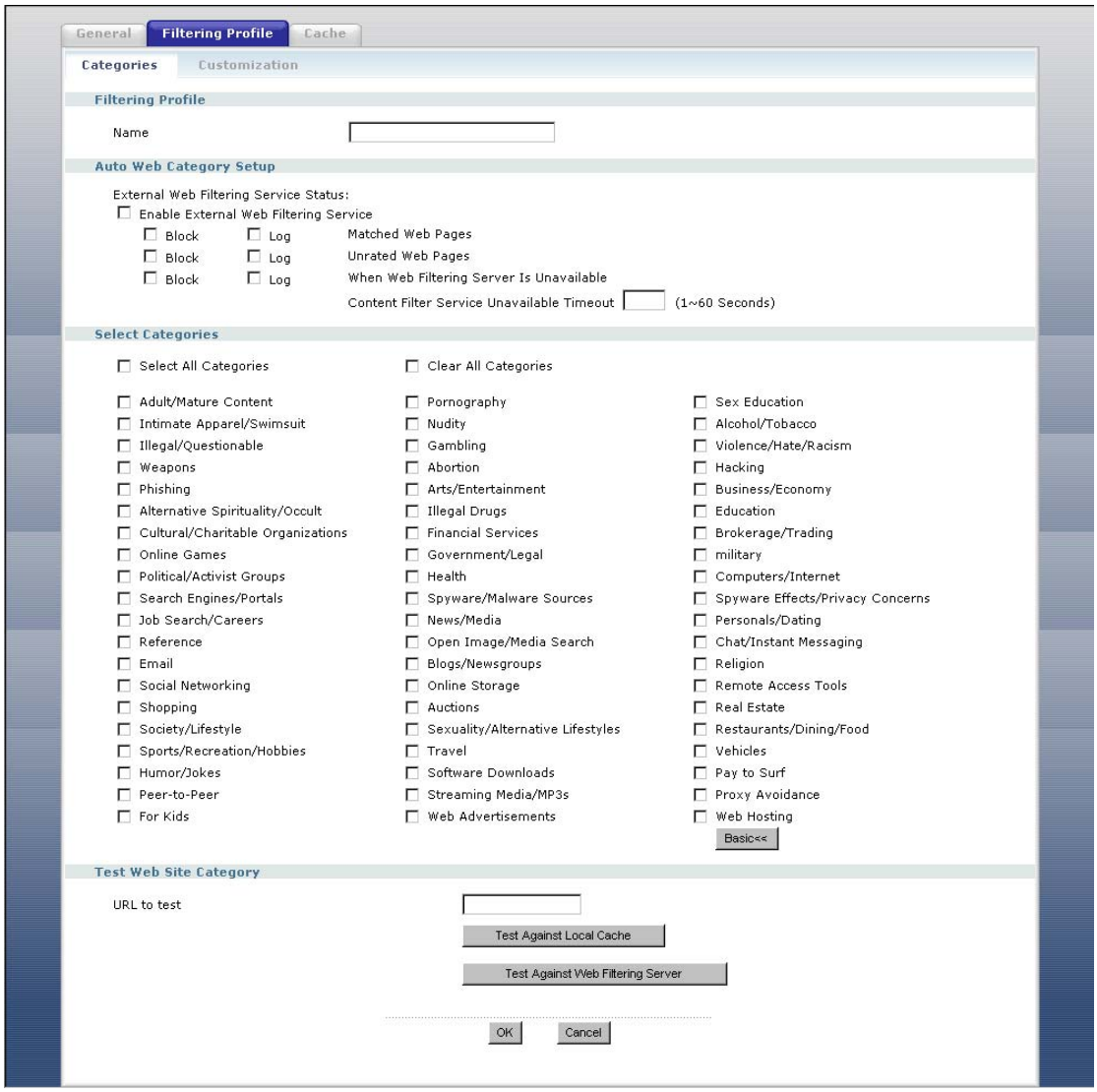
[no] content filter *CF_PROFILE* url category *CATEGORY_NUMBER*

no content filter *CF_PROFILE* url category *BACKWARD_COMPATIBLE_CATEGORY_SET*

The following CLI commands are used to configure category set for a profile:

[no] content filter *CF_PROFILE* url category {*CATEGORY_SET* | *BACKWARD_COMPATIBLE_CATEGORY_SET}*

New GUI Page (Content Filter->Filtering Profile->Categories)



Note

1. To provide backward compatibility, all obsolete CLI commands are allowed but ZyWALL 1050 would give warnings and try to convert it to new category.
2. For those who use older firmware, they may experience incorrect website classification which leads to fail to block/forward certain websites. It is strongly recommended that use firmware newer than 1.01(XL.0).

Appendix 6. VRPT 3.0 Support

VRPT standing for Vantage Report is used to collect logs generated by device and provide a clear and comprehensive report instead of viewing massive logs. In VRPT 3.0, ZyWALL supports the interface statistics, more detailed traffic log, and IKE logs.

Interface statistics provides the detailed information like, interface status, Rx packets, Tx packets, collisions, rx byte/s, tx byte/s, and up time. Now the supporting interfaces of this function include the physical ports, Ethernet interface, VLAN interfaces and PPP interfaces. To show interface statistics in enable mode and configure mode, the command syntax is like this:

show { ETH_IFACE | PPP_IFACE | VLAN_IFACE | Port } status

Argument	Description	Valid Value	Default Value
ETH_IFACE	The name of thernet interface	ge[1-5]	N/A
PPP_IFACE	The name of ppp interface	ppp[0-11]	N/A
VLAN_IFACE	The name of vlan interface	vlan[0-31]	N/A
Port	Physical port	1-5	N/A

Users can use adjust the interval (seconds) to send statistic logs. To configure the send log internal timer in configure mode, the command syntax is like this:

interface send statistics interval <15..3600>

show interface send statistics internal

User can disable the interface-statistics in syslog category to stop sending logs to remote server. For example:

Router(config)# logging syslog 1 category interface-statistics disable

There are two enhancements of VRPT 3.0 in traffic logs. One is the extension of direction field. The other is the expected connection which uses the same proto name as the one its parents used. The direction in VRPT 3.0 supports the tunnel name of IPsec VPN. The traffic connection may come from some IPsec tunnels, or come from some tunnels and go to some tunnels in VPN concentrator case. For example, the connection is from interface to tunnel, the direction field will be like this:

dir="ge1:tunnel/VPN_CONN:0x2958a81f"

“ge1” means the interface name and “tunnel/VPN_CONN:0x2958a81f” means the tunnel name is VPN_CONN, and its SPI is 0x2958a81f. This enhancement for direction field provides more precise information, such as the tunnel name and SPI to indicate which IPsec SA is used to encrypt or decrypt the VPN traffic.

Another enhancement for traffic log is the expected connection will use the same proto name as the one its parent use. For example, the FTP can be thought as signal connection and data

connection. However both connections belong to the FTP. But in original design, the data connection will be thought as “others” in proto name because the destination port number may be 21. Original design may cause incorrect traffic statistic for FTP connections.

There are some log changes for IKE in VRPT 3.0. The target of these modifications is to provide more correct information to indicate which IPsec SA or IKE has caused the events. Another log changes are to identify if the VPN tunnel is for site-to-site or remote access, and to provide the xauth user name when VPN tunnel is built or re-key successfully.

User can enable the IKE logs in log category by the following CLI command.

Router(config)# logging system-log category ike level normal

or

Router(config)# logging syslog 1 category ike level normal

User can disable the IKE logs in log category using following CLI command.

Router(config)# logging system-log category ike disable

or

Router(config)# logging syslog 1 category ike disable