ZyXEL

ZyXEL

Firmware Release Note

ZyWALL 1050

Release 1.01(XL.2)

Date: Nov 21, 2006

Author: Edward Lu

Project Leader: Andrew Chu

ZyXEL ZyWALL 1050

Release 1.01(XL.2)

Release Note

Date: Nov 21, 2006

Supported Platforms:

ZyXEL ZyWALL 1050

Versions:

ZLD Version: 1.01(XL.2) | 11/21/2006
Bootbase: V1.08 | 05/05/2006

Read Me First

1. If user upgrades from 1.01(XL.0) or 1.01(XL.1) 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.

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.

Policy Routing:

1. [SPR: 061115853]

    [Symptom] If user chooses spill-over algorithm in a trunk for load balancing, it is possible that traffic would go via a dead link when all available active interfaces are over-loaded.

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.

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.

ZyXEL Confidential

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.

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.

ZyXEL Confidential

Features:

Modifications in 1.01(XL.2) - 2006/11/21

Modify for formal release.

Modifications in 1.01(XL.2)b1 - 2006/11/10

1. [BUG FIX] 061011308
    Symptom:
       If configuring too long descriptions for Device HA rule,
       startup-config.conf can't be applied successfully when booting ZW1050.
    Condition:
       1. To edit a Device HA rule and enter longest description (60 characters).
       2. Reboot Zw1050.
       3. Console show: % (after
            12345655555555555555555555555555555555555555555): Parse   error
       4. Failed to apply startup-config.conf. ZW1050 reset itself to system default.

2. [BUG FIX] 061102131
    Symptom:
       ZyWALL1050 can not accept @ as part of the username. this will affect the Microsoft AD
       server authentication process. Most of the AD username will in the format like
       xxx@company.com. Thus, '@' is necessary for username.
    Condition:
       1. Switch to ZyWALL1050 User/Group configuration page.
       2. Add a new user name leo@zyxel.com.tw
       3. System can not accept this username format and return a warning message.

3. [BUG FIX] 061102083
    Symptom:
       After adding 1000 tunnels, remove them and then reboot zw1050, it may cause IPSec
       engine crash
    Condition:
       1. After adding a lot of tunnels, such as 1000 tunnels
       2. Reboot zw1050 and IPSec engine may crash
          The message is as below
          Kernel panic: ../../../ipsec/quicksec/engine/engine_rules.c:259
          SshEngineRules ssh_engine_delete_rule Assertion failed:
          In interrupt handler - not syncing

4. [BUG FIX] 061018604
    Symptom:
       IPSec tunnel cannot accept packet size $>$ 2020 bytes
    Condition:
       PC1 - zw70 $<-->$ zw1050 - PC2
       1. ZW1050 builds a tunnel with zw70

2. PC2 try to ping PC1, packet size $>$ 2020, such as in Linux, ping x.x.x.x -s 2021
the packet cannot enter IPSec Engine, and no logs for dropping.

5. [BUG FIX] 061017483
    Symptom:
        IPsec Pre-share key cannot accept special characters
    Condition:
        Set preshare key = ",;|`~!@#$%^&*()_+\{}':./<>=-." and try the following scenarios.
            zw1050 <> zw1050 => pass
            zw1050 <> zw70/zw35 => failed
            zw1050 <> softremote => failed

6. [BUG FIX] 061020668
    Symptom:
        Xauth client password cannot accept special characters
    Condition:
        When building a IPsec tunnel, if we set the phase 1 Xauth client password to
        ",;|`~!@#$%^&*()_+\{}':./<>=-." , authentication would fail (then XML cannot accept the
        special characters, such as $<>$).

7. [BUG FIX] 061024855
    Symptom:
        kernal panic
    Condition:
        [topology]:
            Caller (LAN) callee(WAN) signal port: user defined(ex:5060 or 5678)
            LAN-ge1, WAN(192.168.105subnet)-ge2, LAN-ge3, no firewall, no
            content-filter
        [tooles]: X-lite
        [steps]:
            When caller calls callee, callee receives ringing and then callee picks
            up phone, kernel panic occurs in the end

8. [BUG FIX] 061103207
    Symptom:
        Failed on deleting one Auth.Method (if configuring too long method name)
    Condition:
        1. Create one Auth.Method with method list of ldap, local and radius
        2. Delete the Auth.Method
        3. Following message appears
            Error: [-24009], Delete AAA method has failed.

9. [Enhancement]
    Description:
        Support configuring gateway that is not in the same subnet as the interface IP. With this
        enhancement, PPPoA scenario is now supported.

Modifications in 1.01(XL.1)b2 - 2006/11/3

1. [BUG FIX] 061016458

    Symptom:

    Crashed as being MIS gateway

    Condition:

    1. After upgrading firmware to MIS gateway, it may crash in several hours or days.

    2. It is hard to re-produce it in LAB.

Modifications in 1.01(XL.1)b1 – 2006/10/11

1. [BUG FIX] 060830674

    Symptom:

    Long DNS Domain Zone will cause DUT "zysh daemon is terminated".

    Condition:

    1. System ＞ DNS，add a Name Server Record rule, input Domain Zone with

    long characters (＞=235 character) and save it.

    2. Console will show zysh daemon is terminated:

    zysh daemon is terminated at Wed Aug 30 15:47:33 2006

    by signal: Segmentation fault

    last command function: 0x80ace50

2. [BUG FIX] 060831779

    Symptom:

    ZW1050 does not accept \ in PPPoE password.

    Condition:

    1. Use wizard to setup one ISP pppoe interface.

    2. Password key in 12345673\. Device does not accept this password.

3. [BUG FIX] 060830672

    Symptom:

    DNS Domain Zone and Domain Name have not shown warning message and
    restrict to input "_" character.

    Condition:

    1. System ＞ DNS，Domain Zone or Domain Name field input "aaa_bbb.ccc.eee"
       and save it.

    3. GUI will not load any dns record.

4. [BUG FIX] 060906284

    Symptom:

    GUI can not display log category "interface statistics" correctly.

    Condition:

    1. Maintenance ＞ Log page

    2. Select Display field to "interface Statistics"

    3. The Display field only shows "Debug Log"

5. [BUG FIX] 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.

Condition:
1. On device ha scenario, create one virtual server entry.
2. Ping from WAN side to global IP on master device.
3. You can see the ping reply from master's LAN PC
4. Turn off master device
5. The WAN's PC can't get ping response.
6. The reason is slave device don't send gratuitous ARP for global IP. So the WAN's side PC always send ping to master's WAN MAC.
7. Suggest keepalived send all IP's gratuitous ARP including alias IP.

6. [BUG FIX] 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.

   Condition:
   ---ZW1050(master)---+L3 switch-----------Remote ZW1050
   ---ZW1050(slave)-----|
   1. ZW1050（master）LAN IP = 192.168.1.1，WAN1 IP = 10.0.0.1
   2. ZW1050（slave）LAN IP = 192.168.1.1，WAN1 IP = 10.0.0.1，VRRP manage IP on LAN = 192.168.1.2，VRRP manage IP on WAN1 = 10.0.0.2
   3. Create 1 dynamic rule for ZW1050（master），ZW1050（slave）
   4. Create 100 IPSec rules with one IKE for Remote ZW1050
   5. Initiate from Remote ZW1050 LAN side by Smartbit and the total traffic is 45Mbps.
   6. At beginning, the 100 IPSec tunnels were built between Master and Remote ZW1050.
   7. Power off ZW1050 (master), and the slave become master. After 8 minutes, the Remote ZW1050 sent DPD check to ZW1050 (slave) and the ZW1050 return ack to Remote ZW1050.
   8. The 100 IPsec tunnels can't be triggered again because remote zw1050 still keep 100 tunnels alive.
   9. After a night, the 100 IPSec tunnels still couldn't be rebuilt successfully.

7. [BUG FIX] 060904101
   Symptom:
   ZW1050 will crash if using CA for IKE but no certificate in Trust CA.
   Condition:
   ZW_A ＜＜ IPSEC ＞＞ ZW_B

   ZW_A Setting:
   IKE using Cer_A
   My Certificates: Cer_A
   Trusted Certificate: Cer_B

   ZW_B Setting:

IKE using Cer_B
My Certificates: Cer_B
Trusted Certificate: Cer_A

1. ZW_A initiates IPSEC Tunnel successfully.
2. ZW_A deletes Tunnel.
3. ZW_A deletes Trusted Certificate Cer_B.
4. ZW_A initiates IPSEC Tunnel again.
5. ZW_A crashes.

8. [BUG FIX] 060825495
   Symptom:
   When configuring IPSec VPN Authentication Method as Certificate user can't edit
   IP on Peer ID Type=IP.
   Condition:
   1. Add a certificate called DUT1_IP.
   2. Create a VPN Gateway; Edit Certificate=DUT1_IP, and Peer ID Type become to
      IP automatically but can't edit Content field.
   3. Change Peer ID Type to any and to IP again, and then can edit Content field.

9. [BUG FIX] 060908420
   Symptom:
   Use bridge interface to create tunnel with remote security gateway might cause
   device crash.
   Condition:
   PC1(ftp-client)----(ge5)DUT1(br0)---PQA_Lab---(ge2)DUT2(ge1)----PC2(ftp-server)
   1. DUT1:ge4 and ge5 are bridged to br0.
   2. DUT2: All interfaces are default settings.
   3. Establish a vpn tunnel from br0 to ge2, and then built-up successfully.
   4. PC1 ftp to PC2 and uploaded data to PC2.
   5. After uploading data, DUT1 had kernel panic.

10. [BUG FIX] 060821250
    Symptom:
    Intra-zone blocking works incorrectly if destination is tunnel.
    Condition:
    Intra-zone blocking works incorrectly if destination is VPN tunnel.

11. [BUG FIX] 060824406
    Symptom:
    If virtual server IP and virtual interface IP are on the same subnet, shutdown virtual
    interface will cause virtual server IP disappear.
    Condition:
    1. Set 1.1.1.1/24 in virtual interface
    2. Set 1.1.1.2/24 in virtual server
    3. Shutdown 1.1.1.1 virtual interface
    4. The virtual server interface in the same subnet disappears too.

12. [BUG FIX] 060824416
    Symptom:

Object Schedule "Recurring" can not be unchecked all of weekly days.

Condition:

1."Object Schedule Recurring" dis-check all of Weekly Days and save it.

2. Weekly Days will be checked all.

13. [BUG FIX] 060829601

Symptom:

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

Condition:

1. Add One Time schedule rule, type Month is "8".

2. Edit this rule, Month is appeared "08", and then click "OK" will be show warning message.

14. [BUG FIX] 060908395

Symptom:

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

Condition:

1. IDP add a "all" profile and protect WAN, and then using MS05-039 attack tool to attacking WAN PC.

2. We can get WAN PC access control; IDP can not detect this attack just log as below:

[type=Sig(8004131)] SHELLCODE x86 NOOP, Action: No Action, Severity: medium [count=2]

3. Attached is ms05-039 traffic pcap file.

4. IDP can not detect MS06-040 too.

5. User needs to update signature to version1.130 to solve this problem.

15. [BUG FIX] 060920331

Symptom:

Kernel crashes when interface link down

Condition:

Use JP telecom topology

1. Un-Plug all interfaces of Master, let Slave become active

2. Wait for remote zw2+ to build new tunnel with slave

3. Plug all interfaces of Master, let Slave become backup.

Unplug the ge2 or ge3 of Slave, kernel oops happens and link_updown daemon is dead

16. [BUG FIX] 060831768

Symptom:

Virtual Server IP alias does not support Bridge, Vlan.

Condition:

1. Add vlan0 192.168.10.1

2. Add Virtual server interface vlan0 , ip 192.168.10.10

The IP 192.168.10.10 should be added as an IP alias of vlan0, but it is not added.

This Problem also happens on Bridge interface.

17. [BUG FIX] 060816981

Symptom:

ZyXEL Confidential

The IP alias still exists, even delete the virtual server.

Condition:

1. Create a virtual interface GE2:1 192.168.105.2
2. Create a virtual server, do dnat from 192.168.105.2 to 192.168.5.17 (User Defined: 192.168.105.2 Mapped IP: 192.168.5.17)
3. Delete virtual interface GE2:1, and delete the virtual server
4. The IP alias still exists.

18. [BUG FIX] 060817082

Symptom:

After backup synchronizes with master, backup should not add virtual server's ip alias.

Condition:

1. Add several virtual servers on master.
2. Backup synchronizes with master.
3. We can see that virtual server configuration is applied successfully on backup, but the ip alias of virtual servers should not be added on interface.

19. [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 Backup.
3. Perform Device HA Sync, but failed.

20. [BUG FIX] 060823370

Symptom:

Virtual interface disappear after shutdown other virtual interface.

Condition:

1. Set ge2:1 192.168.1.20
2. Set ge2:2 192.168.1.21
   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

21. [BUG FIX] 060823383

    Symptom:

        Intra-zone blocking does not work when add new interface into existing zone.

    Condition:

        1. Use system default configuration.

        2. Remove ge4 from DMZ zone.

        3. Add ge4 into WAN zone and enable intra-zone blocking of WAN zone.

        4. In bash, use the following command to show the firewall rules:

root@zw1050:/etc/zyxel# iptables -t zyfilter -nvL FORWARD |grep intra-zone

0   0 ZYFIRE   all -- eth2 eth2 0.0.0.0/0 0.0.0.0/0

ZYFIRE: cat firewall level notice cli_index=0 from ANY to ANY sevice others unlog mac unlog ob message intra-zone blocking on WAN REJECT

0   0 ZYFIRE   all -- eth2 eth1 0.0.0.0/0 0.0.0.0/0

ZYFIRE: cat firewall level notice cli_index=0 from ANY to ANY sevice others unlog mac unlog ob message intra-zone blocking on WAN REJECT

        5. You can observe that intra-zone blocking rule for ge4 and other interface does not successfully apply to iptables.

22. [BUG FIX] 060630052

    Symptom:

        Backup owns Master's IP when user configures Master's Device HA configuration.

    Condition:

        1. Configure Master and Backup to do Device HA

        2. Configure Master's Device HA configuration

        3. Backup will owns Master's IP several seconds

        4. This will cause Browser cannot get return data from ZySH after applying M aster's Device HA configuration

23. [BUG FIX] 060814841

    Symptom:

        SNMP IP-MIB::ipAdEntIfIndex has wrong mapping with IF-MIB.

    Condition:

        1. From beta tester brian.

        2. The IP indexes are wrong:

IP-MIB::ipAdEntIfIndex.10.10.10.254 = INTEGER: 10

IP-MIB::ipAdEntIfIndex.65.73.29.86 = INTEGER: 9

IP-MIB::ipAdEntIfIndex.69.62.141.251 = INTEGER: 8

IP-MIB::ipAdEntIfIndex.192.168.111.254 = INTEGER: 7

The correct indexes are::

IP-MIB::ipAdEntIfIndex.10.10.10.254 = INTEGER: 9

IP-MIB::ipAdEntIfIndex.65.73.29.86 = INTEGER: 8

IP-MIB::ipAdEntIfIndex.69.62.141.251 = INTEGER: 7

IP-MIB::ipAdEntIfIndex.192.168.111.254 = INTEGER: 6

These are correct:

IF-MIB::ifDescr.6 = STRING: eth0

IF-MIB::ifDescr.7 = STRING: eth1

IF-MIB::ifDescr.8 = STRING: eth2

IF-MIB::ifDescr.9 = STRING: eth3

IF-MIB::ifDescr.10 = STRING: eth4

These are correct:
IF-MIB::ifPhysAddress.6 = STRING: 0:13:49:6c:bb:cf
IF-MIB::ifPhysAddress.7 = STRING: 0:13:49:6c:bb:d0
IF-MIB::ifPhysAddress.8 = STRING: 0:13:49:6c:bb:d1
IF-MIB::ifPhysAddress.9 = STRING: 0:13:49:6c:bb:d2
IF-MIB::ifPhysAddress.10 = STRING: 0:13:49:6c:bb:d3

24. [EXTERNAL][ENHANCEMENT]
    Symptom:
         1. There is no user type information while display user profile
         2. Need to show user type while displaying user profile to improve the usability
    Condition:
         N/A

25. [EXTERNAL][ENHANCEMENT]
    Symptom:
         Support to configure DPD output idle timeout by CLI
    Condition:
         1. The VPN DPD detection is 8 minutes default. It is too long. The ZyNOS default
            is 120 sec and it can be configured.
         2. The ZW1050 can't be configured and default is 8 minutes. The DUT must wait 8
            minutes at most to know peer was dead. The time is too long.

26. [EXTERNAL][ENHANCEMENT]
    Symptom:
         Support logging with destination IP.
    Condition:
         Support user logging with destination IP, including every login and logout event
         log.

27. [BUG FIX] 061003100
    Symptom:
         Only one SA can be built-up when using remote dial-in VPN
    Condition:
         ZW1050 -- ZW70
         1. ZW1050 creates a remote dial-in VPN rule
         2. 70 creates three tunnels to dial
         3. The new connected tunnel will cause the previous tunnel disconnected.

28. [BUG FIX] 060828554
    Symptom:
         Help page of Wizard "Two ISP" error.
    Condition:
         1. Click Wizard, and select "INSTALLATION SETUP, TWO ISP".
         2. The Help page show "Step 2" for first page, it should be Step 1.
         3. Also, in step3 and step4, the help page still show "Step2"

29. [BUG FIX] 060928880

Symptom:

IDP cannot drop ICMP echo packet when adding a custom rule with ICMP type = 8

Condition:

1. Add a custom signature with ICMP type = 8
2. Add a NONE profile with enable the custom signature (enable, drop)
3. Bind the profile on WAN, and ping from LAN to WAN no packet will be dropped
4. If we add a custom signature with TCP dst port = 21, drop this rule can work.

Modifications in 1.01(XL.0)b1 – 2006/8/23

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 support 64 length and "#" character.

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 eliminate 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 latest version 4.3p2.

8. [Enhancement] Private mib support for CPU, Memory and VPN throughtput.
   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. [INTERNAL][ENHANCEMENT]
    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. [INTERNAL][ENHANCEMENT]
    Symptom:
    > 1. Enhance zyinet packet trace to support host/port filtering
    > 2. Provide CLI commands to set kernel console level
    > 3. Support dmesg clearing in debug command
    > 4. Displaying complete command line while using "debug system ps"
    > 5. Don't lookup name for ip address while displaying iptables rules
    Condition:
    > N/A

13. [INTERNAL][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.

14. [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.

15. [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.

16. [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.

17. [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."

18. [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.

19. [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.

20. [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.

21. [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

22. [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".

23. [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.

24. [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.

25. [INTERNAL][ENHANCEMENT]
    Symptom:
        Support routing order change between policy routing and VPN dynamic rules.
    Condition:
        N/A

26. [INTERNAL][ENHANCEMENT]
    Symptom:
        IKE rule swaps for ID in aggressive mode.
    Condition:
        Swap tunnel to the suitable one by the remote proposed ID.

27. [INTERNAL][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.

28. [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

29. [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.

30. [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.

31. [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

Modifications in 1.00(XL.1)b1 – 2006/7/7

1. [BUG FIX] 060109366
    Symptom:
        Firewall LAN to WAN rule display error
    Condition:
        1. Use GUI, add a Firewall Zone pair LAN to WAN, deny FTP service.
        2. Return to Firewall summary page, LAN to WAN rule will disappear.
        3. Check Global rule, there are two LAN to WAN rule exist.
        4. Attach Picture and Conf file.

2. [BUG FIX] 060411661
    Symptom:
        VPN, sometimes when we configure Phase1's parameters, the GUI showed "Error: [-1], Parse error/command not found!."
    Condition:
        1.An example is set Local ID type and Peer ID type.

3. [BUG FIX] 060530933
    Symptom:
        "Web page error" on Policy route page
    Condition:
        1. On GUI, Configuration > Policy > Route > Policy Route > Edit > #1 page, Incoming select Change button, Incoming=Tunnel and don't select any VPN tunnel click OK, click Change button again IE will show "Web page error"

4. [BUG FIX] 060609585
    Symptom:
        Can't change Connection ID from " S:" to blank.
    Condition:
        1. Interface > ISP Account, add one profile "ppp0" for PPTP account, and set the Connection ID to " S: ".
        2. Interface > ISP Account > Edit profile "ppp0", Change Connection ID from " S: " to blank, OK.
        3. Interface > ISP Account > Check profile "ppp0", the Connection ID is still " S: ".

5. [BUG FIX] 060609642
   Symptom:
      IDP"Packet Inspection" still detected attack traffic, even if DUT not registration or
      IDP not licensed.
   Condition:
      1.Do not registration DUT and IDP has not licensed.
      2.Edit eWC/IDP/General, enable IDP, select a "all" profile to match WAN
      Zone, "Activation", and then "Apply", GUI will be show message "IDP service is not
      registered. Packet Inspection feature will not be activated."
      3.Attack from LAN to WAN, IDP "Packet Inspection" still detected that attack traffic .

6. [BUG FIX] 060609661
   Symptom:
      DUT will send RST packet when LAN visit webside
   Condition:
      1. DUT register to DB, Content Filter service had activated.
      2. Add a CF profile, select all Categories, Policies append this rule. Denied Access
      Message=Max. length, Redirect URL=https://192.168.1.1.
      3. LAN PC first visit webside (www.google.com) DUT will return RST packet.
      4. If webside had exist on Cache, it work fine.

7. [BUG FIX] 060609666
   Symptom:
      PC in LAN side can not get any IP from DUT after playing the role of PQA gateway for
      a while.
   Condition:
      PC in LAN side can not get any IP from DUT after playing the role of PQA gateway for
      a while.

8. [BUG FIX] 060612696
   Symptom:
      DHCP server can not enable when netmask=255.255.248.0
   Condition:
      DHCP server can not enable when netmask=255.255.248.0

9. [BUG FIX] 060613781
   Symptom:
      Configuration file name can not set maximum character
   Condition:
      1.Select a configuration file and click rename buttom
      2.Set Configuration file name is maximun character then click OK =>Fail ,browse will pop
      a "File Name is invaild filename" window

10. [BUG FIX] 060613790
   Symptom:
      IDP RST packet's source IP address should be Interface's IP address like ZyNOS.
   Condition:
      1. DUT sent out IDP RST packet with sender IP address (ex. 192.168.1.33) to receiver.
      2. The RST packets will be dropped if the receiver behind router or NAT firewall and then

they can't receive RST packets.
3. The ZyNOS will sent IDP RST packet with Interface IP address to avoid the issue.

11. [BUG FIX] 060614839
Symptom:
PC1 can not search Host of PC2 via VPN tunnel even "NetBIOS broadcast over IPSec" is enabled.
Condition:
PC1-------ZW1050_1=======ZW1050_2-----PC2
1. VPN had been estblished successfully.
2. PC1 can not search Host of PC2 via VPN tunnel even "NetBIOS broadcast over IPSec" is enabled.

12. [BUG FIX] 060619059
Symptom:
Sort's icon on wrong seat when click Log sort by source.
Condition:
1. Logs-> View Log, sort logs by source.
2. Logs-> View Log, Sort's icon displayed on Message's seat. It should be on Source's seat.
3. Attached picture for your reference.

13. [BUG FIX] 060622331
Symptom:
Backup ZW1050 can not switch LAN IP from management IP to physical IP after Master ZW1050 shut down.
Condition:
1. Master ZW1050 and Backup ZW1050 are doing Device HA with LAN and WAN VRRP groups.
2. Backup ZW1050 will automatically sync to Master ZW1050 every one minute.
3. Backup ZW1050 can not switch LAN IP from management IP to physical IP after Master ZW1050 shut down.
4. After shutting down Master ZW1050:
Backup:HA status of LAN is Active and HA status of WAN is Active
5. Backup ZW1050 can not switch LAN IP from management IP to physical IP.
6. After powering on Master ZW1050:
Backup:HA status of LAN is Active and HA status of WAN is Stand-By
7. Everything goes fine after VRRP group of WAN on Backup is disabled then enabled.

14. [BUG FIX] 060615930
Symptom:
Problem of OSPF virtual-link authentication and backbone area
Condition:
1. aera 0 authentication is none.
2. set virtual link authentication to Text or MD5
3. area 0 authentication will be changed to Text or MD5.

15. [BUG FIX] 060623557
Symptom:

CPU usage 100% when enable content filter and block cookie

Condition:

    1. Add a bridge interface members are ge1~ge5

    2. Connect ge2 to NAT router's LAN port

    3. Enable content filter and block cookie

    4. Go to www.kimo.com.tw from ge1 PC =>CPU usage will be100%

16. [BUG FIX] 060621262

   Symptom:

    dhcpd is dead if change ge2 metric.

   Condition:

    1. Change ge2's metric from 1 to 0 and apply.

    2. A PC from ge1 can't get IP address.

    3. Apply ge2 again, and dhcpd will live again. It can be duplicated easily.

17. [BUG FIX] 060613782

   Symptom:

    Admin can not log in system anymore after doing several VPN cases by changing Authentication Method and Extended Authentication.

   Condition:

    1. Admin can not log in system anymore after doing several VPN cases by changing Authentication Method and Extended Authentication.

18. [BUG FIX] 060613774

   Symptom:

    DDNS Profile Name length can only support 14

   Condition:

    1. In GUI, Configuration > Network > DDNS > Edit > #1 page, Profile Name length more than 14 will be cut.

    2. Ex: A234567890123456 will be cut to A2345678901234

19. [BUG FIX] 060608584

   Symptom:

    Kernel panic every times when setting manual VPN rule.

   Condition:

    1.Reset to default setting.

    2.Edit a manual VPN rule as the following: SPI=2345, Encryption Key=1111111111, Authentication key = 11111111111111111111, Local policy=LAN_SUBNET, Remote policy=LAN_SUBNET, My Address=1.1.1.1, Secure Gateway Address = 2.2.2.2, then OK.

    3.After pressing any item, DUT crashed.

20. [BUG FIX] 060613779

   Symptom:

    IKE cert + xauth problem cause QS xml parser failed

   Condition:

    1. VPN tunnel can be established with invalid peer ID if it used to do authentication by Certificate and Extended Authentication with any peer ID to establish tunnel successfully before.

    2. Attach configuration files in SPR system.

21. [BUG FIX] 060614837
   Symptom:
       No log while IKE search cert failed
   Condition:
       1. VPN tunnel can not be established in few hours if it authenticates by DNS certificate
       that signed from ZW1050 itself.
       2. Suggest to show logs to figure out what if Certificate is valid or not for VPN
       authentication.

22. [BUG FIX] 060622522
   Symptom:
       After reboot DUT, setting of Device HA will be changed.
   Condition:
       1. Device HA > VRRP GROUP, add a rule
       - Enable= enable; Name= ZW1050_GE1, VRID= 50; VRRP Interface=ge1; Role=Backup;
       Priority=50; Preempt= disable ; Manage IP= 192.168.1.2; Manage IP Subnet
       Mask= 255.255.255.0; Authentication=None.
       2. Reboot DUT.
       3. Device HA > VRRP GROUP, check Preempt = enable, it should be disable.

Modifications in 1.00(XL.0) – 2006/6/23

First release

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.
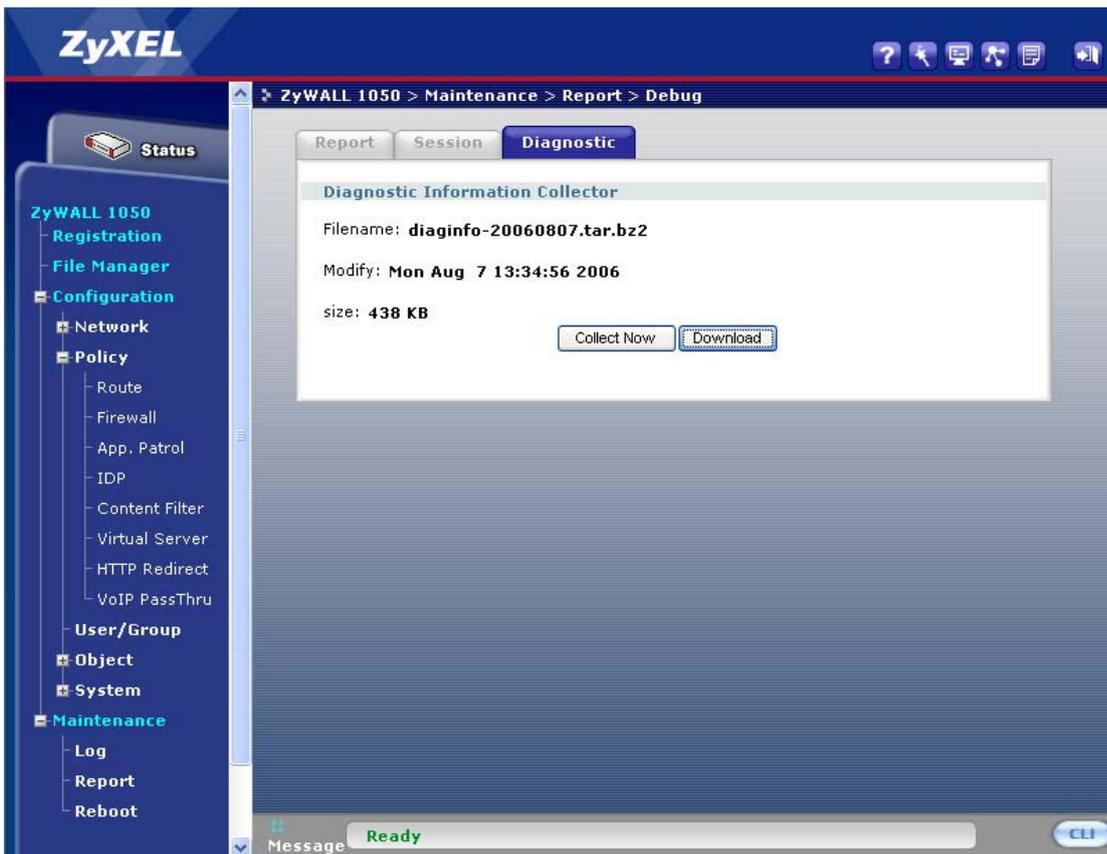
How to use it

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.
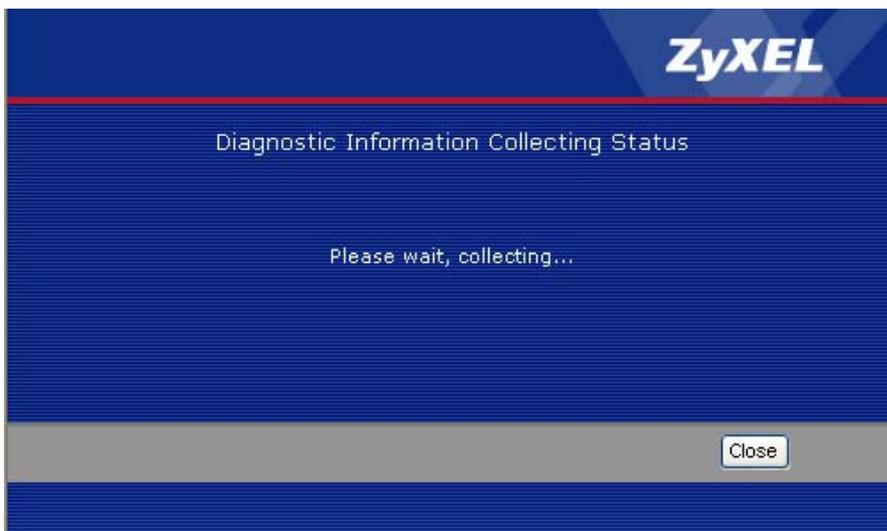
Show collected package file information CLI command:
Router > show diag-info
Filename : diaginfo-20060803.tar.bz2
File size : 1026 KB
Date   : 2006-08-04 06:52:51

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.

ZyXEL Confidential
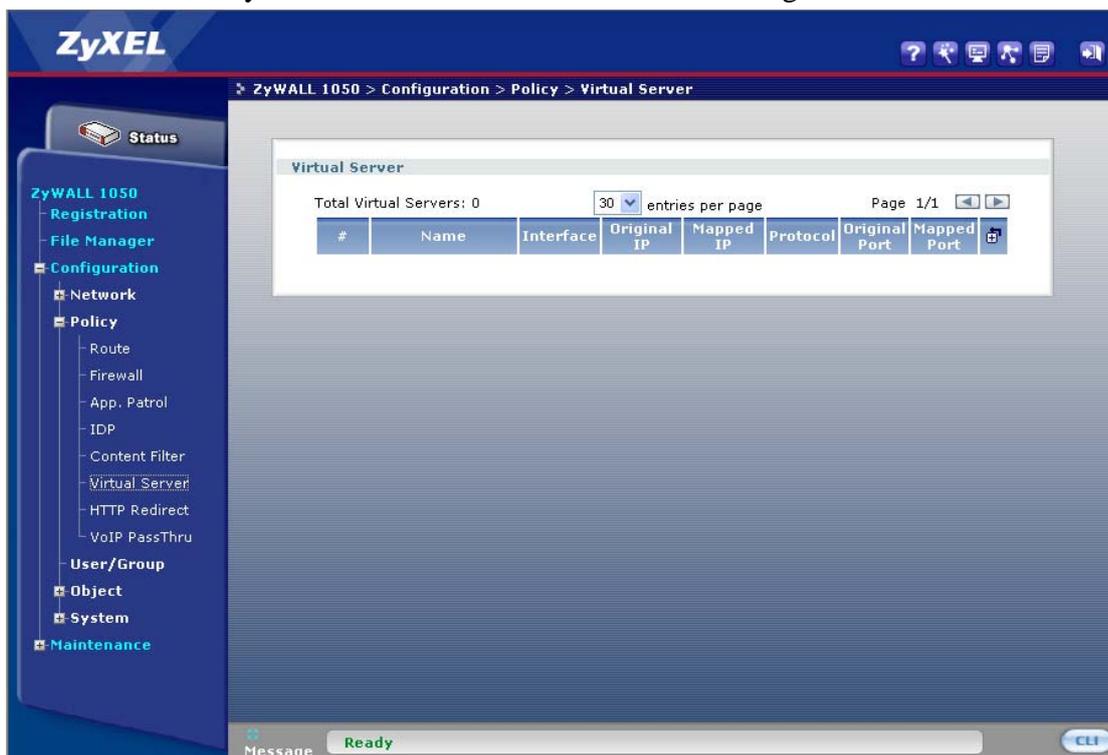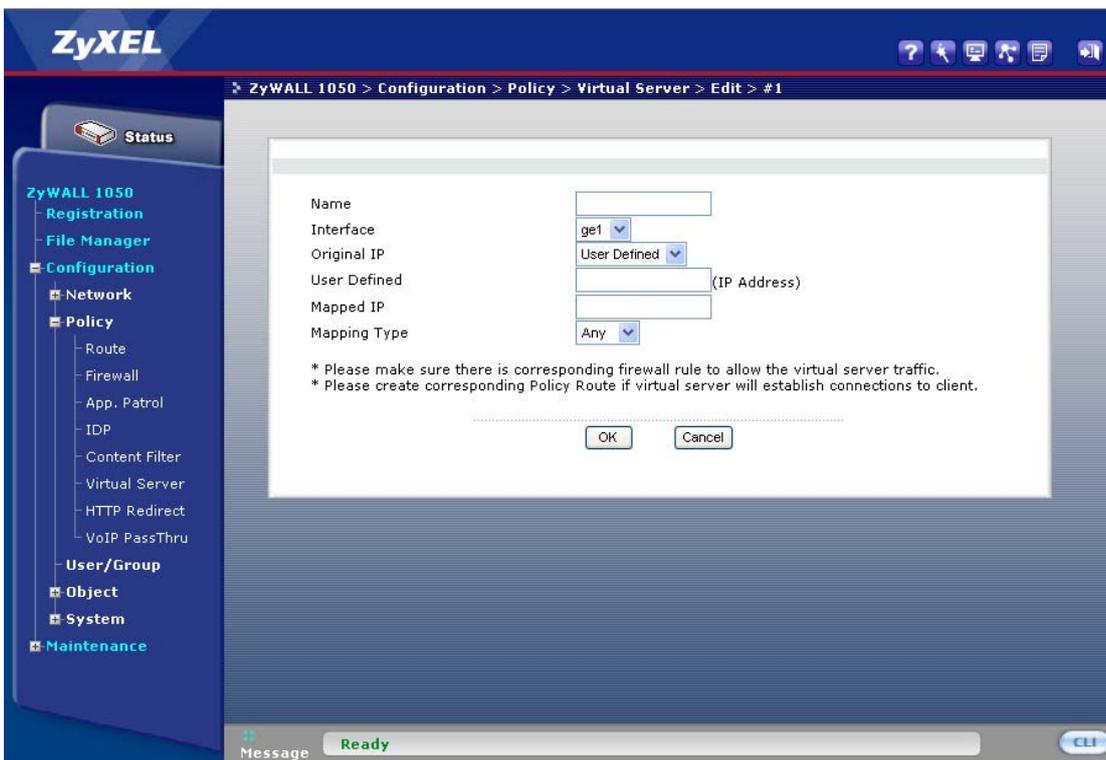
In CLI configuration, the following two examples of commands is supported:
Router(config)# ip virtual-server VR1 interface ge2 original-ip any map-to 192.168.3.2 map-type any
Router(config)# show ip virtual-server
virtual server: VR1
  active: yes
  interface: ge2
  original IP: any, netmask 255.255.255.255 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)

ZyXEL
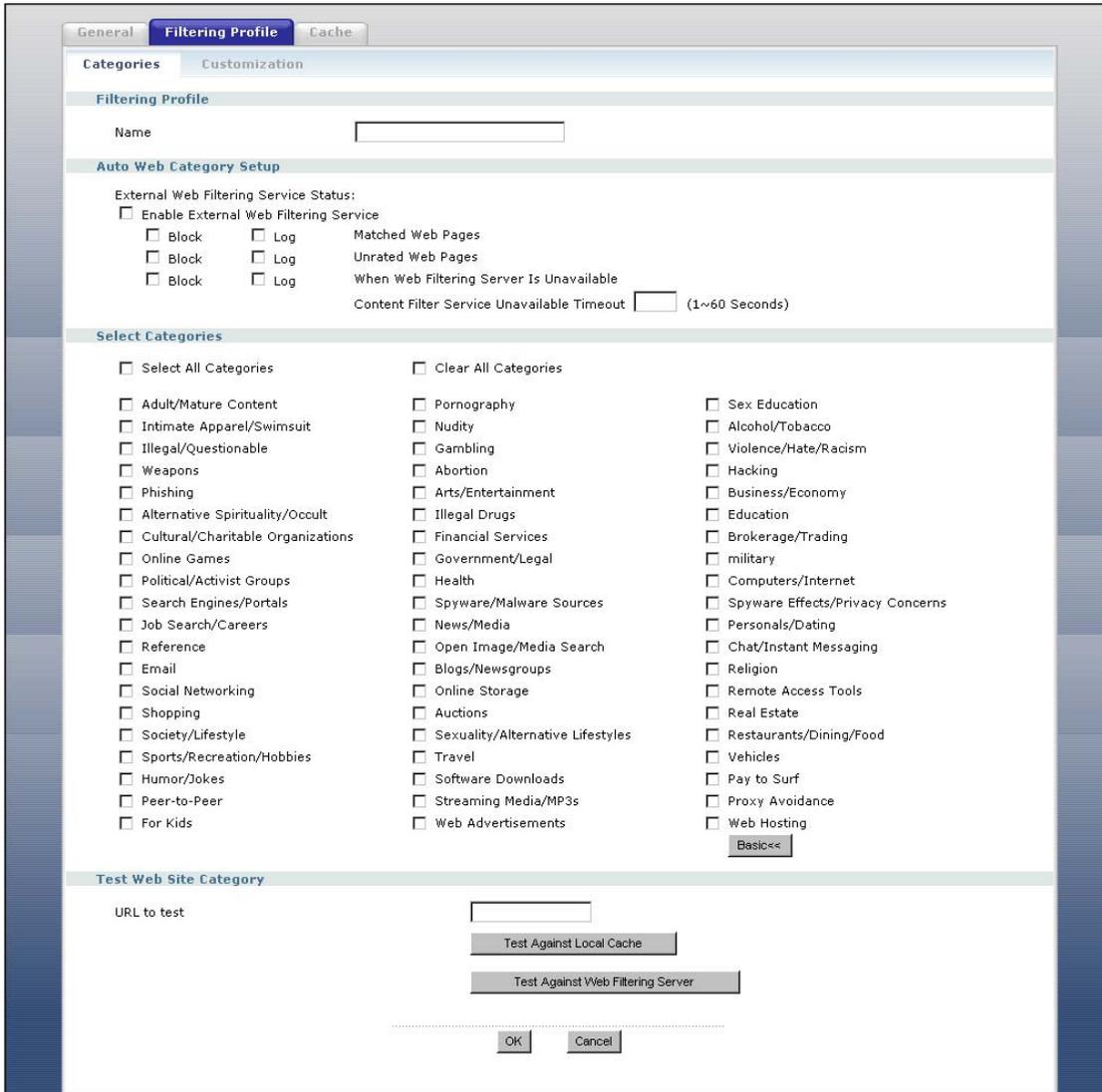
Note

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