ZyXEL

Firmware Release Note

ZyWALL IDP 10

Release 2.00(XA.1)C0

Date: **AUG 15, 2005**
Author: **Jerry Tsai**

ZyXEL ZyWALL IDP 10 Standard Version
Release 2.00(XA.1)C0
Release Note

Date: Aug. 15, 2005

Supported Platforms:

ZyWALL IDP 10

Versions:

2.00(XA.1) C0

Note:

Known Issues:

N/A

Features:

Modifications in Version 2.00(XA.1) C0 | 8/15/2005
None

Modifications in Version 2.00(XA.1) b5 | 8/08/2005
[BUG FIX]
Symptom: Cannot upgrade IDP policy from 2.x to 3.0.
Condition:

a. The minor version number of the IDP policy set in use is greater than 0.
b. Launch IDP policy upgrade by either automatic or manual upgrade procedures.

Solution: Fix the logic of version number comparison.

Modifications in Version 2.00(XA.1) b4 | 7/06/2005
[ENHANCEMENT] Rename the interface name from “management” to “MGMT” in SNMP query result for RFC1213 standard MIB.

Modifications in Version 2.00(XA.1) b3 | 7/06/2005
1. [ENHANCEMENT] Support RFC 1213 MIB for SNMP in IDP-10.
2. [ENHANCEMENT] Extend ping packet length up to 65500.

Modifications in Version 2.00(XA.1) C0 | 6/07/2005

1. [ENHANCEMENT] Support private MIB for SNMP in IDP-10.

Modifications in Version 2.00(XA.0) C0 | 5/25/2005

None

Modifications in Version 2.00(XA.0) b4 | 5/13/2005

[BUG FIX]
Symptom: When the DUT under abnormal attacked and the same time user query the Https service, it will cause TCP port 443 service crash.
Solution: Fix it.

[BUG FIX]
Symptom: When we test the throughput on DUT, during the Ixia burst Large number of packets, we found the CPU utilization is always zero.
Solution: Fix it.

Modifications in Version 2.00(XA.0)b3 | 4/13/2005

[BUG FIX]
Symptom: After update firmware from 2.00(XA.0)b1 to 2.00(XA.0)b2, We want to manual update signature, but update server "check" and "update now" button are gray, it can not work.
Solution: Fix it.

[BUG FIX]
Symptom: Configured customizations are reset after a policy update.
Solution: Fix it.

[BUG FIX]
Symptom: When user changed the snmp port to the 80、22、443 in the console command. The system is not show that the selected port is already in use!
Solution: Fix it.

[BUG FIX]
Symptom: When user changed the ssh port to the 161 in the console command. The system is not show that the selected port is already in use!, it's shown the change ZyWALL IDP 10 SSH server port OK.
Solution: Fix it.

[BUG FIX]
Symptom: When user changed the web port to the 161 in the console command. The system is not show that the selected port is already in use!, it's shown the Change ZyWALL IDP 10 WEB server port OK.
Solution: Fix it.

[BUG FIX]
Symptom: When user changed the https port to the 161 in the console command. The system is not show that the selected port is already in use!, it's shown the Change ZyWALL IDP 10 HTTPS server port OK.
Solution: Fix it.

[BUG FIX]

Symptom: When user disabled all the policy and than get system in the console command. You discovered that the wan and lan port policy number is only 41 anomaly pattern.
Solution: Fix it.

[BUG FIX]
Symptom: Change the SSH port, the system can not link to device right away
Solution: Fix it.

[BUG FIX]
Symptom: "Step1: When user type an error activation key and click apply button, the registration status will be shown Unregistration, and than we used the schedule update the pattern, the system will be show that activation key is NULL or Invalid. Step2: When user typed a correct activation key and than try again schedule update. The system is not update pattern success, because the Check and Update Now button is lock.
Solution: Fix it.

[BUG FIX]
Symptom: When user typed an error or null activation key, and than update the pattern or kernel, the system will be show the error key word in the system log message.
Solution: Fix it.

[BUG FIX]
Symptom: Enabled the log mail. Some times will be show error message in the console command. This message is SMTP HandShake [username] ReturnCode Error~!!
Solution: Fix it.

[BUG FIX]
Symptom: Web UI/System log message fail, because the system log message will be show unknown word.
Solution: Fix it.

[BUG FIX]
Symptom: Change the Https port many times, the system will be happen can not link to the device, because the service is not release.
Solution: Fix it.

Modifications in Version 2.00(XA.0)b2 | 2/24/2005

2. [ENHANCEMENT] The syslog format updates from version 1.1 to version 1.5.
3. [ENHANCEMENT] Update new on-line helps on web pages.
4. [BUG FIX]
   Symptom: "Syslog PRI field (the part in the <...>) is longer then the RFC3164 allows:<1701719540>Feb 8 09:06:48 10.10.1.245 src=""81.221.22.34:0"" dst=""194.191.19.253:0"" cat=""IDP"" class=""Other"" msg=""Traffic Log""devid=""b7b019"" act="""" note="""".
   Solution: Fix it.
5. [BUG FIX]
   Symptom: It can be modified the maximum of year to 2038 through GUI. Actually, it only can be modified to 2037.

Cause: The boundary of the CGI of time checking is 2038.
Solution: Fix it. Modify the new boundary to 2037.

6. [BUG FIX]
   Symptom: When Users turn on "WEB UI/Report/Syslog/Traffic Logging" in IDP-10, there are two log records listed in the syslog server. But, one of them should not be shown on the syslog server.
   Solution: Fix it.
7. [BUG FIX]
   Symptom: When users turn on the function of "Web UI/Remote Mgmt/WWW, SNMP, SSH/Server Access" in IDP-10 and then select the option which is "All", it should not show up the "warning page" after applying the setting.
   Cause: Because the checking logic of the CGI is wrong.
   Solution: Fix it.
8. [BUG FIX]
   Symptom: When users modify the function of "Remote Management/WWW、SNMP、SSH", all of the error messages should be the same. Currently, it is not the same.
   Solution: Fix it.
9. [BUG FIX]
   Symptom: When users turn on the function of "Web UI/Remote Mgmt/WWW, SNMP, SSH/Server Access" in IDP-10 and then select the option which is "All", it should not show up the "warning page" after applying the setting.
   Cause: Because the checking logic of the CGI is wrong, causing to output the error page.
   Solution: Fix it.
10. [BUG FIX]
    Symptom: When users modify administrator inactivity time through HTTPS, the message in the log record is improper.
    Solution: Fix it.
11. [BUG FIX]
    Symptom: The direction information in logs is not correct. Lack of the direction for WAN to LAN.
    Solution: Fix it.
12. [BUG FIX]
    Symptom: When users reset IDP-10 from GUI, all the policies disappear.
    Solution: Fix it.
13. [BUG FIX]
    Symptom: When the number of user-defined policy is 128, users delete all of them. The total policy number shown on console is the same before deleting.
    Solution: Fix it.
14. [BUG FIX]
    Symptom: The function of schedule update in IDP-10 is improper. First, there is a wrong log. Second, although the file was downloaded completely from DUC, users have to manually reboot.
    Solution: Fix it.
15. [BUG FIX]

Symptom: There is a script error occurrence, when users type the key words in IDP query page.
Solution: Fix it.

Modifications in Version 2.00(XA.0)b1 | 1/14/2005

[ENHANCEMENT] Add "port selection" by user no matter in WWW, SNMP, SSH
[ENHANCEMENT] Support HTTPS protocol.
[ENHANCEMENT] Support Doskey functionality and in console.
[ENHANCEMENT] Add a new error message when stealth and remote control functions conflict.
[ENHANCEMENT] Support two time protocols, Daytime (RFC 867) and Time (RFC 868).
[ENHANCEMENT] Add traffic log in IDP 10, it can be enabled in GUI or CLI.
[ENHANCEMENT] Direction and threshold for Pre-defined policies can be modified.
[ENHANCEMENT] Add a new function in GUI to select all function in Pre-defined policy and support showing 25, 50,100,250 policies per page.
[ENHANCEMENT] Hyperlink to from policy ID to mySecurityZone https://mysecurity.zyxel.com/mysecurity/jsp/policy.jsp?ID=PolicyID. The PolicyID is respond to the signature file from BSST.
[ENHANCEMENT] The attack direction can be record in IDP 10 logs.
[ENHANCEMENT] When stealth function on network interfaces is start, IDP-10 can normally update the newest signatures and firmware.
[ENHANCEMENT] Add a new function to be accepted username and password for SMTP.
[BUG FIX]
Symptom: IDP 10 can't block "Netbus", please check the tool.
Cause: BSST does not create the signature for this case.
Solution: Fix it.
[BUG FIX]
Symptom: SNMP in IDP 10, when "drop" packet, the SNMP shows "error" message, should revise the message!
Solution: Fix it.

Modifications in Version 1.00(XA.1)c0 | 1/7/2005

None

Modifications in Version 1.00(XA.1)b2 | 12/27/2004

1. [BUG FIX]
   Symptom: It failed to reset connections of attackers, which are located in LAN side.
   Condition: (1) Generate attacks from LAN side. (2) IDP10 failed to reset connections of attackers, which are located in LAN side.
   Cause: Source MAC addresses and destination MAC addresses are reversed
   Solution: Interchange them.

2. [BUG FIX]
   Symptom: IDP10 failed to detect port-scan attacks.
   Condition: (1) Generate TCP and UDP port scan attacks. (2) NK failed to detect port-scan attacks.
   Cause: In order to save memory, the old port-scan module incorrectly counted the number of probes with destination port number being great than 1023.
   Solution: Change the algorithm.

3. [BUG FIX]
   Symptom: The system is not able to detect UDP smurf and ICMP smurf.
   Condition: (1) Generate UDP and ICMP smurf attacks. (2) The system fails to detect them.
   Cause: Those two policies belong to flooding attack. In other words, they have their own thresholds. But they should be of protocol anomaly.
   Solution: Modify those two policies to protocol anomaly.

4. [BUG FIX]
   Symptom: The web UI shows an error string (Time Setup Failed: the value of Month column have to set between 1 and 31) in WIZARD RESULT page after setting device date/time error.
   Condition: Setup IDP10 thru Web UI in the wizard page and make a typo mistake while setting date/time.
   Cause: It is a typo error.
   Solution: Fix it in code.

5. [BUG FIX]
   Symptom: Another typo error in IDP10 Web UI while device is updating policy.
   Condition: Change any policy rule and apply it in IDP10 Web UI.
   Cause: It is a typo error.
   Solution: Fix it in the source code.

Modifications in Version 1.00(XA.1)b1 | 12/07/2004

1. [BUG FIX]
   Symptom: The enable/disable function of Web UI (IDP Page) will be failed after upgrade pre-define rules and insert a user-defined rule in User-define web page.
   Condition: Under IDP firmware version: 1.00(XA.0) and Policy version: 2.55.
   Cause: While programming IDP Web UI, we use 2 integers (32 bits long each) to represent 20 checkboxes. There is a logical process bug happen during saving user's modification request of Enable/Disable checkboxes.
   Solution: Change program by using variables instead of bit oriented process.

2. [BUG FIX]
   Symptom: User interface display error. When INTERNAL_VERSION_RELEASE (a internal used macro) is 0xC0 or 0xc0.

Condition: User DIP firmware version: 1.00(XA.0). Policy version doesn't matter.
Cause: In the original program we did not check value of INTERNAL_VERSION_RELEASE while print out the version string on user interfaces.
Solution: Add code to check on INTERNAL_VERSION_RELEASE when its value is 0xC0 or 0xc0, the value will not be displayed.

Modifications in Version 1.00(XA.0)c0 | 08/19/2004

None

Modifications in Version 1.00(XA.0)b12 | 08/16/2004

1. [ENHANCEMENT] The behavior of registration page has been changed. The AK is sent to registration servers to check its validation immediately after it is applied to the system.
2. [ENHANCEMENT] In debug mode, users are able to use the CLI command "upgrade tftp server_ip file_name" to upgrade firmware.
3. [BUG FIX]
   Symptom: The IDP event syslogs cannot be sent to syslog servers.
   Condition:
   a. Generate attack traffic to raise IDP event logs.
   b. At most 250 IDP event syslogs are sent to syslog servers.
   Solution: Clear an event log entry whenever the syslog client module is notified to send IDP event syslogs.
4. [BUG FIX]
   Symptom: The system crashes whenever it attempts to mail reports.
   Condition:
   a. Schedule the system to mail reports when log pool is full.
   b. Generate traffic to raise logs.
   c. The system crashes when it attempts to mail reports.
   Solution: The index of next log of 0^{th} one is changed to be the pool size minus 1 to fix the bug.
5. [BUG FIX] The system raise false positives.
   Condition:
   a. Visit http://oac.idv.tw/html/
   b. The false positives "EXPERIMENTAL MISC successful gobbles ssh exploit (uname)" appear in the logs.
   Solution: Get rid of cover field.
6. [BUG FIX] The help page of "Registration" was gone.
   Condition:
   a. Users fail to get the help page of registration by clicking the help icon.
   Solution: Add the hyper-link to the help page.

Modifications in Version 1.00(XA.0)b11 | 08/03/2004

1. [ENHANCEMENT] The FQDN instead of IP address is sent in the HELO

message.

2. [ENHANCEMENT] The system prompts what makes firmware update failed in the progress of firmware update.
3. [BUG FIX]
   Symptom: The number of TCP connections increases all the time.
   Condition: The system gets some strange TCP segments in EST state. They raise BAD_TCP_STATE and their physical connection entries are recycled, but the system doesn't decrease logical connection number
   a. Generate P2P traffic.
   b. Take a look at the "Current TCP session" shown on the HOME page. It keeps growing. Users need to reboot the system.

.

   Solution: Fix it.
4. [BUG FIX]
   Symptom: The action of the pre-defined policy "BAD_TCP_STATE" is "no action". But it appears in the logs and its action shows "drop packet".
   Condition: The original design does not allow users to change settings related anomaly policies.
   a. Make sure the action associated with the pre-defined policy "BAD_TCP_STATE" is no action.
   b. Generate TCP traffic against normal state transition.
   c. Take a look at the LOGS web page. Many "BAD_TCP_STATE" log appear.

   Solution: Take changes in anomaly policies into consideration.
5. [BUG FIX]
   Symptom: The word "Unknow" is spelled incorrectly. And the phrase "Unknown ERROR" should be replaced with "DATA ERROR".
   Condition:
   a. Users launch firmware/policy update.
   b. Take a look at the "LOGS" web page. There is a "Unknow ERROR" log.

   Solution: Fix it. Replace it with "Data ERROR".
6. [BUG FIX]
   Symptom: The "policy number" shown on the HOME page is incorrect. It should be the sum of numbers of pre-defined and user-defined policies.
   Condition:
   a. Users disable user-define policies.
   b. Users change user-defined policies.
   c. The policy number is not equal to the sum of numbers of predefined and user-defined policies.

   Solution: Count user-defined policies no matter whether they are enabled or not.
7. [BUG FIX]
   Symptom: The policy IDs of every logs shown on the mail reports are the same as first one.
   Condition:

   a. Configure mail report.
   b. Generate attack packets then trigger off a mail report.
   c. Take a closer look at policy IDs.

   Solution: Fix it.
8. [BUG FIX]
   Symptom: Users are not able to do time setup via wizard.
   Condition:
   a. Users enable daylight saving.
   b. Users fail to change time setup via wizard.

   Solution: Get current time before change it to take DST into account.
9. [BUG FIX]
   Symptom: Daylight saving functions improperly.
   Condition:
   a. Users configure start date and end day of daylight saving time.
   b. Users change current time to be within the period of daylight saving.
   c. The system doesn't add one hour.

   Solution: Fix it.
10. [BUG FIX]
    Symptom: The time shown on mail subject does not take DST into consideration.
    Condition:
    a. Generate mail reports.
    b. Take a closer look at the time shown on mail subject.

    Solution: The time appears in SMTP header is changed to GMT. And the system add time zone information at the end of mail subject.
11. [BUG FIX]
    Symptom: Users fail to insert user-defined policies.
    Condition:
    a. Insert a user-define policy then delete it.
    b. Users cannot insert user-defined policies.

    Solution: Close the file at the proper time.

Modifications in Version 1.00(XA.0)b10 | 07/12/2004

1. [ENHANCEMENT] Users are able to backup/restore configuration to/from a TFTP server.
2. [ENHANCEMENT] When there is no user-defined policy in Web UI, disable the following items: Enable User-define Policy checkbox, Move button, and move policy numbers.
3. [ENHANCEMENT] The format of reports has been changed to text.
4. [BUG FIX]
   Symptom: The number of TCP connections remains unchanged for a long time.
   Condition:
   Generate TCP traffic
   Stop TCP traffic going through the system by unplugging connections attached to both LAN and WAN ports.

Solution: DequeueTask attempts to clean dirty TCP connections every minute if no TCP packets go through the system for a while.

5. [BUG FIX]
   Symptom: The priority of SSH should be greater than web.
   Condition:
   A user logs in the system via web.
   One another user fails to log in the system via SSH.
   Solution: Get rid of this limitation.
6. [BUG FIX]
   Symptom: Display Policy ID number in Log, when it is a user-defined policy.
   Condition:
   a. When show log on Web UI.
   Solution: In HTMLReport.c, TextReport.c and CGI_Log.c, checks type_id of items in the log pool. If it belongs to user-defined policy, don't show it.
7. [BUG FIX]
   Symptom: When click query button in pre-defined policy Web UI, it shows a JavaScript error, says it needs an object.
   Condition:
   a. Click the "Query" button on the predefined web page.
   b. A window pops up to tell users that it needs an object.
   Solution: In CGI_idp.c, add document.forms[0] for the object referenced.
8. [BUG FIX]
   Symptom: When click Apply or Synchronize Now buttons on Time and Date page of Web UI, it shows it need an object.
   Condition:
   a. Click "Apply" or "Synchronize Now" buttons on the "Time" and Date" web page.
   b. A window pops up to tell users that it needs an object.
   Solution: In CGI_Time.c, eliminate the unused script.
9. [BUG FIX]
   Symptom: Sometimes, when click Apply button on user-defined policy, it shows "flash" undefined.
   Condition:
   a. Click "Apply" button on the user-defined web page.
   b. A window pops up to tell users that a 'flash' is undefined.
   Solution: In CGI_Time.c, add JavaScript to define "flash".
10. [BUG FIX]
    Symptom: When you modify a user-defined policy, the contents are different from what you have been edited.
    Condition:
    a. Insert a user-defined policy.
    b. Fill the name with 17 Chinese characters, note with 40 Chinese characters, and selects all operating system and actions.
    c. Apply the policy then modify it.
    Solution: Implement CGI_pl_editor.c with the latest URL parsing method. It will extend the capability of MiniWeb to handle more arguments from web client.

11. [BUG FIX]
    Symptom: When you re-check user-defined policies with multiple contents after you apply it, only the first content shows, the other contents just disappear.
    a. Insert a user defined policy with 10 more Chinese characters in the each content field.
    b. Re-check the policy. Only the first content shows.
    Solution: Fix it.
12. [BUG FIX]
    Symptom: After users fill in each content fields of policy editor with 127 characters, all the contents will be disappeared.
    Condition:
    a. Edit a user-defined policy.
    b. Fill each content field with 127 characters.
    c. Re-check it after applying it.
    d. Every content filed is empty.
    Solution: Fix it.
13. [BUG FIX]
    Symptom: The web server seems to be crashed, when the policy engine in the kernel is re-parsing the user-defined policies.
    Condition:
    a. Edit at least a user-defined policy with one-byte content.
    b. Apply it. Then the system hangs.
    Solution: Add a JavaScript to check the content length of each content field in CGI_pl_editor.c.
14. [BUG FIX]
    Symptom: The policy group setting is not function well. Did not do what users expected.
    Condition:
    a. Selects pre-defined policies by group setting.
    b. Apply group settings.
    c. Policies belonging to a group which is disabled are enabled.
    Solution: Implement the correct logic to check pre-defined policy's type, in CGITask.c.
15. [BUG FIX]
    Symptom: The web UI shows that "PageJump is undefined".
    Condition:
    a. When you query pre-defined policy again, after a previous query that has no policy applied.
    b. A window pops up to tell users that a 'PageJump' is undefined.
    Solution: A window pops up to tell users that a 'PageJump' is undefined.
16. [BUG FIX]
    Symptom: If you import an invalid user defined policy, it will success. But the content is a mess.
    Condition:
    a. Import a user-defined policy whose format is incorrect.
    b. Take a look at the policy. The content is a mess.

Solution: Implement validation function in CGI_user_define.c.

17. [BUG FIX]
    Symptom: Users cannot insert and modify user-defined policy after you export 128 policies and delete all policy.
    Condition:
        a. Insert 128 user-defined policies.
        b. Export and delete all user-defined policies.
        c. Import those policies. Then users fail to modify any policy.
    Solution: Move the file I/O function into CGITask.c (because, it need more CPU ticks), and write the output file to a temporary file first to make sure the file I/O is completed.
18. [BUG FIX]
    Symptom: The policy date shown on the “Home” page is a mess.
    Condition:
        a. Enter CLI command “reset all”.
        b. Then take a look at the “HOME” web page.
    Solution: Add “&” to the variable to hold the result of registry read.

Modifications in Version 1.00(XA.0)b9 | 06/28/2004

1. [ENHANCEMENT] Users are able to import and export backup file via TFTP.
2. [ENHANCEMENT] Users are able to import and export user-defined policies.
3. [ENHANCEMENT] Users are able to search predefined policies by type ID.
4. [ENHANCEMENT] Users are able to query predefined policies by combination of policy type, severity and OS type.
5. [ENHANCEMENT] The system is able to synchronize time with remote time servers (NTP).
6. [BUG FIX]
   Symptom: GUI status: “Update Server ALIVE! ", but in the Log show "UPDATE: Update Server Not Found! “
   Condition:
       a. The DUC is alive and reachable.
       b. Click “check” button to check whether the DUC is alive or not.
       c. The status shows “Update Server Alive”. But the log “Update Server Not Found!” appears instead of “Update server Alive”.
   Solution: Fix the message.
7. [BUG FIX]
   Symptom: In quick setup, users don’t change any settings. But the result shows that some settings change OK.
   Condition:
       d. Use wizard to configure the system.
       e. Keep original settings, don’t change them.
   Solution: Fix the status message.
8. [BUG FIX]
   Symptom: Users fail to update firmware and signature due to no latest releases available. But the log “No file existed” appears. It should be “No New Version

File".
Condition:

f. Both firmware and signature are up to date.
g. Perform firmware or policy update via DUC.
h. Update fails due to no latest files in DUC.
i. Take a closer look at system logs.

Solution: Fix the status message.

9. [BUG FIX]
   Symptom: False positives appear.
   Condition:
   j. Generate NetMeeting or VPN traffic.
   k. False positives "P2P Overnet UDP connet" and "P2P eDonkey UDP Server status request" appear in logs.
   Solution: Solution: Get rid of OT.

Modifications in Version 1.00(XA.0)b8 | 06/07/2004

1. [ENHANCEMENT] Users are able to configure the action type of predefined policies.
2. [ENHANCEMENT] Users are able to configure syslog setting via web GUI. And the report exporting by FTP is obsolete.
3. [ENHANCEMENT] There are two types of log prefix wording: one is "Attack" for logs with severity 4 or 5, the other is "Warning" for logs with severity 1, 2 or 3.
4. [ENHANCEMENT] Both the default values of maximum length and number per second of ping packets have been changed to 1500 and 3000 respectively.
5. [ENHANCEMENT] The "action type" column is newly added to log, report as well as alarm.]
6. [BUG FIX]
   Symptom: The system accepts invalid IP addresses.
   Condition:
   a. Users enter an invalid IP address as a parameter of some network settings.
   b. No error messages display.
7. [BUG FIX]
   Symptom: The wording "NK3002" appears on console at the time of booting.
   Condition:
   a. Power off/on the system or reboot the system.
   b. Take a closer look at console when message display.
8. [BUG FIX]
   Symptom: Users are redirected to the login page before timeout.
   Condition:
   a. Login in the system via web.
   b. Users launch any kinds of requests after "timeout" minutes from logging.
9. [BUG FIX]
   Symptom: Users are confused with some CI commands which are used to turn on/off functions such as TCP state check.

10. [BUG FIX]
    Symptom: “Disk” usage displayed on the HOME page should be replaced by “Flash” usage.
11. [BUG FIX]
    Symptom: E-mailed logs contain nothing.
    Condition:
    a. No system and attack events occur. Hence, the system has no logs to report by e-mail.
    b. Users receive an empty e-mailed report after scheduled time expires.
12. [BUG FIX]
    Symptom: Reports and alarms cannot be delivered by e-mail to the recipients except first one.
    Condition: Users configure at least two recipients.
13. [BUG FIX]
    Symptom: Customizations of pre-defined policies are lost due to policy update.
    Condition:
    a. Configure pre-defined policies.
    b. Perform policy update.
14. [BUG FIX]
    Symptom: DOM will be full after a couple of days.
    Condition: The used space of the DOM in an IDP continues to grow as long as the IDP is power-on.
15. [BUG FIX]
    Symptom: Users fail to backup user-defined policies.
    Condition:
    a. Edit at least one user-defined policy.
    b. Perform backup to save the current configuration.
    c. Change user-defined policies.
    d. Restore the system to previous configuration.
16. [BUG FIX]
    Symptom: There are some false positives.
    Condition: Generate packets whose header parts match some policies with only 2-byte patterns.

Modifications in Version 1.00(XA.0)b7 | 05/28/2004

1. [ENHANCEMENT] Users can search predefined policies by attack name, case-insensitively.
2. [ENHANCEMENT] Add DNS server function, and can be set via wizard.
3. [ENHANCEMENT] Users can configure “Administrator Inactivity Timer” via web and console.
4. [ENHANCEMENT] Logs whose severity is equal to or greater than 4 appear in red color.
5. [ENHANCEMENT] At most one user can operate the system no matter via console, web, or SSH at any time. The priority is shown as follows: console > SSH= web.

6. [ENHANCEMENT] The valid value of VLAN ID is from 1 to 4094. The default value is 1.
7. [BUG FIX]
   Symptom: Incorrect status message of policy update.
   Condition:
   a. Perform policy update successfully.
   b. The status shows that update policy failed.
8. [BUG FIX]
   Symptom: The icon and prompting message shown on the “User-defined” web page is incorrect.
   Condition:
   a. At least one user-defined policy appears on the “User-defined” web page. Hence, an incorrect icon is shown on the “Modify” column of each policy.
   b. The cursor is on top of the icon. Then prompting message is shown but incorrect.
9. [BUG FIX]
   Symptom: An IDP reboots on a daily basis.
   Condition:
   a. Set the schedule of “Check & Reboot” on the "F/W Upload" web page.
   b. There is no latest firmware saved in DOM.
   c. The IDP reboots at the time scheduled everyday.
10. [BUG FIX]
    Symptom: Incorrect IE title. It should be “ZyXEL ZyWALL IDP 10 Internet Security Appliance”.
11. [BUG FIX]
    Symptom: The word “kernel” appears somewhere on console and web pages will be all changed to “firmware”.
12. [BUG FIX]
    Symptom: The arrangement and appearance of attributions “Operating System” and “Severity” shown on the "POLICY SELECT" web page was not the same as those shown on the "ADD USER_DEFINED POLICY" web page.
    Condition:
    a. Get both web pages.
    b. Check to see the arrangement and appearance of attributions “Operating System” and “Severity.
13. [BUG FIX]
    Symptom: Button could not be pressed.
    Condition:
    a. The DNS is not defined.
    b. Fill out domain name instead of IP address in the blank of "Update Server".
    c. Press "Check" or "Update Now" button. Then the button is gray-out forever.
14. [BUG FIX]

Symptom: The shell prompts incorrect message to indicate the need of the parameter "interface" whenever CI command "set int link" is entered.
Condition:

a. Enter CI command "set int link". Then the shell will prompt the lack of an interface to apply.
b. The prompting message is "Need interface name: [wan+mgmt | lan+mgmt | mgmt]". It should be "Need interface : [wan | lan | mgmt]".

15. [BUG FIX]
Symptom: The shell prompts incorrect message to indicate the need of the parameter "interface" whenever CI command "set sys det pingmax" is entered.
Condition:
    a. Enter CI command "set sys det pingmax". Then the shell will prompt the lack of an interface to apply.
    b. The prompting message is "Need interface : [lan+mgmt | wan+mgmt]". It should be "Need interface : [lan | wan]".
16. [BUG FIX]
Symptom: The word "NK3002" appears as SNMP system name on console.
Condition:
    a. Enter CI command "get rem" to get the information of remote access settings.
    b. Take a closer look at the SNMP system name.
17. [BUG FIX]
Symptom: Users could not check system logs by using CI command “get log”.
Condition:
    a. At lease one system log is kept in the system.
    b. Enter CI command "get log". But nothing is displayed on console.
18. [BUG FIX]
Symptom: Predefined policies cannot backup.
Condition:
    a. Edit at least one user-defined policy.
    b. Perform backup to save the current configuration.
    c. Change user-defined policies.
    d. Restore the system to previous configuration.
19. [BUG FIX]
Symptom: The same alarms appear again and again.
Condition:
    a. Some policies with alarm are matched
    b. Stop traffic.
    c. Users receive the same alarms again and again periodically.
20. [BUG FIX]
Symptom: Login attempt via web is failed.
Condition:
    a. Login in the system from LAN port, then logout.
    b. Login in the system from Mangement port, then logout.

c. Fail to login in the system from both LAN port and WAN port.

Modifications in Version 1.00(XA.0)b6 | 05/14/2004

1. [BUG FIX]
   Symptom: State message is incorrect in web GUI state.
   Condition:
   a. Firmware upgrade process is under going but the state shown failed.
   b. After download new firmware from the internet, the device will automatically reboot, but the state shown DUC failed.
2. [BUG FIX]
   Symptom: Fix the incorrect words shown on console or web GUI.
   Condition:
   a. Concurrent connections will be 8000 instead of 2000 in the web GUI.
   b. System name will be “ZyWALL IDP 10” instead of “NK3002” on console.
3. [BUG FIX]
   Symptom: Update events are not logged.
   Condition:
   a. Perform firmware or policy update.
   b. Take a closer look at logs. No related logs appear.
4. [BUG FIX]
   Symptom: The search result of predefined policies just needs to display keyword.
   Condition:
   a. Perform policy search by keyword.
   b. The searched result is displayed. But it just needs to show keyword.

5. [BUG FIX]
   Symptom: Users need to tries many times in order to accomplish remote update successfully.
   Condition:
   a. Perform firmware or policy live update. The system is going to get latest files from a update server.
   b. The update attempt fails.
   c. Continue to try until the system gets latest files from a update server.
6. [BUG FIX]
   Symptom: The message “DUC Server ALIVE” should be replaced by “Update Server ALIVE”.
   Condition:
   a. Click “check” button to see if the update server is alive and reachable or not.
   b. The system connects to the update server successfully. The

status shows “DUC Server ALIVE”.

7. [BUG FIX]
   Symptom: Users cannot configure DNS via “Wizard”.
   Condition:
   a. Click “Quick Setup” button on the HOME page to launch wizard to configure the system.
   b. No blank of DNS setting available.
8. [BUG FIX]
   Symptom: The “:” symbol should not appear anywhere on web pages.
   Condition:
   a. Login in the system via web.
   b. Take a closer look at every web page. The “:” symbol appear somewhere.
9. [ENHANCEMENT] The default TCP idle time is changed to 3600 seconds. And it has been removed from web GUI.
10. [ENHANCEMENT] Users are able to setup multiple recipients on the web page of E-Mail report setup.
11. [ENHANCEMENT] Each letter contained in any acronyms is capitalized in web GUI, and the “:” symbol will no longer appear on web pages.

Modifications in V1.00(XA.0)b5 | 04/28/2004

1. [BUG FIX]
   Symptom: The policy number is incorrect. It should be the sum of predefined policy number and user-defined policy number.
   Condition:
   a. The system contains 1486 predefined policies and 12 user-defined policies.
   b. But the value of policy number is not equal to 1498 (1486 + 12).
2. [BUG FIX]
   Symptom: The netmask always is 255.255.255.0. Users cannot change it via web.
   Condition:
   a. Configure the device’s netmask via web. And the inputted value is not a class-C, B, or A netmask.
   b. Fails to configure it.
3. [BUG FIX]
   Symptom: The setting of remote management via WWW cannot be hold.
   Condition:
   a. Change the setting of remote management via WWW.
   b. Reboot the system.
   c. The setting is lost.
4. [BUG FIX]
   Symptom: The web-GUI cannot be refreshed in case of rebooting after updating firmware successfully.
   Condition:

   a. Perform firmware live update.
   b. After getting the latest firmware successfully from the update server, the system reboots.
   c. Web-GUI should be redirected to login page after the system starts to run.

5. [BUG FIX]
   Symptom: Time information displayed in the alarm logs is early than received time of alarm report by 2 hours.
   Condition:
   a. Generate attacks to raise alarm.
   b. Use Outlook to receive alarm reports.
   c. Take a closer look at time information of alarm logs and compare with the received time of alarm reports.
6. [BUG FIX]
   Symptom: Some strange logs appear.
   Condition:
   a. Pay attention to logs. Some strange logs with undefined attack names appear from time to time.
7. [BUG FIX]
   Symptom: Some attacks cannot be matched.
   Condition:
   a. Generate attacks to test the system's sensitivity.
   b. Some attacks cannot be detected by the system.
8. [ENHANCEMENT] Add the function that can use "keyword" to query the specific policy.
9. [ENHANCEMENT] Add registered status/expired day in web UI.
10. [ENHANCEMENT] Colors in graphical bars: before critical point: green; after critical point: red.
11. [ENHANCEMENT] DUC supports debug kernel update.

Modifications in Version 1.00(XA.0)b3 | 03/30/2004

1. [BUG FIX] Symptom: Users can just insert at most 3 user-defined policies.
   Condition:
   a. Insert 3 user-defined policies.
   b. Users fail to insert forth user-defined policy.
2. [BUG FIX]
   Symptom: Users cannot modify or delete a user-defined policy with a long attack name.
   Condition:
   a. Insert a user-defined policy with a long attack name.
   b. Fail to modify or delete it.
3. [BUG FIX]
   Symptom: The system crashes after inserting a user-defined policy with long note or content.
   Condition:

   a. Edit a user-defined policy and fill note or content with characters as many as possible.
   b. Apply the user-defined policy. The system will crash.

4. [BUG FIX]
   Symptom: The “start” field of update schedule can be filled with an invalid value. The system should prompt an error message.
   Condition:
   a. Fill the field with an invalid value.
   b. The system accepts it.
5. [BUG FIX]
   Symptom: The attack names of some logs have strange symbols.
   Condition:
   a. Generate attacks in order to raise logs.
   b. Take a closer look at attack names of all logs. Some strange symbols appear.
6. [BUG FIX]
   Symptom: Users need to re-login after change time setting on the “maintenance-time setting” web page.
   Condition:
   a. Change current time via web.
   b. Users are logged out after applying the new values.
7. [BUG FIX]
   Symptom:
   Condition:
   a. Configure firmware check and update schedules. Note that check schedule cannot be the same as that of update.
   b. At the scheduled time of firmware check, the system gets an up-to-date firmware.
   c. Both log of “Write kernel file to server” and log of “Update kernel file to device” appear. The later log should not appear because the scheduled time of firmware update has not come.
8. [BUG FIX]
   Symptom: Users cannot log in the system via web.
   Condition:
   a. Log in the system via web from a host attached to WAN port.
   b. Log out. Then users cannot log in the system via web from a host attached to LAN port or MANAGEMENT port.
9. [BUG FIX]
   Symptom: Some of attacks cannot be detected.
   Condition:
   a. Generate attacks to test system’s sensitivity.
   b. Some of the attacks cannot be detected.

Modifications in Version 1.00(XA.0)b2 | 03/08/2004

1. [ENHANCEMENT] Add web / console timeout. Default value is 5 minutes.
2. [ENHANCEMENT] Add web session. At most one host can access the system via web at any time.
3. [ENHANCEMENT] The system prompts users to change password whenever they attempt to login via web if default password remains unchanged. Its style is the same as that of ZyWALL 70 Web-GUI.
4. [ENHANCEMENT] Users are allowed to key in domain name in blanks of mail server, FTP server as well as update server.
5. [ENHANCEMENT] Users are able to configure DNS via web and console.
6. [ENHANCEMENT] Users are able to upload firmware and policy files from a local host, and backup current configuration.
7. [BUG FIX]
   Symptom: Web-GUI status displays improper message in case of failure in checking whether a DUC is alive or not.
   Condition:
   a. Click “check” button to make sure whether the intended update server is alive or not.
   b. The update server is not alive. Hence, the status just be changed to “timeout”.
8. [BUG FIX]
   Symptom: The status message is incorrect in case of policy update.
   Condition:
   a. The system has the latest policy set.
   b. Perform policy update.
   c. The status shows “Receive from Server Message Fail~”. It should be changed in order to point out what happened.
9. [BUG FIX]
   Symptom: The error message is incorrect in case of configuring schedule of report by FTP.
   Condition:
   a. Key in an invalid time on the web page. (e.g. 25 hour)
   b. The system should prompt that the inputted data is unacceptable.
10. [BUG FIX]
    Symptom: Web-GUI status displays improper message in case of failure in configuring Web-GUI System/Network TCP idle time.
    Condition:
    a. Configure System/Network TCP idle time with an invalid value.
    b. The status displays error message. The word “shoule” is incorrect. It should be “should”.
11. [BUG FIX]
    Symptom: The system is not able to detect attacks and raise incorrect alerts.
    Condition:
    a. Generate attacks to test the system’s sensitivity.

b. Most of the attacks cannot be detected and correctly logged.

12. [BUG FIX] Symptom: Users fail to backup user-defined policies.
    Condition:
    a. Backup current configuration by entering the CLI command “backup”.
    b. Change user-defined policies.
    c. Restore the previous configuration to the system by entering the CLI command “restore”.
    d. User-defined policies cannot be restored.

CLI Command List

System related Command

Command					Description
Set	Log	logmax			Setup maximum log number the device generated every second
	System	passwd <value>			Setup login password
		system tomeout			Setup login idle timeout
		backup			Backup configuration
		restore			Restore configuration
		vlan	id		Setup vlan id
			link <UnTAg|Tag>		Enable/disable vlan tag
		ip <ip address>			Setup device ip address
		mask			Setup device subnet mask
		gateway			Setup device gateway ip address
		detect	vpnbypass <ON/OFF>		Enable/disable vpn packet bypass
			portscan <ON/OFF>		Enable/disable portscan function
			fragment <ON/OFF>		Enable/disable fragment function
			stateful <ON/OFF>		Enable/disable TCP state check
			integrity <ON/OFF>		Setup TCP idle timeout
			tcptimeout <value>		Setup maximum ping length
			pinglen <value>		Setup maximum ping packet number per second
			pingmax <value>	wan	Setup maximum ping packet accepted at wan port
				lan	Setup maximum ping packet accepted at lan port
			policy	wan <ON/OFF>	Setup policy check on/off wan port
				lan <ON/OFF>	Setup policy check on/off loan port
	Interface	link	wan	10 <half/full>	Setup wan port speed 10/100; full/half duplex
				100 <half/full>	
				auto <half/full>	Enable auto negotiation
			lan	10 <half/full>	Setup lan port speed 10/100; full/half duplex
				100 <half/full>	
				auto <half/full>	Enable auto negotiation
		stealth	wan <ON/OFF>		Enable/disable stealth mode on wan port
			lan <ON/OFF>		Enable/disable stealth mode on lan port
	Remote	snmp	on <LAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote snmp access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote snmp access
			acl <ip address>		Setup access control list ip address
			commnuity	ro <value>	Setup community read only string
				rw <value>	Setup community read/write string
				trap <value>	Setup snmp trap
			system name <value>		Setup remote snmp system name
			trap <ON/OFF>		Enable/disable remote snmp trap
			trap ip <value>		Setup remote snmp trap send to ip address
			port		Modify the port of snmp service
		ssh	on <CAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote SSH access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote SSH access
			acl <ip address>		Setup access control list ip address

			port		Modify the port of ssh service
		web	on <CAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote web access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote we access
			acl <ip address>		Setup access control list ip address
			port		Modify the port of web service
		https	on <CAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote https access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote https access
			acl <ip address>		Setup access control list ip address
			port		Modify the port of https service
	duc	timeout			Set DUC connection timeout value
Get	State				Get system state
	Log				Get device log
	System				Get system information
	Time				Get device time
	Interface				Get interface information
	All				Get all information
	Remote				Get remote access information
Reboot					Reboot device
Help					CLI help message
Reset					Reset configuration to factory default
ResetAll					Reset configuration to factory default and clear policy to none
Netstat					Display network state
Ping					Ping
Arp					Display arp information