ZyXEL

Firmware Release Note

USG20W-VPN

Release V4.16(ABAR.0)C0

Date: December 28, 2015
Author: Mike Yu
Project Leader: Eric Liu

Contents

ZyXEL USG20W-VPN

Release V4.16(ABAR.0)C0

Release Note

Date: December 28, 2015

Supported Platforms:

ZyXEL USG20W-VPN

Versions:

ZLD Version: V4.16(ABAR.0) | 2015-12-28 16:46:23
Boot Module Version: V1.12 | Sep 10 2015 10:13:15

Files lists contains in the Release ZIP file

File name: 416ABAR0C0.bin
Purpose: This binary firmware image file is for normal system update.
Note: The firmware update may take five or more minutes depending on the scale of device configuration. The more complex the configuration, the longer the update time. Do not turn off or reset the ZyWALL/USG while the firmware update is in progress. The firmware might get damaged, if device loss power or you reset the device during the firmware upload. You might need to refer to Appendix 3 of this document to recover the firmware.

File name: 416ABAR0C0.conf
Purpose: This ASCII file contains default system configuration commands.

File name: 416ABAR0C0.pdf
Purpose: This release file.

File name: 416ABAR0C0.ri
Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.
Note: The ZyWALL/USG firmware could be damaged, for example by the power going off or pressing Reset button during a firmware update.

File name: 416ABAR0C0-MIB.zip

Purpose: The MIBs are to collect information on device. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

The zip file includes several files: 416ABAR0C0-enterprise.mib, 416ABAR0C0-private.mib, ZYXEL-ES-SMI.MIB, ZYXEL-ES-CAPWAP.MIB, ZYXEL-ES-COMMON.MIB and ZYXEL-ES-ProWLAN.MIB. Please import ZYXEL-ES-SMI.MIB first.

File name: 416ABAR0C0-opensource-list.xls

Purpose: This file lists the open source packages.

File name: 3G dongle compatibility table v106.xlsx, 3G patch file v106.wwan

Purpose: Mobile broadband dongle support list.

Read Me First

1. The system default configuration is summarized as below:
   - The default device administration username is “admin”, password is “1234”.
   - The default LAN interface is lan1, which is P3 port on the front panel. The default IP address of lan1 is 192.168.1.1/24.
   - By default, WWW/SSH/SNMP service can only be accessed from LAN subnet.
   - The default WAN interface is wan, and the secondary WAN interface is sfp. These two interfaces will automatically get IP address using DHCP by default.
2. It is recommended that user backs up “startup-config.conf” file first before upgrading firmware. The backup configuration file can be used if user wants to downgrade to an older firmware version.
3. If user upgrades from previous released firmware to this version, there is no need to restore to system default configuration.
4. When getting troubles in configuring via GUI (popup java script error, etc), it is recommended to clear browser’s cache first and try to configure again.
5. To reset device to system default, user could press RESET button for 5 seconds and the device would reset itself to system default configuration and then reboot.
   - Note: After resetting, the original configuration would be removed. It is recommended to backup the configuration before this operation.
6. If ZyWALL/USG can’t reboot successfully after firmware upgrade, please refer to Appendix 3: Firmware Recovery.

Design Limitations:

Note: Design Limitations described the system behavior or limitations in current version. They will be created into knowledge base.

Build in Service

1. [SPR: 061208575]
   [Symptom]
   If users change port for built-in services (FTP/HTTP/SSH/TELNET) and the port conflicts with other service or internal service, the service might not be brought up successfully. The internal service ports include 50001/10443/10444/1723/2601-2604/953. Users should avoid using these internal ports for built-in services.
   [Workaround]
   Users should avoid using these internal ports for built-in services.

DNS

1. [SPR: 140425458]
   [Symptom]
   DUT does not support *.com A-record PTR.
2. [SPR: 150122977]
   [Symptom]
   DNS security option will deny device local out DNS query
   [Condition]
   1. Edit the customize rule of DNS security option, and set the query recursion as deny.
   2. If device's WAN IP address is in the customize address range, device local-out DNS query will be deny.

GUI

1. [SPR: 100415854]
   [Symptom]
   The GUI's initial help page's behavior was wrong.
   [Condition]
   1. In the GUI Interface page press the Site Map page, it will pop up the window.
   2. Press the question mark(?), GUI will open the Site Map's help page.
   3. Close the help and Site Map window, press the Interface page's Help link.
   4. It still open the Site Map's help page.[SPR: 100914249][Symptom]IE7/8 sometimes shows "Stop running this script? A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive." when configuring device. Please update IE patch: http://support.microsoft.com/kb/175500 for fixing this issue

Interface

1. [SPR: 100105242, 100105292]

   [Symptom]

   PPTP might not be able to connect successfully if it is configured via Installation Wizard/Quick Setup. This is because:

   1. Installation Wizard/Quick Setup only allows PPTP based interface to be configured with Static IP.
   2. Installation Wizard/Quick Setup doesn't allow user to configure PPTP based interface's Gateway IP Address. This may cause PPTP cannot connect successfully if the PPTP Server IP is not at the same subnet with PPTP's based interface

   [Workaround]

   Before dial PPTP connection, configure the Gateway IP of PPTP interface's based interface

IPsec VPN

1. [SPR: 070814168]

   [Symptom]

   VPN tunnel could not be established when:

   1. a non ZyWALL/USG peer gateway reboot and
   2. ZyWALL/USG has a previous established Phase 1 with peer gateway, and the Phase 1 has not expired yet. Under those conditions, ZyWALL/USG will continue to use the previous phase 1 SA to negotiate the Phase 2 SA. It would result in phase 2 negotiation to fail.

   [Workaround]

   User could disable and re-enable phase 1 rule in ZyWALL/USG or turn on DPD function to resolve problem.

2. [SPR: 100429119]

   [Symptom]

   VPN tunnel might be established with incorrect VPN Gateway

   [Condition]

   1. Prepare 2 ZyWALL/USG and reset to factory default configuration on both ZyWALL/USGs
   2. On ZyWALL/USG-A:
      1. Create 2 WAN interfaces and configure WAN1 as DHCP Client
      2. Create 2 VPN Gateways. The "My Address" is configured as Interface type and select WAN1 and WAN2 respectively
      3. Create 2 VPN Connections named VPN-A and VPN-B accordingly which bind on the VPN Gateways we just created
   3. On ZyWALL/USG-B

1. Create one WAN interface
2. Create one VPN Gateway. The Primary Peer Gateway Address is configured as WAN1 IP address of ZyWALL/USG-A and the Secondary Peer Gateway Address is configured as WAN2 IP address of ZyWALL/USG-A

4. Connect the VPN tunnel from ZyWALL/USG-B to ZyWALL/USG-A and we can see VPN-A is connected on ZyWALL/USG-A
5. Unplug WAN1 cable on ZyWALL/USG-A
6. After DPD triggered on ZyWALL/USG-B, the VPN Connection will be established again
7. On ZyWALL/USG-A, VPN-A is connected. But actually ZyWALL/USG-B should connect to VPN-B after step 5.

[Workaround] Change the WAN1 setting of ZyWALL/USG-A to Static IP

3. [SPR: 140304057]
   [Symptom]
   After inactivating GRE over IPsec, old connection may remain if the traffic flows continuously. This may cause traffic bounded with old connection.
   [Workaround] Stop traffic for 180 seconds and the internal connection record will time out.
4. [SPR: 140416738]
   [Symptom]
   Ignore don't fragment setting cannot take effect immediately if there already existed the same connection.
   [Workaround] Stop traffic for 180 seconds and the internal connection record will time out.
5. The following VPN Gateway rules configured on the ZyWALL/USG cannot be provisioned to the IPSec VPN Client:
   1. IPv4 rules with IKEv2 version
   2. IPv4 rules with User-based PSK authentication
   3. IPv6 rules

SSL VPN

1. Following are the table list for SSL VPN supporting applications and operating systems:

Applications Operating System	Full Tunnel Mode	Reverse Proxy Mode File Sharing(Web-based Application)	RDP	VNC
Windows 7 (X64) (SP1) Java 7 -	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version Opera latest version Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version

Windows 7 (X32) (SP1) Java 7 -	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Opera latest version Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version	Internet Explorer 8.x, 9.x, 10.x, 11.x	Internet Explorer 8.x, 9.x, 10.x, 11.x Chrome latest version Firefox latest version - Safari latest version
Windows 8 (X64) Java 7	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
Windows 8 (X32) Java 7	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version	Internet Explorer 10.x, 11.x	Internet Explorer 10.x, 11.x Chrome latest version Firefox latest version Safari latest version
MAC OSX 10.9 Java 7	Safari 7.0.x Chrome 33.0.x Firefox 27.0.x	Safari 7.0.x Firefox 27.0.x	Not support	Firefox 27.0.x

2. [SPR: 100419034]

   [Symptom]

   SSLVPN of VNC cannot work if user connects VNC application by FQDN.

L2TP VPN

1. Following are the table list for L2TP VPN supporting L2TP client and operating systems:

L2TP Client	OS type	Client Version
Windows L2TP client	Windows 7 32/64 Windows 8 32/64	
iPhone/iPAD L2TP client	iPhone5 iPAD	6.1.2 6.1.2
Android L2TP client	Google Phone	
Mac L2TP client	X10.8.3	

2. [SPR: N/A]

   [Symptom]

   L2TP connection will break sometimes with Android device. This issue comes from the L2TP Hollow packet will not by replied by Android system.

User Aware

1. [SPR: 070813119]

   [Symptom]

   Device supports authenticating user remotely by creating AAA method which includes AAA servers (LDAP/AD/Radius). If a user uses an account which exists in 2 AAA server

and supplies correct password for the latter AAA server in AAA method, the authentication result depends on what the former AAA server is. If the former server is Radius, the authentication would be granted, otherwise, it would be rejected.

[Workaround]

Avoid having the same account in AAA servers within a method.

IPv6

1. HTTP/HTTPS not support IPv6 link local address in IE7 and IE8.
2. Windows XP default MS-DOS FTP client cannot connection to device's FTP server via iPv6 link-local address.
3. [SPR: 110803280]
   [Symptom]
   Safari cannot log in web with HTTPS when using IPv6
4. [SPR: 110803293]
   [Symptom]
   Safari fails to redirect http to https when using IPv6
5. [SPR: 110803301]
   [Symptom]
   Safari with IPv6 http login when change web to System > WWW, it pop up a logout message. (HTTP redirect to HTTPS must enable)

MAC Authentication

1. [SPR: 150127103]
   [Symptom]
   Client use Internal MAC-Auth connection Auth. Server can’t get IP successful.
   [WORKAROUND]
   Set short ARP timeout value on monitored interface's switch and gateway side.

Wireless

1. [SPR: 150127103]
   [Symptom]
   MAC authentication use internal and auth. method set USG, wireless client can’t get IP successful.

Known Issues:

Note: These known issues represent current release so far unfix issues. And we already plan to fix them on the future release.

IPSec VPN

1. [SPR: 120110586]
   [Symptom]
   When set IPsec VPN with certificate and enable x.509 with LDAP, the VPN session must dial over two times and the session will connect successfully
2. [SPR: 140317624]
   [Symptom]
   DUT fails to fall back using primary WAN port when all DUT WAN's IP address were same subnet.
3. [SPR: 140818615]
   [Symptom]
   After Enable and Disable NAT rule, IPsec VPN traffic cannot forward to LAN subnet immediately.
   [Condition]
   1. Topology:
      PC1 ---LAN1 USG60W WAN1 ---- WAN1 USG60 LAN1 --- PC2 & PC3
   2. USG60W
      WAN1: 10.1.4.45/24
      WAN2: 192.168.9.x/24 (Can reach to 172.23.x.x network through NAT router.)
      LAN1: 192.168.181.x/24
      PC1: 192.168.181.33
   3. USG60
      WAN1: 10.1.6.79/24
      LAN1: 192.168.1.1/24
      PC2: 192.168.1.33
      PC3: 192.168.1.34
   4. USG60 sets a policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=VPN tunnel
      USG60W sets
      1. policy route, src= 172.0.0.0/8, dst=192.168.1.0/24, next-hop=VPN tunnel
      2. policy route, src=192.168.1.0/24, dst=172.0.0.0/8, next-hop=WAN2
   5. PC2 ping 172.23.x.x is OK
   6. Add a 1:1NAT rule which is from WAN1 10.1.6.79 mapping to 192.168.1.34 (PC3) on USG60.

7. PC2 ping 172.23.x.x will fail now.
8. Disable 1:1 NAT rule.
9. PC2 still cannot ping to 172.23.x.x.

Need to reboot device or wait several minutes, it works.

4. [SPR: 141209575]

[Symptom]

IPsec VPN tunnel sometimes can be built up while initiator and responder devices use CA with the same subject name in IKE authentication. This tunnel should not be allowed to build.

IPv6

1. [SPR: 131226738]

[Symptom]

Only one prefix delegation can be added in IPv6 address assignment.

2. [SPR: 141125082]

[Symptom]

DHCPv6 relay cannot work.

SSL VPN

1. [SPR: N/A]

[Symptom]

Windows 7 users cannot use SSL cipher suite selection as AES256.

[Workaround]

You can configure Windows cipher with following information

http://support.microsoft.com/kb/980868/en-us

2. [SPR: 121203072]

[Symptom]

ext-group name and any password can login SSL VPN

System

1. [SPR: 130207529]

[Symptom]

When change SSH, Telnet and FTP Service default port, the connect session still exist.

2. [SPR: 150529308]

[Symptom]

Console sometime dump XXX daemon dead message during rebooting.

Features: V4.16(ABAR.0)C0

Modifications in V4.16(ABAR.0)C0 - 2015/12/28

First release.

Appendix 1. Firmware upgrade / downgrade procedure

The following is the firmware **upgrade** procedure:

1. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
   - Use Browser to login into ZyWALL/USG as administrator.
   - Click Maintenance > File Manager > Configuration File to open the Configuration File Screen. Use the Configuration File screen to backup current configuration file.
   - Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "416ABAR0C0.bin".
   - Click Maintenance > File Manager > Firmware Package to open the Firmware Package Screen. Browser to the location of firmware package and then click Upload. The ZyWALL/USG automatically reboots after a successful upload.
   - After several minutes, the system is successfully upgraded to newest version.

The following is the firmware **downgrade** procedure:

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

Now the system is successfully downgraded to older version.

Note: ZyWALL/USG 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. SNMPv2 private MIBS support

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

1. Have ZyWALL/USG mib files (**416ABAR0C0-enterprise.mib** and **416ABAR0C0-private.mib**) and install to your MIBs application (like MIB-browser). You can see 416ABAR0C0-private.mib (OLD is 1.3.6.1.4.1.890.1.6.22).
2. ZyWALL/USG SNMP is enabled.
3. Using your MIBs application connects to ZyWALL/USG.
4. SNMPv2 private MIBs support three kinds of status in ZyWALL/USG:
    1. CPU usage: Device CPU loading (%)
    2. Memory usage: Device RAM usage (%)
    3. VPNIpsecTotalThroughput: The VPN total throughput (Bytes/s), Total means all packets (Tx + Rx) through VPN.

Appendix 3. Firmware Recovery

In some rare situation(symptom as following), ZyWALL/USG might not boot up successfully after firmware upgrade. The following procedures are the steps to recover firmware to normal condition. Please connect console cable to ZyWALL/USG.

1. Symptom:
   - Booting success but device show error message “can’t get kernel image” while device boot.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
Wrong Image Format for bootm command
ERROR: can't get kernel image!
Start to check file system...
```

   - Device reboot infinitely.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
```

   - Nothing displays after “Press any key to enter debug mode within 3 seconds.” for more than1 minute.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................
```

   - Startup message displays “Invalid Recovery Image”.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................




Invalid Recovery Image

ERROR

EnterDebug Mode

ZW1100>
```

- The message here could be “Invalid Firmware”. However, it is equivalent to “Invalid Recovery Image”.

```
Invalid Firmware!!!

ERROR
```

2. Recover steps
   - Press any key to enter debug mode

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....................................................

EnterDebug Mode

ZW1100>
```

   - Enter atkz –f –l 192.168.1.1 to configure FTP server IP address

```
>
>
>
>
> atkz -f -l 192.168.1.1
```

   - Enter atgof to bring up the FTP server on port 1

```
ZyWALL 1100> atgof

Booting...
```

   - The following information shows the FTP service is up and ready to receive FW

```
Building ...

Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.
```

   - You will use FTP to upload the firmware package. Keep the console session open in order to see when the firmware update finishes.

- Set your computer to use a static IP address from 192.168.1.2 ~ 192.168.1.254. No matter how you have configured the ZyWALL/USG's IP addresses, your computer must use a static IP address in this range to recover the firmware.
- Connect your computer to the ZyWALL/USG's port 1 (the only port that you can use for recovering the firmware).
- Use an FTP client on your computer to connect to the ZyWALL/USG. This example uses the ftp command in the Windows command prompt. The ZyWALL/USG's FTP server IP address for firmware recovery is 192.168.1.1
- Log in without user name (just press enter).
- Set the transfer mode to binary. Use "bin" (or just "bi" in the Windows command prompt).
- Transfer the firmware file from your computer to the ZyWALL/USG (the command is "put 310AAAC0C0.bin" in the Windows command prompt).

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<*>)=-.:. (( Welcome to PureFTPd 1.0.11 )) .:.-=(<*>)=-
220-You are user number 1 of 50 allowed
220-Local time is now 00:00 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put C:\ZLD_FW\310AAAC0C0.bin
```

- Wait for the file transfer to complete.

```
200 PORT command successful
150 Connecting to port 5001
226-944.6 Mbytes free disk space
226-File successfully transferred
226 5.540 seconds (measured here), 9.32 Mbytes per second
ftp: 54141580 bytes sent in 5.55Seconds 9760.52Kbytes/sec.
ftp>
```

- The console session displays "Firmware received" after the FTP file transfer is complete. Then you need to wait while the ZyWALL/USG recovers the firmware (this may take up to 4 minutes).

```
Firmware received ...

[Update Filesystem]
       Updating Code
       ..
```

- The message here might be "ZLD-current received". Actually, it is equivalent to "Firmware received".

```
ZLD-current received ...

[Update Filesystem]
       Updating Code
       ..
```

- The console session displays "done" when the firmware recovery is complete. Then the ZyWALL/USG automatically restarts.

```
.....
.....
.....
.....
.....
.....
.....
       done

[Update Kernel]
       Extracting Kernel Image
       ..
       done
       Writing Kernel Image ... done
Restarting system.
```

- The username prompt displays after the ZyWALL/USG starts up successfully. The firmware recovery process is now complete and the ZyWALL/USG is ready to use.

```
U-Boot 2011.03 (Development build, svnversion: u-boot:422M, exec:exported)
 (Build time: Feb 21 2013 - 10:15:57)


BootModule Version: V1.07 | 02/21/2013 10:45:46
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.
.....
Start to check file system...
/dev/sda3: 33/20480 files (0.0% non-contiguous), 57481/81920 blocks
/dev/sda4: 97/23040 files (1.0% non-contiguous), 7623/92160 blocks
Done

INIT: version 2.86 booting
Initializing Debug Account Authentication Seed (DAAS)... done.
Setting the System Clock using the Hardware Clock as reference...System Cl
ock set. Local time: Tue May 28 08:54:07 GMT 2013

INIT: Entering runlevel: 3
Starting zylog daemon: zylogd zylog starts.
Starting syslog-ng.
Starting ZLD Wrapper Daemon....
Starting uam daemon.
Starting periodic command scheduler: cron.
Start ZyWALL system daemon....
.....
Got LINK_CHANGE
.....
Got LINK_CHANGE
Port [1] Copper is up --> Group [1] is up
.....Applying system configuration file, please
 wait...
no startup-config.conf file, Applying system-default.conf
Use system default configuration file (system-default.conf)
ZyWALL system is configured successfully with system-default.conf

Welcome to ZyWALL 1100

Username:
```

- If one of the following cases occurs, you need to do the “firmware recovery process” again. Note that if the process is done several time but the problem remains, please collect all the console logs and send to ZyXEL/USG for further analysis.
  - One of the following messages appears on console, the process must be performed again ./bin/sh: /etc/zyxel/conf/ZLDconfig: No such file
    Error: no system default configuration file, system configuration stop!!

