ZLD NAT Troubleshooting

Port Forward Rules not working

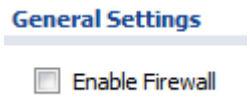
Please use the port forwarding document to verify your rules are correct and that no steps have been left out. [*Link to ZyWALL port forwarding walkthrough*]

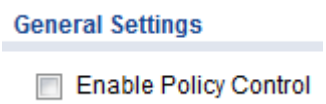
- Is the service accessible locally? If you cannot access the service locally, it will not work from the internet either. Test the service(s) locally (internal network) to make sure the server is replying to the traffic.

- Verify that the port(s) you are attempting to forward are correct. You may need to contact the software manufacturer tech support or visit their website to verify the port number their service/software utilizes. Also, check the IP address of the device to make sure you are forwarding the port traffic to the correct address.

- Disable the ZyXEL device firewall/policy control.

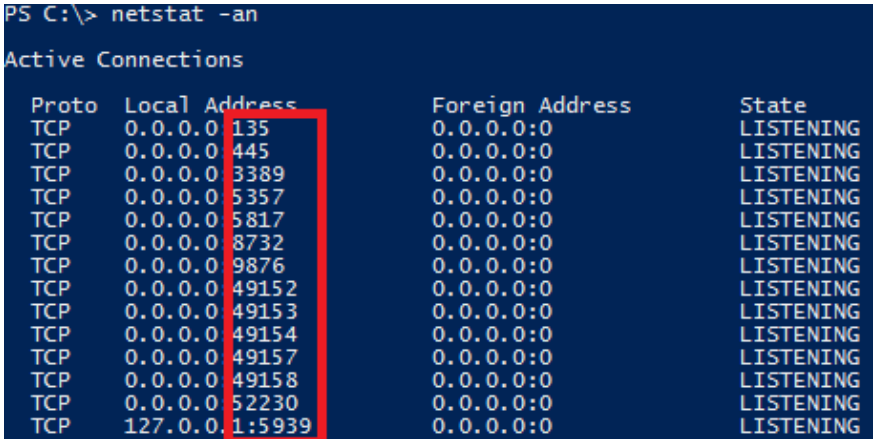
  To disable the device firewall/policy control, go to: **Configuration → Firewall** *OR* **Configuration → Security Policy → Policy Control**





- If you running the services on a Windows, Mac OS X or Linux computer you can use the commands below to get a printout of the ports the system is listening for.

Windows: Open command prompt or PowerShell and type **netstat -an** for a list of listening ports.



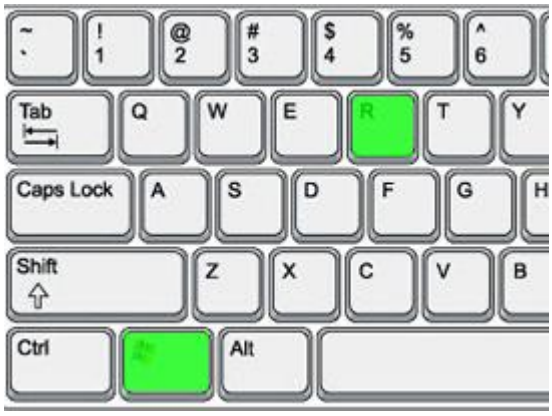
```
PS C:\> netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5817           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8732           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9876           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:52230          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING
```

Linux/Mac OS X: Open terminal and type **sudo lsof -i -n -P** for a printout of the listening ports.

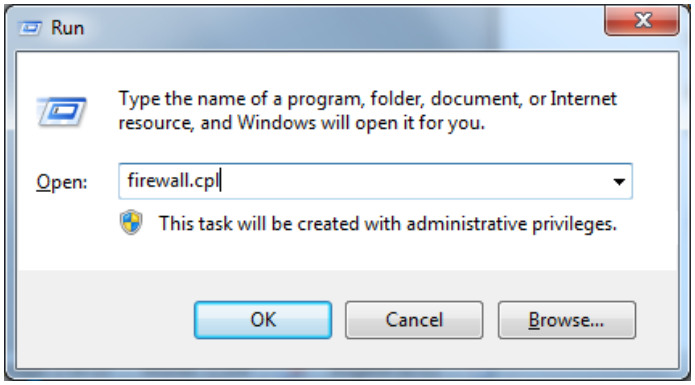
```
bash-3.2# sudo lsof -i -n -P
COMMAND     PID            USER   FD   TYPE             DEVICE SIZE/OFF   NODE NAME
launchd       1            root   23u  IPv4 0x70f4d2d066d1f5       0t0    UDP *:138
launchd       1            root   31u  IPv4 0x70f4d2d066cf9d       0t0    UDP *:137
launchd       1            root   38u  IPv6 0x70f4d2d0c2a1fd       0t0    TCP *:5900 (LISTEN)
launchd       1            root   40u  IPv6 0x70f4d2d0c2a1fd       0t0    TCP *:5900 (LISTEN)
launchd       1            root   41u  IPv4 0x70f4d2d0c3014d       0t0    TCP *:5900 (LISTEN)
launchd       1            root   44u  IPv6 0x70f4d2d0c29cfd       0t0    TCP [::1]:631 (LISTEN)
launchd       1            root   45u  IPv4 0x70f4d2d0c2f87d       0t0    TCP 127.0.0.1:631 (LISTEN)
launchd       1            root   46u  IPv4 0x70f4d2d0c3014d       0t0    TCP *:5900 (LISTEN)
launchd       1            root   51u  IPv4 0x70f4d2d0c2f87d       0t0    TCP 127.0.0.1:631 (LISTEN)
launchd       1            root   52u  IPv6 0x70f4d2d0c29cfd       0t0    TCP [::1]:631 (LISTEN)
```

- Disable the firewall on the computer/device that is running the service(s) to make sure it is not blocking the traffic.

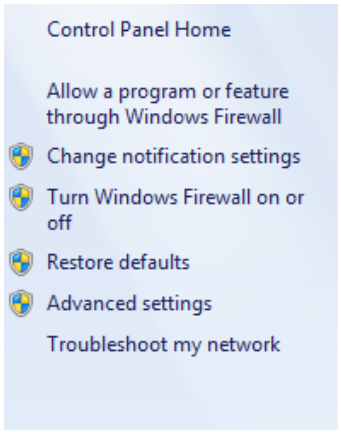
Windows: To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.



Type "firewall.cpl" and click OK or hit the Enter/Return key.

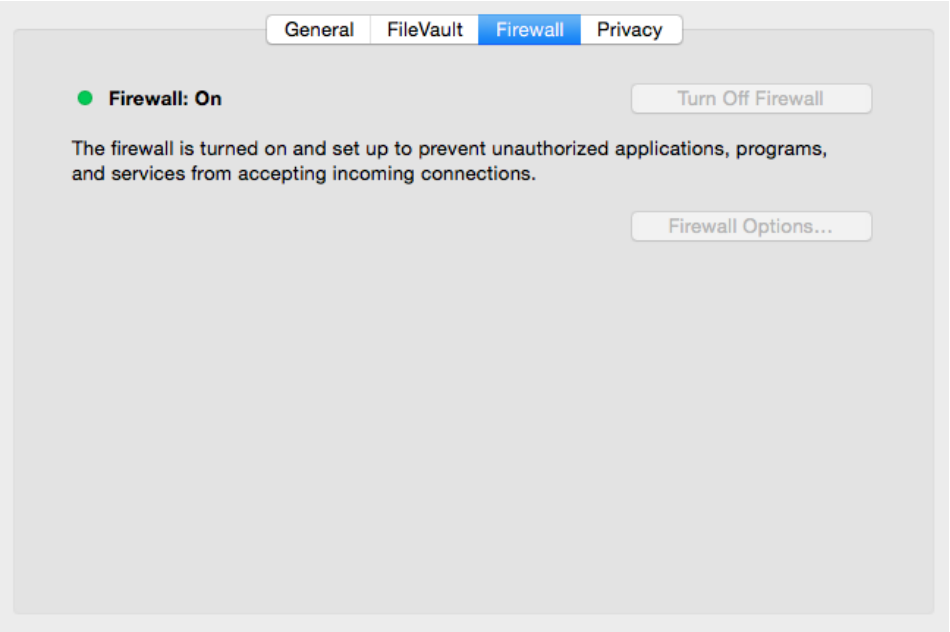


Select the option to "Turn Windows Firewall on or off" on the left. Disable the firewall by selecting the "Turn off Windows Firewall" and click the OK button to save the settings.

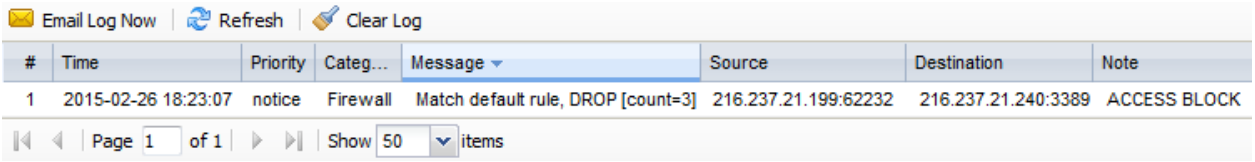


Note: *If you're using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the softwares control panel and disable the firewall feature.*

Mac OS X: To disable the firewall on Mac OS X open **System Preferences → Security & Privacy**, click the Firewall tab and press the "Turn Off Firewall" button to disable.



- Set the firewall rule that was created on the ZyWALL to allow the port traffic through to "LOG ALERT" the traffic. Next check the logs (**Monitor → Logs**) to see if there is any traffic triggered for the port.



The log will will show in the "Message" area what rule is blocking the traffic. In the case for the log entry above, the DEFAULT rule is blocking the RDP TCP:3389 traffic. If the default firewall rule is catching the traffic, this means there is no firewall rule created to allow the traffic through or the incorrect packet direction has been assigned to the firewall rule.

- Make sure the server hosting the service(s) is pointing to the ZyWALL as the default gateway.

- Bypass any other piece of networking equipment (switches, access points, etc.) and connect the server directly to the

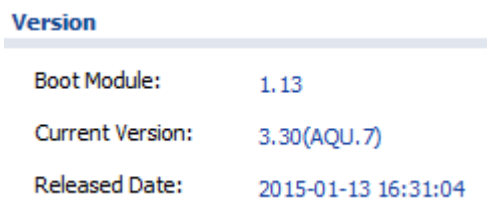
ZyWALL (if possible). This will rule out the devices between the ZyWALL and server from causing the problem.

- Verify the port forwarding rules on the ZyWALL to make sure the port is not being forwarded to different devices. To check the port forwarding (NAT) rules login to the ZyWALL's WebGUI and go to menu **Configuration → Network → NAT**.

- If the logs on the ZyWALL show that traffic is being allowed through, run a packet capture on the server to make sure it is receiving the port traffic and that it is replying to said traffic.

  To run the packet capture you can download and install Wireshark from https://www.wireshark.org/download.html, this tool will scan the packets coming to your computer which you can then look at to verify the port traffic is making its way to the server.

- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**



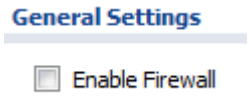
One-to-One NAT not working

Please use the 1:1 NAT document to verify your rules are correct and that no steps have been left out. [*Link to ZyWALL 1:1 NAT walkthrough*]

- Test all public IP addresses to make sure they are routing properly. To do this take each of the addresses and one by one assign them to the ZyWALL's WAN port. Test to make sure you have internet access with the public IP address and with an external client/host make sure you can access the ZyWALL on the public IP. If you cannot access the ZyWALL from the internet will all IP addresses on your public block this is a routing issue on the service end, contact the ISP to fix the routing for the public IPs.

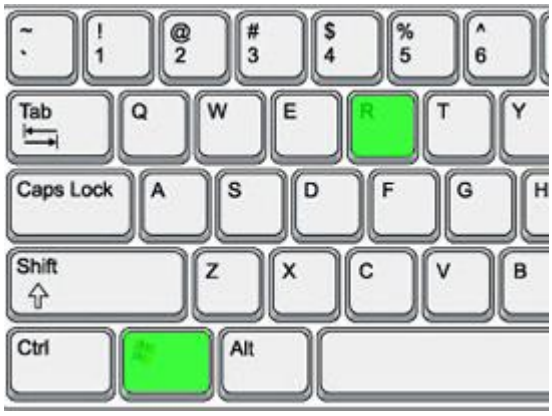
- Disable the ZyWALL's firewall/policy control.

  To disable the ZyWALL's firewall/policy control, go to: **Configuration → Firewall** *OR* **Configuration → Security Policy → Policy Control**

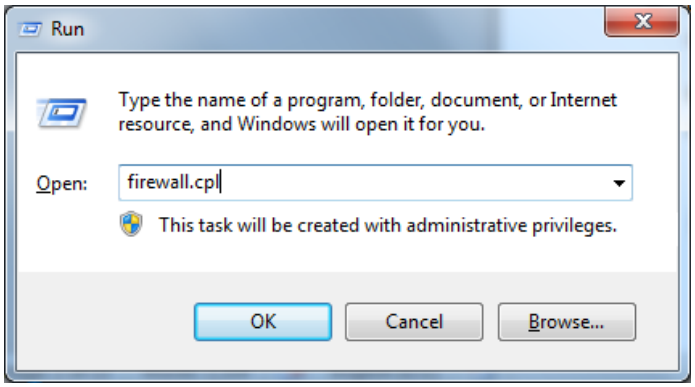


- Disable the firewall (if applicable) on the device you are creating the 1:1 NAT rule for to make sure it is not blocking the traffic.

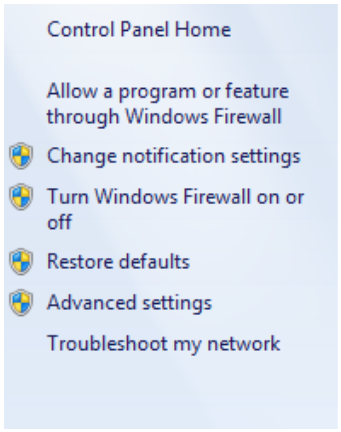
  Windows: To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.



Type "firewall.cpl" and click OK or hit the Enter/Return key.

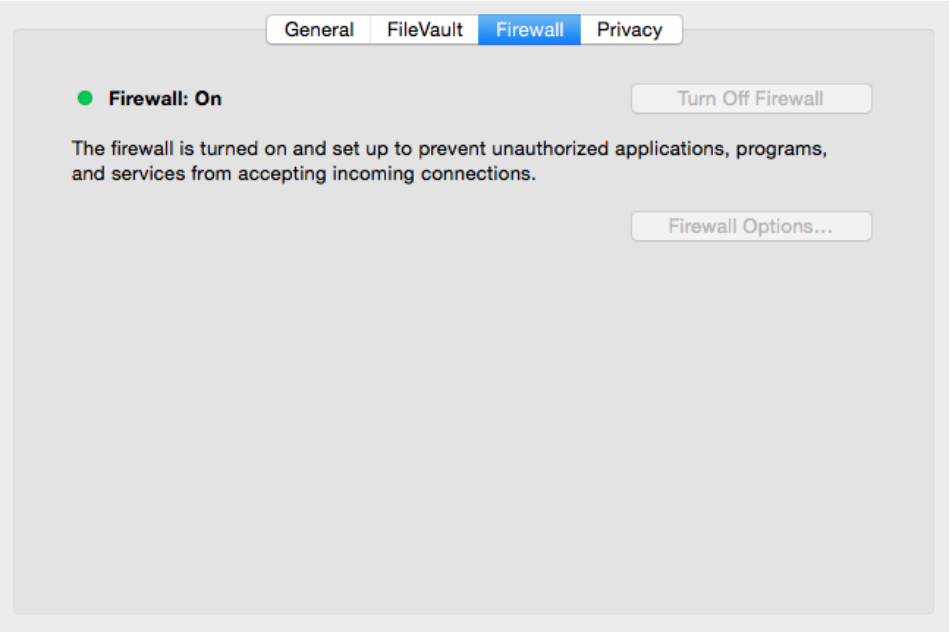


Select the option to "Turn Windows Firewall on or off" on the left. Disable the firewall by selecting the "Turn off Windows Firewall" and click the OK button to save the settings.

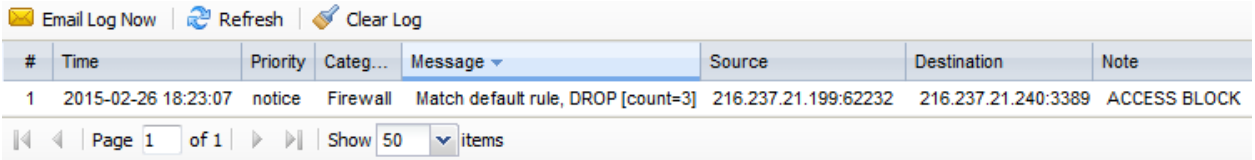


Note: *If you're using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the softwares control panel and disable the firewall feature.*

Mac OS X: To disable the firewall on Mac OS X open **System Preferences → Security & Privacy**, click the Firewall tab and press the "Turn Off Firewall" button to disable.



- Set the firewall rule that was created on the ZyWALL to allow the port traffic through to LOG ALERT the traffic. Next check the logs (**Monitor → Logs**) to see if there is any traffic triggered for the port.



The log will will show in the "Message" area what rule is blocking the traffic. In the case for the log entry above, the DEFAULT rule is blocking the RDP TCP:3389 traffic. If the default firewall rule is catching the traffic, this means there is no firewall rule created to allow the traffic through or the incorrect packet direction has been assigned to the firewall rule.

- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

Version

Boot Module:	1.13
Current Version:	3.30(AQU.7)
Released Date:	2015-01-13 16:31:04

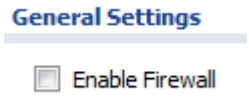
Port Translation now working

Please use the NAT Port Translation document to verify your rules are correct and that no steps have been left out. [*Link to ZyWALL Port Translation walkthrough*]

Note: *The troubleshooting steps provided below are based on walkthrough scenario.*

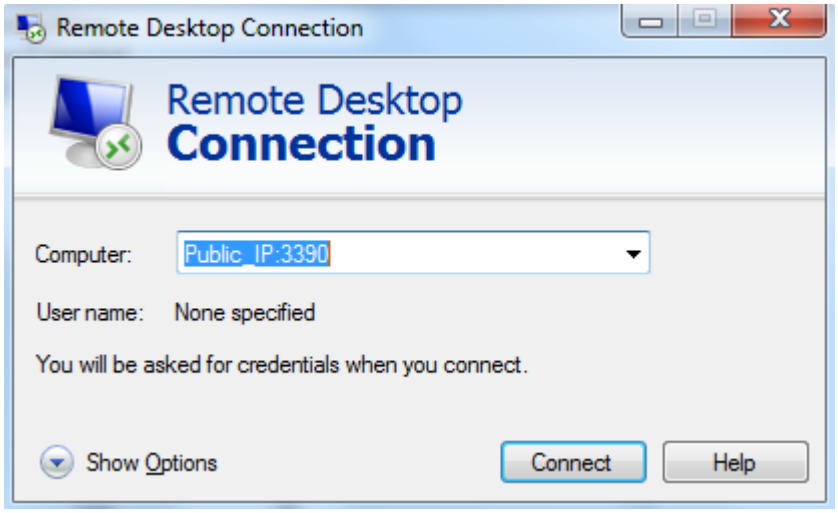
- Make sure you have set the firewall to allow the destination/mapped port through, not the source port. Disable the ZyWALL's firewall/policy control if necessary to make sure it is not blocking the traffic from entering the network.

  To disable the ZyWALL's firewall/policy control, go to: **Configuration → Firewall** *OR* **Configuration → Security Policy → Policy Control**



- Check the NAT (port forwarding) rule to make sure the source/original port is not conflicting with any other rule. To check the port forwarding rules login to the ZyWALL and go to menu, **Configuration → Network → NAT**.

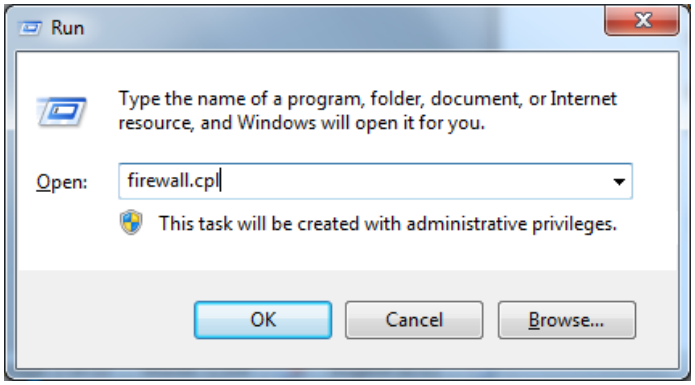
- When attempting to access the service from the internet, make sure you specify which port to use on the client.



- Disable the firewall on the device/computer running the service to make sure it is not blocking the traffic.

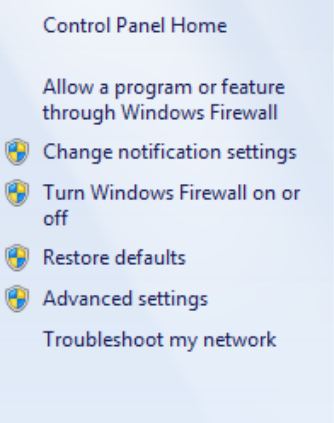
  Windows: To disable the Windows firewall, open a RUN dialog box. You can access this by pressing the Windows + R keys on the keyboard.

Type "firewall.cpl" and click OK or hit the Enter/Return key.



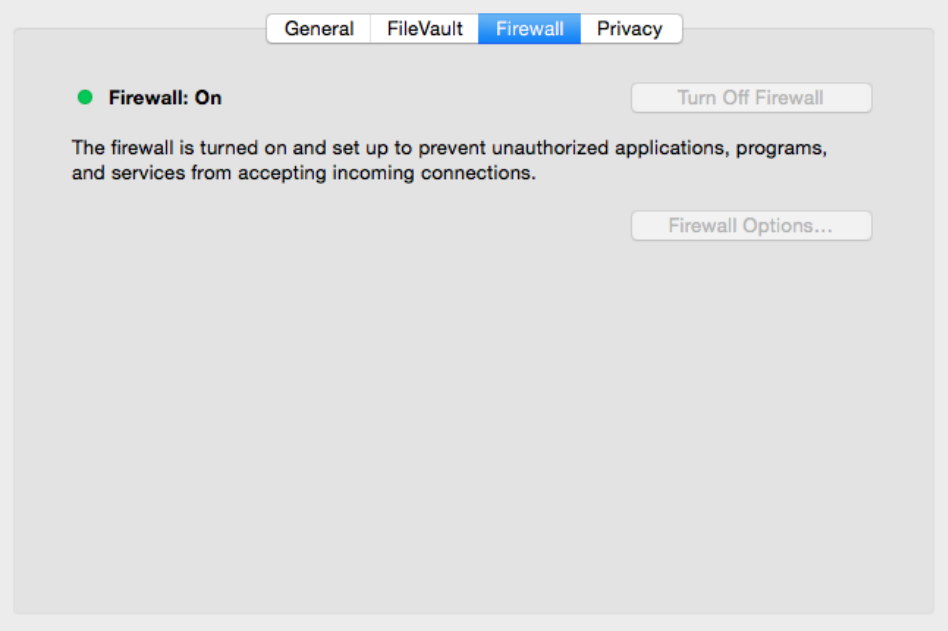
Select the option to "Turn Windows Firewall on or off" on the left.

Disable the firewall by selecting the "Turn off Windows Firewall" and click the OK button to save the settings.



Note: *If you're using a third party software firewall, Trend Micro, Norton, McAfee, etc., please open the softwares control panel and disable the firewall feature.*

Mac OS X: To disable the firewall on Mac OS X open **System Preferences → Security & Privacy**, click the Firewall tab and press the "Turn Off Firewall" button to disable.



- Verify the firmware is up to date and contact tech support for further assistance. To check the current version of firmware on the ZyWALL go to **Maintenance → File Manager → Firmware Package**

Version

Boot Module:	1.13
Current Version:	3.30(AQU.7)
Released Date:	2015-01-13 16:31:04