

SonicWALL Tech Support FAQ

- Q. When attempting to connect to SonicWALL for initial configuration, the Web browser displays "Host not responding" errors. How is this corrected?**
- A. Make sure to set the IP address of the computer being used for initial configuration to the same subnet address of the SonicWALL. During initial configuration, it is suggested that this address be 192.168.168.200 with a Subnet Mask of 255.255.255.0. If smart hubs or switches are on the LAN, they could be interfering with the connection. In this case, use the supplied crossover cable to connect the LAN port of SonicWALL directly to the Management Station.
- Q. Once SonicWALL is installed, is it necessary to change the IP settings of each node on the network?**
- A. No, SonicWALL is installed between the router and LAN and configures itself to intercept and pass traffic destined for the Internet router. No client configuration is required, unlike for proxy servers (see below).
- Q. A proxy server firewall was removed when SonicWALL was installed. Now clients on the LAN are unable to access any Internet services. What is going wrong?**
- A. Proxy servers require the client software be configured to connect to the proxy, breaking the basic client-server model of the Internet. To allow client access to the Internet without the proxy, disable the proxy setting in each client application.
- Q. Users on the LAN are unable to reach the Internet after installing SonicWALL. The Internet connection was working fine before SonicWALL was installed. What is wrong?**
- A. Make sure to restart the Internet router after installing SonicWALL. This is especially important if NAT is enabled. If that doesn't solve the problem, check the Status page of the Web Management Interface for error messages and correct any errors listed in red text.
- Q. Why aren't changes made to the SonicWALL configuration in the Management screens retained?**
- A. The most likely cause is a bug in the browser's implementation of Java or JavaScript. Netscape Navigator 3.0 or newer is recommended for all management functions. It is also possible that the browser is displaying cached pages, which may be resolved by clicking the browser's Reload button.
- Q. SonicWALL is managed fine from any computer in the Accounting department, but not from a computer in Sales. What is the reason for this?**
- A. The most likely cause for this is a safety feature built into SonicWALL. Management is only possible from computers that are connected to the LAN port - in other words, only computers that are protected by SonicWALL have access to its management function.

In a company with multiple routers, or one in which the SonicWALL is being used to protect one segment of a LAN from another, the management function cannot be accessed from outside the protected LAN. The reason for this is that it would not be advisable to let someone on an unprotected segment of a network, such as the Internet, to have access to SonicWALL's administration. Therefore, computers connected via SonicWALL's WAN or DMZ ports are not permitted to manage the firewall.

Q. Why can't the name of the administrator account be changed? Isn't this potentially dangerous? A hacker that is trying to break in to the firewall will already know the account name because it can't be changed.

A. No. Even if a hacker knows the administrator's password and login name, access to the management functions are not allowed from the Internet (WAN port). A hacker trying to access the SonicWALL from a remote location will not be able to access or modify its management functions.

Q. The administrator's password was lost. How is access to the unit restored?

A. The following procedure will erase all settings and revert the unit to the factory default state. It will be necessary to follow the Initial Configuration procedures detailed in the manual's QuickStart section to reconfigure the SonicWALL.

1. Unplug the SonicWALL from power and the network.
2. Open the SonicWALL unit by unscrewing the two screws on the bottom and gently pull the top cover off (the front and back panels remain in place). You will see a blue button towards the front between the Power/Test, and WAN LEDs.
3. Push and hold down the blue button and then plug the SonicWALL power in. Hold down the blue button until the "Test" LED starts to flash. You can then let go of the blue button.
4. Reassemble the case.
5. It will be necessary to upload new firmware to the SonicWALL and reconfigure as outlined in the QuickStart section of the SonicWALL manual.

Q. How does SonicWALL for 10 nodes keep track of which ten machines are allowed through?

A. SonicWALL remembers the IP addresses of the first ten computers to access the Internet. These computers are allowed through (or, in the case of SonicWALL/50, the first fifty computers). Note that even though a limited number of computers are allowed access through the SonicWALL, all nodes on the LAN are protected from

hackers and attacks. Restarting the SonicWALL resets the list of IP addresses allowed through.

Q. Which machines should be put on the DMZ?

A. Any computer that users on the Internet will access should be placed on the DMZ. This would include publicly accessible Web, FTP, DNS, and E-mail servers.

Q. Can IP addresses from the private address range be used for machines on the DMZ if NAT is enabled?

A. No. Only valid IP addresses may be used on the DMZ. If addresses from the private range are used, access to that host from the Internet will not be possible.

Q. Can machines on the DMZ be accessed from the LAN using AppleTalk or IPX?

A. No. SonicWALL is an IP firewall and blocks all non-IP traffic. This includes AppleTalk and IPX.

Q. Ever since SonicWALL was installed, E-mail from the Internet is not being received. Other Internet services, including sending mail, are working fine. What is wrong?

A. Make sure to put the Internet E-mail server on the DMZ or create a Public LAN Server for the SMTP protocol. The reason for this is that when a message is sent, the E-mail server sending the message logs onto the recipient's E-mail server to transfer the message. If the recipient's E-mail server is behind a firewall, the sending server will be unable to log in to send the message.

Q. What is NAT and how does it work?

A. Short for Network Address Translation, NAT is an Internet standard that enables a local-area network (LAN) to use "private" or "invalid" IP addresses for LAN nodes. This range of private IP addresses are then translated to a single, valid IP address which is visible to the Internet. A NAT box such as SonicWALL is located where the LAN meets the Internet and makes all necessary IP address translations by maintaining a table of internal IP addresses and associated TCP/IP activity. Since only a single IP address is visible to the outside world, all LAN activity seems to originate from a single computer.

Q. How does SonicWALL support Public LAN servers if NAT is enabled?

A. SonicWALL may be configured to allow access from the Internet to specific machines on the private LAN, called "Public LAN Servers". For example, access to a company's inventory database may be allowed so suppliers can track inventory levels to maintain JIT ("Just In Time") delivery schedules. By utilizing a service called "plug-to", SonicWALL is able to support Public LAN Servers with NAT enabled. A plug-to directs all network traffic received by SonicWALL over a specified IP port to a host on the LAN configured as the Public LAN Server for that IP port. For example, if a Public LAN Server for port 80 (Web) is created, all Web connections that are directed at SonicWALL's Public NAT Address would be

forwarded to, and served by, the internal host configured as a Public LAN Server for port 80.

Q. Why isn't authenticated remote access allowed if NAT is enabled?

- A. NAT maps all IP addresses on the LAN to a single public IP address that is available to the Internet. From the Internet, all computers on the LAN are hidden behind this public IP address, making connecting to the desired IP address impossible. This is true with SonicWALL as well as any other NAT device.

Q. SonicWALL is blocking access to Web sites that should not be on the CyberNOT list. Why does this happen and how is it resolved?

- A. If a site is erroneously blocked by the CyberNOT list, the administrator may grant access to the site by adding it to the "Trusted Domains" list. To do this, log into the SonicWALL Web Management Interface and click the Filter button. Next, click the Customize tab and add the site to the "Trusted Domains" list.

Sites may be erroneously blocked for two reasons.

In some cases, a site is blocked because the ISP has located it on a server that also contains objectionable sites. To avoid this, many ISPs set up servers that are specially designated not to contain objectionable material.

Occasionally, the organization that maintains the CyberNOT list accidentally adds a site to the list that should not be blocked.

Please report all errors in the CyberNOT filter list to Sonic at [<listerrors@sonicsys.com>](mailto:listerrors@sonicsys.com). It will be helpful to also include the log entry showing why the site was blocked. Sonic will work with the organization that maintains the CyberNOT list to resolve the issue.

Q. Why do connections to servers often close after a period of inactivity?

- A. If a connection to a server outside the LAN remains idle for more than five minutes, the SonicWALL closes the connection. This is done for security purposes. Without this timeout, it is possible that connections could stay open indefinitely, creating potential security holes.

Q. After downloading the firmware file on a Macintosh, Stuffit reports errors when trying to decode the file.

- A. The ".bin" file extension of the firmware file denotes binary, not Macbinary. The firmware file does not need to be decoded or decompressed. Upload it as-is to the SonicWALL.

Q. Can a user customize IP addresses behind the firewall to block only certain IP addresses from gaining access to the Internet?

A. SonicWALL does not block LAN users from accessing the Internet. It only restricts access to certain Web sites (and Newsgroups). Users can be given a password to allow them to bypass the filter.

Q. Can a user define certain protocols, like FTP, from entering the LAN, like a proxy server?

A. There is no need to 'define' protocols. By default, SonicWALL blocks all protocols that originate from the Internet, and all that originate from the LAN are allowed. SonicWALL may not be configured to allow only certain protocols to access the Internet. That is a function supported by proxy servers which leads to complexity.

Q. Ever since all servers were moved to the DMZ, users have been reporting network problems. People are complaining that they no longer have access to the Internet or even company-wide E-mail. What is wrong?

A. If a DHCP server is being used on the LAN, and this server is moved to the DMZ, then this type of problem could result. To fix this problem, the DHCP server should be placed on the internal LAN, either by moving the DHCP server back to the LAN or by using the DHCP server built into SonicWALL.

Some E-mail servers use an optional "Finger" mechanism to alert users when new E-mail arrives. These do not work when the E-mail server is on the DMZ because all connections that originate from the DMZ, including Finger, are blocked by SonicWALL.

If the E-mail server is Microsoft Exchange it should be placed on LAN and set up as a Public LAN server for best results. This procedure is detailed at <http://www.sonicsys.com/support/faq/tn-msExchange.html>

Users will be unable to access non-IP resources on the DMZ, such as IPX or AppleTalk file servers, because SonicWALL blocks all non-IP traffic.