

“I Cannot Connect to the Internet”

Version 1.0 – February 15, 2008
Cisco ASA 5505 Firewall

A guide to help identify and resolve problems connecting to the Internet in local Church facilities

How to use this guide

This document will lead you through several tests. As you perform each test, record your results on the Troubleshooting Log, the last page of this document. This log will be very helpful if you require additional help from a technician.

Symbols used in this guide

-  Step number
-  Working example
-  Non-working example
-  Information to record
-  Action to take

The Church of Jesus Christ of Latter-day Saints

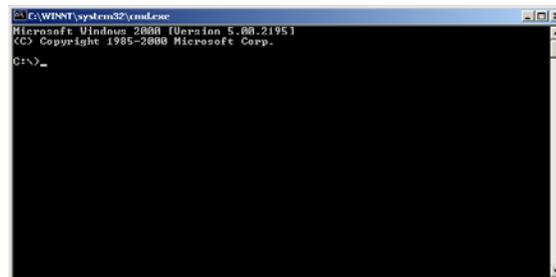
1 Does your computer have a valid IP address?

A. Open a command prompt window.

Go to **Start > Run...** and then type **command** and click **OK** (see example below).



Example in Windows NT/2000/XP



Example of a command prompt

B. Renew the IP address.

- Windows 2000/XP/NT: In the command prompt, type **ipconfig /renew**
- Windows 9x/ME: In the command prompt, type **ipconfig /renew_all**

C. Find your Troubleshooting Log and enter the numbers listed:

- IP address (your computer)
- Default gateway (firewall's IP address)

D. Compare your results with the two examples below. Which one most resembles your setup?

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix. . . : ea.ldsglobal.net
    IP Address. . . . . : 10.128.75.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.128.75.1

C:\>
```

 This looks like a PC with a valid IP address.

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix. . . :
    Autoconfiguration IP Address. . . . : 169.254.49.151
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :

C:\>
```

 This shows an auto-configured IP address, which means there are problems with the connection from the PC to the firewall.

E. Repeat this step on a different computer.

If you get a valid address on the other computer but it cannot connect to the Internet, **go to step 2**.

If the other computer can connect to the Internet, **go to step 10**.

E. Reboot your computer and try again.

If you still see an auto-configured address, try this test on another computer connected to this network.

If the other computer has the same problem, **go to step 6**.

2 Can you ping the firewall?

In step 1 you found the IP address for the computer and the default gateway (the firewall). Use the IP address for the default gateway to do a ping test.



A. Ping the firewall.

At the command prompt, type **ping x.x.x.x** (where x.x.x.x is the default gateway IP address) and press **Enter**.

In the example below we use 10.128.75.1 as the IP address of the default gateway.



B. Record the packet loss in the Troubleshooting Log.

The packet loss is the percentage of packets that did not come back. It is shown after the test runs in parentheses (see example below).



C. Compare the ping results and the packet loss with the two examples below. Which one most resembles your setup?

```
C:\>ping 10.128.75.1

Pinging 10.128.75.1 with 32 bytes of data:

Reply from 10.128.75.1: bytes=32 time<10ms TTL=255

Ping statistics for 10.228.75.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms

C:\>
```

```
C:\>ping 10.128.75.1

Pinging 192.168.75.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.128.75.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



The firewall is replying. This shows that the connection from the computer to the firewall is working.



The firewall is **not** replying. The connection from the computer to the firewall is **not** working.



If you can ping the firewall, **go to step 3**.

If you cannot ping the firewall, **go to step 6**.

3 Is the name server working properly?

If you are not running Windows NT, Windows 2000, or Windows XP, skip to step 4.



A. Try to retrieve an IP address with the name server.

At the command prompt, type **nslookup www.google.com** and press **Enter**.



B. Record the name server's IP address and Google's IP address in the Troubleshooting Log.

The name server's IP is the first IP address. If your computer can find the name server, it will show IP addresses for Google below that (see examples below).



C. Compare your results with the two examples below. Do you see Google's IP addresses?

```
C:\>nslookup www.google.com
Server:  ns1.intellectualreserveinc.org
Address:  216.49.176.201

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  66.102.7.99, 66.233.167.147
Aliases:  www.google.com

C:\>
```



The name server is replying. This means that the connection from the computer to the name server is working. Some of Google's IP addresses are listed here (for example, 66.102.7.99). These numbers may be different than the ones you see, but if you get numbers, the name server is connected and working properly.

```
C:\>nslookup www.google.com
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address
216.49.176.201: Timed out
Server:  Unknown
Address:  216.49.176.201

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to Unknown timed-out

C:\>
```



The name server is **not** replying. The connection from the computer to the name server is **not** working.

The name server's IP address is displayed as 216.49.176.201, but notice that it displays "Server: Unknown" and the requests are timing out.



If you can ping the name server, **go to step 4**.

If you cannot ping the name server, **go to step 4**.

4 Can you ping www.google.com?



A. Try to ping Google.

At the command prompt, type **ping www.google.com** and press **Enter**.



B. Record the packet loss in the Troubleshooting Log.

See step 2 for more information about packet loss.



C. Compare your results with the two examples below. Is Google replying to the ping?

```
C:\>ping www.google.com

Pinging www.google.org [66.102.7.99] with 32 bytes of
data:

Reply from 66.102.7.147: bytes=32 time=151ms TTL=122
Reply from 66.102.7.147: bytes=32 time=150ms TTL=122
Reply from 66.102.7.147: bytes=32 time=151ms TTL=122
Reply from 66.102.7.147: bytes=32 time=160ms TTL=122

Ping statistics for 66.102.7.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 150ms, Maximum = 160ms, Average = 153ms

C:\>
```

```
C:\>ping www.google.com

Pinging www.google.org [66.102.7.99] with 32 bytes of
data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.128.75.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



The name server is working to give you Google's IP address. Google is responding and there is no packet loss.



Google's IP address was found but it is not responding to pings (100% packet loss).



If you can ping **www.google.com**, **go to step 5**.

If Google does not reply to pings, **go to step 9**.

5 Can you view pages on www.lds.org?



A. Open Internet Explorer.

Use the shortcut on your desktop or in the Quick Launch bar to open Internet Explorer.



B. Direct Internet Explorer to LDS.org.

In the address bar, type www.lds.org



C. Browse through a few pages on LDS.org.

If the home page of LDS.org comes up, click on a few links to ensure that Internet Explorer is not displaying cached Web pages.



D. Record the results in the Troubleshooting Log.

Were you able to see pages on LDS.org?



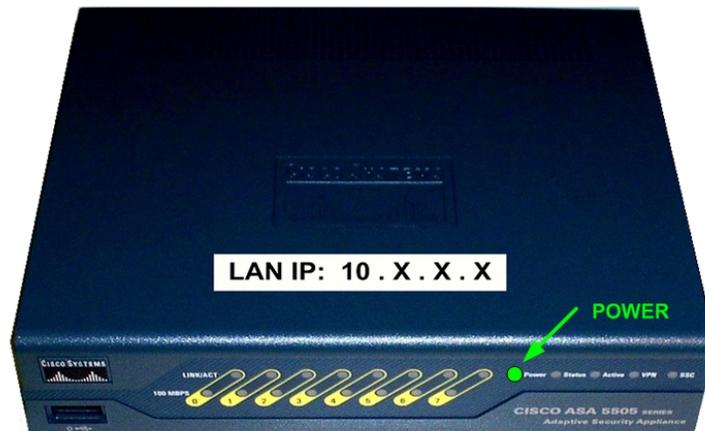
Go to step 10.

6 Does the firewall have power?



A. Locate the firewall (Cisco ASA 5505).

It should look like the picture below. It is a little bigger than a typical copy of the Book of Mormon. If it is in a locked cabinet and you don't have access, contact the local facility manager or facility representative before proceeding.



Picture courtesy of Cisco Systems, Inc. Unauthorized use not permitted.



B. Check the power light.

Verify that the “Power” light is lit green to confirm that the firewall is on.



C. Record the status of the power light in the Troubleshooting Log.



😊 If the power light is green, then the firewall is powered on.



☹️ If the power light is off, check to see that the power cord is connecting the firewall to the outlet and that the outlet has power.

Contact the facility manager or facility representative if the outlet does not have power. Once this is fixed, if the firewall can be turned on, check to see if you can connect to the Internet. If you still cannot connect, repeat the tests in this guide from step 1.



If the power light is on, go to step 7.

If you have power to the outlet but the firewall's power light remains off, go to step 10.

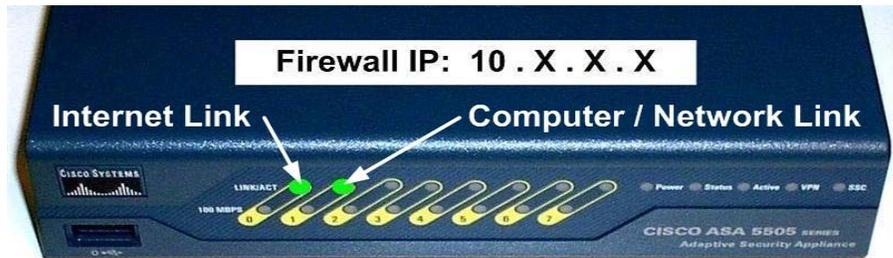
7 Is the firewall connected to your network?



A. Check the link lights.

Verify that one or more of the link lights (top row of lights on the firewall above the labels 1-7) are on. There should be a light for every cable plugged in to the ports 1-7.

Cisco ASA 5505 Firewall
(Front View)



Port 1 is active and is connected to a computer or network device.

Picture courtesy of Cisco Systems, Inc. Unauthorized use not permitted.



B. Record which link lights are on in the Troubleshooting Log.



 If at least one of the four link lights is on, go to step 8.



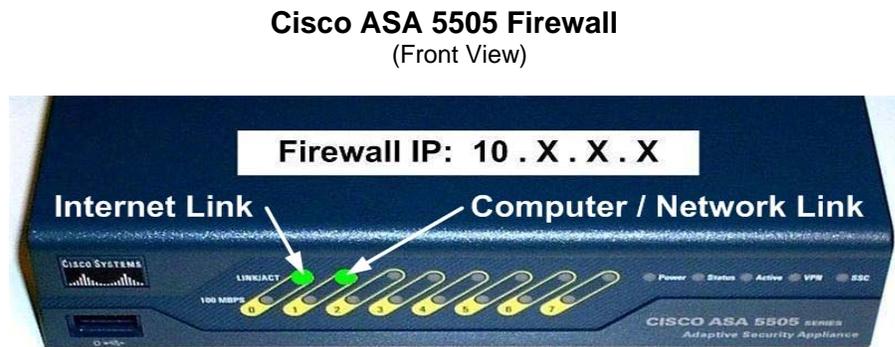
If no link lights are on, verify that there are cables connected to at least one of the slots labeled 1, 2, 3, 5, 6, or 7 on the back of the firewall.

Unplug and reconnect each cable into its slot.

8 Is the firewall connected to the broadband modem?

A. Check the Internet link light.

Verify that the green light above the “0” label is on.



Port 0 is active and has a connection to the ISP router or modem.

Picture courtesy of Cisco Systems, Inc. Unauthorized use not permitted.



B. Record whether the Internet link light is on in the Troubleshooting Log.



 If the Internet link light is on,
go to **step 9**.



If the Internet link light is not on, check the cable connecting the firewall to the broadband router or modem that your Internet service provider (ISP) provided. This should be connected to the port on the back of the firewall labeled with a “0.”

Modem sizes vary, but the modem is probably about the same size as the firewall.

Disconnect the cable on each device and reconnect it.

If the link light above the “0” label on the firewall does not turn on, go to **step 9**.

9 Does the broadband modem have power?



A. Check the power cord on the broadband modem.

Check the power cord from the broadband modem to the power outlet. Verify that it is well connected and has power. The broadband modem should have some lights on the front that are either on or flashing.



B. Record whether the broadband modem has power in the Troubleshooting Log.



 If the broadband modem does have power, unplug the power and then plug it back in. Wait a few minutes and then unplug the firewall and plug it back in. Wait a few more minutes, and then try to connect to a Web page on the Internet.

Check to see if the proper lights (described in step ) come on. If they come on, verify that your Internet connection is now working by going back to step  and repeating just that one step.

If you are still unable to connect to the Internet, go to step .



If the broadband modem does not have power, work with the facility manager or facility representative to verify that the outlets have power.

If the outlets have power but the broadband modem doesn't power on, go to step .

10 ISP Information?



A. Work with the appropriate support organization.

For problems with local Church unit connections, contact your stake or district technology specialist. If you don't know who that is, consult your stake or district president.

The stake or district technology specialist should contact the Internet service provider (ISP) to have them check service availability or ISP hardware failure.

If the ISP indicates that all the services are up and available, contact the Global Service Center (see  "Contact support" below).



B. Record all the information in the Troubleshooting Log.

Please be sure to know your ISP information and record it in the troubleshooting log at the end of this guide (last page). The Global Service Center can assist you better with the ISP information.



Contact support.



A. Open a service ticket.

If the problem is with a local Church unit connection, the stake technology specialist or equivalent person should contact the Global Service Center.

- +1-866-678-2763 (North America)
- +800-2950-2950 (Europe and Africa)

NOTE: If you cannot dial one of these numbers, please phone your area office and have them transfer your call to the Global Service Center.



B. Record your ticket number in the Troubleshooting Log.

Reminder: Every issue that is opened with the Global Service Center is assigned a ticket number to keep details of the problem and what has been done to try and resolve it. You should refer to the ticket number whenever you discuss details of this issue with technical support so they can better assist you.

Troubleshooting Log

Please record your results in this log as you follow the test procedures. Have this information available if you need to contact technical support.

1	Does your computer have a valid IP address?	Host IP address:	
		Firewall IP address:	
2	Can you ping the firewall?	Packet loss (%):	
3	Is the name server working properly?	Name server address:	
		Google's address:	
4	Can you ping www.google.com?	Packet loss:	
5	Can you view pages on www.lds.org?	Circle one:	Yes No
6	Does the firewall have power?	Circle one:	Yes No
7	Is the firewall connected to your network?	Circle one:	Yes No
8	Is the firewall connected to the broadband modem?	Circle one:	Yes No
9	Does the broadband modem have power?	Circle one:	Yes No
10	Name of ISP: ISP phone number: ISP customer account number: Name of customer on the ISP bill:		
	Contact support.	Ticket number:	