

Firewall Configuration Guidelines

If your connection to the Internet utilizes a firewall, several ports will have to be opened to allow your Net2Phone Max gateway to make and receive calls to other Net2Phone devices.

UDP Port 6801 must be opened. The following port types/ranges must also be opened (the numbers displayed are the default start points for each):

1. UDP Port (OPAL) 7000
2. TCP Port 4000
3. UDP Port 21000

The table below explains the procedure for opening firewall ports for your Max gateway. This example illustrates the UDP Port (OPAL) assignments (with a default start point of 7000) for an 8-port Max gateway.

Max Port #	Firewall Port Type	Firewall Port Numbers
1	UDP Port (OPAL)	7000 - 7001
2	UDP Port (OPAL)	7002 - 7003
3	UDP Port (OPAL)	7004 - 7005
4	UDP Port (OPAL)	7006 - 7007
5	UDP Port (OPAL)	7008 - 7009
6	UDP Port (OPAL)	7010 - 7011
7	UDP Port (OPAL)	7012 - 7013
8	UDP Port (OPAL)	7014 - 7015

In this example, the range to be opened is 7000 to 7015. The range is determined by the following formula:

$$\text{Max Default Start Port} + (\text{Number of Max Ports} * 2) - 1$$

or in this example:

$$7000 + (8 * 2) - 1 = 7015$$

The table shows the firewall port assignments based on the default start port. If the Max gateway default start ports noted above are in conflict with your corporate firewall settings, you may assign port numbers in the range of 4000 to 65000 by applying the same principle illustrated in the table.

The TCP Port and UDP Port start parameters in the Network Configuration table must match the open firewall ports.

If there are multiple Max gateways behind a firewall, this process must be repeated for each unit, using different UDP ports & TCP ports.

NOTE: The Net2Phone Max gateway will not work behind a proxy server.

Firewall FAQs

Question: What is the firewall and NAT?

Answer: A *firewall* is a security feature that protects the corporate network from intruders, such as hackers, by blocking ports that connect to the Internet on the corporate data network.

NAT stands for **Network Address Translator**, which it is a function of a router in the corporate data network.

Firewalls and NATs are two different types of network elements, however, they are often combined.

Some advanced devices, such as Checkpoint or PIX, have various standard protocol profiles built in, allowing an administrator to easily enable a protocol with a single click of a checkbox or a CLI (Command Line Interface) invocation.

The Net2Phone protocol works with most NAT implementations. It may not work with symmetric NATs. We are still studying those scenarios to better understand them.

Question: How can we make MAX work when there is a firewall?

Answer: In order for Net2Phone devices such as MAX (or any protocol/service) to work with a firewall, it must allow various packet types to flow. This is true for proxy-type firewalls and packet-inspecting firewalls.

Net2Phone corporate uses a Cisco PIX firewall. This firewall is *packet-inspecting* (it can look deep into the packet contents and act upon them) and creates tunnels like a proxy firewall.

A *proxy firewall*, which does not allow transparent network access to applications, will probably cause problems. These are extremely rare (I only knew of them in AT&T corporate). In situations with this type of security implemented, you must coordinate the installation of a VoIP gateway with the network security administrators.

Question: What types of packets are the firewall ports required to open for the MAX to work?

Answer: There are three key packet flows which are required for Net2Phone outbound phone calls to work and two packet flows for Net2Phone presence (inbound calls) to work:

A) Phone Calls (regular PC to Phone, PC-PC calls)

- 1) *Service Location:* UDP Packets are sent to call1.net2phone.com and call2.net2phone.com. The firewall or NAT must allow response packets from these servers to return to the MAX (a dedicated port; 6801).
- 2) *Call Signaling:* Outbound TCP connections are made to a call controller in the net2phone.com network address space. Typically, firewalls allow "inside the firewall" clients to make outbound TCP connections.
- 3) *Voice:* UDP Packets are sent to a net2phone.com gateway. UDP Packets are also received from a net2phone.com gateway. The firewall or NAT must allow packets to flow both ways.

B) Presence (Inbound Calls such as DID)

- 1) *Service Location:* UDP Packets are sent to call1.net2phone.com and call2.net2phone.com. The firewall or NAT must allow response packets from these servers to return to the MAX.
- 2) *Online Presence:* UDP Packets are sent to a net2phone.com presence server. The firewall or NAT must allow response packets from this server to return to the MAX. Packets are sent at regular intervals to allow a tunnel to be created and kept open.

Question: If we open these firewall ports to allow the MAX to work, is it safe from a corporate security point of view?

Answer: The ports mentioned above, which are required to be open for the MAX to work in the corporate environment, are not in danger from hackers unless the PC processes using ports above 1023. Ports 1024 and below must be blocked behind the corporate firewall.

Please note that although UDP is safer than TCP with respect to hackers, it still has potential weaknesses. Since the MAX requires opening port numbers well above 1024, in the range of 4000~65000, it is okay to ask the firewall administrator to open those ports without being concerned about security.

Question: What if the corporate firewall administrator does not want to open any ports due to the company policy?

Answer: *Option 1:* You may suggest that they use a static IP address. Some firewalls let the computers with designated IP address operate freely. But the simplest alternative solution is to lease a dedicated Internet connection line for VoIP purposes only. (128 kbps = 8 calls, 256kbps = 16 calls, 384kbps = 24 calls, 512 kbps = 30 calls)

Option 2: You may set up a separate Cisco 2600 router or any other router on the corporate network and configure it to open the ports required for MAX products only to operate with pre-assigned dedicated port numbers.

Option 3: Set up a Linux computer on the corporate network and configure all MAX products behind the Linux server.

Question: Are there known firewall routers that work well with MAX products?

Answer: Yes, the NetGear FVS318 router works well.