



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

TID: Technical Information Document
“Network Firewall Rules for NTS version 7”
Date: April 28, 2008

NTS version 7 supports the same features as earlier NTS versions; however, NTS-7 has a new and improved video/audio module. This TID will discuss the firewall rules for deploying NTS-7 software within an organization.

Background

It should be understood that NTS is a client-server product, and there are two distinct NTS server modules.

- NTS server module 1: The “base” NTS client login module.
- NTS server module 2: The video/audio NTS server module.

The “base” NTS client login supports many features, including (a) TTY access for the entire organization for both incoming and outgoing TTY calls, (b) text chat and text instant messaging within the organization, (c) Message Notification Services, and so on. The “base” NTS client login also lets a administrator within the organization view and configure operation within the NTS system.

The video/audio client-server module allows video and audio calls between PCs, as well video/audio calls between PCs and standard H.323 video devices.

When evaluating firewall rules for NTS within an organization, the location of the two servers above must be understood in the design. One organization might wish to run the “base” NTS system without video/audio links at all, while another may wish to run only a simplified NTS video/audio only client. A third organization may wish to support both the “base”, and the video/audio, links. Additionally, a given organization may wish to be fully “hosted”, where the organization does not maintain its own NTS servers, while another organization may wish to place the “base” NTS server, and/or the video/audio server module, on-premise. The decisions or preferences above will affect the firewall rules required for NTS operation.

The six most common scenarios will be described below, along with the firewall rules needed for each.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

Scenario #1: The organization is fully “hosted” by off-premise NTS servers, and both video/audio and “base” operations are desired.

Firewall rules needed for Scenario #1:

Firewall Rule #1 for the base NTS client login:

“Outbound port 2591 (TCP only) to the IP address
“nts7.nextalk.net”.

- Note: Redundant port 2591 servers exist at nts72.nextalk.net and nts73.nextalk.net.

Firewall Rule #2 for video and audio links:

“Outbound port 1853 (TCP and UDP) to the five IP addresses starting with “video.nextalk.net” (75.125.90.242 to 75.125.90.246).

Notes:

- For video communications, the above port (1853) is needed as an outbound connection. The 2-way video stream needed uses an “established port” notion where the initial communication is established outbound from within the organization to the video.nextalk.net address. The firewall should then allow reply packets (TCP and UDP) to come back on the established port(s).
- The five IP addresses starting with video.nextalk.net (75.125.90.242 to 75.125.90.246) on just one port will allow the PC within the organization to set up a video/audio call with outside H.323 video devices or remote NTS-7 systems, users, and video interpreters.

Scenario #2: The organization is fully hosted (no on-premise NTS servers), and desires only video/audio links.

In Scenario #2, Firewall Rule #2 above is needed, but Firewall Rule #1 is not needed.

Note: Scenario #2 is common for organizations using NTS for VRI (Video Remote Interpreting) services. In Scenario #2 the users within the organization typically access NTS/VRI services from a browser or simplified video/audio-only application. The resulting video/audio link to an off-site interpreter supports sign-language, and foreign-language, translation services for the organization. Only the 1853 TCP/UDP port above is needed across the organization’s firewall in this scenario.

Note: Organizations desiring only VRI services in Scenario #2 may wish to implement Firewall Rule #1 as well for system administration and diagnostics purposes. An administrator within the organization can gain access to additional NTS services and diagnostics using a “base” NTS login. This “base” login could be restricted to certain PCs used by on-site administrators only if desired.



The NexTalk Company

4505 S. Wasatch Blvd, Suite 120 • Salt Lake City, UT 84124
801.274.6001 • 801.274.6002 fax • 801.274.6004 tty
www.nextalk.com • mail@nextalk.com
www.nextalk.net

Scenario #3: The organization is fully hosted (no on-premise NTS servers), and desires only “base” NTS features.

In Scenario #3, Firewall Rule #1 above is needed, but Firewall Rule #2 is not needed.

Scenario #3 is used by organizations wishing to solve TTY accessibility problems or to obtain the other “base” features described above in a convenient and hosted fashion, but video/audio links are not desired.

Scenario #4: The organization has an on-premise “base” NTS server, and both video/audio and “base” operations are desired.

In Scenario #4, the NTS video server is off-site, but the organization installs and maintains an on-premise “base” NTS server.

- Note: There are some advantages to Scenario #4. For example, in this scenario any text chat, or instant messages, from the NTS system are stored on-site within the organization. Scenario #4 also makes it simpler to connect to phone lines owned by the organization to the NTS system for TTY calling and etc.
- In Scenario #4, only Firewall Rule #2 is needed:
“Outbound port 1853 (TCP and UDP) to the five IP addresses starting with “video.nextalk.net” (75.125.90.242 to 75.125.90.246).

Scenario #5: The organization has an on-premise “base” NTS server, and desires only “base” NTS features.

In this case, there are no firewall openings required to the outside world for network communications. In Scenario #5, the organization commonly installs analog or T1 phone trunks to allow TTY, voice, and/or fax calls to occur to/from the NTS system, and this phone link is the only link between the NTS system and the outside world.

Scenario #6: The organization has both an on-premise “base” NTS server, and an on-premise NTS video module server.

Scenario #6 is possible but rare due to the cost and complexity of installing and maintaining an NTS video module server within an organization. Network security is typically not enhanced in Scenario #6 since video streams are usually needed to off-site video interpreters and so on anyway, and this scenario does not then eliminate Firewall Rule #2 above.

Conclusion:

This Technical Information Document describes the network firewall settings needed in a variety of scenarios using the NTS-7 client-server product.