



STEP 1 – PREPARING YOUR FIREWALL

The firewall rules required to access a Visual Nexus Meeting Server are very simple and secure.

Your Firewall needs to allow:

- Outbound initiated TCP/HTTP connections to port 8080, and allow responses
- Outbound initiated TCP connections to ports 8081 and 8079 and allow responses

STEP 2 – OPTIONAL FIREWALL CONFIGURATIONS

When Visual Nexus is to be used on error prone connections, Visual Nexus Secure Transport can be optionally configured to send media as UDP. If your administrator allows UDP then the Firewall needs to allow:

- Outbound initiated UDP connections to port 8081 and 8082, and allow responses

STEP 3 – LOCKING DOWN FIREWALL CONFIGURATIONS

If you wish to add a further level of security, you can limit the above rules specifically to the Visual Nexus meeting server by restricting the following access:

- To port 8079/80/81 only on the Meeting Server IP address
- To port 8081/82 only on the Secure Transport Server IP address

CHECKING YOUR FIREWALL CONFIGURATIONS

If you need to check whether your current firewall rules allows connectivity to the Visual Nexus meeting server, run the NetCheck utility which may be downloaded from the download pages on VNOnline at your meeting server. The Netcheck utility must be able to connect to TCP port 8078 on the IP address of your meeting server.

