



## STEP 1 – PREPARING YOUR FIREWALL

The firewall rules required to access the Visual Nexus Internet Service are very simple and very secure.

Your Firewall needs to allow:

- Outbound initiated TCP/HTTP connections to port 8080, and allow responses
- Outbound initiated TCP connections to ports 8079, 8081 and 8083 and allow responses
- Outbound initiated UDP connections to port 8081 and 8082, and allow responses

## STEP 2 – 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 System by restricting the following access:

- To port 8079 to 8083 only on the Meeting Server IP address [216.205.98.125](http://216.205.98.125)
- To port 8081 to 8082 only on the Secure Transport Server IP address [216.205.98.121](http://216.205.98.121)

## STEP 3 - CHECKING YOU FIREWALL CONFIGURATIONS

If you need to check whether your current firewall rules allows connectivity to the Visual Nexus demonstration service, run the NetCheck utility which may be downloaded from the download pages on VNOnline at <http://s01.virtualmeeting.com:8080/>. The Netcheck utility must be able to connect to TCP port 8078 on IP address [216.205.98.125](http://216.205.98.125). The NetCheck utility is programmed with the above IP addresses for the Meeting Server and Secure Transport Server.

