

Network Configuration

This White Paper describes how to configure the network, firewall and DMZ (Demilitarized Zone) to ensure optimal functioning of Netviewer software.

Netviewer communication channels in general

Setting up and conducting a Netviewer session with multiple participants is achieved through a centralized Netviewer server. The Netviewer server has two components: connection server (ConnS) and communication server (Comms). The connection server is responsible for the authentication and login of the participants. The communication server transfers the session data during a Netviewer session.

The benefit of such a server-based (indirect) communication, instead of a direct connection, is that the clients always initiate the session and therefore most firewalls will allow the session to take place (see figure 1).

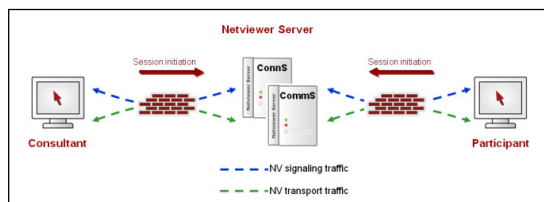


Figure 1

Netviewer Support and Netviewer Admin are able to establish a peer-to-peer connection between the two client PCs (configurable). 'Peer-to-peer' means a direct connection between the two clients during the session without using a communication server. Nevertheless, the authentication and login of the session participants has to be accomplished by the connection server. Peer-to-peer can only be used if there are no firewalls between the Netviewer clients (see figure 2).

Netviewer Meet always requires a communication server to transfer the session data between the session participants.

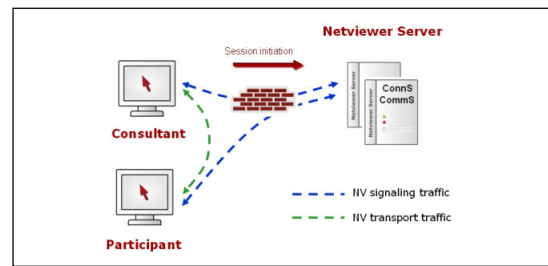


Figure 2

The following sections will discuss two variants of using Netviewer: Either with

- the Netviewer ASP (Application Service Provider) infrastructure, or with
- a server infrastructure at the customer's premises.

Utilisation of the Netviewer SaaS infrastructure

As an software as a service provider (SaaS), Netviewer operates connection servers and communication servers. When buying a Netviewer license the customer also acquires the right of using the Netviewer servers. The Netviewer servers are located at different locations to ensure high availability and performance.

After having purchased a Netviewer license the customers receive their individually configured Netviewer programs. These customized programs contain the addresses of preferred connection servers. If the client program is not able to reach a server, it will contact the next server within its internal server list. The Netviewer clients must be able to reach all Netviewer servers on port 80 HTTP.

After authentication the connection server transfers the address of a available communication server to the client.

The communication during the Netviewer session can either be handled through HTTP port 80 or through the TCP ports 2000 or 443.

The client programs first try to use the TCP port 2000 to establish the connection, then port 443 TCP, followed by HTTPS (SSL) through port 443 and then HTTP port 80. The exact sequence of ports and proxy handling can be seen in figure 3.

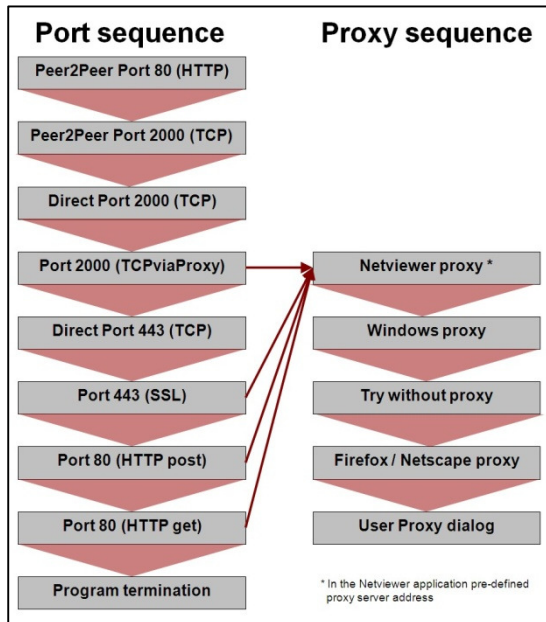


Figure 3

If the firewall allows communication over TCP port 2000 or 443, the session data is transferred directly through TCP. If the firewalls blocks the TCP communication on port 2000 or 443 the connection goes through port 80 HTTP and therefore often via a proxy server (see figure 4). Using a TCP based communication may increase the performance.

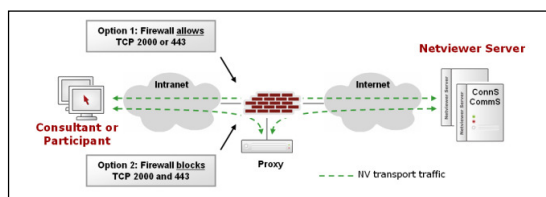


Figure 4

Utilization of server infrastructure at the customer's premises

Alternatively, customers can operate their own server infrastructure instead of using the Netviewer SaaS portfolio.

Netviewer offers a server product: The Netviewer Server.

In the following, we describe the network configuration for the Netviewer Server. With the Netviewer Server, the connection server and the communication server are often installed on the same server. For redundancy or scalability reasons more than one Netviewer server can be coupled.

Ports on client side

On client side the Netviewer servers should be accessible on HTTP port 80 and TCP port 2000 and / or 443 for outgoing traffic.

Ports on server side

In most cases the Netviewer servers must be reachable from the Intranet and the Internet. Therefore it is advisable to place the Netviewer server into a DMZ (Demilitarized Zone). To the Intranet as well as to the Internet only the following incoming connections should be permitted: HTTP port 80 (incoming request), TCP port 2000 or 443 (incoming request).

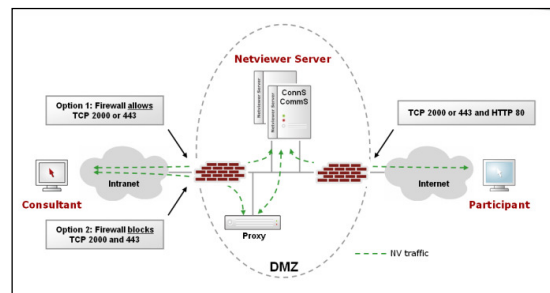


Figure 5

The Netviewer traffic goes either through port 2000, port 443 or port 80.

Administration

In addition, for maintenance reasons (e.g. Netviewer client configuration kit) the ports 8088 and 8098 should be available for the administrator of the Netviewer server from the intranet.

Netviewer external database support

The Netviewer database can alternatively be installed on the Netviewer server or on a centralized database server.

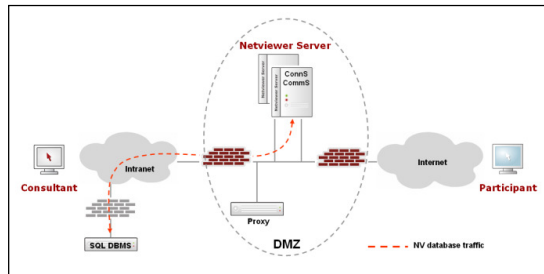


Figure 6

For the communication between Netviewer server and database server port 1433 TCP (bidirectional) is used.

Summary

The setup of a Netviewer session is handled through port 80 (HTTP). When the clients are connected to the Netviewer server the session traffic is handled through port 2000 or 443 TCP. If both ports are blocked by the firewall port 80 (HTTP) will be used for the session traffic.

A customer based Netviewer server infrastructure should be placed into a DMZ. The HTTP port 80 and TCP port 2000 or TCP port 443 should be opened in both directions, to the Intranet as well as to the Internet. For administration purposes port 8088 and 8098 should be permitted. The connection to an external database server is handled through port 1433 TCP.

Version 1.4 - December 2009
Reference to Server- and Client Version: G3 & G3.1

© 2009 Netviewer AG. Netviewer Support, Meet, Admin, Server, and the Netviewer Logo are registered trademarks of Netviewer. All rights reserved. All other trademarks are the property of their respective owners.