

White Paper Security: Netviewer Meet 6.0

This White Paper describes the security mechanisms within the Netviewer Meet product. In the first part we focus on security aspects at the network transport layer. In the second part we describe the application layer related security mechanisms.

Security at the Network Transport Layer

The security at the network transport layer is the basis for a secure communication. This section describes how Netviewer assures that the communication channel is secured in terms of mutual authentication and encryption.

Session setup

The session setup is shown in figure 1 and will be explained in detail in this section. The moderator starts the moderator program and the program contacts the connection server (ConnS) to request a session (1). After the moderator has been authenticated successfully (user name and password) the connection server sends back a 9-digit session number and the address of the communication server (CommS) to the moderator (2). Then the moderator will contact the communication server and wait for the participants to join the session (3).

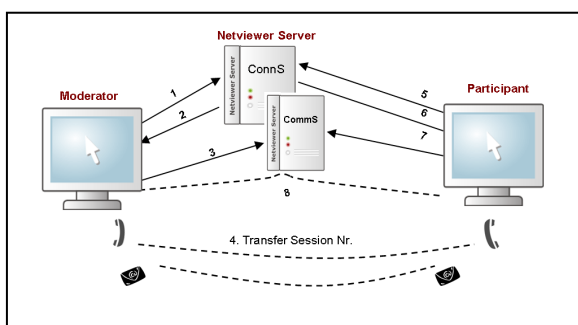


Figure 1

In the next step, the moderator gives the 9-digit session number to the participants via telephone or e-mail invitation (4). The participants start the program and enter the session number in the assigned field.

The participant programs then send a request to the connection server (5). The connection server sends back the address of the communication server where the moderator is waiting (6). The participant program contacts the communication server (7). The session is then established between the moderator and the participants through the communication server (8). The integrity of the data during the session is secured.

The connection server and the communication server are independent entities. Signalling data (e.g. authentication, keys) and session data are therefore logically separated.

Encryption methods

Since the connection server and the communication server perform different tasks different methods for securing the communication are used.

The communication between the clients and the connection server is secured by TLS (standard RFC 2246). Here a 2048-bit RSA Server Certificate is used. Client programs authenticate themselves at this level by HTTP Digest Access Authentication (RFC 2617).

The communication between the clients via the communication server is secured by AES in CBC mode and 256-bit long session keys. The integrity of the data is secured up with authentication headers (according to standard RFC 2404)

Figure 2 shows how the network session is setup in detail.

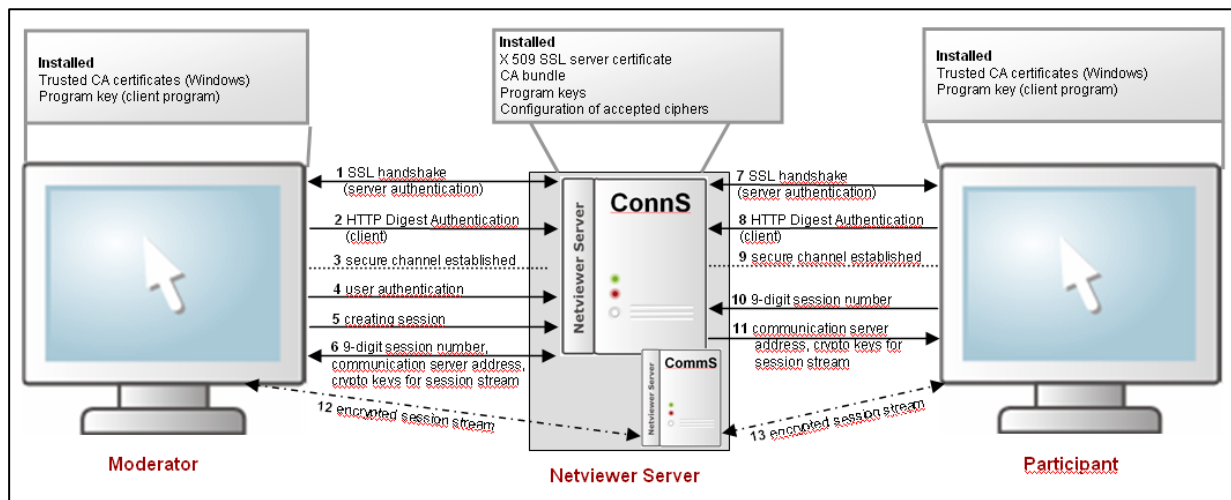


Figure 2

Security at the Application Layer

At the application layer Netviewer supports a variety of security functions that enable additional levels of security. These concepts are technology and process based. Many of the following functions are configurable.

Session setup

Moderator and participants are able to verify the authenticity of the Netviewer software. The software is signed with a certificate from the independent certification authority VeriSign.

To start the moderator program the moderator needs an e-mail address and a password. After a successful authentication, a unique 9-digit session number, generated by the connection server, will be transferred to the moderator program. This number will be forwarded by phone or e-mail to the participants (see figure 1).

A session password can be used in addition.

During a Session

The privacy of each participant and his data during a Netviewer Meet session are protected by different methods and settings.

Neither the moderator nor the participants are able to remotely control the PC of another party without approval.

The participants will always need to approve any change of the status of their PC (change direction of view, remote control, file transfer, information about the configuration of the PC). Only after the approval the second party will be able e.g. to remotely control the PC.

Applications or files which shall not be shown to the other parties can be selected. For example it is possible to hide the desktop or the task bar. In this case, these applications can not be used by remote control either.

The participant in show mode can freeze the screen to secure the secret use of the own PC while working with another program (monitor pause function). Pushing the security key (default F11) immediately stops the remote control.

The moderator is able to exclude a participant from the session.

A session can be locked by the moderator.

Logging

The moderator program creates a .txt file at the end of a session to log the duration of a session and the number of transferred bytes.

All parts of the session, including video and audio, can be recorded and stored in a Netviewer proprietary .nvl file format. It is possible to change this file to an .asf file format manually.

Summary

- The security of Netviewer Meet and the integrity of the data are guaranteed by using different levels of protection:
- The Netviewer software is signed with a certificate from an independent certification authority (VeriSign).
- SSL/TLS key is used for server authentication, encryption and to ensure the integrity between client and connection server.
- Client programs authenticate themselves by HTTP Digest Access Authentication (RFC 2617).
- A 256-bit AES key is used to encrypt the session data.
- The connection and communication server are independent entities.
- The exchange of the session number is transferred through a different medium (phone or e-mail).
- All sessions are encrypted between the clients and the server.
- All sessions can be logged on moderator, participant and server side.
- All data can be recorded for later review.
- For every session a new session number will be generated.
- No action on the other party's computer is possible without permission. This is valid for both moderator and participants.
- It is possible to use a session password before the session is established.
- The moderator is able to exclude a participant from the session.
- A session can be locked by the moderator.
- When the last moderator leaves, the session will be terminated.

Version 1.0 – February 2010

© 2010 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.