

Netviewer Admin Security

This White Paper describes the security mechanism within the Netviewer Admin product. In the first part it focuses on security aspects at the network transport layer. In the second part it describes 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 basic process of setting up a Netviewer Admin session is shown in figure 1 and will be explained in detail in this section.

The requirement for setting up a session is the installation of the Netviewer Admin Host program on the Host computer. Alternatively the Admin Host can be run as application. After a successful authentication by user name, password and license key the Host periodically sends a ping to the connection server (ConnS) to show its presence and waits for response ①.

After the authentication the administrator can start a Admin session on the Host computer at any time by double-clicking on the Host in the Master program. He will be asked to enter the key phrase of the Host. The key phrase is an 8 - 16 digit number which serves as access control for a certain Host. After having entered the valid key phrase the Master program contacts the connection server (ConnS) to request a session ②.

After the administrator has been authenticated successfully (user name and password, Active Directory...) the connection server sends the address of a communication server to the Master ③.

The Master then contacts the communication server and waits for the Host to join the session ④.

The connection server informs the Host about the session request when answering the next ping of the Host program ⑤.

The Host sends a request to the connection server ⑥.

The connection server sends back the address of the communication server where the Master is waiting ⑦.

The Host program contacts the communication server ⑧.

The session is then established between the Master and the Host through the communication server ⑨.

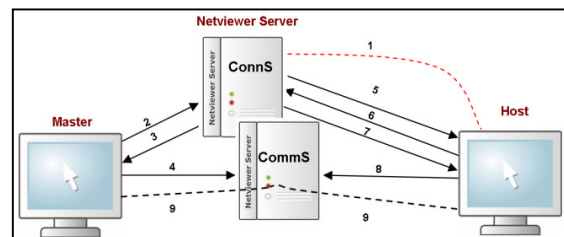


Figure 1

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

Encryption methods

The mutual authentication between the Netviewer clients and the Netviewer servers is done by using asymmetric keys. Both public and private keys are included in the Netviewer software as part of the software generation stage. In addition, the Master and the Host programs are in possession of the 8 - 16 digit key phrases which was chosen individually by the administrator during the installation of the Admin Host program.

The Master program and the Host use the public key of the server and their own private key. The server uses his own private key and the public key of the clients.

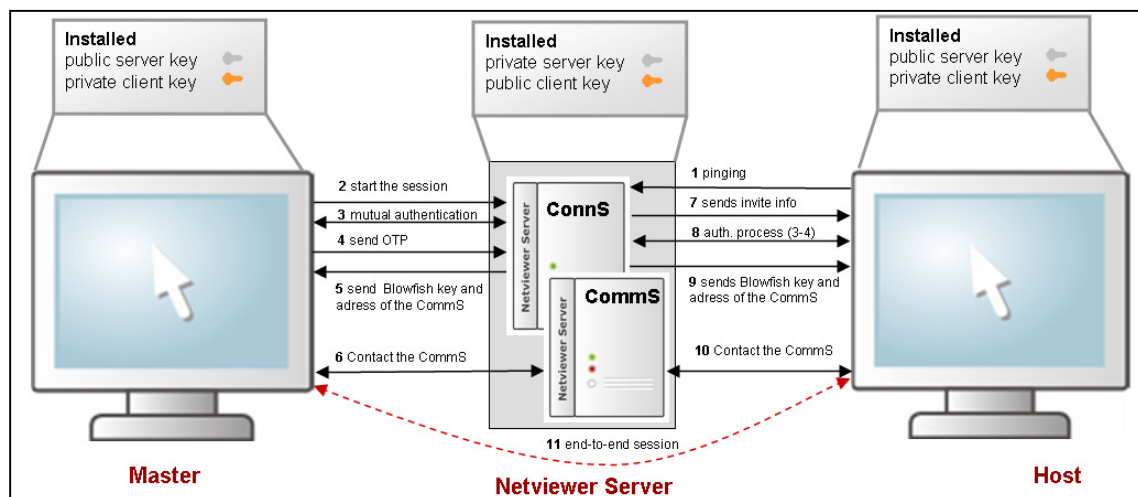


Abbildung 2

The privacy and the integrity of all data are secured by two encryption methods called ECC (Elliptic Curve Cryptography) and Blowfish. The asymmetric 160-bit ECC keys are used for authentication and key exchange. The symmetric 128-bit Blowfish key secures the integrity and the privacy of the communication between Master and Host.

The following section describes the session setup regarding the encryption methods which is visualized in figure 2.

The Host sends pings to the connection server in regular intervals to show its presence ①. If there is no request from the Master, the client continues pinging the server.

If the Master requests a session ②, in the first step the Master and the connection server authenticate each other by using the ECC asymmetric keys and random numbers ③.

The Master then generates an OTP (one time pad) and sends it encrypted to the connection server (ConnS) ④.

The connection server decrypts the OTP and generates a symmetric Blowfish key. It sends the address of the communication server and the Blowfish key to the Master ⑤.

From that point all signaling traffic will be encrypted by using this first Blowfish key. The Master contacts the communication Server and will wait for the host to join ⑥.

The connection server will inform the Host about the session request when answering the Host's next ping ⑦.

The Host program contacts the connection server for mutual authentication and key exchange ⑧.

The way of being authenticated is similar to the Master (③-④). The connection server sends the first Blowfish key and the address of the communication server which will be used for the session ⑨.

The Host contacts the communication server where the Master is already waiting ⑩.

After the start of the session both Master and Host discard the first Blowfish key sent by the communication server and create a new one using the key phrase which was created during the installation process of the programs. Now the secure end-to-end encrypted session is established (11).

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

The Master and Host software is certified by Netviewer. The software is using a certificate

signed from the independent certification authority VeriSign.

To start the Master program the administrator needs to enter a user name and a password. After a successful authentication, the administrator has to insert the key phrase to access a certain Host.

There are three ways for the administrator to log on to the Host.

When the Master logs on to the Host, the Host computer will be in one of the following states:

a) A user is logged on to the Host computer.

If the administrator starts a Admin session and a user is logged on to the PC, the current user must explicitly permit the access to his computer. The desktop transfer and the Admin control will not be available for the Master until the Host has agreed. Until then the Master will only see a black screen.

The administrator has the same permissions and restrictions as the logged-on user. To receive further rights (e.g. to access certain files) the administrator may change the user account during the session.

The user of the Host computer can stop the Admin session at any time.

b) The Host computer is locked.

The entire screen is visible, but the computer has to be unlocked first. The administrator can log-on with his administrator account or the account of the local user. The rights of the administrator depend on the user account.

c) The Host computer is logged off.

The Windows login dialogue is visible on the screen. The administrator can log-on with his administrator account or the account of the local user. The rights of the administrator depend on the user account.

During a session

The privacy of each Host and his data during a Netviewer Admin session is protected by different methods and settings. In case that a user is logged on to the Host he has to permit actions of the Master on his computer such as file transfers. It is possible to display a waiting screen while the Master works on the Host computer. This may be helpful when carrying out confidential tasks like inserting CD keys.

During the session the communication server is not able to access the session data as the session is encrypted end-to-end.

Logging

The Master program creates a .txt file at the end of a session to log the duration of the session and the number of transferred bytes. The session data can also be stored as a .csv file on the Master and/or Host side for further use, i.e. for billing. In addition, all static session data will be logged on the server side. 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 convert this file to an .asf file format manually.

Summary

The security of Netviewer Admin and the data integrity are guaranteed by using different levels of protection:

- The Netviewer software is signed with a certificate from an independent certification authority (VeriSign).
- A 160-bit ECC key is used for the mutual authentication and the asymmetric encryption between client and server.
- The session data is encrypted by a 128-bit symmetric Blowfish key.
- Master and Host use the 8-16 digit key phrases to create a Blowfish key which will be used to encrypt the session. This string is chosen individually during installation of the programs.
- Connection server and communication server are independent entities.
- The communication server does not know the Blowfish key which will be used during the session.
- All sessions are encrypted end-to-end.
- All session data can be recorded for later review on the Master and the Host.

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