

NetOp® Remote Control



**Security, access control,
extensive logging, user
management**

The flexible remote control tool

Danware Data A/S
Bregnerodvej 127
3460 Birkerød
Denmark
Tel.: +45 45 90 25 25
Fax.: +45 45 90 25 26
www.netop.com

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Remote Control



Abstract

Remote controlling computers, PDAs and servers over the LAN/WAN or the Internet has for a long time been the wise thing to do. Not only is the supporter able to see, diagnose and fix the downed equipment – he could also risk exposing information.

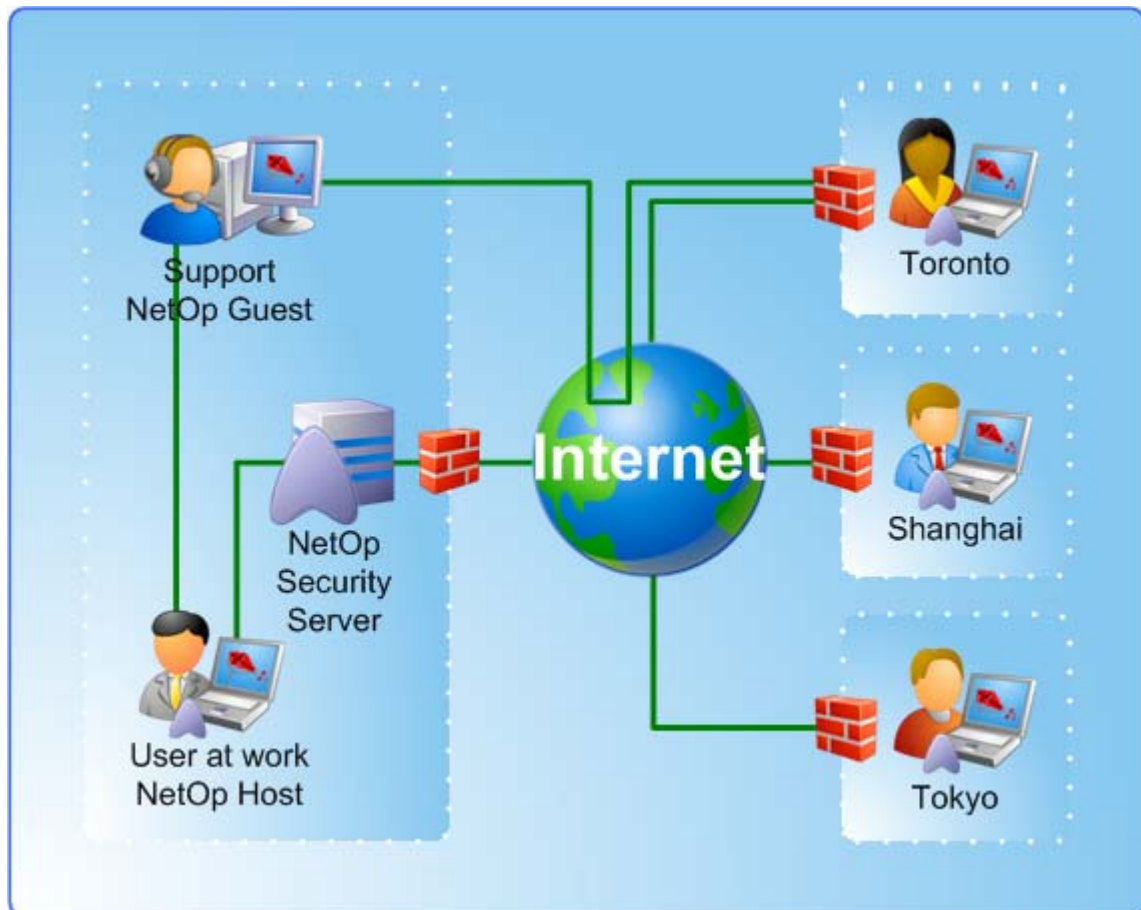


Figure 1: Typical NetOp Security Server setup. The Host authenticates the Guest via the Security Server before the Guest is allowed to remote control the Host.

The point with remote control is to be able to manage and support the user's computer no matter where he may be: On the organization's LAN/WAN, at home or in foreign locations.

Solution

The NetOp Security Server is a special Host module that can answer queries from other NetOp modules about session permissions and rights across a network connection by forwarding queries to the ODBC database. The program must have access to the ODBC database containing security relations between the Guests and the Hosts. The NetOp Security Manager configures how the NetOp Security Server operates in your network. It is a database client program that can edit information in an

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Remote Control



ODBC database of your choice. The database is input to the NetOp Security Servers, and it is from this information the Security Servers allow or deny NetOp Guests access to NetOp Hosts. The NetOp Security Manager must run on a Windows XP, 2000, or NT 4.0 platform for full functionality.

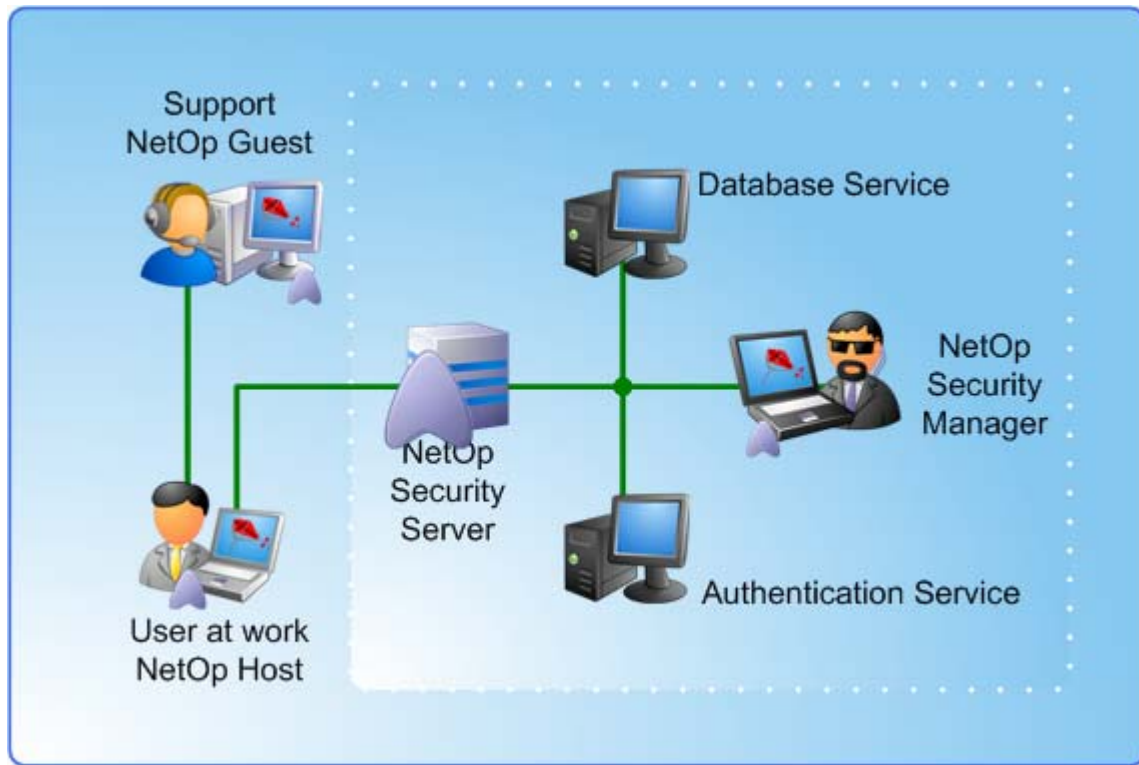


Figure 2: NetOp Security Server setup: The Guest gets access via the Host. The Security Server consists of the Security Server, a database containing security relations, an authentication service checking the users' security roles, and a NetOp Security Manager updating and maintaining the database and the authentication service.

Using the NetOp Security Server the system can authenticate the Guest identity against NetOp, Windows (via the Host), Directory Services, or RSA SecurID Authentication Services. To achieve NetOp authentication the NetOp Security Server verifies the Guest identity against the database service that holds all the predefined Guest IDs and passwords. To achieve Windows authentication the NetOp Security Server verifies the Guest identity by letting the Host relay the authentication process to the Windows Domain controller. Directory Service Authentication via the security server involves the NetOp Security Server verifying the Guest identity against a Directory Service via LDAP.

Centralized authorization means that information about security roles is available in a database on a shared remote computer. Via the NetOp Security Server, the Guest's allowed actions are authorized against a centralized database service containing security roles.

Authentication services are often used to check group membership to determine whether a user belongs to a security role or not. This includes NetOp, Windows, Directory Services, or RSA SecurID authentication services.

- *NetOp Authorization via Security Server*
NetOp Security Server controls allowed actions for the authenticated Guest identity by checking for membership of Guest ID groups at the database service.

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Remote Control



- *Windows Authorization via Security Server*
NetOp Security Server controls allowed actions for the authenticated Guest identity by checking for membership of Windows Security Groups at a Windows Domain Controller.
- *Directory Services Authorization via Security Server*
By checking for membership of groups at a Directory Service, the NetOp Security Server controls allowed actions for the authenticated Guest identity.
- *RSA SecurID Authorization via Security Server*
By checking for membership of special groups at the database service, the NetOp Security Server controls allowed actions for the authenticated Guest identity. This is independent of any RSA ACE/Server groups.

Key Features

Centralized authentication

Centralized authorization means that information about security roles is available in a database on a shared remote computer. Via the NetOp Security Server, the Guest's allowed actions are authorized against a centralized database service containing security roles.

Authentication services are often used to check group membership to determine whether a user belongs to a security role or not. This includes NetOp, Windows, Directory Services, or RSA SecurID authentication services.

Centralized logging

Event logging records session activity and log on attempts and proves that your security settings are working.

NetOp Remote Control includes an extensive event-logging feature that enables you to log session activity and log on attempts to multiple logging destinations. These logging destinations include a local file (you can log NetOp events on the local computer), the NetOp Security Server (you can log NetOp events in the database of a central NetOp Security Server group), a Windows Event Log (you can log NetOp events to the local and remote Windows Event Log), and an SNMP enabled management console (you can log NetOp events by sending SNMP traps to a SNMP enabled central management console, such as HP OpenView). More than 100 NetOp events can be logged.

Protected traffic

There are several ways that information moving between the Host and Guest modules can be protected:

- **Encryption** - Data transmitted between modules can be encrypted end-to-end using the Advanced Encryption Standard (AES) with key lengths up to 256 bits. Seven different levels are available including NetOp 6.x/5.x compatible for communication with older NetOp modules.
- **Integrity and message authentication** - The integrity and authenticity of encrypted data is verified using the Keyed-

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Remote Control



Hash Message Authentication Code (HMAC) based on the Secure Hash Standards SHA-1 (160-bit) or SHA-256 (256-bit).

- Key exchange - Encryption keys for encrypted data transmissions are exchanged using the Diffie-Hellman method with key lengths up to 2048 bits and up to 256-bit AES and up to 512-bit SHA HMAC verification.

Protecting the Host

To gain access to the Host computer, the Guest computer can be forced to meet up to six access criteria:

- MAC/IP address check
- Closed user group
- Authentication
- Callback
- User controlled access
- Authorization

Target Industries

Financial institutions, military and government agencies, health organizations, airlines and global organizations etc.

Questions & Answers

Does the system have built in load balancing?

No. Multiple servers can provide fault-tolerance and load balancing so it is preferable to use more than one NetOp Security Server.

Which types of databases are supported?

NetOp Security Server follows the SQL92 Standard and is known to support the following databases:

- DB2, MS JetEngine, MS SQL and Oracle

Note: NetOp does not support MySQL because it does not use 'named primary key', which is crucial for NetOp Security Server.

Which possibilities does the Host user have to maintain or regain control of his computer during a remote control session?

NetOp Remote Control Host can be set up to address this in several ways. The Host can actively allow the Guest to different tasks, i.e. keyboard control and file transfer.

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.

NetOp® Remote Control



How can I communicate with my users?

NetOp Remote Control offers three types of communication between the Guest and the Host: Chat, voice chat and video chat.

Who is Danware?

Danware's core business is to develop and market software products based on the NetOp core technology – a technology enabling swift, secure and seamless transfer of screens, sound and data between two or more computers.

The company's three product areas are Desktop Management, Education and Security. The core Desktop Management product, NetOp Remote Control, enables remote control of one or more computers from another computer and can be used across different system platforms. NetOp School, the Education core product, is a software application for computer-based classroom teaching in both physical and virtual classrooms via the Internet or other networks. The Security business products are NetOp Desktop Firewall and NetOp Netfilter. All are plug 'n play products offering extensive functionality, flexibility and user-friendliness.

See more at: <http://www.netop.com/netop-13.htm>

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufactures. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice.