ADMINISTRATION

Netop

Netop Remote Control Security Server

Product Whitepaper

ABSTRACT

Security is an important factor when choosing a remote support solution for any enterprise. Gone are the days where security was just a matter of the highest degree of encryption. Today, a truly secure remote support solution will allow organizations to centrally control who can do what and where safe in the knowledge that when each remote session has finished it should be able to document what actually took place.

- Netop Remote Control Security Server provides centralized security, administration, authentication and authorization of all remote control users. All remote control activity can be logged and recorded. You are in full control of who can do what and where across the enterprise.

To provide enterprise-level remote support security requires:

Seamless integration

You must be able to authenticate your support staff in a way that complies with your existing security scheme, e.g. using Directory Services, Smart Cards or RSA authentication.

Granular level of control

Users of any remote support solution can be varied and therefore require different levels of access. It is crucial to differentiate between your workforce including administrators, support staff, external consultants, etc and dictate what machines can be accessed and what remote support privileges are assigned.

Easy, centralized and scalable management

If security settings are managed locally on the client or server it becomes a difficult task to change settings even in relatively small networks. Managing groups and access permissions should be achievable within a few clicks and without changing any local settings on each client machine. Fault tolerance is also essential in order to provide high availability and maintain critical uptime.

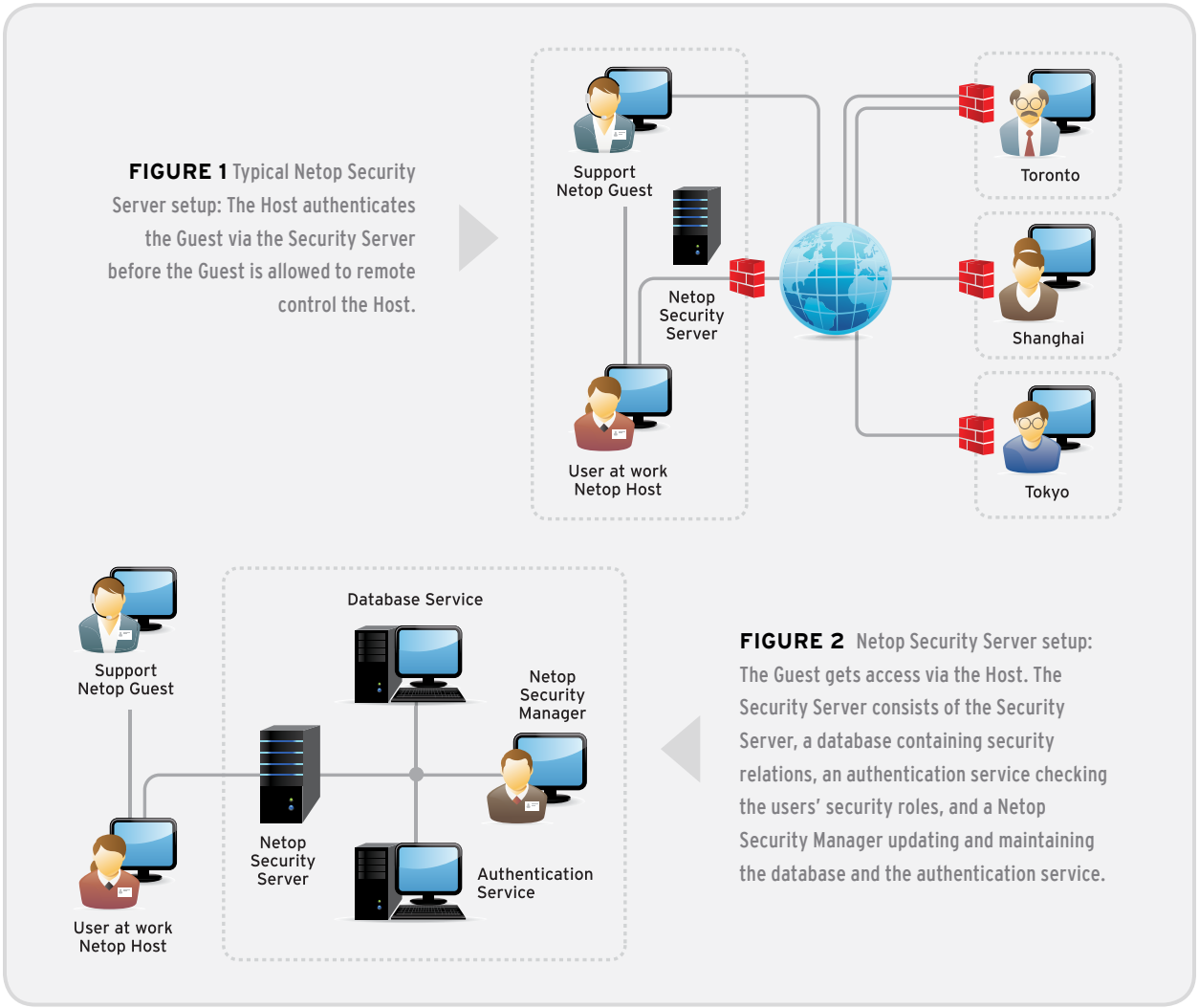

FIGURE 1 Typical Netop Security Server setup: The Host authenticates the Guest via the Security Server before the Guest is allowed to remote control the Host.

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.

SOLUTION

The Netop Security Server is a special Host module that can answer queries from other Netop modules about session permissions and access rights across a network connection. The Security Server uses an ODBC compliant database containing security relations between your Guest and Host modules, which are configured through a management console called the Netop Security Manager. It is from this management console and database that you can decide who can support who and what privileges will be assigned during each session.

Using the Netop Security Server, you can centrally authenticate the Guest identity against Netop, Windows, Directory Services, Smart Card or RSA SecurID authentication services.

- Netop authentication - the Netop Security Server verifies the Guest identity against the database service that holds all the predefined Guest IDs and passwords. These IDs are specific to Netop and are not linked to any existing security scheme such as Directory Services.

- Windows authentication - the Netop Security Server verifies the Guest identity by letting the Host relay the authentication details to the Windows Domain controller.

- Directory Service authentication - involves the Netop Security Server verifying the Guest identity against a Directory Service using the LDAP protocol and includes support for Directory Services from Microsoft, Novell and Sun.

- Smart Card authentication – by using a Smart Card and reader at the Guest machine, the Guest credentials can be authenticated against a Microsoft CA environment. Secure tunnelling also allows the Guest user to logon remotely to the Host machine using their Smart Card credentials

- RSA SecurID authentication – validate your Guest credentials against your RSA ACE/Server using their username and passcode. Combining this with Netop authentication also provides 3-factor authentication

Centralized authorization means that access permissions for each remote support session can be defined using Security Roles via the Netop Security Manager. Once the authentication process has taken place and the Guest credentials have been validated against the Host, the accumulated access privileges are assigned to the Guest for that remote support session. These permissions can be easily managed using the Security Manager and offers great flexibility with different levels of control depending on the Guest users role within the organization.

KEY FEATURES

Centralized authentication

Integrate with your existing security scheme and authenticate your Guests using Netop authentication, Windows authentication, Directory Services via LDAP, Smart Cards or RSA SecurID.

Centralized authorization

Define flexible security roles to dictate which Host machines your authenticated Guests can access and what remote support privileges they will be assigned.

Centralized logging

Maintain an audit trail by recording remote support session activity. Netop Security Server acts as a central repository for enterprise-wide remote support activity so you can keep track of what happened and where using extensive log events.

Protected traffic

There are several ways that information moving between the Netop 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- 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 can be forced to meet up to six access criteria:

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

QUESTIONS & ANSWERS

Does the system have failover capabilities?

Yes. Multiple Security Servers can exist to provide a fault-tolerant environment with maximum availability. Should one server fail, the remaining servers will seamlessly handle the authentication and authorization process.

What type of databases are supported?

Netop Security Server follows the SQL92 Standard (ODBC-compliant) 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 a requirement for Netop Security Server.

What if my Host users have concerns over remote access to their systems?

Using Netop Security Server means that only authenticated Guests are allowed to access specific Host machines. This does not mean that once authenticated, the Guest will have complete control over the Host system. There are many different levels of control and notification features that can be made available to the Host users including Confirm Access dialogs, notification features and disconnect hotkeys.

All remote support activity can also be logged and therefore audited including the actual remote session allowing organizations to trace and deal with any unauthorized access attempts.

Where should the Security Servers be installed and what network access is required?

Because the Security Server is the focal point for authenticating your Guest users, it should be installed on a server based operating system for maximum availability. The server does not need to be dedicated and can run Windows Server 2000, 2003 or 2008 (32-bit and 64-editions including 2008 R2) including virtual environments. You will require a UDP connection via your chosen port (6502 by default) between your Hosts and Security Servers.

ABOUT NETOP SOLUTIONS A/S

Netop develops and sells software solutions that enable the swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet. The company has three business areas: Administration, Education and Communication.

Netop's unique and cost saving Administration solutions make life easier for IT professionals with Remote Control and IT Asset Management. With the market-leading solutions for Education, classroom management and corporate e-learning, Netop helps students and teachers to achieve optimum results through virtual education. Netop Communication solutions including unified communications let customers, partners and colleagues meet easily and safely in the virtual space via video conferencing, instant messaging, voice and file sharing over the Internet.