ADMINISTRATION

Netop

Netop Remote Control Security Server

Produkt-Whitepaper

KURZBESCHREIBUNG

Bei der Auswahl einer Fernsupport-Lösung für Unternehmen spielt die Sicherheit eine entscheidende Rolle. Die Zeiten, in denen Sicherheit ausschließlich eine Frage starker Verschlüsselung war, sind vorbei. Heute muss eine wirklich sichere Fernsupport-Lösung Unternehmen in die Lage versetzen, zentral festzulegen, wer was tun darf und wo er es tun darf. Außerdem muss sie die Möglichkeit bieten, gesamte Fernwartungssitzungen aufzuzeichnen, um so die tatsächlichen Ereignisse zu dokumentieren.

- Netop Remote Control Security Server bietet zentralisierte Funktionen für die Sicherheit, Administration, Authentifizierung und Autorisierung aller Benutzer von Fernsteuerungslösungen. Sämtliche Aktivitäten im Rahmen von Fernsupport-Sitzungen können protokolliert und aufgezeichnet werden. Sie haben innerhalb Ihres gesamten Unternehmens die volle Kontrolle darüber, wer was tun darf und wo er es tun darf.

Um sicheren Fernsupport innerhalb des gesamten Unternehmens zu gewährleisten, muss eine Lösung Folgendes bieten:

Nahtlose Integration

Sie müssen in der Lage sein, Ihr Support-Personal auf eine Art und Weise zu authentifizieren, die Ihrem vorhandenen Sicherheitsmodell entspricht, z. B. anhand von Verzeichnisdiensten, Smartcards oder RSA.

Detaillierte Kontrollmöglichkeiten

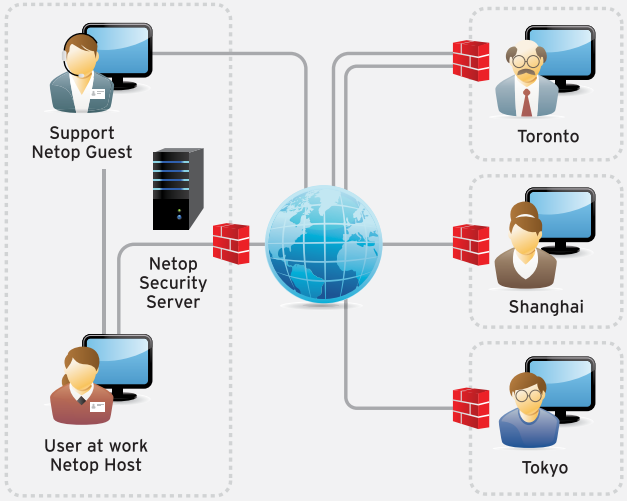
Da es bei Fernsupport-Lösungen in vielen Fällen unterschiedliche Arten von Benutzern gibt, müssen auch unterschiedliche Zugriffsrechte festgelegt werden können. Es ist von größter Wichtigkeit, zwischen den einzelnen Funktionen innerhalb Ihrer Belegschaft (Administratoren, Support-Mitarbeiter, externe Berater usw.) unterscheiden zu können, um festzulegen, auf welche Rechner sie zugreifen können und welche Fernzugriffsrechte ihnen eingeräumt werden.

Einfache, zentralisierte und skalierbare Verwaltung

Falls die Sicherheitseinstellungen lokal auf dem Client oder Server verwaltet werden, werden Änderungen an Einstellungen selbst in relativ kleinen Netzwerken zu einer schwierigen Aufgabe. Die Verwaltung von Gruppen und Zugriffsrechten sollte sich anhand weniger Klicks bewerkstelligen lassen und keine Änderungen an den lokalen Einstellungen von Client-Rechnern erfordern. Ein weiteres entscheidendes Kriterium ist Fehlertoleranz, da sie für eine hohe Verfügbarkeit und ununterbrochene Laufzeiten sorgt.

ABBILDUNG 1

Typische Netop Security Server Konfiguration: Der Host authentifiziert den Guest über den Security Server, bevor dem Guest die Fernsteuerung des Host erlaubt wird.



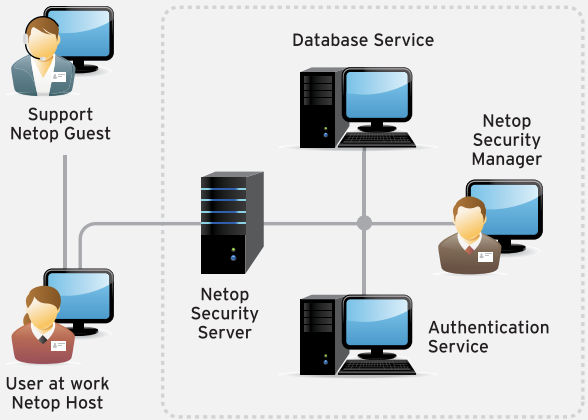


ABBILDUNG 2

Netop Security Server Konfiguration: Der Guest erhält über den Host Zugriff. Der Security Server besteht aus einer Datenbank mit Sicherheitsrollen, einem Authentifizierungsdienst, der die Sicherheitsrollen der Benutzer überprüft und einem Netop Security Manager, der die Datenbank und den Authentifizierungsdienst aktualisiert und verwaltet.

LÖSUNG

Der Netop Security Server ist ein spezielles Host-Modul, das Anfragen anderer Netop Module zu Sitzungsberechtigungen und Zugriffsrechten über eine Netzwerkverbindung beantwortet. Der Security Server nutzt eine ODBC-konforme Datenbank mit den Sicherheitsrelationen zwischen Ihren Guest- und Host-Modulen. Anhand der Verwaltungskonsole Netop Security Manager werden die Sicherheitsrelationen den verschiedenen Gruppen zugeordnet. Über diese Verwaltungskonsole und Datenbank legen Sie fest, wer für wen Support leisten darf und welche Rechte ihm während einer Sitzung eingeräumt werden.

Anhand des Netop Security Servers authentifizieren Sie die Identität der Netop Guest zentral; dies geschieht über Verzeichnisdienste, Authentifizierungsdienste wie Netop oder Windows, Smartcards oder RSA SecurID.

- Netop Authentifizierung – Der Netop Security Server prüft die Identität des Guest gegen den Datenbankdienst, in dem alle vordefinierten Benutzernamen und Passwörter für Guests gespeichert sind. Die Benutzernamen und Passwörter sind Netop-spezifisch und nicht abhängig von Sicherheitssystemen wie z. B. Verzeichnisdiensten.

- Windows Authentifizierung – Der Netop Security Server prüft die Identität des Guest, indem er den Authentifizierungsprozess von den Hosts an einen Windows Domain Controller weiterleitet.

- Authentifizierung über Verzeichnisdienste – Der Netop Security Server prüft die Identität des Guest anhand des LDAP-Protokolls gegen einen Verzeichnisdienst, wobei Verzeichnisdienste von Microsoft, Novell und Sun unterstützt werden.

- Smartcard-Authentifizierung – durch Verwendung einer Smartcard und eines entsprechenden Lesegeräts am Guest-Rechner können die Zugangsdaten über eine Microsoft CA Umgebung authentifiziert werden. Außerdem ermöglicht sicheres Tunneling dem Guest-Benutzer, sich anhand seiner Smartcard-Zugangsdaten per Fernzugriff am Host-Rechner anzumelden.

- Authentifizierung mit RSA SecurID – hierbei werden Benutzername und Passwort des Guest über Ihren RSA ACE/Server authentifiziert. Durch die Kombination mit der Netop Authentifizierung erhalten Sie eine 3-Faktor-Authentifizierung.

Unter zentralisierter Authentifizierung versteht man die Möglichkeit, Zugriffsrechte für jede Fernsupport-Sitzung unter Verwendung von Sicherheitsrollen über den Netop Security Manager zu definieren. Nach Abschluss des Authentifizierungsvorgangs und der Validierung der Guest-Zugangsdaten gegen den Host werden dem Guest die zusammengefassten Zugriffsrechte für die jeweilige Fernsupport-Sitzung zugewiesen. Diese Rechte können anhand des Security Managers problemlos verwaltet werden, wobei je nach der Rolle des Guest-Benutzers innerhalb der Organisation aus einer Vielzahl unterschiedlicher Berechtigungsebenen ausgewählt werden kann.

WICHTIGE FUNKTIONEN

Zentralisierte Authentifizierung

Integrieren Sie die Lösung in Ihr vorhandenes Sicherheitsmodell und authentifizieren Sie Ihre Guest-Benutzer anhand von Netop Authentifizierung, Windows Authentifizierung, Verzeichnisdiensten über LDAP, Smartcards oder RSA SecurID.

Zentralisierte Autorisierung

Definieren Sie flexible Sicherheitsrollen, um festzulegen, auf welche Host-Rechner authentifizierte Guests zugreifen können und welche Fernsupport-Rechte ihnen eingeräumt werden.

Zentralisierte Protokollierung

Garantieren Sie einen lückenlosen Audit-Trail, indem Sie sämtliche Aktivitäten im Rahmen von Fernsupport-Sitzungen aufzeichnen. Netop Security Server fungiert als zentrale Quelle für unternehmensweite Support-Aktivitäten und ermöglicht es Ihnen, anhand umfassender Ereignisprotokolle stets nachzuverfolgen, was, wann und wo passiert ist.

Geschützter Datenverkehr

Daten, die zwischen den Netop Modulen transportiert werden, können auf verschiedene Arten geschützt werden:

- Verschlüsselung – Von Modul zu Modul übertragene Daten können anhand von End-to-End-Verschlüsselung geschützt werden, wobei der Advanced Encryption Standard (AES) mit Schlüssellängen bis zu 256 Bit zum Einsatz kommt. Es stehen sieben verschiedene Verschlüsselungsebenen zur Verfügung, unter anderem eine mit Netop 6.x/5.x kompatible Ebene für die Kommunikation mit älteren Netop Modulen.

- Datenintegrität und Nachrichtenauthentifizierung – Die Integrität und Authentizität verschlüsselter Daten wird anhand von Keyed-Hash Message Authentication Code (HMAC) auf Basis der sicheren Hash-Algorithmen SHA-1 (160 Bit) oder SHA-256 (256 Bit) gewährleistet.

- Schlüsselaustausch – Der Austausch von Schlüsseln für verschlüsselte Datenübertragung erfolgt anhand der Diffie-Hellman-Methode mit Schlüssellängen von bis zu 2048 Bit und bis zu 256-Bit-AES oder bis zu 512-Bit-SHA-HMAC-Authentifizierung.

Schutz des Host

Um Zugriff auf einen Host-Computer zu erhalten, kann der Guest verpflichtet werden, bis zu sechs Sicherheitskriterien zu erfüllen:

- MAC-/IP-Adressprüfung
- Geschlossene Benutzergruppe
- Authentifizierung
- Callback
- Benutzerkontrollierter Zugriff
- Autorisierung

FRAGEN UND ANTWORTEN

Verfügt das System über eine Ausfallsicherung?

Ja. Es können mehrere Security Server eingesetzt werden, um eine fehlertolerante Umgebung mit maximaler Verfügbarkeit zu schaffen. Sollte ein Server ausfallen, können die verbleibenden Server den Authentifizierungs- und Autorisierungsprozess nahtlos fortführen.

Welche Arten von Datenbanken werden unterstützt?

Netop Security Server entspricht dem SQL-92-Standard (ODBC-Konformität) und unterstützt folgende Datenbanken: DB2, MS JetEngine, MS SQL und Oracle.

HINWEIS: Da der Primärschlüssel „named primary key“von MySQL nicht unterstützt wird und eine Voraussetzung für Netop Security Server ist, kann diese Datenbank nicht verwendet werden.

Was, wenn meine Host-Benutzer Bedenken hinsichtlich Fernzugriff auf ihre Systeme haben?

Wenn Netop Security Server eingesetzt wird, können ausschließlich authentifizierte Guests auf bestimmte Host-Rechner zugreifen. Dies bedeutet jedoch nicht, dass der Guest nach der Authentifizierung die vollständige Kontrolle über das Host-System übernehmen kann. Es gibt viele verschiedene Kontrollstufen und Benachrichtigungsfunktionen, die den Hostbenutzern zur Verfügung gestellt werden können; dazu zählen Dialogfenster für die Zugriffsbestätigung und Tastenbefehle für die sofortige Unterbrechung der Verbindung.

Außerdem können sämtliche Fernsupport-Aktivitäten, darunter auch die eigentliche Fernsitzung, protokolliert und somit auditiert werden, so dass Organisationen unautorisierte Zugriffsversuche stets zurückverfolgen und die nötigen Schritte einleiten können.

Wo sollte Netop Security Server installiert werden und was für ein Netzwerkzugang ist erforderlich?

Da der Security Server eine zentrale Rolle bei der Authentifizierung Ihrer Guest-Benutzer einnimmt, sollte er unter einem serverbasierten Betriebssystem installiert werden, um maximale Verfügbarkeit zu gewährleisten. Bei dem Servercomputer muss es sich nicht um einen dedizierten Server handeln. Er kann mit Windows Server 2000, 2003 oder 2008 (32- oder 64-Bit-Editionen inklusive 2008 R2) betrieben werden; auch virtualisierte Betriebsumgebungen werden unterstützt. Des Weiteren benötigen Sie eine UDP-Verbindung über einen Port Ihrer Wahl (standardmäßig 6502) zwischen Ihren Hosts und dem Security Server.

ÜBER NETOP SOLUTIONS A/S

Netop entwickelt und verkauft Software-Lösungen, die eine rasche, sichere und nahtlose Übertragung von Video- und Audiomaterial, Bildschirminhalten und anderen Daten zwischen zwei oder mehr Computern über das Internet ermöglichen. Das Unternehmen besteht aus drei Geschäftsbereichen: Administration, Education und Communication.

Netops einzigartige und kostensparende Administration-Lösungen erleichtern IT-Experten durch sichere Fernsteuerungsfunktionen die Arbeit. Durch seine erstklassigen Education-Produkte, darunter Lösungen für Klassenraum-Management und E-Learning-Programme von Unternehmen, hilft Netop Schülern, Studenten und Lehrkräften dabei, anhand virtueller Lehrmethoden optimale Ergebnisse zu erzielen. Die Netop Communication Lösungen ermöglichen die einfache und sichere Kommunikation mit Kunden, Partnern und Kollegen per Chat, Video und Audio über das Internet.