Datenblatt

NCP Secure Enterprise VPN Server

Hybride IPsec / SSL VPN Gateway Software Universelle Plattform für den Fernzugriff auf das Firmennetz

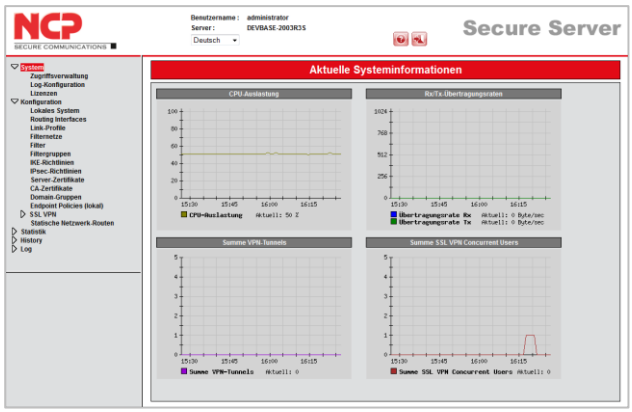
- Integrierte IP-Routing- und Firewall-Funktionalitäten
- Einbindung von iPhone, iPad, iOS, Android, Windows Phone/Mobile7 und Blackberry (ab Version 6)
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Automatische Tunnelweiterleitung
- Network Access Control*
- FIPS Inside
- Mandantenfähigkeit
- Endpoint Policy Enforcement
- Virtualisierbar, Ideal für Cloud-VPN
- Unterstützt elliptische Kurven (ECC)
- Multi-Prozessor Unterstützung, beliebig skalierbar

Kompatibilität

Der NCP Secure Enterprise Server ist ein Baustein von NCPs Next Generation Network Access Technology – der ganzheitlichen Remote Access VPN-Lösung. Über das VPN Gateway werden mobile und stationäre Teleworker in einem unternehmensübergreifenden Datennetz integriert. Die Software wird auf einem Standard-PC unter Windows oder Linux installiert und fungiert als zentrale "Schalt- und Kontrollstelle" entweder hinter einer Firewall in der DMZ (Demilitarisierte Zone), direkt am öffentlichen Netz (Wide Area Network) oder als VM-Ware.

Der Secure VPN Enterprise Server lässt sich problemlos in vorhandene IT-Infrastrukturen integrieren. In IPsec-Umgebungen ist er kompatibel zu VPN-Gateways anderer Hersteller. Zudem bietet er nicht nur Connectivity für NCP Secure Clients, sondern auch für alle Third Party IPsec VPN Clients.

Der modulare Aufbau des NCP Secure Enterprise Servers bietet Unternehmen ein hohes Maß an



Planungs- und Investitionssicherheit. Die Anzahl an Remote Usern und VPN-Tunnel ist beliebig skalierbar.

Management/Mandantenfähigkeit

Service Provider schätzen die ausgeklügelte Mandantenfähigkeit des VPN Gateways. Sie ermöglicht die gleichzeitige Nutzung eines VPN Gateways durch mehrere Unternehmen (Ressource Sharing). Über eine komfortable Zugriffsverwaltung lassen sich die NCP VPN Clients durch Administratoren der angebundenen Unternehmen managen*.

Zudem verfügt der NCP Secure Enterprise VPN Server über einen besonderen virtuellen Netzwerkadapter der die Daten so abschottet, dass sie weder vom Gateway-Betreiber noch vom umgebenden Betriebssystem einsehbar sind. Diese NCP Technologie ist besonders im Bereich Cloud Computing- oder für SaaS Provider-Umgebungen wichtig. Die Daten werden innerhalb eines virtuellen Netzwerkadapters (NCP Virtual Network Interface Adapter) entschlüsselt, von dort direkt in einen anderen VPN-Tunnel weitergeleitet und wieder verschlüsselt.

In großen Remote Access VPN-Netzen mit mehreren VPN Gateways sorgen die NCP High Availability Services für hohe Verfügbarkeit und gleichmäßige Auslastung aller installierten VPN Gateways.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Die Benutzerverwaltung erfolgt flexibel über Backend-Systeme wie z.B. RADIUS, LDAP oder MS Active Directory oder direkt am VPN Gateway. Integrierte IP-Routing und Firewall-Funktionalitäten sorgen für die erforderliche Connectivity und Sicherheit z.B. bei Filial-anbindungen.

Konfiguration und Verwaltung des NCP Secure Enterprise VPN Servers erfolgen über das NCP Secure Enterprise Management* mittels Plug-in oder über ein Webinterface. Die Managementfunktionen dienen der Steuerung und Überwachung aller VPN-Komponenten. Integrierte Automatismen sorgen für Transparenz, Optimierung der Performance, Sicherheit und Wirtschaftlichkeit der VPN-Lösung.

NCP VPN Path Finder

Mit dem "NCP VPN Path Finder" stellt NCP eine einzigartige Technologie bereit, die Remote Access auch hinter Firewalls ermöglicht, deren Einstellung IPsec-Datenverbindungen grundsätzlich verhindert (z.B. in Hotels) Hierbei wird automatisch in einen modifizierten IPsec-Protokoll-Modus gewechselt, der den zur Verfügung stehenden HTTPS-Port für den VPN-Tunnel nutzt.

Sicherheit/Starke Authentisierung

Weitere Security Features sind die Unterstützung von OTP-Lösungen (One Time Passwort) und Zertifikaten in einer PKI (Public Key Infrastructure) sowie Zertifikate mit elliptischen Kurven. Die Gültigkeit von Zertifikaten wird bei jedem Verbindungsaufbau anhand von Sperrlisten offline oder online gegenüber der Certification Authority (CA) überprüft.
Die integrierte „Advanced Authentication“ bietet eine Zwei-Faktor-Authentifizierung via SMS. Der Anwender erhält ein Einmalpasswort über den NCP Advanced Authentication Connector oder es wird durch einen SMS Service Provider an seine SIM Karte geschickt.

Endpoint-Security und Sandbox (Network Access Control = NAC**)

Mobile wie auch stationäre Endgeräte können vor dem Zugriff auf das Firmennetz auf deren aktuellen Sicherheitszustand hin überprüft werden. Alle Parameter werden dabei zentral vorgegeben. In Abhängigkeit davon erfolgt die Zugriffs-berechtigung des Teleworkers. In einem IPsec-VPN bestehen die Optionen "Disconnect" oder "Verbleib in der Quarantänezone". In einem SSL-VPN werden Zugriffsberechtigungen auf bestimmte Applikationen nach vorher festgelegten Sicherheitsstufen erteilt. Während einer SSL VPN-Session werden alle gespeicherten Daten in einem vom Betriebssystem abgekoppelten Arbeitsbereich – dem NCP Virtual Private Desktop (Sandbox) - verschlüsselt abgelegt. Nach Beenden der SSL VPN-Session werden alle in diesem "Container" abgelegten Informationen gelöscht. Die Einhaltung der Sicherheitsrichtlinien ist zwingend und vom Anwender nicht umgeh- bzw. manipulierbar.

IPSec und SSL

dem NCP Secure Enterprise Server lassen sich beliebig viele Datenverbindungen auf Basis eines IPsec- und/oder SSL-VPN zum Firmennetz aufbauen. Es besteht die Möglichkeit, dem NCP Secure Client bei jeder Verbindung die gleiche IP-Adresse zuzuweisen. Hierbei handelt es sich um eine private IP-Adresse aus dem Adressbereich des Unternehmens. Jeder Telearbeiter ist somit eindeutig anhand seiner IP-Adresse identifizierbar, was die remote Administration enorm vereinfacht.
Bei dynamischer Zuweisung einer IP-Adresse aus einem Pool wird diese innerhalb einer definierten Haltedauer (Lease Time) für einen bestimmten User reserviert. Für die Erreichbarkeit des VPN Gateways auch bei wechselnden IP-Adressen sorgt das Feature Dynamic DNS (DynDNS).

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

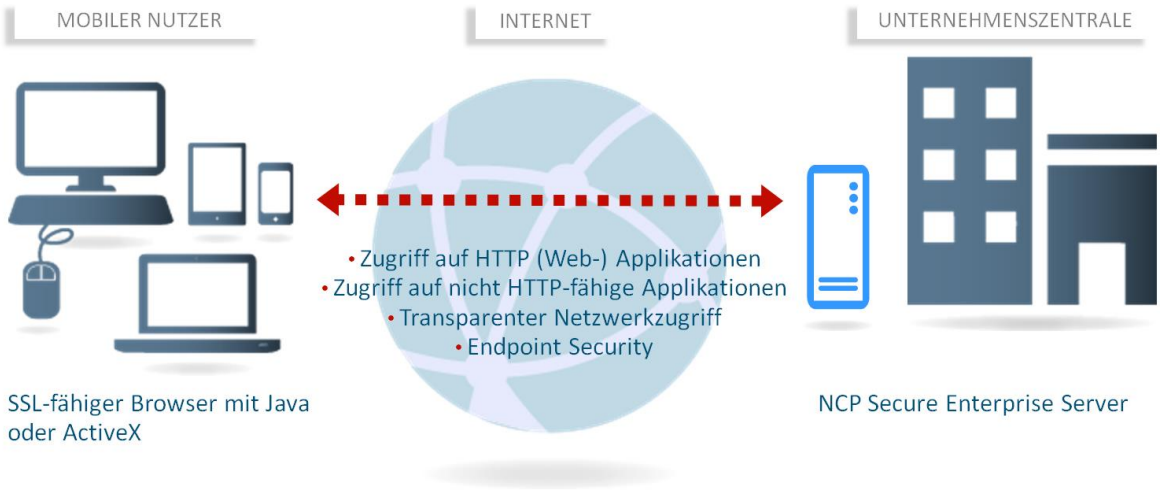
Bei der NCP SSL VPN-Lösung haben Sie folgende Optionen:

- **Web Proxy** - Dieses Modul ermöglicht autorisierten Benutzern den sicheren Zugriff auf interne Web-Applikationen.
- **Port Forwarding** – Der Thin Client dient für den Zugriff auf Client-/Server-Anwendungen (TCP/IP). Anbindung lokaler Client-Applikationen (http-fähig) via Port Forwarding. Dieser Thin Client wird bei jedem Zugriff automatisch auf das Endgerät heruntergeladen und ist Voraussetzung für die Nutzung zusätzlicher Sicherheitsoptionen wie Cache Protection, Endpoint Security und NCP Virtual Private Desktop.
- **PortableLAN** – Dieser Fat Client bietet transparenten Netzwerkzugriff und ist auf jedem Endgerät zu installieren.

Ausführliche Informationen entnehmen Sie bitte dem separaten Datenblatt zum NCP SSL VPN Server)

*) Nur in Verbindung mit dem NCP Secure Enterprise Management

**) Network Access Control ist fester Bestandteil des NCP SSL VPN Gateways. In einem IPsec VPN ist hierzu das NCP Secure Enterprise Management erforderlich



Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

IPsec VPN und SSL VPN – Allgemeines

Betriebssysteme	64-Bit: Windows Server 2016, Windows Server 2012 R2 und Windows Server 2008 R2 Linux Kernel ab Version 2.6.16 (Distributionen auf Anfrage)
Management	Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management mittels VPN Server Plug-in oder über Webinterface
Network Access Control (Endpoint Security)	Endpoint Policy Enforcement für kommende Datenverbindungen. Überprüfung vordefinierter, sicherheitsrelevanter Client-Parameter Maßnahmen bei Soll-/Ist-Abweichungen im IPsec VPN: • Disconnect oder Verbleib in die Quarantänezone mit Handlungsanweisungen (Messagebox) oder Starten externer Anwendungen (z.B. Virenscanner-Update), Protokollierung in Logfiles. (siehe hierzu Datenblatt „NCP Secure Enterprise Management“) Maßnahmen bei Soll-/Ist-Abweichungen im SSL VPN: • Granulare Abstufung der Zugriffsberechtigungen auf bestimmte Applikationen entsprechend vorgegebener Sicherheitslevels
Dynamic DNS (DynDNS)	Verbindungsaufbau via Internet mit dynamischen IP-Adressen. Registrierung der jeweils aktuellen IP-Adresse bei einem externen Dynamic DNS-Provider. Die Etablierung des VPN-Tunnels erfolgt dann über Namenszuordnung (Voraussetzung: VPN Client unterstützt DNS-Auflösung – wie NCP Secure Clients)
DDNS	Registrierung der verbundenen VPN Clients am Domain Name Server via DDNS, Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse
Netzwerkprotokolle	IP, VLAN-Support
Mandantenfähigkeit	Gruppenfähigkeit; Unterstützung von max. 256 Domänen-Gruppen (d.h. Konfiguration von: Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.) Unterstützung mehrerer Server-Zertifikate: • Es kann für verschiedene Domain-Groups ein anderes "Default"-Zertifikat eingestellt werden • Der SES kann aus mehreren konfigurierten Zertifikaten dasjenige aussuchen, welches am besten zur Anfrage des Client passt (z.B. längste Laufzeit)
Benutzerverwaltung	Lokale Benutzerverwaltung (bis zu 750 Benutzer); OTP-Server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistik und Logging	Detaillierte Statistik, Logging-Funktionalität, Versenden von SYSLOG-Meldungen
FIPS Inside	Der IPsec Client integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1747). Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden:

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

	• Diffie Hellman-Gruppe: Gruppe 2 oder höher (DH ab einer Länge von 1024 Bit) • Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit • Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES
IF-MAP	Das Gesamtziel des ESUKOM Vorhabens ist die Konzeption und Entwicklung einer Echtzeit-Sicherheitslösung für Unternehmensnetze, die basierend auf der Konsolidierung von Metadaten arbeitet. Dabei soll insbesondere der durch mobile Endgeräte wie Smartphones erzeugten Bedrohungslage Rechnung getragen werden. ESUKOM setzt auf die Integration vorhandener Sicherheitslösungen (kommerziell und Open Source) basierend auf einem einheitlichen Metadatenformat gemäß der IF-MAP-Spezifikation der Trusted Computing Group (TCG). Derzeit kann der IF-MAP Server der Fachhochschule Hannover kostenfrei für Tests genutzt werden. Die URL lautet http://trust.f4.hs-hannover.de/
Client/Benutzer Authentifizierungsverfahren	OTP-Token, Zertifikate (X.509 v.3): Benutzer- und Hardwarezertifikate (IPsec), Benutzername und Password (XAUTH)

Zertifikate (X.509 v.3)

Server-Zertifikate	Es können Zertifikate verwendet werden die über folgende Schnittstellen bereitgestellt werden: PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); PKCS#12 Interface für Private Schlüssel in Soft-Zertifikaten
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, vorm. CRL), CARL (Certification Authority Revocation List, vorm. ARL)
Online Check	automatische Downloads der Sperrlisten einer CA in bestimmten Zeitintervallen; Online-Check: Überprüfung der Zertifikate mittels OCSP oder OCSP over http

IPsec VPN und SSL VPN – Verbindungsmanagement

Übertragungsmedien	LAN; Direktbetrieb am WAN: Unterstützung von max. 120 ISDN B-Kanälen (SO, S2M)
Line Management	DPD mit konfigurierbarem Zeitintervall; Short Hold Mode; Kanalbündelung (dynamisch im ISDN) mit frei konfigurierbarem Schwellwert; Timeout (zeit- und gebührengesteuert)
Point-to-Point Protokolle	PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet; LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool-Adressverwaltung	Reservierung einer IP-Adresse aus einem Pool innerhalb einer definierten Haltedauer (Lease Time)
Lockruf	Direktanwahl des dezentralen VPN Gateways über ISDN, „Anklopfen im D-Kanal“

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

IPsec-VPN

Virtual Private Networking	IPsec (Layer 3 Tunneling), RFC-konform; Automatische Behandlung der MTU Size, Fragmentation und Reassembly; DPD; NAT-Traversal (NAT-T); IPsec Modes: Tunnel Mode, Transport Mode; Seamless Rekeying; PFS
Internet Society RFCs und Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (inkl. MOBIKE), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP
Verschlüsselung	Symmetrische Verfahren: AES 128,192,256 Bits; Blowfish 128,448 Bits; Triple-DES 112,168 Bits; Dynamische Verfahren für den Schlüsselaustausch: RSA bis 4096 Bits; Diffie-Hellman Groups 1,2,5,14-21, 25, 26; Hash Algorithmen: (MD5), SHA1, SHA 256, SHA 384, SHA 512
Firewall	Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN-Adapterschutz
VPN Path Finder	NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist (Voraussetzung: NCP Secure Enterprise VPN Server 8.0)
Seamless Roaming	Automatische Umschaltung des VPN-Tunnels auf ein anderes Internet-Übertragungsmedium (LAN/WLAN/3G/4G) ohne IP-Adresswechsel, so dass über den VPN-Tunnel kommunizierende Anwendungen nicht beeinflusst werden, bzw. die Anwendungs-Session nicht getrennt wird
Authentisierungsverfahren	IKE (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards, USB Tokens, Zertifikate mit ECC-Technologie; Pre-Shared Keys; One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready
IP Address Allocation	DHCP (Dynamic Host Control Protocol) over IPsec; DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server; IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse an die Clients aus dem internen Adressbereich (private IP) Unterscheidung des Pools anhand des Verbindungsmediums möglich (Client VPN-IP)
Datenkompression	IPCOMP (lzs), Deflate

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Empfohlene VPN Clients / Kompatibilitäten	
NCP Secure Entry Clients	Windows 32/64, macOS, Windows Mobile, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Windows Mobile, Android, Windows CE, Linux

SSL-VPN

Protokolle	SSLv1, SSLv2, TLSv1 (Application-Layer Tunneling)
Web Proxy	Zugriff auf interne Web-Anwendungen und Microsoft Netzlaufwerke über ein Web-Interface Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität
Secure Remote File Access*	Up- und Download, Erstellen und Löschen von Verzeichnissen, entspricht in etwa den Funktionalitäten des Datei-Explorers unter Windows. Voraussetzungen am Endgerät: siehe Web Proxy
Port Forwarding	Zugriff auf Client-/Server-Anwendungen (TCP/IP), Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V1.5) oder ActiveX, SSL Thin Client für Windows 10, 8.x, 7 (32/64 Bit) und Linux
NCP Virtual Private Desktop	Der Virtual Private Desktop ist ein vom Basis-Betriebssystem abgekoppelter Arbeitsbereich, der dem Anwender für eine SSL VPN-Session zur Verfügung gestellt wird. Anwendungen, die in diesem Bereich gestartet werden, werden vom Basis-Betriebssystem entkoppelt. Innerhalb des Virtual Private Desktop gespeicherte Daten, beispielsweise Dateianhänge empfangender E-Mails, werden in einem Container AES-verschlüsselt gespeichert. Bei Beendigung der SSL VPN-Session werden alle im Container abgelegten Dateien gelöscht.
Cache Protection für Internet Explorer und Edge	Alle übertragenen Daten werden nach dem Verbindungsabbau automatisch am Endgerät gelöscht.
PortableLAN	Transparenter Zugriff auf das Firmennetz Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V5.0) oder ActiveX Control, PortableLAN Client für Windows 10, 8.x, 7
Single Sign-on	Single Sign-on kann immer dann eingesetzt werden, wenn die Web Server-Anwendung die gleichen Zugangsdaten benötigt wie der SSL VPN Client. Die zentrale Verwaltung von Benutzername und Passwort kann dazu unter anderem über Active Directory, RADIUS oder LDAP erfolgen.

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com

Je nach Anwendung kann zwischen Single Sign-on mit HTTP-Authentisierung (Basic (RFC2617), HTTP Digest (RFC2617) und NTLM (Microsoft)) oder Single Sign-on nach der Post Form-Methode unterschieden werden.
Single Sign-on mit Web-Applikationen wurde mit Outlook Web Access (OWA) 2003, 2007 und 2010, RDP Client und CITRIX Webinterface 4.5, 5.1 getestet.
Single Sign-on mit Port Forwarding wird nur von Anwendungen unterstützt, die Parameter (wie Benutzername und Passwort) in ihrer Kommandozeile entgegennehmen können

FIPS 140-2 Inside

Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299 • V 11.0
Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com