Datenblatt

NCP Secure Enterprise VPN Server

Leistungsstarke IPsec VPN Gateway Software

Universelle Plattform für den Fernzugriff auf das Firmennetz

- Hohe Skalierbarkeit durch Multi-Prozessor/Core-Unterstützung
- Integrierte IP-Routing- und Firewall-Funktionalitäten
- Kompatibel zu NCP Secure Clients für Windows, macOS, Linux, iOS, Android und zahlreichen anderen IPsec-VPN Clients
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Automatische Tunnelweiterleitung
- FIPS Inside
- Mandantenfähigkeit
- Endpoint Policy Enforcement / Network Access Control*
- Unterstützt elliptische Kurven (ECC)

Kompatibilität

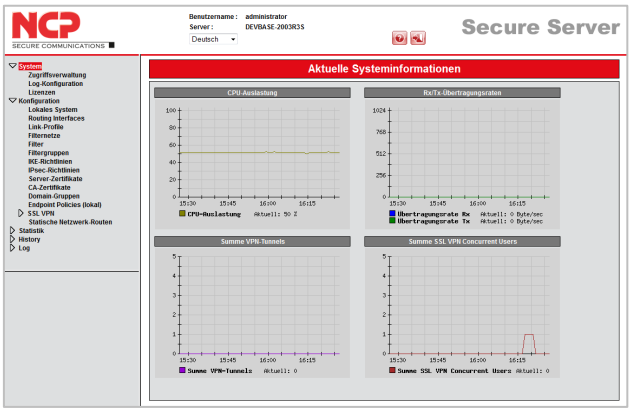
Der NCP Secure Enterprise Server ist ein Baustein der ganzheitlichen NCP Remote Access VPN-Lösung. Über das VPN Gateway werden mobile und stationäre Mitarbeiter in einem unternehmens-übergreifenden Datennetz integriert. Die Software wird auf einem Server unter Windows oder Linux installiert und fungiert 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). Aufgrund der Mandantenfähigkeit des NCP Secure Enterprise Management Servers lassen sich für den jeweiligen Mandanten zuständige Administratoren konfigurieren*.

Zudem verfügt der NCP Secure Enterprise VPN Server über einen virtuellen Netzwerk-Adapter, der die Daten so abschottet, dass sie weder vom Gateway-Betreiber noch vom umgebenden Betriebssystem einsehbar sind.

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.

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.

Die Konfiguration und Verwaltung des NCP Secure Enterprise VPN Servers erfolgt 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 basierend auf Elliptic Curve Cryptography. 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 SM- Service-Provider an seine SIM Karte geschickt.

Endpoint-Security (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 Mitarbeiters. In einem IPsec-VPN bestehen die Optionen „Disconnect“ oder „Verbleib in der Quarantänezone“.

IPSec VPN

Mit dem NCP Secure Enterprise Server lassen sich beliebig viele Datenverbindungen auf Basis eines IPsec-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 Remote Mitarbeiter 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).

*) Nur in Verbindung mit dem NCP Secure Enterprise Management

IPsec VPN – Allgemeines

Betriebssysteme	Windows Server 2022, Windows Server 2019; Debian, Red Hat, SLES; Linux-Distributionen mit Kernelversion ab 4.9, glibc ab 2.23
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“)
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. 1024 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 Clients 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). Die FIPS Kompatibilität ist immer gegeben, wenn einer der folgenden Algorithmen für Aufbau und Verschlüsselung der IPsec-Verbindung genutzt werden: • 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

Verbindungsmanagement

Line Management	DPD mit konfigurierbarem Zeitintervall; Timeout (zeit- und gebührengesteuert)
Point-to-Point Protokolle	LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool-Adressverwaltung	Reservierung einer IP-Adresse aus einem Pool innerhalb einer definierten Haltedauer (Lease Time)

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, IKEv2-Authentisierung nach RFC 7427 (Padding-Verfahren)
Verschlüsselung	Symmetrische Verfahren: AES (CBC/CTR/GCM) 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, 25-30; Hash Algorithmen: SHA-1, 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

Seamless Roaming	In Verbindung mit einem NCP Secure Client ist folgende Funktionalität gegeben: 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	IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung; IKEv2, EAP-PAP/MD5/MS-CHAP v2/TLS Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, 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
Empfohlene VPN Clients / Kompatibilitäten	
NCP Secure Entry Clients	Windows, macOS
NCP Secure Enterprise Clients	Windows, macOS, iOS, Android, Linux

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg
Germany

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com