NCP Secure Enterprise VPN Server (Linux)
Release Notes

Service Release: **11.03 r48720**
Datum: **Juli 2021**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Absturz des ncpsrvmgmd-Dienstes

In seltenen Fällen kam es zum Absturz des ncpsrvmgmd-Dienstes. Dieses Problem wurde behoben.

Verbesserung der HA Server Verfügbarkeitsüberprüfung und Erweiterung der zugehörigen Log-Ausgaben

Fehlerbehebung in OpenSSL Bibliothek hinsichtlich [CVE-2020-1971]

Die verwendete OpenSSL Bibliothek war anfällig hinsichtlich der Sicherheitslücke [CVE-2020-1971]. Diese trat im Bereich der Zertifikatsprüfung via CRL auf. Jedoch musste hierfür sowohl das Zertifikat als auch die CRL kompromittiert sein. Dieses Problem wurde behoben.

3. Bekannte Einschränkungen

Keine.

Projektfreigabe: **11.02 r44405**
Datum: **Juni 2019**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine.

2. Verbesserungen / Fehlerbehebungen

Absturz – segmentation fault

Dieses Problem wurde behoben.

Allgemeine Stabilitätsverbesserungen im NCP SSL VPN-Dienst sowie in Verbindung mit Advanced Authentication

3. Bekannte Einschränkungen

Keine.

Projektfreigabe: **11.01 r41055**
Datum: **Mai 2018**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Fehlerbehebung im IP-NAT Modul

Korrektur bei der Benennung von Core-Dump-Verzeichnissen

Fehlerbehebung bei eingehenden L2TP-Verbindungen

Das Gateway hat maximal nur 10 eingehende L2TP-Verbindungen akzeptiert. Dieser Fehler wurde behoben.

Die max. Größe von String-Radius-Parametern wurde auf 253 Byte hochgesetzt.

3. Bekannte Einschränkungen

Keine

Projektfreigabe: **11.01 r39590**
Datum: **Mai 2018**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

L2TP/L2Sec-Tunnelweiterleitung

Bei einer L2TP/L2Sec Site-2-Site-Verbindung zweier Gateways konnten trotz aktiv angezeigter Verbindung keine Daten transferiert werden. Dieser Fehler ist nun behoben.

Probleme beim Start des Serverdienstes des NCP Secure Enterprise VPN Servers nach Update

Nach einem Update des NCP Secure Enterprise VPN Servers der Version 10 auf die Version 11 konnte

ein zusätzlicher Neustart des Systems für einen korrekten Start der Serverdienste notwendig sein. Dieses Fehlverhalten ist mit dieser Release behoben.

Verbesserter Datendurchsatz nach Rechnerneustart

Durch eine fehlerhafte Initialisierungsreihenfolge im Linux-Betriebssystem wurden Kernelmodule zu spät geladen, daher wurde beim Start des NCP Secure Enterprise VPN Servers nicht erkannt, dass das System die Load-Balancing Funktionalität der NFQueue beherrscht. Dieses Problem ist nun behoben.

Ein Problem bei der Übertragung von Netzadressen und -masken via RADIUS-IPsec-Selektoren wurde behoben

Eine Sicherheitslücke in Verbindung mit NET-SNMP Version 5.7.2 wurde behoben (CVE-2018-1000116)

3. Bekannte Einschränkungen

Keine

Service Release: **11.01 r38204**
Datum: **Dezember 2017**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.4
- Debian GNU/Linux 9.2.1
- SUSE Linux Enterprise Server 12 SP3
- Ubuntu Server 16.04.3 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 4.05 oder höher
- Management Console Version 4.05 oder höher
- Management Plug-in Server Configuration Version 11.00 oder höher
- Secure Enterprise HA Server Version 10.01 oder höher

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Die Ausführung des VRRP-Scripts funktioniert nun auch unter CentOS 7.4.

Bei der Installation unter Debian ab 9.0 wird der Fall berücksichtigt, dass bei der Betriebssystem-Installation dem Root-Benutzer kein Passwort zugewiesen wurde.

Nach einem Update auf Version 11.0 oder deren Neu-Installation musste ein Reboot des Systems durchgeführt werden, bevor der Server gestartet werden konnte. Dieser Fehler ist behoben. Nach einem Neustart des SNMP-Dienstes sind auch SNMP-Abfragen möglich.

Beim Download der CRL-Liste konnte ein Absturz des Dienstes ncpsrvmgm erfolgen. Dieser Fehler ist behoben.

SEM-Anfragen für Software Update über LAN werden nicht mehr weitergeleitet.

Mit dem RADIUS-Attribut "NCPS-PCCertCN" = "*" wird die Verwendung eines Hardware-Zertifikats erzwungen.

Weiterleitung von "nicht an den Secure Server Adapter gebundenen VPN IP-Adressen" funktioniert wieder.

Die Auswahl des Server-Zertifikates erfolgt so wie sie eingestellt wurden, entweder „automatisch“ vom Server oder „manuell konfiguriert“.

Der Server änderte beim Start die Reihenfolge in der Konfigurationsdatei ncpwsupd.conf. Dieser Fehler wurde behoben.

Wenn keine Daten über die VPN-Verbindung mehr geschickt werden, bleiben die Path Finder Sessions nicht länger geöffnet, sondern werden automatisch abgebaut.

Der Secure Enterprise Server unterstützt nun auch Pathfinder 2 und SSL-VPN, wenn ECC-Zertifikate konfiguriert werden.

In der Konfigurations-Webseite des SES erschien sporadisch fälschlicherweise die Meldung: „Änderungen erfordern einen Neustart des NCP Secure Enterprise Servers!“

Bei konfigurierter „ARRE-Option“ konnte es vorkommen, dass der Server keine VPN-Verbindungen mehr akzeptierte. Dieser Fehler ist behoben.

Wurden Filter für den VPN-Datenstrom gesetzt, so wurden äußerst sporadisch Datenpakete dennoch weitergeleitet. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Keine

Major Release: **11.0 r36600**
Datum: **August 2017**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Gelöschte Domaingruppen nach Update auf Version 11.0

Ist innerhalb der Domain-Gruppen-Konfiguration im NCP Secure Enterprise VPN Server die Option „Erlaube nur die ausgewählten CA-Zertifikate“ ausgewählt, werden mit dem Update des NCP Secure Enterprise VPN Servers auf die Version 11.0 die Domain-Gruppen, einschließlich der Standard-Domain-Gruppe, gelöscht. Dieser Fehler ist behoben.

3. Bekannte Einschränkungen

Keine

Major Release: **11.00 r36322**
Datum: **Juli 2017**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server produktiv nutzen zu können.

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

IKEv2-Verbindung mit Computer- und Benutzerzertifikat

War für eine VPN-Verbindung über IKEv2 die Authentisierung des Gerätes über Computerzertifikat **und gleichzeitig** die Authentisierung des Benutzers über Benutzerzertifikat erforderlich, schlug der Verbindungsaufbau fehl. Dieser Fehler ist nun behoben.

Anzeige von Benutzern, die über LDAP authentisiert werden

VPN-Benutzer, die über LDAP authentisiert werden, wurden fälschlicherweise in der Statistik unter „Link-Profile (lokal)“ aufgelistet. Dieser Fehler ist behoben, sodass sie nun korrekt unter „Link-Profile (RADIUS/LDAP)“ angezeigt werden.

Die maximale Anzahl der gleichzeitig möglichen LDAP-Benutzer wurde von 10.000 auf 40.000 erhöht.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/gateway/

Major Release: **11.00 r36173**
Datum: **Juli 2017**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server mit dem Secure Enterprise HA Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Erweitertes Lizenzmanagement für iOS Clients

Ab dieser Version des NCP Secure Enterprise VPN Servers wird das Lizenzmanagement des NCP Secure Enterprise iOS Clients unterstützt.

Deutliche Performanceverbesserungen

Erhöhung möglicher ausgehender Verbindungen

Die maximale Anzahl von ausgehenden VPN-Verbindungen wurde von 750 auf 10000 erhöht.

IKEv2 Signature Authentication nach RFC 7427 mit RSA-PSS-Padding

Im Client und Server wurde eine neue Zertifikats-Authentisierungsmethode nach RFC7427 implementiert.

Für Benutzer- und Hardware-Zertifikate werden folgende Schlüsseltypen unterstützt: RSA, ECC NIST, ECC BP in verschiedenen Schlüssellängen.

In der „Zertifikatsüberprüfung“ einer Domain-Gruppe ist der Schalter „Erlaube RSA Authentisierung mit PKCS#1 V1.5 Padding“ standardmäßig aktiv. Nur wenn dieser Schalter deaktiviert wird, kann die bisherige IKEv2 RSA-Zertifikatsauthentisierung noch genutzt werden.

Client VPN-IP-Adresszuweisung für getaktete Verbindung

Diese Funktionalität findet Verwendung in Home Office-Umgebungen, bei denen die Internetanbindung des Routers über ein Medium mit volumenabhängiger Abrechnung erfolgt, vorzugsweise Mobilfunk. Der Anwenderarbeitsplatz ist dabei über WLAN an den Internet-Router angebunden. In diesem Fall kann das zugehörige WLAN-Profil des NCP Secure Clients in den Profileinstellungen als „getaktete Verbindung“ („metered connection“) konfiguriert werden. Dieses Merkmal wird zur weiteren Verarbeitung an den NCP Secure Enterprise VPN Server gesendet.

Zur Kostenersparnis bei Volumentarifen, erhält der Client beim Tunnelaufbau vom Server eine IP-Adresse aus einem dafür angelegten Pool für Clients mit Mobilfunkanbindung. Zentralseitige Anwendungen, die den Client mit Updates versorgen, können nur Datenpakete an den Client übertragen, die auf das Nötigste reduziert sind.

Am Server werden unter „Adressvergabe“ die Pool-Bereiche für getaktete Verbindungen definiert und erhalten eine Ordnungsnummer. Mit dem Eintragen dieser Nummer im Link-Profil unter „Routing“ wird dem Client eine IP-Adresse aus dem entsprechenden Pool zugewiesen. Werden an dieser Stelle die Pool-Nummern auf null gesetzt und ist keine feste IP-Adresse vergeben, so wird der IP-Adressbereich des konfigurierten DHCP-Servers genutzt.

Unterstützung mehrerer Server-Zertifikate

Pro Domain-Gruppe können nun verschiedene Standard-Zertifikate eingestellt werden. Der Secure Enterprise VPN Server kann daraus für die jeweilige Domain-Gruppe dasjenige selektieren, welches am besten zur Anfrage des Clients passt (z.B. längste Laufzeit).

Zusätzliche Sicherheitsbarriere

Die sicherheitskritischen Server-Dienste ncpwsupd und ncpsrvmgmd werden mit eingeschränkten Rechten betrieben, um potentielle Systemangriffe zu erschweren.

Anzeige zusätzlicher Verbindungsinformationen

Folgende Informationen werden in der Statistik unter „Link-Profile“ angezeigt:
– NCP VPN Path Finder Version
– Seamless Roaming
Im Account Log wird angezeigt, auf welche lokale Endpunkt-IP-Adresse sich der Client einwählt.

2. Verbesserungen / Fehlerbehebungen

Beim Verbindungsaufbau der Clients wurde die Netzmaske nicht korrekt übertragen. Dieser Fehler ist behoben.

Neues Tool zur Erstellung der Scripte für dve_up und dve_down unter [SES-INSTALL-DIR]/sbin/ses-vrrp-setup.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:
https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/gateway/

5. Leistungsmerkmale des NCP Secure Enterprise VPN Servers

Zentrale Verwaltung mit Konfigurations-Manager

Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management (SEM) mittels VPN Server Plug-in oder über Webinterface.

Betriebssysteme

Beachten Sie dazu die “Voraussetzungen” auf Seite 1.

Security Features

Unterstützung aller IPsec-Standards nach RFC.

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:

- 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“

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;

Encryption
Symmetric processes: AES 128,192,256 bits;
Blowfish 128,448 bits; Triple-DES 112,168 bits;
Dynamic processes for key exchange: RSA to 4096 bits;
Diffie-Hellman Groups 1,2,5,14-21, 25, 26;
Hash algorithm: MD5, SHA1, SHA 256, SHA 384, SHA 512;

Firewall
Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN adapter protection;

VPN Path Finder
NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500, respectively UDP encapsulation is not possible (Prerequisite: NCP Secure Enterprise VPN Server 8.0);

Seamless Roaming
With Seamless Roaming, the system automatically connects the VPN tunnel to a different Internet communication medium (LAN/ WiFi/ 3G/ 4G) without changing the IP address, so that the communication of the application through this tunnel is not interfered with and the application's session is not disconnected.

Authentisierungsverfahren
IKE (Aggressive and Main Mode), Quick Mode;
XAUTH for extended user authentication;
Support of certificates in a PKI: Soft certificates, smart cards, USB tokens, certificates with ECC technology; Pre-shared keys;
One-time passwords and challenge response systems; RSA SecurID ready;

IP Address Allocation
DHCP (Dynamic Host Control Protocol) over IPsec;
DNS: Selection of the central gateway with changing public IP address by querying the IP address via a DNS server; IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP);

Data Compression
IPCOMP (lzs), Deflate;

VPN- Architektur

Empfohlene Systemvoraussetzungen
CPU: ab Pentium III oder kompatible CPU;
Arbeitsspeicher: Mind. 512 MByte zzgl. 0,256 MByte pro gleichzeitig genutztem VPN-Tunnel;
64 MByte bei 250 gleichzeitigen VPN-Tunneln;
Datendurchsatz (inkl. symmetrischer Verschlüsselung):
Single Core: Datendurchsatz [MBit/Sek.] ≈ Taktfrequenz [MHz]/150 MHz* 8,5 MBit/Sek.
Dual Core: Datendurchsatz [MBit/Sek.] ≈ Taktfrequenz [MHz]/150 MHz*12,5 MBit/Sek.
Triple Core: Datendurchsatz [MBit/Sek.] ≈ Taktfrequenz [MHz]/150 MHz*15,5 MBit/Sek.
Quad Core: Datendurchsatz [MBit/Sek.] ≈ Taktfrequenz [MHz]/150 MHz*17,5 MBit/Sek.
Wie aus obiger Näherungsformel zum Datendurchsatz ersichtlich ist, liefert eine weitere Erhöhung der Anzahl an CPU Cores keine proportionale Steigerung des Datendurchsatzes.

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 7/8/10 (32/64 Bit) oder Linux;

NCP Virtual 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.
Voraussetzungen am Endgerät: SSL-fähiger Web-Browser mit Java Script-Funktionalität, Java Runtime Environment (>= V5.0), SSL Thin Client für Windows 7/8/10 (32/64 Bit);

Portable LAN
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 7/8/10;

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.
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.

Empfohlene Systemvoraussetzungen*
1-100 Concurrent User:
CPU: Intel Dual Core 1,83 GHz oder vergleichbarer x86 Prozessor,
1024 MB Arbeitsspeicher
200+ Concurrent User:
CPU: Intel Dual Core 2,66 GHz oder vergleichbarer x86 Prozessor,
1024 MB Arbeitsspeicher

*) Abhängig vom Endgerätetyp. Es gibt Einschränkungen bei mobilen Endgeräten wie Tablet PCs (z.B. unter iOS, Android), Smartphones, PDAs etc.