Release Notes

NCP Secure Enterprise VPN Server

Service Release 10.0 r29844 (Linux 64)
Mai 2016

Voraussetzungen

Diese Version ist nur für 64-Bit-Versionen folgender Distributionen freigegeben:

- SuSE Linux Enterprise Server 12
- CentOS 7.1
- Ubuntu Server 14.04.2
- Debian GNU/Linux 8.1.0

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)

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

- Secure Enterprise Management Server: Version 3.02 or later
- Management Plugin - Server Configuration: Version 10.00 r26953 or later

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

Keine

2. Fehlerbehebung und Änderungen

Anpassung der Installationsroutine

Mit diesem Release wurden Anpassungen der Installationsroutine für die Linux-Plattformen vorgenommen.

Denial-of-Service-Verwundbarkeit

Eine Denial-of-Service-Verwundbarkeit wurde beseitigt, die in früheren Versionen unter besonderen Umständen zu einem Absturz des Servers führen konnte.

Verbesserung der Kompatibilität bei IKEv2 und Rekeying

Eine Kompatibilitätsanpassung an den IKEv2-Standard wurde mit diesem Release durchgeführt. Beachten Sie bitte bei Einsatz von Rekeying, dass das Rekeying-Intervall des Clients der Standardeinstellung entspricht und kleiner ist als das des Servers.

Sollte das Rekeying-Intervall des Clients größer sein als das Rekeying-Intervall des Servers, so können Verbindungsabbrüche auftreten.

Adressvergabe über DHCP

Bei Einsatz von IKEv2 konnte im Fall der Adressvergabe über DHCP der Hostname des Anwender-PCs nicht an den DHCP-Server übertragen werden, sondern lediglich der VPN-Benutzer.

3. Bekannte Einschränkungen

Keine

Release Notes

Service Release 10.0 r28737 (Linux 64)
März 2016

Voraussetzungen

Diese Version ist nur für 64-Bit-Versionen folgender Distributionen freigegeben:

- SuSE Linux Enterprise Server 12
- CentOS 7.1
- Ubuntu Server 14.04.2
- Debian GNU/Linux 8.1.0

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)

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

- Secure Enterprise Management Server: Version 3.02 or later
- Management Plugin - Server Configuration: Version 10.00 r26953 or later

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

Keine

2. Fehlerbehebung und Änderungen

Instabilität beim Neustart

Wurde der Secure Enterprise VPN Server während des Betriebs neu gestartet, ohne bestehende VPN-Verbindungen zu beenden, so konnte es aufgrund client-seitig weiterhin bestehender VPN-Sessions zu einem Absturz des Dienstes ncpwsup kommen. Dieser Fehler wurde behoben.

3. Bekannte Einschränkungen

Keine

Release Notes

Service Release 10.0 r27571 (Linux 64)
Januar 2016

Voraussetzungen

Diese Version ist nur für 64-Bit-Versionen folgender Distributionen freigegeben:

- SuSE Linux Enterprise Server 12
- CentOS 7.1
- Ubuntu Server 14.04.2
- Debian GNU/Linux 8.1.0

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)

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

- Secure Enterprise Management Server: Version 3.02 or later
- Management Plugin - Server Configuration: Version 10.00 r26953 or later

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.

Für den Betrieb dieses Secure Enterprise Servers im HA-Verbund wird ein HA Server ab der Version 10.0 r26952 benötigt.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Fehlerbehebung und Änderungen

VRRP-Adresse des Servers

Wurde die VRRP-Funktionalität im SES konfiguriert und dabei eine VRRP-Adresse eingetragen, die nicht im IP-Adressbereich des LAN-Adapters lag, so kam es zu einer Fehlfunktion. Dieser Fehler ist nun behoben.

3. Bekannte Einschränkungen

Keine

Release Notes

Service Release 10.0 r26968 (Linux 64)
Dezember 2015

Voraussetzungen

Diese Version ist nur für 64-Bit-Versionen folgender Distributionen freigegeben:

- SuSE Linux Enterprise Server 12
- CentOS 7.1
- Ubuntu Server 14.04.2
- Debian GNU/Linux 8.1.0

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)

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

- Secure Enterprise Management Server: Version 3.02 or later
- Management Plugin - Server Configuration: Version 10.00 r26953 or later

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.

Für den Betrieb dieses Secure Enterprise Servers (10.0 r26968) im HA-Verbund wird ein HA Server der Version 10.0 r26952 benötigt.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Fehlerbehebung und Änderungen

Sortierung in der Filtertabelle

Die Einträge der Filtertabelle am Server werden alphabetisch sortiert. Das Server Configuration Plugin ab Version 10.00 r26953 wurde dementsprechend angepasst.

Anzahl der Domain-Gruppen

Der Funktionsfehler des Management-Dienstes, der bei einer großen Anzahl von Domain-Gruppen auftrat, wurde behoben. Das Server Configuration Plugin ab Version 10.00 r26953 wurde dementsprechend angepasst.

3. Bekannte Einschränkungen

Keine

Major Release 10.0 r25102 (Linux 64)
August 2015

Voraussetzungen

Diese Version ist nur für 64-Bit-Versionen folgender Distributionen freigegeben:
- SuSE Linux Enterprise Server 12
- CentOS 7.1
- Ubuntu Server 14.04.2
- Debian GNU/Linux 8.1.0

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)

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

- Secure Enterprise Management Server: ab Version 3.02
- Management Plugin - Server Configuration: ab NCP_MgmPlugin_SrvCfg 10.00 rev24663
- HA Server, bei HA-Nutzung: ab Version 10.0 rev24099

1. Neue Leistungsmerkmale und Erweiterungen

Lizenzierung der Server-Komponenten Secure Enterprise VPN Server und Secure Enterprise HA Server

Ab den Software-Versionen 10.0 wird ein Lizenzschlüssel der gleichen Version benötigt, um die Server-Komponenten produktiv nutzen zu können. Server früherer Versionen 8.x, die ohne die entsprechende Aktualisierung des Lizenzschlüssels auf die Version 10.0 oder höher mit einem Update angehoben werden sollen, verlieren ihre Funktionalität.

Die Notwendigkeit gleicher Software-Version und Lizenzschlüssel-Version zur Freischaltung der Software gilt ab der Version 10.0 für alle späteren Versionen.

Keine Unterstützung mehr für IPsec over L2TP-Protokoll

Die Unterstützung von IPsec over L2TP ist ab dieser Version nicht mehr im NCP Secure Enterprise VPN Server enthalten.

Kompatibilität mit nativen IPsec/IKEv2-Clients

Native IPsec Clients der Plattformen Blackberry und Windows Phone 8.1 sind beim IKEv2-Schlüsselaustausch kompatibel zum NCP Secure Enterprise VPN Server, wenn einer dieser Authentisierungsmodi eingesetzt wird:
- Benutzername und Passwort
- Zertifikat (EAP-TLS/EAP-MD5/EAP-OTP/EAP-MSCHAPv2)

IP-Adresszuweisung für Clients

Die Adresszuweisung für Clients kann anhand folgender Merkmale über einen externen DHCP-Server erfolgen:
- MAC-Adresse
- Host-Name oder
- Benutzername

Unterstützung weiterer Verschlüsselungsalgorithmen (Suite B Cryptography)

Folgende Algorithmen werden zusätzlich unterstützt:

- AES-CTR/GCM
- Elliptic Curve Digital Signature Algorithm/Diffie-Hellman
- Secure Hash Algorithm 2 (SHA-256, SHA-384)

Erweiterte Konfigurations-Regeln (Adv. Configuration Rules)

Innerhalb einer Domain-Gruppe am Server können Attribute aus dem Verzeichnisdienst eines Mandanten zur Bestimmung der Zugangsparameter des Clients verwendet werden.

Für den Netzzugang der Clients können folgende Parameter genutzt werden:

- IP-Pool
- Filter-Gruppe
- Benutzer-Priorität
- Policy Name (Richtlinien-Name) / Filter-Gruppe
- DHCP Source-IP-Address / Netzwerkmaske (Network Masc)

Das Parameterfeld „Erw. Konfigurations-Regeln" befindet sich im Konfigurationszweig „Domain-Gruppen

IPv6 innerhalb des VPN-Tunnels

Das IPv6-Protokoll ist grundsätzlich für die Kommunikation innerhalb des VPN-Tunnels verfügbar. Dies betrifft folgende Parameter:

- Link-Profile / Routing
- Link-Profile / IPsec-Selektoren
- Link-Profile / IPsec-Optionen
- Filternetze
- Filter
- Domain-Gruppen / RADIUS
- Domain-Gruppen / OTP
- Domain-Gruppen / Link-Profile

Derzeit sind noch nicht alle Funktionalitäten (Mechanismen) IPv6-fähig, wie beispielsweise die für die IP-Adressvergabe. Deren Integration erfolgt mit künftigen Wartungs-Releases.

Load Balancing Unterstützung für Apple iOS Geräte (mit und ohne VRRP)

Der in iOS integrierte VPN IPsec Client kann sich mit NCP Secure Enterprise VPN Servern, die im Load Balancing Verbund arbeiten, verbinden. Der Client wird dann mit dem am wenigsten ausgelasteten Server verbunden.

NCP VPN Path Finder II

Der NCP Secure Enterprise VPN Server bietet das NCP VPN Path Finder Protokoll als Fallback zu einer IPsec-Verbindung an, falls IPsec im Signalweg zwischen Client und Server z.B. wegen eines Proxies nicht möglich ist. NCP VPN Path Finder II steht ab dieser Serverversion ergänzend zur Verfügung und bietet eine echte SSL-Verschlüsselung, so dass auch die seltenen Fälle in denen NCP VPN Path Finder geblockt wurde zukünftig nicht mehr auftreten. Der NCP Secure Client versucht bei einem Scheitern des IPsec Verbindungsaufbaus zunächst eine Verbindung mit NCP VPN Path Finder aufzubauen. Sollte diese scheitern, so wird im Client automatisch auf echte SSL-Verschlüsselung – NCP VPN Path Finder II – umgeschaltet.

Performancesteigerungen bzw. Durchsatzsteigerungen

Die Multiprozessorunterstützung des NCP Secure Enterprise VPN Servers wurde deutlich erweitert und damit die Performance signifikant erhöht. Da der Einsatz von OpenSSL im FIPS-Modus einen starken Einfluss auf die Performance hat, wird der FIPS-Modus in der Standardeinstellung nicht mehr gesetzt. Mit folgender Konfiguration kann der Administrator den FIPS-Modus unter Linux wieder aktivieren:

In der Konfigurationsdatei /opt/ncp/ses/etc/cfg/ncpwsupd.conf den Eintrag EnableFipsMode 1 hinzufügen.

Danach muss der NCP Secure Enterprise VPN Server-Dienst ncpwsup neu gestartet werden.

2. Fehlerbehebung und Änderungen

SNMP-Modul

Zur Statusabfrage über SNMP muss ein Fremdmodul verwendet werden. Das SNMP-Tool wird von NCP nicht mehr geliefert.

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 NCP-Website.

5. Leistungsmerkmale

Betriebssysteme

64-Bit Betriebssysteme

Linux Kernel 2.6 from 2.6.16

Linux Distributionen

Siehe Voraussetzungen, Seite 1

Empfohlene Systemvoraussetzungen

Rechner CPU:

- Pentium III (oder höher) 150 MHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher (Mindestausstattung), pro 250 gleichzeitig nutzbarer Tunnel 64 MB Arbeitsspeicher.

Taktung:

- pro 150 MHz bei einer Single Core CPU kann ein Datendurchsatz von ca. 4,5 Mbit/s realisiert werden (incl. symmetrischer Verschlüsselung),
- pro 150 MHz bei einer Dual/Quad Core CPU kann ein Datendurchsatz von ca. 9 Mbit/Sek. realisiert werden (incl. symmetrischer Verschlüsselung)

Systemvoraussetzungen bei gleichzeitigen SSL VPN Sessions

10 Concurrent User (CU)

- CPU: Intel Pentium III 700 MHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher

50 Concurrent User

- CPU: Intel Pentium VI 1,5 GHz oder vergleichbarer x86 Prozessor, 512 MB Arbeitsspeicher

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

Es gibt Einschränkungen bei mobilen Endgeräten wie Tablet PCs (z.B. unter IOS, Android), Smartphones, PDAs etc., abhängig vom jeweiligen Endgerätetyp.

Die angegebenen Werte sind Richtgrößen, die stark vom Benutzerverhalten bzw. den Anwendungen beeinflusst werden. Wenn mit vielen gleichzeitigen Dateitransfers (Datei Up- und Download) zu rechnen ist, empfehlen wir den oben angegebenen Speicherwert um den Faktor 1,5 zu erhöhen.

Netzwerkprotokolle

IP (Internet Protocol),
VLAN-Support

Management

Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management mittels VPN Server Plug-in oder über das Web-Interface des Servers

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
  - Meldungen in Messagebox oder Starten externer Anwendungen (z.B. Virenscanner-Update)
- Protokollierung in Logfiles
- Maßnahmen bei Soll-/Ist-Abweichungen im SSL VPN:
  - Granulare Abstufung der Zugriffsberechtigungen auf bestimmte Applikationen entsprechend vorgegebener Sicherheitslevels.
- Dynamische Umschaltung der Filterregeln nach Vorgabe der Endpoint Security
- *(8.10) Endpoint Security nur für NCP Clients durchführen*
- *(8.10) Unterstützung von IF-MAP (Interface for Metadata Access Points)*
  - *(8.10) Realtime Enforcement durch das IF-MAP-Protokoll*

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
- Erweiterung des Domain Name Servers (DNS), Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse
- Periodische Updates das DNS Server mit Benutzername und IP_Adresse des aktuell verbundenen Clients

Multi Company Support

Gruppenfähigkeit: max. können 256 Domänen-Gruppen konfiguriert werden, die sich zum Beispiel unterscheiden in:
Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.

Benutzerverwaltung

- Lokale Benutzerverwaltung (bis zu 750 Benutzer)
- externe Authentiserung über:
  - OTP-Server
  - RADIUS
  - LDAP
    - LDAP über SSL-Unterstützung
  - Novell NDS
  - MS Active Directory Services
- RADIUS-, LDAP- und SEM-Weiterleitung

Statistik und Protokollierung

- Detaillierte Statistik
- Logging-Funktionalität
- Versenden von SYSLOG-Meldungen

Client/Benutzer Authentifizierungsverfahren

- OTP-Token
- Benutzer- und Hardware-Zertifikate (IPsec) nach X.509 v.3
- Benutzername und Password (XAUTH)
- Externe Authentisierung mit LDAP Bind

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
- Erstellen und Verteilen der Server-Zertifikate mit dem PKI Enrollment Plug-in
- Übertragung der SubCA-Zertifikate
- SNMP-Abfrage der Server-Zertifikate

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 von der CA in bestimmten Zeitintervallen
- Überprüfung der Zertifikate mittels OCSP oder OCSP over http gegenüber der CA

IPsec VPN und SSL VPN - Verbuindungen

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

Pooladressenverwaltung

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"

Virtual Private Networking mit IPsec

- IPsec (Layer 3 Tunneling), RFC-konform
- MTU Size Fragmentation und Reassembly
- DPD (Dead Peer Detection)
- NAT-Traversal (NAT-T)
- IPsec Modes: Tunnel Mode, Transport Mode
- Seamless Rekeying

- PFS (Perfect Forward Secrecy)
- Automatische Rück-Routen-Ermittlung (ARRE)
- *(8.10) Unterstützung für Seamless Roaming im NCP Secure Enterprise Client.*

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 (v1 und v2)
- *(8.10) IKEv2 inkl. MobIKE. EAP Protokoll-Unterstützung:*
  - *EAP-MD5-Challenge*
  - *EAP-TLS*
  - *EAP-MSCHAP-V2*
- XAUTH
- IKECFG
- DPD
- NAT Traversal (NATT)
- UDP encapsulation
- IPCOMP

(8.10) FIPS inside

Der Secure Enterprise VPN Server integriert kryptografische Algorithmen nach FIPS-Standard. Das eingebettete Kryptografiemodul, das diese Algorithmen beinhaltet, ist nach FIPS 140-2 zertifiziert (Zertifikat #1051).

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 bis 14 (DH Länge von 1024 Bit bis 2048 Bit)*
- *Hash-Algorithmen: SHA1, SHA 256, SHA 384 oder SHA 512 Bit*
- *Verschlüsselungsalgorithmen: AES mit 128, 192 oder 256 Bit oder Triple DES*

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; 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)

Authentisierungsverfahren

- IKE (Aggressive und Main Mode), Quick Mode

- IKEv2
- XAUTH für erweiterte User-Authentisierung
- Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Smart Cards und USB Tokens
- 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), *(8.10) oder IP Addressvergabe über DHCP*

Datenkompression

- IPCOMP (lzs)
- Deflate

Andere Fuktionaltät

- VPN via L2TP over IPsec für Android und IPsec für Apple iOS

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

(8.10) Single Sign-on (SSO) für SSL VPN

SSO Unterstützung in Web Proxy.

Authentisierung mit Single Sign-on:

- *Die Web Server Anwendung muss die gleichen Zugriffsdaten benötigen wie der SSL VPN Client; dabei werden Benutzernamen und Passwörter zentral verwaltet von: Active Directory, RADIUS oder LDAP.*
- *Unterstützung von HTTP-Authentisierungsprotokollen (Basic (RFC2617), HTTP Digest (RFC1617) und NTLM (Microsoft)) oder nach der Post Form-Methode.*

Unterstützte Web-Applikationen:

- *Vordefinierte Konfigurationsdateien für SSO für Outlook Web Access (OWA) 2003, 2007 und 2010, CITRIX Webinterface 4.5 und 5.1.*
- *Benutzerspezifische Anwendungskonfigurationen.*

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
SSO-Funktionaliät – Benutzername und Passwort für Network Sharing kann ersetzt werden durch SSL Benutzername und Passwort.

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 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)

Unterstützung für Port-Weiterleitung unter Mac OS X

(8.10) SSO-Unterstützung – anwendungsabhängig. Wird nur unterstützt von Anwendungen, Benutzername und Passwort als Kommandozeilenparameter übernehmen können.

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 7 (32/64 Bit), Windows Vista (32/64 Bit), Windows XP (32/64 Bit)

(8.10) 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.

Voraussetzungen am Endgerät:

- *Microsoft Windows 7 (32/64 bit), Windows Vista (32/64 bit), Windows XP (32/64 bit)*
- *Applikationen, die unter dem Virtual Private Desktop unterstützt werden: Microsoft Word, Excel, Powerpoint, Outlook und Outlook Web Access, Adobe Acrobat Reader und Flashplayer, Foxit Reader, SSH (putty) und WinZip. Eine detailierte Aufstellung von unterstützten Betriebssystemen und Anwendungen ist auf Anfrage verfügbar.*

Cache Protection für Internet Explorer V.6, 7 und 8:

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 (32/64 Bit), Windows Vista (32/64 Bit) oder Windows XP (32/64 Bit)

Security Features

- Beschränkung der Cipher Suite (nur AES256-SHA oder DES-CBC3-SHA oder AES128-SHA)
- Vermeidung von Cross Site Scripting

Other Features

- Erweiterte SSL VPN-Unterstützung für alle mobile Endgeräte

Configuration and User Interface (SSL VPN Start Page)

- Die SSL VPN-Startseite kann mit firmenspezifischen Texten und Grafiken gestaltet werden
- Platzhalter vereinfachen die Handhabung komplexer Konfigurationen