NCP Secure Enterprise VPN Server

für Linux

Release Notes

Major Release: **12.10 r44217**
Datum: **Juni 2019**

Voraussetzungen

Linux Distributionen:

Die folgenden Linux Distributionen werden mit diesem Release unterstützt:

- Debian GNU/Linux 9.9
- Red Hat Enterprise Linux Release 7.5 & 8.0

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen im Handbuch nach.

Für den Einsatz anderer NCP-Komponenten werden folgende Versionen benötigt

- Secure Enterprise Management Server Version 5.20 oder höher
- Management Console Version 5.20 oder höher
- Management Plug-in Server Configuration Version 12.10 oder höher
- Management Plug-in License Management Version 11.30
- Secure Enterprise HA Server Version 12.10 oder höher

1. Neue Leistungsmerkmale und Erweiterungen

IPv4 / IPv6 Dual Stack-Unterstützung

Innerhalb des VPN-Tunnels wird sowohl das IPv4 und IPv6 Protokoll unterstützt.

Web-Interface mit „Notifications“

Wichtige Informationen werden im Web-Interface hervorgehoben dargestellt.

EAP Pass-Through

Verwendet ein VPN Client das EAP-Protokoll zur Authentisierung des Benutzers, so können diese EAP-Daten an einen weiteren Authentisierungsdienst wie beispielsweise Microsoft Active Directory oder FreeRADIUS weitergeleitet werden.

VRRP-Konfiguration

Die VRRP-Konfiguration kann nun im Web-Interface, alternativ zu `vrrp-setup`, durchgeführt werden.

Anbindung an den NCP Secure Enterprise Management Server

Die Anbindung an den NCP Secure Enterprise Management Server kann ab dieser Version auch über das Web-Interface erfolgen.

Konfiguration der Gültigkeitsdauer von Richtlinien (Policy Lifetimes)

Innerhalb eines Link Profiles ist es nun für ausgehende Verbindungen möglich die Gültigkeitsdauer von IPsec- oder IKE-Richtlinien zu konfigurieren.

Konfiguration der VPN-Interface-IP Adresse

Die Konfiguration der VPN-Interface-IP Adresse geschieht ab dieser Version über das Web-Interface. Das Konfigurationsprogramm `ses-config` wurde entfernt.

2. Verbesserungen / Fehlerbehebungen

Entfernung produktspezifischer Benutzer im Betriebssystem nach Deinstallation

In älteren Serverversionen blieb nach deren Deinstallation der Benutzer `ncp` oder `ncpweb` im Betriebssystem zurück. Dieser Fehler wurde behoben.

Erstellen eines Konfigurations-Backups

Die Erstellung von Konfigurations-Backups schlug fehl. Dieser Fehler wurde behoben.

Versionsausgabe über Kommandozeile

Mit Hilfe des Parameters `--version` konnte über die Kommandozeile befehle `ses-control` und `ses-sentinel` die Version des Produktes abgefragt werden. Ab dieser Version geschieht dies über über den Kommandozeilenbefehl `ses-license`.

Kommunikation trotz sperrender Filterregeln

Unter bestimmten Voraussetzungen konnte es vorkommen, dass einiger Filterregeln nicht aktiv waren. Dieser Fehler wurde behoben.

Fehlerbehebung innerhalb IKEv2 und RFC7427-Implementierung

Automatisches Löschen von Core dumps

Um den durch Core dumps benötigten Platzbedarf auf dem Datenträger nicht zu groß werden zu lassen, werden Core dumps ab der Anzahl 20 oder einem maximalen Alter von 30 Tagen beim Anlegen eines neuen Core dumps gelöscht. Ebenso werden Core dumps komprimiert abgelegt.

Erweiterung der Systeminformationen in den Absturzberichten

Die Systeminformationen innerhalb der Absturzberichte wurden um eine Liste installierter Pakete ergänzt.

Verbesserung der Kompatibilität zu 3rd-Party Authentisierungslösungen

Der Inhalt des Suffix-Feldes innerhalb der Domain Gruppen-Konfiguration kann als RADIUS NAS-Identifier an 3rd-Party Authentisierungslösungen gesendet werden.

3. Bekannte Einschränkungen

Fehler im Updateprozess

Eine bereits bestehende Datei `global.conf` wird beim Updateprozess von einer Vorversion nicht angepasst. Die Einstellungen für „Privilege Separation“ und „Löschen von Core dumps“ sind dadurch nicht korrekt gesetzt. Zur Behebung des Problems geben Sie
`sudo cp /opt/ncp/ses/etc/global.{sam,conf}` auf der Kommandozeile ein.

Konfigurationsübernahme beim Update von alten Produktversionen

Das direkte Update einer alten NCP Secure Enterprise VPN Server-Installation mit Version 7.x oder älter wird nicht unterstützt. In diesem Fall ist vorher auf die Version 11 des NCP Secure Enterprise VPN Servers ein Update durchzuführen.

Entfernung von Konfigurationsparametern

Innerhalb der Konfiguration wurden folgende Parameter entfernt:
Innerhalb „Lokales System“

- ISDN
- xDSL (PPP over Ethernet)
- RADIUS-Konfiguration für ausgehende Verbindungen
- LDAP-Konfiguration für ausgehende Verbindungen
- Endpoint Policies Download vom Management Server
- alle Parameter im Register Modem
- alle Parameter im Register DynDNS

Innerhalb „Link Profile“

- Verbindungsarten: ISDN, PPPoE, Modem
- Rufnummer Ziel
- Kompression (L2TP):
- Security-Modus
- Verschlüsselungsart (L2Sec):
- Dynamischer Schlüsselaustausch:
- Identitätsschutz
- Pre-shared Key:
- Umbenennen von "Tunnel Secret" nach "Tunnel Secret (L2TP)"

Innerhalb „Domain Gruppen“

- Domain Suchreihenfolge

Die Konfiguration der SSL VPN-Funktionalität ist aktuell noch vorhanden, wird zukünftig jedoch nicht mehr unterstützt bzw. entfernt.

Web-Interface und Microsoft Edge

Bei der Verwendung des Microsoft Edge-Webbrowsers wird mindestens dessen Version EdgeHTML 18.17763 vorausgesetzt.

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

IPsec VPN – Allgemeines

Betriebssysteme	Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 Debian, Red Hat oder andere Linux-Distributionen mit Kernelversion ab 3.10, glibc ab 2.17
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. 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

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

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 32/64, macOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux

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