NCP Secure Enterprise VPN Server

für Linux

Release Notes

Major-Release: **13.10 r29631**
Datum: **November 2022**

Voraussetzungen

Linux Distributionen:

Die folgenden Linux Distributionen werden mit diesem Release unterstützt:

- Debian GNU/Linux 11
- Red Hat Enterprise Linux 9
- SUSE Linux Enterprise Server 15

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 5.30 oder höher
- Management Console Version 5.30 oder höher
- Management Plug-in Server Configuration Version 13.10 oder höher
- Secure Enterprise HA Server Version 13.10 oder höher

Entfernte Funktionalitäten

Die folgenden Funktionalitäten sind ab der Major-Release 13.0 nicht mehr im Produkt enthalten:

- Interface for Metadata Access Points (IF-MAP)
- FIPS-Modus
- SSL VPN-Funktionalität

  Achtung: Das zugehörige Management Plug-in Server Configuration enthält auch für ältere Server-Versionen keine SSL VPN-Konfiguration. Wird diese benötigt ist ein älteres Plug-in zu verwenden.

1. Neue Leistungsmerkmale und Erweiterungen

Konfiguration für bis zu 255 Split Tunneling Netzwerke

Innerhalb der SES-Konfiguration können nun bis zu 255 Split Tunneling Netze konfiguriert werden. Diese Konfiguration wird innerhalb des IKE Config Mode während des Verbindungsaufbaus an den NCP Secure Client übergeben.

Neue Option: Direkten Datenaustausch zwischen den VPN-Instanzen innerhalb einer Domain gestatten

Ist am SES eine Tunnelweiterleitung konfiguriert, kann durch Setzen der Option „Direkten Datenaustausch zwischen den VPN-Instanzen innerhalb einer Domain gestatten“ / „Allow direct data exchange between VPN instances within a domain“ Kommunikation von einem VPN-Tunnel zu einem anderen erfolgen.

Neue Option: Im Tunnel aufgelöste Domain-Namen

Die Option „Im Tunnel aufgelöste Domain-Namen“ befindet sich innerhalb der Domain-Gruppen-Konfiguration. Wird am Client eine der für diese Option konfigurierten Domains aufgerufen, so wird in Verbindung mit konfiguriertem Split Tunneling der DNS-Request durch den VPN-Tunnel gesendet.

Neue Option: Domain Search Order

Die „Domain Search Order“ befindet sich innerhalb der Domain-Gruppen-Konfiguration und wird als String an das vorhandene Client-Betriebssystem übergeben.
Sie ergänzt beispielsweise den Computernamen innerhalb eines DNS-Requests auf die konfigurierten Domains, z.B. `company.local`, `company.com`, ….
Ein Anwender könnte so durch den VPN-Tunnel seine Zielrechner ausschließlich durch deren Computernamen ansteuern. Er gibt beispielsweise `computer-xy` ein, was vom Betriebssystem zu `computer-xy.company.local` für den DNS Request ergänzt wird. Sollte der Request nicht beantwortet werden so wird vom Betriebssystem für `computer-xy.company.com` angefragt.

Trennen aller aktiven Verbindungen innerhalb einer Domaingruppe

Innerhalb des Menüpunktes Statistik / Domain-Gruppen wurde sowohl im Web-Interface als auch im Server Plug-in die Option hinzugefügt alle aktiven Verbindungen innerhalb einer Domaingruppe zu trennen.

2. Verbesserungen / Fehlerbehebungen

Verbesserung der Gesamtperformance

Interne Umbaumaßnahmen des SES führen zu einer besseren Gesamtperformance, vor allem auf aktuellen CPUs mit hoher Anzahl an CPU-Cores oder NUMA-Hardware.

Unterstützung mehrerer Traffic Selektoren für eine Security Association

Für ausgehende IPv4- oder IPv6-IPsec-Verbindungen werden mehrere Traffic Selektoren für eine Security Association unterstützt.

Umstellung der NFQueue auf NFTables

Neue OpenSSL Version 1.1.1n

Standard TLS-Version: 1.2

Der SES verwendet standardmäßig die TLS-Version 1.2. Sollte aus Kompatibilitätsgründen für VPN Path Finder II eine ältere TLS-Version nötig sein, so lässt sich dies in der Datei `ncpsslvpn.conf` konfigurieren:

```
[General]
...
MinTlsVersion=1.0

Mögliche Werte: 1.0, 1.1, 1.2
```

Schwachstellen im ncpweb-Dienst

Die ncpweb-Dienst enthielt eine Schwachstelle für einen Clickjacking-Angriff sowie eine Anfälligkeit für Cross-Site-Scripting (XSS)-Attacken. Diese Schwachstellen wurden behoben, ebenso wurde „HTTP Strict Transport Security“ aktiviert.

Anzeige der Rechte in der Zugriffsverwaltung fehlerhaft

Nach der Installation wurden die Rechte des Standard-Administrators in der Zugriffsverwaltung fehlerhaft angezeigt. Dieses Problem wurde behoben.

Fehlerhafte Darstellung von Umlauten und Lizenzinformationen im Web-Interface wurde behoben

Linux Gelöschte Default-Route des Betriebssystems

Unter bestimmten Umständen wurde die Default-Route des Betriebssystems gelöscht. Dieses Problem wurde behoben.

Problembehebung für Fehlermeldung: User(Link) configuration error for User

Problembehebung: GRE-Protokoll ohne Source IP Adresse

Problembehebung innerhalb der GRE-Weiterleitung

Falsche SessionID im RADIUS Account-Log

Ist ein Benutzer mittels eines lokalen Link Profiles angelegt, so sendet der SES in der RADIUS Accounting Message immer dieselbe SessionID. Dieses Problem wurde behoben.

Problembehebung bei Site2Site-Kopplung und DHCP

Bei der Verwendung eines DHCP-Relays in einer Filiale und einem DHCP-Server in der Zentrale wurden eingehende DHCP-Requests verworfen. Dieses Problem wurde behoben.

Option: Use LDAP Bind for Authentication

Die Option „Use LDAP Bind for Authentication“ funktionierte in Verbindung mit IKEv2 EAP nicht. Dieses Problem wurde behoben.

Update auf zlib Version 1.2.12

Die im SES verwendete zlib-Version wurde auf 1.2.12 angehoben. Damit wurde die zlib-Sicherheitslücke [CVE-2018-25032] geschlossen.

Update auf cURL-Library 7.84.0

Die im NCP Secure Enterprise VPN Server und Server-Plug-in verwendete cURL-Version wurde auf 7.84.0 angehoben. Damit wurden die cURL-Sicherheitslücken [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207] und [CVE-2022-32208] geschlossen.

Problembehebung bei der Auswertung konfigurierter Link Selektoren für IPv6

Konfigurierte Link-Selektoren für IPv6 wurden nicht korrekt ausgewertet. Dieses Problem betrifft die clientseitige Split Tunneling Konfiguration innerhalb der Domain-Gruppe und wurde behoben.

Problembehebung mit 4096 Bit langen RSA-Schlüsseln im SES-Keystore

Problembehebung innerhalb des Web-Interfaces

In Verbindung mit aktuellen Chrome-basierten Webbrowsern wurde das Web-Interface nur read-only dargestellt. Dieses Problem wurde behoben.

Problembehebung: SES startet nicht wenn SEM auf gleicher Hardware installiert ist

Unterstützung des RFC 3527 zur Verbesserung der Kompatibilität mit Microsoft DHCP-Servern

DNS Server-Konfiguration via IPv6

Im Zuge der Dual Stack-Unterstützung ist der im VPN-Tunnel genutzte DNS-Server mittels IPv6-Adresse konfigurierbar.

Anzeige des GIT-Hashes als CommitID in der Web-Oberfläche des SES und High Availability-Servers (HA-Server)

Nur ein Default-Gateway im Web-Interface innerhalb der Netzwerkkonfiguration zugelassen

Die versehentliche Eingabe mehr als eines Default-Gateways führt zu einer Fehlersituation. Dieses Problem wurde behoben.

Problembehebung bei fehlerhafter Anzeige der VPN-Tunnel im High Availability-Server (HA-Server)

Wurde bei einem SES die Rufablehnung aktiviert oder wurde er im HA-Server auf inaktiv gestellt, so reduzierte sich dadurch fälschlicherweise die angezeigte Anzahl der VPN-Tunnel. Dieses Problem wurde behoben.

Verbesserung der Lastverteilung für eine große Anzahl lizenzierter VPN-Tunnel

Problembehebung: Die Syslog-Konfiguration innerhalb der Domain-Gruppen kann nicht als Benutzer-Parameter geschaltet werden

Problembehebung: Copy/Paste-Fehler beim Einfügen der MAC-Adresse in die Serverkonfiguration

Problembehebung mit identischen Benutzernamen in Link-Profilen

Wurden zwei Linkprofile mit identischen Benutzernamen via SEM auf den SES verteilt, so erzeugte dies eine Fehlersituation die sich durch Umbenennen des Benutzers in einem Linkprofil nicht lösen lies (Replication Error). Dieses Problem wurde behoben.

Problembehebung einer am NCP Secure Client auftretenden Fehlermeldung: „PKI: Verification failed! CA certificate is not valid for hardware certificates."

Rsuinit-Konfiguration ohne Failsafe Management Server

Bisher musste innerhalb der Rsuinit-Konfiguration immer ein Failsafe Management Server angegeben werden. Mit dieser Version kann diese Eingabe auch weggelassen werden.

Kein Neustart des SES nach Änderung der Lizenz oder des „HA LB Modus" innerhalb der Lizenzierung mehr nötig

Schwachstellen im ncpweb-Dienst

Die ncpweb-Dienst enthielt eine Schwachstelle für einen Clickjacking-Angriff. Diese Schwachstellen wurden behoben.

Kopieren- und Einfügen-Funktion in Server Plug-in

Die Kopieren- und Einfügen-Funktion ist nun für die folgenden knoten in der Server-Vorlage verfügbar:

- Link-Profile
- IKEv1, IKEv2 und IPsec Richtlinien
- Filter, Filter Netze, Filter Gruppen
- Server Zertifikate
- Domain Gruppen
- Listeners

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

IPsec VPN – Allgemeines

Betriebssysteme	Windows Server 2022, Windows Server 2019 Debian, Red Hat oder SUSE Linux Enterprise Server in den genannten Versionen
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
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; RFC 3527; 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