NCP Virtual Secure Enterprise VPN Server
Release Notes

Service Release: **12.01 r43907**
Datum: **Mai 2019**

Voraussetzungen

Virtuelle Umgebungen:
Die folgenden virtuellen Umgebungen werden mit diesem Release unterstützt:

- VMware vSphere Hypervisor (ESXi)
- Microsoft Hyper-V für Windows Server 2017 und 2019 *
- KVM *

* Verfügbar ab Version 12.1x

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Problembehebung bei der Updatefunktionalität

Die im NCP Virtual Secure Enterprise VPN Server enthaltene Updatefunktionalität bedient sowohl das Basisbetriebssystem als auch die darin integrierten NCP-Komponenten. Die Updatefunktionalität war nach einer bestimmten Zeit der Inbetriebnahme nicht mehr funktionsfähig. Dieses Problem wurde behoben.
Alternativ kann dieses Problem auch wie nachfolgend beschrieben behoben werden, so dass eine Neuinstallation mit Konfigurationsexport und -import vermieden werden kann:

1. Melden Sie sich mit dem Benutzer `root` und Ihrem vergebenen Passwort in der Konsole des NCP Virtual Secure Enterprise VPN Server an.
2. Öffnen Sie die Konfiguartionsdatei `/etc/apt/apt.conf.d/00ncp` mit einem Editor.
3. Fügen Sie am Ende der Datei folgende Zeile
   ```
   Acquire::Check-Valid-Until 0;
   ```
   hinzu und speichern Sie die Datei ab.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Virtual 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 Virtual Secure Enterprise VPN Servers

Allgemeines

Virtuelle Appliance	Virtuelle Appliance mit gehärtetem Basisbetriebssystem; verfügbar als ISO-Image zur Installation innerhalb einer virtuellen Umgebung z. B. VMware vSphere Hypervisor (ESXi) (Microsoft Hyper-V für Windows Server 2017 und 2019 und KVM in Vorbereitung)
Management	Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management mittels VPN Server Plug-in oder über Webinterface (verfügbar ab Version 12.1x)
HA-Server	Betrieb mehrerer NCP Virtual Secure Enterprise VPN Server im Load Balancing oder Failsafe Verbund
Endpoint Security* (Network Access Control)	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 Logdateien. (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 Domänen-Gruppen ein anderes „Default“-Zertifikat eingestellt werden • Der Virtual Secure Enterprise VPN Server kann aus mehreren konfigurierten Zertifikaten dasjenige aussuchen, welches am besten zur Anfrage des Clients passt (z. B. längste Laufzeit)
Benutzerverwaltung	Lokale Benutzerverwaltung; 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. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · 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
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; 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)

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

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
Systemvoraussetzungen	Mindestvoraussetzungen zur Installation in einer virtuellen Umgebung: Virtuelle Maschine: VMware VMware vSphere Hypervisor (ESXi); Hyper V and KVM (verfügbar in Version VSES 12.1) • BIOS (nicht UEFI) • Ca. 5 GB Speicherplatz • Minimum 2GB RAM • Bereitstellung mehrerer Prozessorkerne in Produktivumgebungen empfohlen Bei der Erstellung der virtuellen Maschine "Debian 9" auswählen

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

Empfohlene VPN Clients / Kompatibilitäten	
NCP Secure Entry Clients	Windows 32/64, macOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux