



**Service Release:** 12.02 r43975  
**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. Im Falle eines Kernelupdates für das Basisbetriebssystem konnte dieses Update nicht korrekt ausgeführt werden. Dieses Problem wurde behoben.

## 3. Bekannte Einschränkungen

Keine.



**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 Konfigurationsdatei `/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

# NCP Virtual Secure Enterprise VPN Server

## Release Notes



### Allgemeines

|  |   |
|--|---|
| <b>Virtuelle Appliance</b>                             | 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)  |
| <b>Management</b>                                      | Konfiguration und Verwaltung erfolgen über das NCP Secure Enterprise Management mittels VPN Server Plug-in oder über Webinterface (verfügbar ab Version 12.1x)  |
| <b>HA-Server</b>                                       | Betrieb mehrerer NCP Virtual Secure Enterprise VPN Server im Load Balancing oder Failsafe Verbund   |
| <b>Endpoint Security*<br/>(Network Access Control)</b> | Endpoint Policy Enforcement für kommende Datenverbindungen.<br>Überprüfung vordefinierter, sicherheitsrelevanter Client-Parameter<br>Maßnahmen bei Soll-/Ist-Abweichungen im IPsec VPN: <ul style="list-style-type: none"><li>• Disconnect oder Verbleib in die Quarantänezone mit Handlungsanweisungen (Messagebox) oder Starten externer Anwendungen (z. B. Virenschanner-Update) Protokollierung in Logdateien.<br/>(siehe hierzu Datenblatt „NCP Secure Enterprise Management“)</li></ul>   |
| <b>Dynamic DNS (DynDNS)</b>                            | 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).   |
| <b>DDNS</b>  | Registrierung der verbundenen VPN Clients am Domain Name Server via DDNS, Erreichbarkeit des VPN-Clients unter einem (festen) Namen trotz wechselnder IP-Adresse  |
| <b>Netzwerkprotokolle</b>                              | IP, VLAN-Support  |
| <b>Mandantenfähigkeit*</b>                             | Gruppenfähigkeit; Unterstützung von max. 256 Domänen-Gruppen (d. h. Konfiguration von: Authentisierung, Weiterleitung, Filtergruppen, IP-Pools, Bandbreitenbegrenzung etc.)<br>Unterstützung mehrerer Server-Zertifikate: <ul style="list-style-type: none"><li>• Es kann für verschiedene Domänen-Gruppen ein anderes „Default“-Zertifikat eingestellt werden</li><li>• 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)</li></ul> |
| <b>Benutzerverwaltung</b>                              | Lokale Benutzerverwaltung;<br>OTP-Server; RADIUS; LDAP, Novell NDS, MS Active Directory Services  |
| <b>Statistik und Logging</b>                           | 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).

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 Passwort (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)

# NCP Virtual Secure Enterprise VPN Server

## Release Notes



|                                  |  |
|----------------------------------|--|
| <b>Verschlüsselung</b>           | Symmetrische Verfahren: AES (CBC/CTR/GCM) 128, 192, 256 Bits;<br>Blowfish 128, 448 Bits; Triple-DES 112, 168 Bits;<br>Dynamische Verfahren für den Schlüsselaustausch: RSA bis 4096 Bits;<br>Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30;<br>Hash Algorithmen: SHA-1, SHA- 256, SHA- 384, SHA- 512   |
| <b>Firewall</b>                  | Stateful Packet Inspection;<br>IP-NAT (Network Address Translation);<br>Port Filtering; LAN-Adapterschutz  |
| <b>VPN Path Finder</b>           | NCP VPN Path Finder Technology, Fallback IPsec /HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist  |
| <b>Seamless Roaming</b>          | In Verbindung mit einem NCP Secure Client ist folgende Funktionalität gegeben:<br>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   |
| <b>Authentisierungsverfahren</b> | IKEv1 (Aggressive und Main Mode), Quick Mode; XAUTH für erweiterte User-Authentisierung;<br>IKEv2, EAP-PAP/MD5/MS-CHAP v2/TLS<br>Unterstützung von Zertifikaten in einer PKI: Soft-Zertifikate, Zertifikate mit ECC-Technologie;<br>Pre-Shared Keys;<br>One-Time Passwords und Challenge Response Systeme; RSA SecurID Ready   |
| <b>IP Address Allocation</b>     | DHCP (Dynamic Host Control Protocol) over IPsec;<br>DNS: Anwahl des zentralen Gateways mit wechselnder öffentlicher IP-Adresse durch Abfrage der IP-Adresse über einen DNS-Server;<br>IKE-Config-Mode für die dynamische Zuteilung einer virtuellen Adresse an die Clients aus dem internen Adressbereich (private IP)<br>Unterscheidung des Pools anhand des Verbindungsmediums möglich (Client VPN-IP)   |
| <b>Datenkompression</b>          | IPCOMP (Izs), Deflate  |
| <b>Systemvoraussetzungen</b>     | Mindestvoraussetzungen zur Installation in einer virtuellen Umgebung:<br>Virtuelle Maschine: VMware VMWare vSphere Hypervisor (ESXi);<br>Hyper V and KVM (verfügbar in Version VSES 12.1) <ul style="list-style-type: none"><li>• BIOS (nicht UEFI)</li><li>• Ca. 5 GB Speicherplatz</li><li>• Minimum 2GB RAM</li><li>• Bereitstellung mehrerer Prozessorkerne in Produktivumgebungen empfohlen</li></ul> Bei der Erstellung der virtuellen Maschine "Debian 9" auswählen |

# NCP Virtual Secure Enterprise VPN Server

## Release Notes



---

### Empfohlene VPN Clients / Kompatibilitäten

NCP Secure Entry Clients

Windows 32/64, macOS, Android

NCP Secure Enterprise Clients

Windows 32/64, macOS, iOS, Android, Linux



**NCP** PATH FINDER<sup>®</sup>

Next Generation Network Access Technology