



NCP

Release Notes

NCP Virtual Secure Enterprise VPN Server



Major-Release: 14.00 r32190
Datum: Dezember 2025

Voraussetzungen

Virtuelle Umgebung

Die folgenden virtuellen Umgebungen werden mit diesem Release unterstützt:

- VMware vSphere Hypervisor (ESXi) 8
- VMware Workstation Version 26
- Microsoft Hyper-V für Windows Server 2025
- Debian KVM Version 13

Anforderungen für den Betrieb des NCP Virtual Secure Enterprise VPN Server (vSES)

- Secure Enterprise Management Server (SEM) Version 8.10 oder höher
- Management Console Version 8.00 oder höher
- Management Plug-in Server Configuration Version 14.00 oder höher

Wichtige Hinweise zum Update auf die aktuelle vSES-Version

Diese neue Version des vSES benötigt eine Neuinstallation, d.h. das direkte Update von einer Vorversion ist nicht möglich. Weitere Information zur Migration von der Vorgängerversion auf diese Version kann dem Handbuch entnommen werden.

Änderungen innerhalb der Netzwerkkonfiguration

Mit der Installation des vSES werden die Netzwerkadapter in `eth_int[n]` bzw. `eth_ext[n]` umbenannt (bei der Verwendung von nur einem Netzwerkinterface in `eth_int`). Mittels dem Konfigurationstool `vs-es-network-config` können diese Netzwerkadapter bei Bedarf individuell benannt werden. Im Unterschied zu den Vorgängerversionen des vSES wird auf die einzelnen Netzwerkadapter nicht mehr über deren MAC-Adresse referenziert, sondern über deren Namen. Weitere Information, insbesondere für den Updatefall, können dem Handbuch entnommen werden.

1. Neue Leistungsmerkmale und Erweiterungen

Wartungsmodus

Der Wartungsmodus bietet die einfache Option ein oder mehrere VPN Gateways aus dem Produktivbetrieb zu entfernen. So werden an den betreffenden Gateways keine eingehenden Verbindungen mehr akzeptiert, so dass zu einem späteren Zeitpunkt ein Update oder andere Arbeiten daran erledigt werden können. Danach ist der Wartungsmodus wieder zu deaktivieren.

Server-Zertifikatsverteilung

Ein im Server Plug-in importiertes Server-Zertifikat kann über den NCP Secure Enterprise Management



Server ab der Version 8.0 auf verwalteten Gateways verteilt werden.

GeoIP-Blocking

Um den Zugriff aus unerwünschten Regionen der Welt zu verhindern, wurde eine IP-basierte Zugriffskontrolle implementiert. In dieser ersten Version kann diese Funktionalität nur durch lokal am NCP Secure Enterprise VPN Server vorhandene Dateien – eine Länder-IP-Adressbereichs-Datenbankdatei der Fa. Maxmind und eine zugehörige Konfigurationsdatei – genutzt werden. Für künftige Versionen ist die zentrale Konfiguration via SEM für diese Funktion geplant.

Innerhalb der Konfigurationsdatei können Länder oder eigene IP-Adressbereiche als Black- oder Whitelist für Domaingruppen individuell konfiguriert werden.

UEFI-Unterstützung

Neben BIOS wird vom vSES ab dieser Version auch UEFI unterstützt.

Erweiterung der Statistik

Die Statistik wurde im Bereich „lokales System“ um die verworfenen Pakete innerhalb der Linux NFQueue erweitert.

2. Verbesserungen / Fehlerbehebungen

Update des Basisbetriebssystems auf Debian 12

Update auf OpenSSL 3.5 und Aktualisierung weiterer Open Source Bibliotheken

Die im SES verwendete OpenSSL-Version wurde auf die Version 3.5 angehoben. Des Weiteren wurden die im SES enthaltenen Open Source Bibliotheken aktualisiert. Die jeweiligen Versionen sind im Dokument „OpenSourceLicenseTerms.pdf“ einzusehen.

Stabilitätsverbesserung in Verbindung eines Neustarts

Wurde der aufgrund einer Konfigurationsänderung ein Neustart des vSES durchgeführt, so kam es während einer gleichzeitigen Prüfung auf vorhandene Updates im Repository zu einem Absturz des Sysconfig-Daemon. Dieses Problem wurde behoben.

Stabilitätsverbesserung der Salted Hash-Funktionalität

Mit der Einführung des Salted Hash-Features konnte es unter bestimmten Voraussetzungen vorkommen, dass der Dienst `ncpsrvmgmd` abstürzte. Dieses Problem wurde behoben.

Problembhebung: Option „SEM Anfragen weiterleiten“ hat keine Wirkung

Die Option "Domain Gruppe"/"Weiterleitung"/„SEM Anfragen weiterleiten“ hatte keine Wirkung. Das Problem wurde behoben.



Stabilitätsverbesserung in Verbindung mit dem Herunterfahren des SES

In seltenen Fällen konnte es bei dem Herunterfahren des SES zu einem Absturz des VPN Server Daemons kommen. Dieses Problem wurde behoben.

DNS-Server wird per DHCP nicht übergeben

Wurde in einer Domaingruppe ein DHCP-Server konfiguriert und die Konfiguration für die DNS-Server ausgelassen, so wurden die via DHCP verteilten DNS-Server nicht oder nur einer davon auf die Clients übertragen. Dieses Problem wurde behoben.

Problembhebung: Absturz eines Außenstandort-Gateways bei der Einwahl in die Zentrale

Wegen einer fehlerhaften VRRP-Konfiguration versuchte das Backup-Gateway an einem Außenstandort fälschlicherweise eine Verbindung in die Zentrale aufzubauen. Dabei kam es zum Absturz des Backup-Gateways. Das Problem, welches zum Absturz führte wurde behoben.

Deaktivieren von IPv6 auf dem NCP-Adapter

Wie bei den anderen Netzwerkadaptern, lässt sich IPv6 ab dieser Server-Version auch für den NCP-Netzwerkadapter deaktivieren.

Neuer Ablageort der Datei `ncpwsupd.conf`

Der Ablageort der Datei `ncpwsupd.conf` ist künftig in `/opt/ncp/vses/etc/ncpwsupd.conf`. Beim Update des SES wird die Datei automatisch dorthin verschoben und ist damit nur noch von root beschreibbar.

Fehlermeldung beim Aufruf von `vses-license`

Beim Aufruf von `vses-license` bzw. `vhas-license` wurde im Betriebssystem-Log eine Fehlermeldung erzeugt. Dieses Problem wurde behoben.

Fehler bei der Auswahl des Server-Zertifikates

Sind in einer Domaingruppe mehrere Server-Zertifikate konfiguriert, so wurde unter bestimmten Umständen nicht das vom Administrator ausgewählte Zertifikat zur Authentisierung gegenüber dem Client verwendet. Dieses Problem wurde behoben.

Remote SES bei Site2Site-Verbindung sporadisch nicht erreichbar

In einem Site2Site-Szenario baut ein Remote-SES eine Verbindung zum zentralen SES auf. In seltenen Fällen ist von der zentralen Seite aus zwar jede IP-Adresse des Remote-Netzwerkes ansprechbar, der Remote-SES selbst jedoch nicht. Dieses Problem wurde behoben.

Angabe der Softwareversion im Installer hinzugefügt

RIP-Unicast nur an einen Masterrouter

Der SES bietet bis zu vier konfigurierbare Master Router als Empfänger eines RIP-Unicasts an. Davon wurde jedoch nur der erste angesprochen. Dieses Problem wurde behoben.



Problembhebung DDNS-Update Paket mit falscher Quell-IP-Adresse

LAN-Adapter schützen

War die Option „LAN-Adapter schützen“ aktiviert, so ist auf dem betreffenden Netzwerkkinterface kein Datenaustausch über IPv6 möglich gewesen. Dieses Problem wurde behoben.

Server Plug-in - DH-Gruppen hinzugefügt

Die IPsec-Optionen wurden für die IKE DH- und PFS-Gruppeneinträge um die Gruppen 27-30 ergänzt.

Problembhebung: Absturz des SES mit Log-Meldung: `ncpwsup -> watchdog expired`

3. Bekannte Einschränkungen

Dienste-Neustart funktioniert nicht

Die Option **Dienste-Neustart** im Server Plug-in veranlasst die Serverdienste sich zu beenden, jedoch starten sie nicht mehr.

Eingegebene Lizenz wird erst nach Neustart angewendet

Im Falle eines Updates von einem lizenzierten SES der Version 13.x, ist nach dem Einspielen der aktuellen Lizenzversion 14 ein Neustart des SES notwendig. Dies gilt ebenso für die Lizenzeingabe nach einer Neuinstallation für den Fall des abgelaufenen Testzeitraumes.

Kombination Client Zertifikat mit ECC und SES mit RSA geht nicht

Werden am Client Zertifikate mit Elliptic Curve Cryptography (ECC) verwendet und am SES ist ein RSA Serverzertifikat konfiguriert, so kommt keine Verbindung zustande. Am Client erscheint die folgende Fehlermeldung:

```
ERROR - 4036: Auth - PKI ERROR: - <> Verify Server certificate with error 2107! (Ext. 'SSL Server Authentication' failed)
```

Dieses Problem wird in einer künftigen Version des Gateways mit der Konfigurationsoption für das RFC7427 Padding-Verfahren behoben.

4. Hinweise zum NCP Virtual Secure Enterprise VPN Server

Weitere Informationen zum letzten Stand der Entwicklung des NCP Virtual Secure Enterprise VPN Servers erhalten Sie auf der Website:

<https://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/gateway>





NCP engineering GmbH
Dombühler Str. 2
90449 Nürnberg
Deutschland

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com