NCP Secure Enterprise VPN Server (Linux)
Release Notes

Major Release: **11.00 r36173**
Datum: **Juli 2017**

Voraussetzungen

Linux Distributionen:
Diese Version ist für folgende Distributionen freigegeben:

- CentOS 7.3
- Debian GNU/Linux 8.7
- SUSE Linux Enterprise Server 12 SP2
- Ubuntu Server 16.04.2 LTS

Hinweise für Updates

Lesen Sie bitte sorgfältig die Beschreibung zu Updates früherer Versionen!
(Siehe: NCP_RN_SES_10_und_HAS_10_Update_und_Lizenz_de.PDF)

Voraussetzung für Server-Konfiguration mit dem Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 oder höher
- Management Plugin - Server Configuration: Version 11.00 oder höher

Voraussetzungen für die High Availability Funktionalität

Bei Einsatz des Secure Enterprise VPN Servers 11.00 im High Availability-Verbund, ist darauf zu achten, dass der High Availability Server (HA Server) mindestens die Version 10.01 besitzen muss.

Bitte beachten Sie: Ab den Software-Versionen 10.x wird ein Lizenzschlüssel der gleichen Version benötigt, um den Secure Enterprise VPN Server mit dem Secure Enterprise HA Server produktiv nutzen zu können.

1. Neue Leistungsmerkmale und Erweiterungen

Erweitertes Lizenzmanagement für iOS Clients

Ab dieser Version des NCP Secure Enterprise VPN Servers wird das Lizenzmanagement des NCP Secure Enterprise iOS Clients unterstützt.

Deutliche Performanceverbesserungen

Erhöhung möglicher ausgehender Verbindungen

Die maximale Anzahl von ausgehenden VPN-Verbindungen wurde von 750 auf 10000 erhöht.

IKEv2 Signature Authentication nach RFC 7427 mit RSA-PSS-Padding

Im Client und Server wurde eine neue Zertifikats-Authentisierungsmethode nach RFC7427 implementiert.

Für Benutzer- und Hardware-Zertifikate werden folgende Schlüsseltypen unterstützt: RSA, ECC NIST, ECC BP in verschiedenen Schlüssellängen.

In der „Zertifikatsüberprüfung“ einer Domain-Gruppe ist der Schalter „Erlaube RSA Authentisierung mit PKCS#1 V1.5 Padding“ standardmäßig aktiv. Nur wenn dieser Schalter deaktiviert wird, kann die bisherige IKEv2 RSA-Zertifikatsauthentisierung noch genutzt werden.

Client VPN-IP-Adresszuweisung für getaktete Verbindung

Diese Funktionalität findet Verwendung in Home Office-Umgebungen, bei denen die Internetanbindung des Routers über ein Medium mit volumenabhängiger Abrechnung erfolgt, vorzugsweise Mobilfunk. Der Anwenderarbeitsplatz ist dabei über WLAN an den Internet-Router angebunden. In diesem Fall kann das zugehörige WLAN-Profil des NCP Secure Clients in den Profileinstellungen als „getaktete Verbindung“ („metered connection“) konfiguriert werden. Dieses Merkmal wird zur weiteren Verarbeitung an den NCP Secure Enterprise VPN Server gesendet.

Zur Kostenersparnis bei Volumentarifen, erhält der Client beim Tunnelaufbau vom Server eine IP-Adresse aus einem dafür angelegten Pool für Clients mit Mobilfunkanbindung. Zentralseitige Anwendungen, die den Client mit Updates versorgen, können nur Datenpakete an den Client übertragen, die auf das Nötigste reduziert sind.

Am Server werden unter „Adressvergabe“ die Pool-Bereiche für getaktete Verbindungen definiert und erhalten eine Ordnungsnummer. Mit dem Eintragen dieser Nummer im Link-Profil unter „Routing“ wird dem Client eine IP-Adresse aus dem entsprechenden Pool zugewiesen. Werden an dieser Stelle die Pool-Nummern auf null gesetzt und ist keine feste IP-Adresse vergeben, so wird der IP-Adressbereich des konfigurierten DHCP-Servers genutzt.

Unterstützung mehrerer Server-Zertifikate

Pro Domain-Gruppe können nun verschiedene Standard-Zertifikate eingestellt werden. Der Secure Enterprise VPN Server kann daraus für die jeweilige Domain-Gruppe dasjenige selektieren, welches am besten zur Anfrage des Clients passt (z.B. längste Laufzeit).

Zusätzliche Sicherheitsbarriere

Die sicherheitskritischen Server-Dienste ncpwsupd und ncpsrvmgmd werden mit eingeschränkten Rechten betrieben, um potentielle Systemangriffe zu erschweren.

Anzeige zusätzlicher Verbindungsinformationen

Folgende Informationen werden in der Statistik unter „Link-Profile“ angezeigt:
– NCP VPN Path Finder Version
– Seamless Roaming
Im Account Log wird angezeigt, auf welche lokale Endpunkt-IP-Adresse sich der Client einwählt.

2. Verbesserungen / Fehlerbehebungen

Beim Verbindungsaufbau der Clients wurde die Netzmaske nicht korrekt übertragen. Dieser Fehler ist behoben.

Neues Tool zur Erstellung der Scripte für dve_up und dve_down unter [SES-INSTALL-DIR]/sbin/ses-vrrp-setup.

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/

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