NCP Virtual Secure Enterprise VPN Server

Release Notes

Service Release: **12.10 r44399**

Date: **June 2019**

Prerequisites

Virtualization Platforms

The following virtualization platforms are supported with this release:

- VMware vSphere Hypervisor (ESXi) 6.7
- Microsoft Hyper-V for Windows Server 2016 and 2019 *
- Debian GNU version 9.9.0

Central Management

- Secure Enterprise Management Server version 5.20 or higher
- Management Console version 5.20 or higher
- Management Plug-in Server Configuration Version 12.10 or higher
- Management Plug-in License Management Version 11.30

1. New Features and Enhancements

Support of the NCP Secure Enterprise Management Server

The NCP Virtual Secure Enterprise VPN Server can be centrally managed with the NCP Secure Enterprise Management Server. Configurations and certificates can be distributed.

IPv4 / IPv6 Dual Stack Support

Both the IPv4 and IPv6 protocols are supported within the VPN tunnel.

Web Interface Notifications

Important information is highlighted in the web interface.

EAP Pass-Through

If a VPN client uses the EAP protocol to authenticate the user, this EAP data can be forwarded to another authentication service such as Microsoft Active Directory or FreeRADIUS.

Configuration of an HTTP(S) Proxy

The NCP Virtual Secure Enterprise VPN Server requires access to `licensing.ncp-e.com` and `packages.ncp-e.com` via HTTP(S) for both subscription licensing and update functionality. If HTTP(S) proxy support is necessary for this communication, it can be configured in the console interface from this version on.

Policy Lifetime Configuration

Within a link profile it is now possible to configure the validity period of IPsec or IKE policies for outgoing connections.

2. Improvements / Problems Resolved

VMware tools Included in Delivery

The open source variant of VMware tools recommended by VMware is included in the NCP Virtual Secure Enterprise VPN Server and is active when using the VMware virtualization environment.

Message in Console Interface

If there is no network interface configured in the virtual environment that is optimized for this purpose (vmxnet3, virtio-net), the console interface displays a message to this effect.

Message in the Web Interface

In the web interface of the NCP Virtual Secure Enterprise VPN Server, the existing network interfaces are configured as internal or external interfaces. To avoid misconfiguration, a message has been added here. Please note that the web interface can only be configured via the internal network.

Setting the Priority in the Operating System Log and Troubleshooting

The input of digits for the configuration of the priority has been replaced by a drop-down list. Furthermore, an internal error has been fixed.

Destination Address for Subscription Licensing

The destination address required for subscription licensing has been changed to `licensing.ncp-e.com`. The previously used destination address `actsrv1.ncp.de` is still valid.

NTP server Set in Default Configuration

Starting with this version, an NTP server is set within the initial configuration.

Troubleshooting Subscription Licensing via External Network Interface

If communication via a proxy server and a configured external interface took place for subscription licensing, a connection error was displayed. This issue has been resolved.

Error when Activating Deactivated Services

If a deactivated service was activated within the web interface, this failed. This issue has been resolved.

Automatic Deletion of Core Dumps

To prevent the space required on the storage medium by core dumps from becoming too large, core dumps are deleted from 20 or a maximum age of 30 days when a new core dump is created. Core dumps are also stored in compressed form.

Enhancement of System Information in Crash Reports

A list of installed packages has been added to the system information within the crash reports.

Improved Compatibility with Third-party Authentication Solutions

The content of the suffix field within the domain group configuration can be sent as a RADIUS NAS identifier to third-party authentication solutions.

Troubleshooting SNMP

3. Known Issues

Update from Version 12.00 to 12.10 Not Possible

The update of version 12.00 of the NCP Virtual Secure Enterprise VPN Server to the current version 12.10 fails. Alternatively, this problem can also be solved as described below:

1. Log on to the console of the NCP Virtual Secure Enterprise VPN Server with the `root` user and your password.
2. Type `apt update && apt upgrade` on the command line.

Service Release: **12.02 r43975**

Date: **May 2019**

Prerequisites

Virtual environments

The following virtualization platforms are supported with this release:

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

* Available from version 12.1x

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Troubleshooting the Update Feature

The update feature contained in the NCP Virtual Secure Enterprise VPN Server includes updates for the operating system and the NCP components. In case of a kernel update for the operating system the update process didn't execute correctly. This problem has been resolved.

3. Known Issues

None.

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

Service Release: **12.01 r43907**

Date: **May 2019**

Prerequisites

Virtual environments

The following virtualization platforms are supported with this release:

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

* Available from version 12.1x

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Troubleshooting the Update Feature

The update feature contained in the NCP Virtual Secure Enterprise VPN Server includes updates for the operating system and the NCP components. The update feature stopped working correctly following a certain period after installation. This problem has been resolved.
Alternatively, this problem can also be solved as described below, so that exporting the configuration, reinstalling the software and importing the existing configuration can be avoided.

1. Log on to the console of the NCP Virtual Secure Enterprise VPN Server with the `root` user and your password.
2. Open the configuration file `/etc/apt/apt.conf.d/00ncp` in a text editor.
3. Add the following line to the end of the file

   ```
   Acquire::Check-Valid-Until 0;
   ```

   and save the file.

3. Known Issues

None.

4. Getting Help for the NCP Virtual Secure Enterprise VPN Server

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

https://www.ncp-e.com/en/products/centrally-managed-vpn-solution/gateway/

5. Features of the NCP Virtual Secure Enterprise VPN Server

General

Virtual Appliance	Virtual appliance with hardened operating system; available as an ISO image for installation within a virtual environment e.g. VMware vSphere Hypervisor (ESXi) (Microsoft Hyper-V for Windows Server 2017/2019 and KVM are under development)
Management	The NCP Secure Enterprise Management VPN Server Plug-in or the web interface are used to configure and manage the server (available with version 12.1x or newer).
HA Server	Operation of several NCP Virtual Secure Enterprise VPN Servers in a load balancing or failsafe network
Endpoint Security* (Network Access Control)	Endpoint policy enforcement for incoming connections Verification of predefined, security-relevant client parameters. Measures in the event of target/actual deviations in IPsec VPN: • Disconnect or continue in the quarantine zone with instructions for action (message box) or start of external applications (e.g. virus scanner update), recording events in log files. (Please refer to the Secure Enterprise Management data sheet for more information.)
Dynamic DNS (DynDNS)	Connection set up via Internet with dynamic IP addresses. Registration of each current IP address with an external Dynamic DNS provider. In this case the VPN tunnel is established via name assignment. (The VPN client must support DNS resolution; this is supported by NCP Secure Clients.)
DDNS	Connected VPN clients are registered with the domain name server via Dynamic DNS (DDNS), meaning that VPN clients with dynamic IPs can be reached via a (permanent) name.
Network Protocols	IP, VLAN support
Multi-Tenancy*	Group capability; support of max. 256 domain groups (i.e. configuration of: authentication, forwarding, filter groups, IP pools, bandwidth management) Multiple Server Certificates • Alternative default certificates can be configured for other domain groups. • The Virtual Secure Enterprise VPN Server can select the most suitable certificate based on the client's request (for example the certificate with the longest validity period)
User Administration	Local user administration; OTP server; RADIUS; LDAP, Novell NDS, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging functionality, sending SYSLOG messages

FIPS Inside	The IPsec client integrates cryptographic algorithms based on the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms has been validated as conformant to FIPS 140-2 (Certificate #1747). FIPS conformance will always be maintained when the following algorithms are used for set up and encryption of a VPN connection: • Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 bits) • Hash algorithms: SHA1, SHA 256, SHA 384 or SHA 512 bits • Encryption algorithms: AES 128, 192 and 256 bits or Triple DES
Client/User Authentication Processes	OTP token, certificates (X.509 v.3): User and hardware certificates (IPsec), user name and password (XAUTH)

Certificates (X.509 v.3)

Server Certificates	It is possible to use certificates which are provided via the following interfaces: PKCS#11 interface for encryption tokens (USB and smart cards); PKCS#12 interface for private keys in soft certificates
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, formerly CRL), CARL (Certification Authority Revocation List, formerly ARL)
Online Check	Automatic download of revocation lists from the CA at predefined intervals; Online validation of certificates via OCSP or OCSP over http

Connection Management

Line Management	Dead Peer Detection (DPD) with configurable time interval; Timeout (controlled by duration and charges)
Point-to-Point Protocols	LCP, IPCP, MLP, CCP, PAP, CHAP, ECP
Pool Address Management	Reservation of an IP address from a pool for a defined period of time (lease time)

Americas: NCP engineering, Inc. • 678 Georgia Ave. • Sunnyvale, CA 94085 • Phone: +1 (650) 316-6273 • www.ncp-e.com
Deutschland: NCP engineering GmbH • Dombühler Str. 2 • 90449 Nürnberg • Fon +49 911 9968-0 • Fax +49 911 9968-299

IPsec VPN

Virtual Private Networking	IPsec (Layer 3 tunneling), RFC-conformant; Automatic adjustment of MTU size, fragmentation and reassembly; DPD; NAT Traversal (NAT-T); IPsec modes: Tunnel Mode, Transport Mode Seamless Rekeying; PFS
Internet Society RFCs and Drafts	RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (incl. MOBIKE), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T), UDP encapsulation, IPCOMP, IKEv2 authentication conformant to RFC 7427 (padding process)
Encryption	Symmetric processes: AES (CBC/CTR/GCM) 128, 192, 256 bits; Blowfish 128, 448 bits; Triple-DES 112, 168 bits; Dynamic processes for key exchange: RSA to 4096 bits; Diffie-Hellman Groups 1, 2, 5, 14-21, 25-30; Hash algorithms: SHA-1, SHA 256, SHA 384 or SHA 512
Firewall	Stateful packet inspection; IP-NAT (Network Address Translation); Port filtering; LAN adapter protection
VPN Path Finder	NCP Path Finder Technology: Fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
Seamless Roaming	With Seamless Roaming in the NCP Secure Client, the system can automatically transfer the VPN tunnel to a different communication medium (LAN / Wi-Fi / 3G / 4G) without changing the IP address to avoid interrupting communication via the VPN tunnel or disconnecting application sessions.
Authentication Processes	IKEv1 (Aggressive and Main Mode), Quick Mode; XAUTH for extended user authentication; IKEv2, EAP-PAP / MD5 / MS-CHAP v2 / TLS Support for certificates in a PKI: Soft certificates, certificates with ECC technology; Pre-shared keys; One-time passwords and challenge response systems; RSA SecurID ready
IP Address Allocation	DHCP (Dynamic Host Control Protocol) over IPsec; DNS: Selection of the central gateway with dynamic public IP address by querying the IP address via a DNS server; IKE config mode for dynamic assignment of a virtual address to clients from the internal address range (private IP)

	Different pool can be assigned depending on the connection medium. (Client VPN IP)
Data Compression	IPCOMP (lzs), Deflate
Installation requirements	Minimum requirements for installation within a virtual environment: Virtual machine: Currently only available for VMware vSphere Hypervisor (ESXi); Hyper V and KVM are available with the release of VSES 12.1) • BIOS (not UEFI) • Approximately 5 GB storage • Minimum 2GB RAM • Multiple processors for production systems • Select "Debian 9" when creating the VM
Recommended VPN Clients / **NCP Secure Entry Clients**	Windows 32/64, macOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux

6.