NCP Virtual Secure Enterprise VPN Server

Release Notes

Minor Release: **13.02 r29612**

Date: **September 2022**

Note for an update from version 13.01

With an installed version 13.01, the update to version 13.02 is not displayed via the "System update" function. The Tomoyo hardening erroneously prevents this update.
To perform the system update nevertheless, the Tomoyo hardening must be deactivated briefly via the console command "`vses-tomoyo-config -s permissive`".
Additionally, in the file `/etc/apt/sources.list.d/01ncp_stretch.list` the line

```
deb https://packages.ncp-e.com/ncp stage main
```

to

```
deb https://packages.ncp-e.com/ncp release1300 main
```

must be corrected. Alternatively, the change can be made using this command:

```
sed -i s/stable/release1300/ /etc/apt/sources.list.d/01_ncp_stretch.list
```

This change loads the update from the correct online repository.
After the system update has been performed and the system has been restarted, Tomoyo hardening is automatically enabled.

Prerequisites

Virtualization Platforms

The following virtualization platforms are supported with this release:

- VMware vSphere Hypervisor (ESXi) 7.0
- VMware Workstation Version 16
- Microsoft Hyper-V for Windows Server 2019
- Debian KVM version 11.3

Central Management

- Secure Enterprise Management Server version 5.30 or higher
- Management Console version 5.30 or higher
- Management Plug-in Server Configuration Version 13.00 or higher. The plug-in is provided as a *.plugin file for importing into NCP Secure Enterprise Management with the Management Console.

Update procedure

To update to this new major release, version 12.19 of the NCP Virtual Secure Enterprise VPN Server

must be installed. To start the update process, enter the command `vses-upgrade` in the shell of the NCP Virtual Secure Enterprise VPN Server with root privileges. The question displayed during the installation process "Continue without installing GRUB?" answer with "No". Then select the first virtual disk (e.g. /dev/sda) for the GRUB installation by pressing the space bar. The update is subsequently executed and completed with a reboot.

Removed Functionalities

The following functionalities are no longer included in the product as of major release 13.0:

- Interface for Metadata Access Points (IF-MAP)
- FIPS mode

1. New Features and Enhancements

None.

2. Improvements / Problems Resolved

Loss of data buffers

During the termination of a VPN connection, data buffers pending in the internal queue could be lost. As a result, required data buffers were not fully released during operation. This problem has been fixed.

3. Known Issues

Porting the NCP Virtual Secure Enterprise VPN Server to another virtual machine

Porting the NCP Virtual Secure Enterprise VPN Server to another host system is usually accompanied by a change of the MAC addresses of the virtual network adapters. This leads to the fact that after a transfer of the configuration and a restart of the NCP Virtual Secure Enterprise VPN Server the network configuration is discarded and must be reconfigured locally.

In case of a "Replication Error 4034" displayed in the log, either

- download the configuration again on the NCP Virtual Secure Enterprise VPN Server via `vses-rsuinit` or
- transfer the configuration to the NCP Virtual Secure Enterprise VPN Server in the NCP Secure Enterprise Management Server via "Full Replication" (vSES → Statistics → Replication status → right-click in the field and "Reload all").

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • 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

NCP Virtual Secure Enterprise VPN Server

Release Notes

Major Release: **13.01 r29606**

Date: **August 2022**

Note

A version 13.00 r29604 was available for a short time and has been withdrawn.
If this version 13.00 r29604 is installed, it must be reset to a version 12.x.

Prerequisites

Virtualization Platforms

The following virtualization platforms are supported with this release:

- VMware vSphere Hypervisor (ESXi) 7.0
- VMware Workstation Version 16
- Microsoft Hyper-V for Windows Server 2019
- Debian KVM version 11.3

Central Management

- Secure Enterprise Management Server version 5.30 or higher
- Management Console version 5.30 or higher
- Management Plug-in Server Configuration Version 13.00 or higher. The plug-in is provided as a *.plugin file for importing into NCP Secure Enterprise Management with the Management Console.

Update procedure

To update to this new major release, version 12.19 of the NCP Virtual Secure Enterprise VPN Server must be installed. To start the update process, enter the command `vses-upgrade` in the shell of the NCP Virtual Secure Enterprise VPN Server with root privileges. The question displayed during the installation process "Continue without installing GRUB?" answer with "No". Then select the first virtual disk (e.g. /dev/sda) for the GRUB installation by pressing the space bar. The update is subsequently executed and completed with a reboot.

Removed Functionalities

The following functionalities are no longer included in the product as of major release 13.0:

- Interface for Metadata Access Points (IF-MAP)
- FIPS mode

1. New Features and Enhancements

New major release of the base operating system

With this version 13.0 of the NCP Virtual Secure Enterprise VPN Server, the used base operating system Debian is raised to version 11 (Bullseye). In this Linux release, the vulnerabilities [CVE-2022-29900] and [CVE-2022-29901] (Retbleed) are already fixed.

New update log

The update log can be viewed in the web interface of the NCP Virtual Secure Enterprise VPN Server or in the server plug-in.

qemu-guest-agent

The `qemu-guest-agent` is included in the feature set of the NCP Virtual Secure Enterprise VPN Server. On QEMU environments, the `qemu-guest-agent` is started automatically for better integration.

New command line command `vses-license` to display the current license version

Configuration for up to 255 split tunneling networks

Up to 255 split tunneling networks can now be configured within the SES configuration. This configuration is transferred to the NCP Secure Client within the IKE Config Mode during the connection setup.

New option: Allow direct data exchange between VPN instances within a domain

If tunnel forwarding is configured on the SES, communication can take place from one VPN tunnel to another by setting the option "Allow direct data exchange between VPN instances within a domain".

New option: Domain names resolved in the tunnel

The option "Domain names resolved in the tunnel" is located within the domain group configuration. If one of the domains configured for this option is called on the client, the DNS request is sent through the VPN tunnel in conjunction with configured split tunneling.

New option: Domain Search Order

The "Domain Search Order" is located within the domain group configuration and is passed as a string to the existing client operating system.
For example, it supplements the computer name within a DNS request to the configured domains, e.g. `company.local,company.com,.....`
A user could thus navigate through the VPN tunnel to his target computers using only their computer

names. For example, he enters `computer-xy`, which is supplemented by the operating system to `computer-xy.company.local` for the DNS request. If the request is not answered, the operating system requests `computer-xy.company.com`.

2. Improvements / Problems Resolved

Improvement of the overall performance

Internal SES rebuilds result in better overall performance, especially on current CPUs with high CPU core counts or NUMA hardware.

Support for multiple traffic selectors for a Security Association

Multiple traffic selectors for a security association are supported for outbound IPv4 or IPv6 IPsec connections.

Core dump files are not created

In the event of a crash, core dump files are stored in the `/var/adm/ncp/vses/crashes/` directory for error analysis. Under certain circumstances, this did not happen. This problem has been fixed.

Change of NFQueue to NFTables

New OpenSSL version 1.1.1n

Default TLS version: 1.2

SES uses TLS version 1.2 by default. If an older TLS version is required for VPN Path Finder II for compatibility reasons, this can be configured in the `ncpsslvpn.conf` file:

```
[General]
...
MinTlsVersion=1.0

Possible values: 1.0, 1.1, 1.2
```

Vulnerabilities in ncpweb service

The ncpweb service contained a vulnerability to a clickjacking attack and a vulnerability to cross-site scripting (XSS) attacks. These vulnerabilities have been fixed, and “HTTP Strict Transport Security” has been enabled.

Display of rights in access management incorrect

After installation, the rights of the default administrator were displayed incorrectly in the access

management. This problem has been fixed.

Incorrect display of umlauts and license information in the web interface has been fixed.

Deleted default route of the operating system

Under certain circumstances the default route of the operating system was deleted. This problem has been fixed.

Issue resolved for error message: User(Link) configuration error for User

Issue resolved: GRE protocol without source IP address

Issue resolved within GRE forwarding

Wrong SessionID in RADIUS account log

If a user is created using a local link profile, the SES always sends the same SessionID in the RADIUS accounting message. This problem has been fixed.

Troubleshooting for Site2Site coupling and DHCP

When using a DHCP relay in a branch office and a DHCP server in the central office, incoming DHCP requests were discarded. This problem has been fixed.

Option: Use LDAP Bind for Authentication

The "Use LDAP Bind for Authentication" option did not work in conjunction with IKEv2 EAP. This problem has been fixed.

Update to zlib version 1.2.12

The zlib version used in SES has been upgraded to 1.2.12. This closed the zlib vulnerability CVE-2018-25032.

Update to cURL library 7.84.0

The cURL version used in the NCP Secure Enterprise VPN Server and Server Plug-in has been raised to 7.84.0. This closed the cURL vulnerabilities [CVE-2022-32205], [CVE-2022-32206], [CVE-2022-32207] and [CVE-2022-32208].

Troubleshooting Configured Link Selectors for IPv6

Configured link selectors for IPv6 were not evaluated correctly. This issue affects client-side split tunneling configuration within the domain group and has been fixed.

Problem solved with 4096 bit long RSA keys in the SES keystore.

Issue resolved within the web interface

In conjunction with current Chrome-based web browsers, the web interface was displayed read-only. This issue has been fixed.

RFC 3527 support to improve compatibility with Microsoft DHCP servers.

DNS server configuration via IPv6

As part of dual stack support, the DNS server used in the VPN tunnel can be configured via IPv6 address.

Display of the GIT hash as CommitID in the web interface of the SES and High Availability server (HA server)

Only one default gateway allowed in the web interface within the network configuration

Accidentally entering more than one default gateway results in an error situation. This problem has been fixed.

Error handling after removed network adapter in virtual environment simplified

If a network adapter was removed from the virtual environment, after restarting the virtual machine it is only necessary to start the vSES service and remove the network adapter from the vSES configuration.

Improved update mechanism

The update mechanism has been improved in terms of a better description of the update packages and a reboot button, as well as general usability.

Improvement in the configuration of a network adapter

With this version, changes to the configuration of a network adapter only affect connections that belong to this network adapter.

Problem solving with incorrect display of VPN tunnels in High Availability Server (HA server)

If call rejection was activated for an SES or if it was set to inactive in the HA server, this incorrectly reduced the number of VPN tunnels displayed. This problem has been fixed.

Improved load balancing for a large number of licensed VPN tunnels.

Issue resolved: Syslog configuration within domain groups cannot be switched as user parameter

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • 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

Issue resolved: Copy/Paste error when pasting the MAC address into the server configuration.

3. Known Issues

Porting the NCP Virtual Secure Enterprise VPN Server to another virtual machine

Porting the NCP Virtual Secure Enterprise VPN Server to another host system is usually accompanied by a change of the MAC addresses of the virtual network adapters. This leads to the fact that after a transfer of the configuration and a restart of the NCP Virtual Secure Enterprise VPN Server the network configuration is discarded and must be reconfigured locally.

In case of a "Replication Error 4034" displayed in the log, either

- download the configuration again on the NCP Virtual Secure Enterprise VPN Server via `vses-rsuinit` or
- transfer the configuration to the NCP Virtual Secure Enterprise VPN Server in the NCP Secure Enterprise Management Server via "Full Replication" (vSES → Statistics → Replication status → right-click in the field and "Reload all").

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
Management	The NCP Secure Enterprise Management VPN Server Plug-in or the web interface are used to configure and manage the server.
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. 1024 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

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)

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;

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • 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

	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 / Cellular) 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 available for VMware vSphere Hypervisor (ESXi); Hyper V and KVM • 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, macOS, Android
NCP Secure Enterprise Clients	Windows, macOS, iOS, Android, Linux

Americas: NCP engineering, Inc. • 19321 US Highway 19 N, Suite 401 • Clearwater, FL 33764 • 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