NCP Secure Enterprise VPN Server

for Linux

Release Notes

Major Release: **13.10 r29631**
Date: **November 2022**

Prerequisites

Linux Distributions:

The following Linux distributions are supported with this release:

- Debian GNU/Linux 11
- Red Hat Enterprise Linux 9
- SUSE Linux Enterprise Server 15

Update Prerequisites

Please read the instructions for updates of previous versions in the manual carefully.

The following versions are required for the use of other NCP components

- Secure Enterprise Management Server version 5.30 or higher
- Management Console version 5.30 or higher
- Management Plug-in Server Configuration Version 13.10 or higher
- Secure Enterprise HA Server version 13.10 or higher

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
- SSL VPN functionality

  Note: The corresponding management Plug-in Server Configuration does not include SSL VPN configuration for older server versions. If this is required, an older plug-in must be used.

1. New Features and Enhancements

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`.

Disconnecting all active connections within a domain group

Within the menu item Statistics / Domain Groups the option to disconnect all active connections within a domain group has been added in the web interface as well as in the server plug-in.

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.

Change of NFQueue to NFTables

New OpenSSL version 1.1.1n

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

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.

Linux 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.

Troubleshooting: SES does not start when SEM is installed on the same hardware

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.

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

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

Troubleshooting identical user names in link profiles

If two link profiles with identical user names were distributed to the SES via SEM, this caused an error situation that could not be solved by renaming the user in one link profile (Replication Error). This problem has been fixed.

Troubleshooting an error message occurring on the NCP Secure Client: "PKI: Verification failed! CA certificate is not valid for hardware certificates."

Rsuinit configuration without failsafe management server

Until now, a failsafe management server always had to be specified within the Rsuinit configuration. With this version, this input can also be omitted.

No restart of the SES after changing the license or the "HA LB mode" within the licensing necessary anymore

Vulnerabilities in the ncpweb service

The ncpweb service contained a vulnerability to a clickjacking attack. These vulnerabilities have been fixed.

Copy and paste function in server plug-in

The copy and paste function is now available for the following nodes in the server template:

- Link Profiles
- IKEv1, IKEv2 and IPsec policies
- Filters, Filters Networks, Filters Groups
- Server Certificates
- Domain Groups
- Listeners

3. Known Issues

None.

4. Getting Help for the NCP 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 Secure Enterprise VPN Server

IPsec VPN – general

Operating Systems	Windows Server 2022, Windows Server 2019 Debian, Red Hat or SUSE Linux Enterprise Server in the mentioned versions
Management	Administrators can configure and manage NCP Virtual Secure Enterprise Server via the NCP Secure Enterprise Management Plug-in or the web interface
Network Access Control (Endpoint Security)	Endpoint policy enforcement for incoming data connections. Verification of predefined, security-relevant client parameters. Measures in the event of target/actual deviations in • 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 limitation) • 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 request (for example the certificate with the longest validity period).
User Administration	Local user administration (up to 750 users); 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)

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

Online Check	Automatic downloads 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; 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; RFC 3527; 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
Recommended VPN Clients / Compatibility	
NCP Secure Entry Clients	Windows, macOS
NCP Secure Enterprise Clients	Windows, macOS, iOS, Android, Linux