NCP Secure Enterprise VPN Server

for Windows

Release Notes

Major release: **12.10 r44217**
Date: **June 2019**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

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 5.20 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
- Secure Enterprise HA Server version 12.10 or higher

1. New Features and Enhancements

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.

Connection to the NCP Secure Enterprise Management Server

From this version, the connection to the NCP Secure Enterprise Management Server can also be made via the web interface.

Policy Lifetime Configuration

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

Configuration of the VPN Interface IP Address

The configuration of the VPN interface IP address is done from this version via the web interface. The configuration program `ses-config` has been removed.

2. Improvements / Problems Resolved

Optimized NCP Filter Driver for Increased Data Throughput

`ncpsslvpn` Service Crashed

An issue has been resolved that caused the `ncpsslvpn service`to crash.

Communication Despite Blocking Filter Rules

Under certain circumstances some filter rules were not active. This issue has been resolved.

Troubleshooting within IKEv2 and RFC7427 Implementation

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.

3. Known Issues

Configuration Transfer when Updating from Old Product Versions

The direct update of an old NCP Secure Enterprise VPN Server installation with version 7.x or older is not supported. In this case, an update to version 11 of the NCP Secure Enterprise VPN Server must be performed beforehand.

Removal of Configuration Parameters

The following parameters have been removed from the configuration:

In "Local System"

- ISDN
- xDSL PPP over Ethernet,

- RADIUS configuration for outgoing connections
- LDAP configuration for outgoing connections
- Endpoint policies download from management server
- All parameters in the Modem tab
- All parameters in the DynDNS tab

In "Link Profile"

- Connection types: ISDN, PPPoE, Modem
- Phone number destination
- Compression (L2TP):
- Security mode
- Encryption type (L2Sec):
- Dynamic key exchange:
- Identity protection
- Pre-shared key:
- "Tunnel Secret" renamed to "Tunnel Secret (L2TP)"

In "Domain Groups

- Domain search order

The configuration of the SSL VPN functionality is currently still available, but will no longer be supported and removed in future releases.

Web Interface and Microsoft Edge

When using the Microsoft Edge web browser, at least EdgeHTML 18.17763 is required.

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 2019, Windows Server 2016, Windows Server 2012 R2 Debian, Red Hat or other Linux distributions with kernel version from 3.10, glibc from 2.17
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
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 with 128, 192 and 256 bits or Triple DES

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

IF-MAP	The overall aim of the ESUKOM Project is the design and development of a real time security solution for company networks which works on the basis of consolidating metadata. The project focuses on threats arising from mobile end devices, such as smartphones. ESUKOM focuses on the integration of existing security solutions (commercial and open source) which are based on a consistent meta data format according to IF-MAP specifications of the Trusted Computing Group (TCG). The IF-MAP server of the Hannover University of Applied Science and Arts can currently be used for free-of-charge testing. The URL is: http://trust.f4.hs-hannover.de/
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 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; 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

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

Recommended VPN Clients / Compatibility	
NCP Secure Entry Clients	Windows 32/64, macOS, Android
NCP Secure Enterprise Clients	Windows 32/64, macOS, iOS, Android, Linux

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