NCP Secure Enterprise VPN Server (Win)

Release Notes

Major Release: **11.01 r38204**

Date: **December 2017**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2008 R2 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2016 64 Bit

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

The following versions are required for using other NCP components

- Secure Enterprise Management Server Version 4.05 or later
- Management Console Version 4.05 or later
- Management Plug-in Server Configuration: Version 11.00 or later
- Secure Enterprise HA Server Version 10.01 or later

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server is required to use this product.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

When downloading the CRL list, the ncpsrvmgm service could crash. This issue has now been resolved.

SEM requests for software updates over LAN are no longer forwarded.

The RADIUS attribute "NCPS-PCCertCN" = "*" enforces the use of a hardware certificate.

Redirection of "VPN IP addresses not bound to the Secure Server Adapter" has been fixed.

The server certificate is selected as configured, either "automatically" by the server or "manually".

When data is no longer sent over the VPN connection, PathFinder sessions no longer remain open, but are automatically closed.

The Secure Enterprise Server now also supports PathFinder 2 and SSL VPN when configuring ECC certificates.

The following message appeared sporadically in the configuration web page of the SES caused by an error: "Changes require restarting the NCP Secure Enterprise Server!"

With the "ARRE" option configured the server may have refused VPN connections. This issue has now been resolved.

If filters were set for the VPN data, packets were still forwarded very sporadically. This issue has been resolved.

3. Known Issues

None

NCP Secure Enterprise VPN Server (Win)

Release Notes

Major Release: **11.0 r36600**

Date: **August 2017**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2008 R2 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2016 64 Bit

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 or later
- Management Plugin - Server Configuration: Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key of the same version of Secure Enterprise VPN Server is required to use this product.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

Removed Domain Groups after update to version 11.0

If the option „Enable selected CA Certificates only“ is set within the Domain Group configuration, configured Domain Groups, including the Default Domain Group, will be removed while updating the NCP Secure Enterprise VPN Server to version 11.0. This issue has now been resolved.

3. Known Issues

None

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

Major Release: **11.00 r36322**

Date: **July 2017**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2008 R2 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2016 64 Bit

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 or later
- Management Plugin - Server Configuration: Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key of the same version of Secure Enterprise VPN Server is required to use this product.

1. New Features and Enhancements

None

2. Improvements / Problems Resolved

IKEv2 Connection with Device and User Certificate

If a VPN connection using IKEv2 required authentication of the device via device certificate and the user authentication via user certificate **at the same time**, the connection failed. This issue has now been resolved.

Incorrect Display of Users Authenticated via LDAP

VPN users authenticated via LDAP are listed incorrectly in the statistics under "Link Profiles (local)". This issue has been fixed so that it is now correctly displayed under "Link Profiles (RADIUS/LDAP)".

The maximum number of LDAP Users has been increased from 10,000 to 40,000.

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/

Major Release: **11.00 r36173**

Date: **July 2017**

Prerequisites

Microsoft Operating Systems:

The following Microsoft Operating Systems are supported with this release:

- Windows Server 2008 R2 64 Bit
- Windows Server 2012 R2 64 Bit
- Windows Server 2016 64 Bit

Update Prerequisites

Please read the instructions for updates of previous versions carefully!
(See NCP_RN_SES_10_and_HAS_10_Update_and_License_de.PDF)

Prerequisites for Configuration via Secure Enterprise Management (SEM)

- Secure Enterprise Management Server: Version 4.05 or later
- Management Plugin - Server Configuration: Version 11.00 or later

Prerequisites for High Availability

If the Secure Enterprise VPN Server 11.00 is used in a high availability network, ensure that the High Availability Server (HA Server) is version 10.01 or later.

Note: From version 10.0, a license key for the same version of Secure Enterprise VPN Server and the Secure Enterprise HA Server is required to use these two products in combination.

1. New Features and Enhancements

Advanced License Management for iOS Clients

From this version of the NCP Secure Enterprise VPN Server the license management of the NCP Secure Enterprise iOS client is supported.

Significant Performance Improvements

Higher Number of Outgoing Connections

The maximum number of outgoing VPN connections has been increased from 750 to 10,000.

Support for IKEv2 Signature Authentication (RFC 7427 with RSA-PSS padding)

A new certificate authentication method according to RFC7427 has added to the client and server.

The following key types are supported for user and hardware certificates: RSA, ECC NIST, ECC BP in different key lengths.

In the "Certificate Verification" of a domain group, the "Enable RSA Authentication with PKCS # 1 V1.5 Padding" option is activated by default. The previous IKEv2 RSA certificate authentication can only still be used if this option is disabled.

Client VPN IP Address Assignment for Metered Connections

This featured is used in home office environments, where the internet connection is metered (particularly routers using mobile data). In this scenario, the user workstation is connected to the Internet router via Wi-Fi. The Wi-Fi profile in the NCP Secure Client can be configured as a “metered connection" under the profile settings. This setting is sent to the NCP Secure Enterprise VPN Server.

In order to reduce costs for metered connections, the client receives an IP address from a pool assigned for clients with a mobile connection during tunnel setup. Centralized applications that provide the client with updates can therefore only transfer the most necessary data traffic.

The pool ranges for metered connections are defined in the server under "address allocation", and each pool receives a number. After entering the pool number in the link profile under "Routing" the client is assigned an IP address from the corresponding pool. If the pool numbers are set to zero and no fixed IP address is assigned, the IP address range of the configured DHCP server is used.

Support for Several Server Certificates

Several standard certificates can now be set for each domain group. The Secure Enterprise VPN Server can select the one that best suits the client's request (e.g. the longest expiry period) for the respective domain group.

Display of Additional Connection Information

The following information is displayed in the statistics under "Link profile":

- NCP VPN Path Finder version
- Seamless Roaming

The account log shows which local endpoint IP address the client connects to.

2. Improvements / Problems Resolved

Netmasks were not not transferred correctly during client connection. This issue has been resolved.

New Tool for Creating the Scripts for dve_up and dve_down under [SES-INSTALL-DIR] / sbin / ses-vrrp-setup.

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

Central Management

The NCP Secure Enterprise VPN Server is configured and managed either via an NCP Secure Enterprise Management (SEM) using the Secure Server plug-in or directly via the Web Interface.

Operating Systems

See the prerequisites on Page 1.

Security Features

Support of all IPsec standards according to RFC

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 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), logging in Log files. (Pleaserefer to the Secure Enterprise Management data sheet for more information)

Measures in the event of target/ actual deviations in SSL VPN:

- Individual grading of access authorization to certain applications in accordance with defined security levels.

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 (prerequisite: The VPN client has to support DNS resolution - as do NCP Secure Clients).

DDNS

Registration of the connected VPN clients at the Domain Name Server via DDNS, reachability of the VPN client under a (permanent) name in spite of changing IP address.

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, etc.)

Unterstützung mehrerer Server-Zertifikate:

- Individual default certificates can be set for different domain groups.
- If several certificates exist, SES will find the certificate which is best suited to the client's request (for example the certificate with the longest expiry period).

User Administration

Local user administration (up to 750 users);

OPT 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 according to the FIPS standard. The embedded cryptographic module, containing the corresponding algorithms, is certified according to FIPS 140-2 (Certificate #1747).

If you use one of the following algorithms for set-up and encryption of an IPsec connection, FIPS compatibility is always given:

- Diffie Hellman-Group: Group 2 or higher (DH starting from a length of 1024 Bit)
- Hash Algorithms: SHA1, SHA 256, SHA 384 or SHA 512 Bit
- Encryption algorithms: AES with 128, 192 and 256 Bit or Triple DES

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 meta data. The special focus of the project is the threat resulting from mobile end-devices, e.g. 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

Es können Zertifikate verwendet werden die über folgende Schnittstellen bereitgestellt werden: PKCS#11 Interface für Verschlüsselungs-Tokens (USB und Smart Cards); PKCS#12 Interface für Private Schlüssel in Soft-Zertifikaten.

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 certain intervals;
Online check: Checking certificates via OCSP or OCSP over http;

IPsec-VPN and SSL VPN – Dial-in Management

Communication Media

LAN;

direct operation on the WAN: Support of max. 120 ISDN B-channels (So, S2M);

Line Management

DPD with configurable time interval;

Short Hold Mode; channel bundling (dynamic in ISDN) with freely configurable threshold value;

timeout (controlled by time and charges);

Point-to-Point Protocols

PPP over ISDN, PPP over GSM, PPP over PSTN, PPP over Ethernet;

LCP, IPCP, MLP, CCP, PAP, CHAP, ECP;

Pool Address Management

Reservation of an IP address from a pool within a defined period (lease time);

Trigger Call

Direct dial of the distributed VPN gateway via ISDN, "knocking in the D-channel";

IPsec VPN

Virtual Private Networking

IPsec (Layer 3 Tunneling), RFC-conformant;

Automatic treatment of MTU size, fragmentation and reassembly;

DPD;

NAT-Traversal (NAT-T);

IPsec Modes: Tunnel Mode, Transport Mode;

Seamless Rekeying;

PFS;

Internet Society, RFCs und Drafts

RFC 2401 –2409 (IPsec), RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation),

IP Security Architecture, ESP, ISAKMP/Oakley, IKE, IKEv2 (inkl. MOBIKE), IKEv2 Signature Authentication, XAUTH, IKECFG, DPD, NAT Traversal (NAT-T),UDP encapsulation, IPCOMP;

Encryption

Symmetric processes: AES 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, 26;

Hash algorithm: MD5, SHA1, SHA 256, SHA 384, SHA 512;

Firewall

Stateful Packet Inspection; IP-NAT (Network Address Translation); Port Filtering; LAN adapter protection;

VPN Path Finder

NCP Path Finder Technology: Fallback IPsec/ HTTPS (port 443) if port 500, respectively UDP encapsulation is not possible (Prerequisite: NCP Secure Enterprise VPN Server 8.0);

Seamless Roaming

With Seamless Roaming, the system automatically connects the VPN tunnel to a different Internet communication medium (LAN/ WiFi/ 3G/ 4G) without changing the IP address, so that the communication of the application through this tunnel is not interfered with and the application's session is not disconnected.

Authentication Processes

IKE (Aggressive and Main Mode), Quick Mode;
XAUTH for extended user authentication;
Support of certificates in a PKI: Soft certificates, smart cards, USB tokens, 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 changing 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);

Data Compression

IPCOMP (lzs), Deflate;

VPN Architecture

Requirements Computer

CPU: Pentium III or higher or compatible CPU;

RAM: 512 MByte minimum plus 0.256 MByte per simultaneously used VPN tunnel;
i.e. 64 MByte with 250 concurrently usable VPN tunnels;

Data Throughput (including symmetric encryption):
Single Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*8.5 MBit/s.
Dual Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*12.5 MBit/s.
Triple Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*15.5 MBit/s.
Quad Core: data throughput [MBit/s] » clock rate [MHz]/150 MHz*17.5 MBit/s.

As can be seen in the approximation formula for data throughput above, a further increase in the number of CPU cores does not provide for an increase in proportion to data throughput.

Recommended VPN Clients / Compatibilities

NCP Secure Entry Clients:
Windows 32/64, macOS, Windows Mobile, Android;
NCP Secure Enterprise Clients:
Windows 32/64, macOS, iOS, Windows Mobile, Android, Windows CE, Linux;

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299

SSL-VPN

Protocols

SSLv1, SSLv2, TLSv1 (Application Layer Tunneling);

Web Proxy

Access to internal web applications and Microsoft network drives via a web interface.

Prerequisites for the end device: SSL-capable web browser with Java Script functionality.

Secure Remote File Access*

Upload and download, creating and deleting directories, approximately corresponds to the functionalities of the File Explorer under Windows. Prerequisites for the end-device: See Web Proxy;

Port Forwarding

Access to client/server applications (TCP/IP),
Prerequisites for the end-device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0) or ActiveX, SSL Thin Client for Windows 7/8/10 (32/64 Bit) and Linux;

NCP Virtual Desktop

The Virtual Private Desktop is a work space which is disconnected from the basic operating system and only temporarily available during one SSL VPN session. Any application which the user starts in this work space, is disconnected from the operating system and the virtual private desktop stores the application data in an AES-encrypted container, for example attachments to emails. After the SSL VPN session has been terminated, the sandbox automatically deletes all data from this container.

Cache Protection for Internet Explorer and Edge

All transmitted data will be automatically deleted from the end-device after disconnect.

Prerequisites for the end-device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0), SSL Thin Client for Windows 7/8/10 (32/64 Bit).

Portable LAN

Transparent access to the corporate network. Prerequisites for the end-device: SSL-capable web-browser with Java Script functionality, Java Runtime Environment (>= V5.0) or ActiveX control, PortableLAN Client for Windows 7/8/10 (32/64 Bit);

Single Sign-on

Single sign-on is used in all those cases in which the web server logon requires the same access data as the SSL VPN Client. It is possible to centrally manage user ID and password via Active Directory, RADIUS

or LDAP.

Depending on the application, you can distinguish between single sign-on with HTTP authentication (Basic (RFC2617), HTTP Digest (RFC2617) and NTLM (Microsoft)) and single sign-on according to the post-form method.

Single Sign-on has been tested with Web applications like Outlook Web Access (OWA) 2003, 2007 and 2010, RDP Client and CITRIX Web interface 4.5, 5.1.

Single Sign-on with Port Forwarding is only supported by applications that are able to accept parameter (like user ID and password) in their command line.

Recommended System Requirements *

1-100 Concurrent User:

CPU: Intel Dual Core 1,83 GHz or comparable x86 Processor,

1024 MB RAM

200+ Concurrent User:

CPU: Intel Dual Core 2,66 GHz or comparable x86 Processor,

1024 MB RAM

*) depends on the type of end-device. Mobile end-devices like Tablet PCs (using IOS or Android), Smartphones, PDAs and others have some restrictions.

Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Others: NCP engineering GmbH · Dombuehler Str. 2 · 90449 Nuremberg · Germany · Fon +49 911 9968-0 · Fax +49 911 9968-299