Release Notes

NCP Virtual Secure Enterprise VPN Server

Major release: 14.00 r32190
Date: December 2025

Prerequisites

Virtualization Platform

The following virtualization platforms are supported with this release:

- VMware vSphere Hypervisor (ESXi) 8.0
- VMware Workstation Version 26
- Microsoft Hyper-V for Windows Server 2025
- Debian KVM version 13

Requirements for operating the NCP Virtual Secure Enterprise VPN Server (vSES)

The following versions are required for using other NCP components:

- Secure Enterprise Management Server (SEM) Version 8.10 or newer
- Management Console Version 8.00 or newer
- Management Plug-in Server Configuration Version 14.00 or newer

Important information about updating to the current vSES version

This new version of vSES requires a new installation, i.e., it is not possible to update directly from a previous version. Further information on migrating from the previous version to this version can be found in the manual.

Changes within the network configuration

When vSES is installed, the network adapters are renamed `eth_int[n]` or `eth_ext[n]` (when using only one network interface in `eth_int`). These network adapters can be named individually as required using the `vses-network-config` configuration tool. Unlike previous versions of vSES, the individual network adapters are no longer referenced by their MAC address, but by their name. Further information, especially for updates, can be found in the manual.

1. New features and enhancements

Maintenance mode

Maintenance mode offers a simple option for removing one or more VPN gateways from productive operation. This means that no incoming connections are accepted at the affected gateways, allowing updates or other work to be carried out at a later date. Maintenance mode must then be deactivated again.

Server certificate distribution

A server certificate imported into the server plug-in can be distributed to managed gateways via the NCP Secure Enterprise Management Server from version 8.0 onwards.

GeoIP blocking

IP-based access control has been implemented to prevent access from unwanted regions of the world. In this first version, this functionality can only be used through files available locally on the NCP Secure Enterprise VPN Server – a country-IP address range database file from Maxmind and an associated configuration file. For future versions, central configuration via SEM is planned for this function.

Within the configuration file, countries or your own IP address ranges can be individually configured as blacklists or whitelists for domain groups.

UEFI support

In addition to BIOS, vSES also supports UEFI starting with this version.

Statistics extension

The statistics in the “local system” area have been extended to include discarded packets within the Linux NFQueue.

2. Improvements / Problems Resolved

Update of the base operating system to Debian 12

Update to OpenSSL 3.5 and update of other open source libraries

The OpenSSL version used in SES has been upgraded to version 3.5. In addition, the open source libraries contained in SES have been updated. The respective versions can be found in the document “OpenSourceLicenseTerms.pdf”.

Stability improvement in connection with a restart

If the vSES was restarted due to a configuration change, the Sysconfig daemon crashed during a simultaneous check for available updates in the repository. This problem has been fixed.

Stability improvement of the salted hash functionality

With the introduction of the salted hash feature, the ncpsrvmgmd service could crash under certain conditions. This issue has been resolved.

Troubleshooting: “Forward SEM requests” option has no effect

The “Domain group”/‘Forwarding’/“Forward SEM requests” option had no effect. The problem has been fixed.

Stability improvement related to SES shutdown

In rare cases, the VPN server daemon could crash when shutting down the SES. This issue has been fixed.

DNS server is not transferred via DHCP

If a DHCP server was configured in a domain group and the configuration for the DNS servers was omitted, the DNS servers distributed via DHCP were not transferred to the clients, or only one of them was transferred. This problem has been fixed.

Troubleshooting: Crash of a remote site gateway when dialing into the head office

Due to an incorrect VRRP configuration, the backup gateway at a remote site incorrectly attempted to establish a connection to the head office. This caused the backup gateway to crash. The problem that led to the crash has been fixed.

Disabling IPv6 on the NCP adapter

As with the other network adapters, IPv6 can also be disabled for the NCP network adapter starting with this server version.

New storage location for the `ncpwsupd.conf` file

The storage location for the `ncpwsupd.conf` file will be `/opt/ncp/vses/etc/ncpwsupd.conf` in future. When the SES is updated, the file is automatically moved there and can then only be written to by root.

Error message when calling `vses-license`

When calling `vses-license` or `vhas-license`, an error message was generated in the operating system log. This problem has been fixed.

Error when selecting the server certificate

If multiple server certificates are configured in a domain group, under certain circumstances, the certificate selected by the administrator was not used for authentication with the client. This issue has been resolved.

Remote SES sporadically unavailable during Site2Site connection

In a Site2Site scenario, a remote SES establishes a connection to the central SES. In rare cases, every IP address in the remote network can be accessed from the central side, but the remote SES itself cannot. This issue has been resolved.

Added software version information to the installer

RIP unicast only to one master router

The SES offers up to four configurable master routers as recipients of a RIP unicast. However, only the first one was addressed. This problem has been fixed.

Troubleshooting: DDNS update packet with incorrect source IP address

Protect LAN adapters

If the “Protect LAN adapters” option was enabled, no data exchange via IPv6 was possible on the relevant network interface. This problem has been fixed.

Server plug-in - DH groups added

The IPsec options for the IKE DH and PFS group entries have been supplemented with groups 27-30.

Troubleshooting: SES crash with log message: ncpwsup -> watchdog expired

3. Known Issues

`Restart Services` does not work

The `Restart Services` option in the Server Plug-in causes the server services to shut down, but they do not restart.

Entered license is only applied after restart

In the event of an update from a licensed SES version 13.x, the SES must be restarted after importing the current license version 14. This also applies to license entry after a new installation in the event of an expired trial period.

Combination of client certificate with ECC and SES with RSA does not work

If certificates with Elliptic Curve Cryptography (ECC) are used on the client and an RSA server certificate is configured on the SES, no connection can be established. The following error message appears on the client:

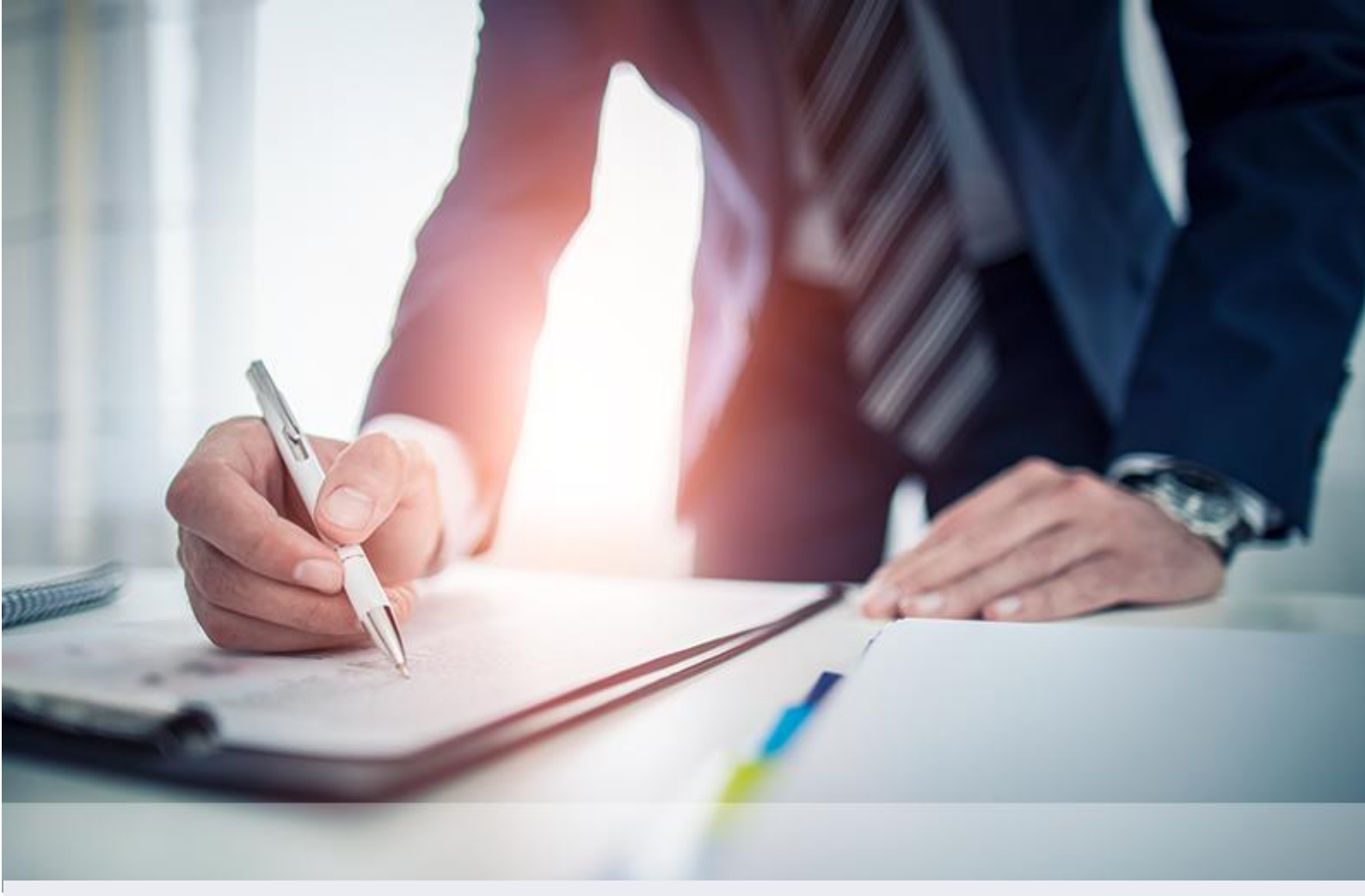
```
ERROR - 4036: Auth - PKI ERROR: - <> Verify Server certificate with error
2107! (Ext. ‘SSL Server Authentication’ failed)
```

This problem will be fixed in a future version of the gateway with the configuration option for the RFC7427 padding method.

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

To ensure that you always have the latest information about the NCP Virtual Secure Enterprise VPN Server, always check the NCP website at:

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



NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Deutschland

+49 911 9968 0
info@ncp-e.com
www.ncp-e.com

NCP engineering, Inc.
19321 US Highway 19 N, Suite 401
Clearwater, FL 33764
USA

+1 650 316 6273
info@ncp-e.com
www.ncp-e.com