NCP

Product Information

VPN software solution for government use

VPN software solution for RESTREINT UE/EU RESTRICTED and NATO RESTRICTED

Government authorities, offices, and companies that are bound to secrecy transmit data containing highly sensitive information of citizens or projects. The security of the communication channels plays a crucial role and must adhere to the recommendations and specifications of authorities and governments.

Politicians, government officials, and employees must be able to access network resources and data quickly, easily, and securely.

The following NCP software components can be used for this purpose:

- **NCP VS GovNet Connector 2.X** is approved for the protection of EU information up to the classification level „RESTREINT UE/EU RESTRICTED" and for the protection of NATO information up to the classification level „NATO RESTRICTED" (BSI-VSA-10710).
- **NCP VS GovNet server** is approved for „RESTREINT UE/EU RESTRICTED" and „NATO RESTRICTED" (BSI-VSA-10711)
- **NCP Secure Enterprise Management**

NCP software components can be used to securely process and transmit sensitive data and information. NCP is committed to the quality of its software products and meets stringent standards with the latest technology:

- Approved by the Federal Office for Information Security (BSI)
- Elliptic curve cryptography
- Network access control (endpoint policy)1
- VPN Path Finder Technology (Fallback IPsec/HTTPS)²
- Friendly net detection
- Hotspot Login
- Strong authentication
- Managed firewall
- Support for Wi-Fi and mobile data
- Custom branding

Software-based solution

NCP VS GovNet Connector provides a secure link between employees' workstations and remote systems (NCP VS GovNet Server). As a purely software-based solution, it can be easily rolled out to Windows workstations using any standard software distribution channel and installed on mobile devices such as laptops. Users benefit from the wide range of features which offer an advanced level of security but remain easy to use.

Based on the IPsec standard, highly secure data connections can be established with the NCP VS GovNet Server. Thanks to the support of standard interfaces, the software can be combined with other approved software (e.g. hard disk encryption).

VPN Path Finder Technology

NCP's patented **VPN Path Finder Technology**[2] also enables remote access even behind firewalls which block IPsec traffic. It automatically switches to a modified IPsec protocol mode which uses the HTTPS port to establish a VPN tunnel. This offers the same security features as IPsec, which means that the VPN Path Finder protocol does not need to be re-evaluated for security reasons.

The budget manager included in the NCP VS GovNet Connector allows volume and time budgets to be set for individual providers to ensure that online costs do not get out of hand. Problems with DS-Lite ports, which are currently widespread in home offices, are also a thing of the past.

Authentication

In addition to supporting certificates or smart cards in a PKI (Public Key Infrastructure), NCP VS GovNet Connector has optional support for **OTP solutions** (One Time Password)[3] or **biometric authentication** before the VPN connection is established, for example via fingerprint or facial recognition. The authentication process begins when users click connect in the connector UI, but the connection is not initiated until biometric authentication has been successfully completed. If the device does not have any hardware for biometric authentication or if this is not activated, the user may alternatively enter a password.

Friendly Net Detection

The Friendly Net Detection feature detects secure corporate or government networks (friendly networks) using certificate-based authentication.

When a friendly network is detected, firewall rules configured in the VS GovNet Connector can be activated automatically to allow secure data exchange without a VPN tunnel or to allow administrative access to the device. Manual VPN connection can also be disabled when the user is connected to a friendly network.

Hotspot Login

Often, users are prevented from accessing Wi-Fi hotspots in an insecure network environment due to security requirements that only allow communication through the VPN tunnel. This restriction prevents the initial login page, accessed via the web browser without a VPN tunnel, from being reachable.

This issue is solved by the Hotspot Logon feature in the VS GovNet Connector, which offers the highest level of security while logging on to hotspots before the VPN tunnel is set up through a dedicated, secure web browser and dynamic firewall rules. If the login is successful, the VS GovNet Connector will automatically set up the VPN tunnel.

Firewall

The NCP VS GovNet Connector includes an **integrated dynamic personal firewall**. This can be managed centrally, so the administrator can set rules for ports, IP addresses, segments, and applications. Firewall rules can also be configured for the VPN tunnel and external networks. The NCP VS GovNet Connector is enabled automatically on system startup.

Central Management

Organizations can deploy, set up, update, and manage the NCP VS GovNet Connector via **NCP Secure Enterprise Management** (SEM) as a single point of administration (a prerequisite for using the NCP VS GovNet Connector). All settings in the NCP VS GovNet Connector can be locked by the administrator. This prevents users from making any unwanted or unintended changes to the configuration.

NCP Secure Enterprise Management consists of a management server and a dashboard for status monitoring. The management server is responsible for configuring and managing all connected NCP components, including both clients and servers. It is a database-driven system that can connect to almost any database. Additionally, the optional backup management server ensures high availability of the management server by mirroring its current state through a replication service.

Custom Branding

With the custom branding option, companies can display their own logo or support information in the client.

Windows Pre-Logon

The NCP Pre-Logon functionality enables users to securely log in to Windows systems through direct authentication via Active Directory – even over the internet. Before the actual Windows login, users are presented with the option to establish a VPN connection to the corporate network immediately after system startup.

This process is handled by the so-called NCP Pre-Logon Access Provider (PLAP). Upon selecting this option, users authenticate themselves using a personal user certificate and the corresponding PIN. Once the VPN tunnel is successfully established, a direct connection to the central network is created.

As a result, the device can be centrally managed, and the subsequent Windows login is performed securely and directly via Active Directory authentication – regardless of the device's location (oder besser: from anywhere in the world).

Installation and Configuration

NCP VS GovNet Server is a software appliance that can be installed on any standard server hardware. It is managed through the central management component. In addition, the VS GovNet Server is compatible with IPsec VPN gateways and third-party clients.

User Management

Users can be managed flexibly via the VPN gateway or back-end systems, such as RADIUS, LDAP or MS Active Directory. Integrated IP routing and firewall features ensure connectivity and security.

Please note:

For NATO RESTRICTED/ EU RESTRICTED compliance, requirements regarding the operating system used must be observed.

[1] Prerequisite: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP VS GovNet Server, NCP Secure Enterprise Management

[2] Prerequisite: NCP Secure Enterprise VPN Server, NCP Virtual Secure Enterprise VPN Server or NCP VS GovNet Server

[3] OTP is not part of the approval

Try the full version for 30 days: ***sales@ncp-e.com***

Do you have any questions or would you like to make an appointment for a product demonstration? Please connect with us.

Europe, Asia and Pacific

NCP engineering GmbH

Dombuehler Str. 2
90449 Nuremberg
Germany

+49 911 9968-333

sales@ncp-e.com
www.ncp-e.com

The Americas

NCP engineering, Inc.

19321 US Highway N, Suite 401
Clearwater, FL 33764
USA

+1 650 316-6273

sales@ncp-e.com
www.ncp-e.com

We look forward to discussing how we can help you.

For more information,
visit our website