Data Sheet

NCP VS GovNet Server

IPsec VPN Gateway Software

Secure Remote Access to Government/Company Networks

- Approval for NATO RESTRICTED and RESTREINT UE/EU RESTRICTED (BSI-VSA-10711)
- Supports elliptical curves (ECC)
- BSI tested random number generator (class DRG.4)
- Integrated IP routing and firewall features
- VPN Path Finder Technology (Fallback IPsec/HTTPS)
- Automated tunnel forwarding
- Load balancing
- Multi-tenancy
- Multi-processor support, highly scalable
- Hardened Linux system – compatible with standard server hardware

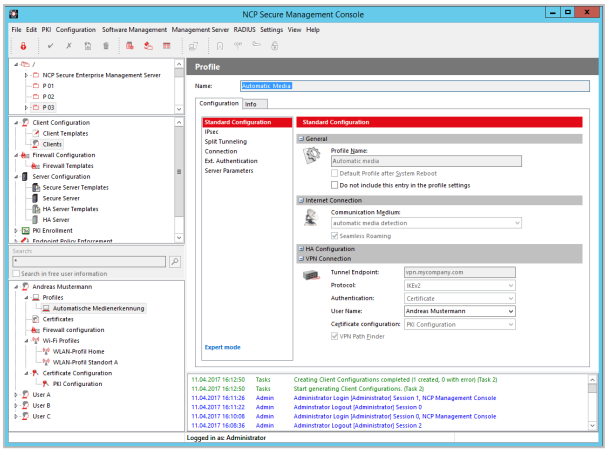
Scope

The NCP VS GovNet Server expands NCP's portfolio with a highly secure variant of the NCP Secure Enterprise VPN Server for use in government environments or companies processing classified data.

The gateway has been approved for processing data classified as RESTREINT UE/EU RESTRICTED and NATO RESTRICTED. It is ideally suited as a remote server for the NCP VS GovNet Connector, which is also approved for processing data at workstations in compliance with RESTREINT UE/EU RESTRICTED and NATO RESTRICTED. NCP VS GovNet Server can also support remote connections from Apple iOS and iPadOS devices configured according to the specifications for Apple indigo (**i**OS **N**ative **D**evices **I**n **G**overnment **O**peration).

Installation and Configuration

The VS GovNet server is provided as a software appliance for execution on standard server hardware. The configuration is done by means of the NCP Secure Enterprise Management Server.



This central instance is also used to manage the NCP VS GovNet connectors required for approved operation. NCP 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 e.g. RADIUS, LDAP or MS Active Directory. Integrated IP routing and firewall features ensure connectivity and security.

NCP VPN Path Finder

The NCP VPN Path Finder is a unique technology that also enables remote access behind proxies/firewalls which block IPsec traffic (for example in hotels). NCP Path Finder maintains all the security features of IPsec/IKE protocols but communicates via the HTTPS port.

Security/Strong Authentication

Security is of the utmost priority in developing the NCP VS GovNet Server. To minimize the risk of attacks on the server, a hardened Linux operating system is used. In the BSI-approved configuration, certificates with elliptical curves are used for communication. Random numbers are generated securely by a random number generator (class DRG.4) with smart card authentication.

General Information

Approved Hardware	Standard server with x86-64 hardware and compatibility with Debian 11.7; two Omnikey 3121 smart card readers (revision A or B) and at least one other identical smart card reader for personalizing the smart cards on the administration PC; two TeleSec TCOs 3.0 Signature Card 2.0 smart cards;
Configuration	Configuration with the central NCP Secure Enterprise Management Server
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.
Multi-tenancy	Group capability; support of max. 1024 domain groups (i.e. configuration of: Authentication, forwarding via GRE, VLAN or VPN tunnel, filter groups, IP pools, bandwidth limitation, etc.)
Firewall	Stateful packet inspection IP-NAT (Network Address Translation) Port filtering; LAN adapter protection
User Management	Local user management; OTP servers; RADIUS; LDAP, MS Active Directory Services
Statistics and Logging	Detailed statistics, logging feature, Syslog messages (via UDP or TCP)
Client/User Authentication Methods	OTP tokens, user and hardware certificates (X.509 v.3, with RSA or ECC key), username and password (XAUTH), EAP
Server Certificates	Certificates can be used that are provided via a PKCS#12 interface for private keys in soft certificates.
Revocation Lists	Revocation: EPRL (End-entity Public-key Certificate Revocation List, form. CRL), CARL (Certification Authority Revocation List, form. ARL)
Online check	Automatic download of revocation lists from the CA at predefined intervals; Online check: Online validation of certificates via OCSP or OCSP over http

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 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), RFC 7427 (IKEv2 Signature Authentication, Padding Method), XAUTH, IKECFG, DPD, Nat Traversal (Nat-T), UDP encapsulation, IPCOMP, RFC 3527 (DHCPv4), RFC 5685 (IKEv2 Redirect)
Encryption	Symmetric encryption: AES 128, 192, 256 bits (IKEv1: AES-CBC, AES-CTR; IKEv2: AES-CBC, AES-CTR, AES-GCM); Blowfish 128, 448 bits; Triple-DES 112, 168 bits;

	Dynamic methods for key exchange: Diffie-Hellman groups 1, 2, 5, 14-21, 25-30 Hash algorithms: (MD5), SHA1, SHA 256, SHA 384, SHA 512 PFS
Authentication Methods	IKEv1 (Aggressive and Main Mode); XAUTH for extended user authentication; PAP, CHAP, MS CHAP V.2 IKEv2 (pre-shared key, certificates, EAP (EAP-MS CHAPv2, EAP-TLS) Support for certificates in a PKI: Soft certificates, smart cards, USB tokens, certificates with ECC technology (NIST, Brainpool) or RSA up to 4096 bits; Pre-shared keys; One-time passwords and challenge response systems; RSA SecurID Ready
VPN Path Finder NCP PATH FINDER	NCP Path Finder Technology (fallback to HTTPS from IPsec (port 443) if neither port 500 nor UDP encapsulation are available
IP Address Assignment	DHCP (Dynamic Host Control Protocol) over IPsec; IKE config mode for dynamic allocation of a virtual address to the clients from an internal pool/address range or a central DHCP server or RADIUS
Data Compression	Deflate
Recommended VPN Clients compatibility	NCP VS GovNet Connector, NCP Secure Client, Standard-compliant IPsec clients
Approval	Approval NCP VS GovNet server for RESTREINT UE/EU RESTRICTED and NATO RESTRICTED BSI-VSA-10711

NCP engineering GmbH
Dombuehler Str. 2
90449 Nuremberg
Germany

+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