

What's New

high security remote access

NCP Secure Enterprise Server

Neue Features von Version 8.0 zu 6.0

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen können ohne Vorankündigung geändert werden und stellen keine Verpflichtung seitens der NCP engineering GmbH dar. Änderungen zum Zwecke des technischen Fortschritts bleiben der NCP engineering GmbH vorbehalten.

Warenzeichen

Alle genannten Produkte sind eingetragene Warenzeichen der jeweiligen Urheber.

© 2010 NCP engineering GmbH. Technische Änderungen vorbehalten

Inhalt

Neue Features von Version 8.03 zu Version 8.02	2
Neue Features von Version 8.02 zu Version 8.0	3
Neue Features von Version 8.0 zu Version 7.x	3
Neue Features von Version 7.0 zu Version 6.11	4
Neue Features von Version 6.11 zu Version 6.0	9

Wichtiger Hinweis:

- Die mit einem "k" gekennzeichneten Features sind kostenpflichtig, d.h. zu dessen Nutzung muss ein neuer Lizenzkey erworben werden.

Neue Features von Version 8.03 zu Version 8.02

Verbesserungen und Erweiterungen

Sicherheits-Erweiterungen am Web Interface

Aus Sicherheitsgründen wird der Web Daemon am Linux Gateway nicht mehr mit Root-Rechten sondern automatisch mit eingeschränkten Benutzerrechten (nobody) ausgeführt.

Zudem werden nur Verbindungen von SSL Clients zugelassen, die Strong Cipher Suites (mindestens AES oder 3DES) unterstützen.

Geänderter Verfügbarkeitstest (Availability Check)

Wurde die Verfügbarkeit über zwei Interfaces mit Ping getestet (ICMP request/reply), galt die Verfügbarkeit bereits dann als gegeben, wenn nur ein Interface erfolgreich geantwortet hat.

Damit der Verfügbarkeitstest als positiv gewertet wird, müssen nun beide konfigurierten Interfaces ordnungsgemäß antworten.

Service Check im HA Server-Verbund

Ein HA Server erkennt sofort, ob der andere HA Server zur Verfügung steht bzw. der Service gestoppt ist (ncpwsup service bei Windows, ncpwsupd daemon bei Linux).

Mit diesem Service Release wurden folgende Funktionen optimiert:

- *CRL Download*
- *Zertifikatsprüfung*
- *LDAP-Authentisierung mit Gruppenzuweisung per Zertifikat*
- *VRRP-Technik für Linux*
- *Konfigurations-/Management-Sitzungen*

Neue Features von Version 8.02 zu Version 8.0

Neue LDAP Attribut-Filter

Neue Filter in der LDAP-Konfiguration der Domain-Gruppen können für das Accounting der Benutzer am LDAP Server und am Active Directory Server genutzt werden.

Nur Benutzer aus Verzeichnis-Diensten, welche die angegebenen Attribute besitzen, bekommen VPN-Zugang.

Unterstützung von SSL VPN- und Path Finder-Verbindungen an einem Gateway

IPsec-Verbindungen mit Path Finder-Protokoll nutzen zum VPN Gateway den Port 443, ebenso SSL VPN-Verbindungen. Sollen beide Verbindungsarten zu einem VPN Gateway möglich sein, so muss dem Client für die IPsec-Verbindung über Path Finder zusätzlich zum alternativen IKE-Port 443 eine eigene IP-Adresse mitgegeben werden. Am Gateway wird diese IP-Adresse als "Path Finder Listener (IP-Adresse)" in der Konfiguration unter "Lokales System / VPN/IPsec" eingetragen.

Direktverbindung von Gateways über ISDN MSN

Mit der MSN (Mehrfachrufnummer) kann ein anderes Gateway für eine Direktverbindung über ISDN mit DSS1 adressiert werden. Die MSN des jeweiligen Gateways wird in der Konfiguration unter "Lokales System / VPN/IPsec" eingegeben. Das andere Gateway muss diese MSN der Rufnummer anhängen.

Neue Features von Version 8.0 zu Version 7.x

Erweitertes Web-Interface

Verbessertes, vollwertiges Web-Interface löst die Konfiguration über SNMP mit dem Server Manager ab. Die Statusmeldungen sind über SNMP und Webinterface verfügbar. Alternative: Über NCP Secure Enterprise Management Plug-in.

Achtung: Eine Konfiguration mit dem bisherigen Server Manager über SNMP ist ab der Server-Version 8.0 nicht mehr möglich! Der Import alter INI-Dateien wird noch unterstützt, soweit diese vom Remote Server Plug-in erzeugt wurden.

NCP VPN Path Finder

Die NCP VPN Path Finder Technology bewirkt ein automatisches Umschalten auf ein alternatives Verbindungsprotokoll (TCP Encapsulation mit SSL Header über Port 443), wenn Standard IPsec über Port 500 bzw. UDP Encapsulation über einen frei konfigurierbaren Port nicht möglich ist. (In Verbindung mit NCP Secure Clients ab 9.2)

Windows Server 2008 (k)

Der Windows Server 2008 wird als 32- und 64-Bit Betriebssystem unterstützt.

Erhöhung gleichzeitiger Sessions

Der Secure Server wurde von 1000 auf bis zu 10.000 gleichzeitige Sessions erweitert.

Server Plug-in für SEM 2.03 (k)

Alternativ zum Web-Interface: Vorständige Konfiguration mit dem NCP Secure Enterprise Management 2.03 mit Server Configuration Plug-in 8.0

Optimierung der SSL VPN Funktionalitäten

Web Proxy-Erweiterungen:

- Kompatibel mit Outlook Web Access 2003 und 2007
- Erweiterte Ansicht von Microsoft Outlook Web Access (mit Internet Explorer)
- Kein Caching mit Microsoft Internet Explorer
- Unterstützung für Apple Safari Mac OS X/Windows

Thin Client-Erweiterungen:

- Microsoft ActiveX Unterstützung zusätzlich zu Java (≥ 1.5)
- Port-Redirection verbessert
 - o Umschreiben von CITRIX ICA-Konfigurationsdateien
 - o Unterstützung für Windows Standard Webbrowser (ohne HTTP-Proxy)

PortableLAN (k)

- mit PKCS#11 Unterstützung

Weitere Neuerungen

- XML-basierte, flexiblere Konfiguration
- Weiter verbessertes Logging

Neue Features von Version 7.0 zu Version 6.11

SSL VPN-Server

Der NCP Secure Enterprise Server verfügt in seiner neuen Version 7.0 über zwei Module: den IPSec und den SSL VPN-Server. In einem SSL VPN ist am Benutzer-PC keine VPN Client-Software erforderlich.

Voraussetzung am Telearbeitsplatz ist lediglich ein SSL-fähiger Browser (entspricht Web-Proxy). Wird Port Forwarding (Port-Weiterleitung) benötigt, Endpoint Security eingesetzt oder der Internet Explorer mit einer Einstellung zum Löschen des Cache benutzt (Cache Protection), so muss zusätzlich Java Runtime V1.5 installiert sein.

Funktionsprinzip einer SSL VPN-Verbindung

Der Anwender-PC wählt sich mit dem Browser über HTTPS am zentralen SSL VPN-Server (Gateway) an und gelangt über die Gateway-Adresse auf eine Login-Seite, wo sich der Benutzer mit Passwort und Benutzername authentisieren muss.

Passwort und Benutzername können die gleichen sein, wie für einen optional zusätzlich zu installierenden VPN Client. Auch kann die Authentisierung über Zertifikat erfolgen, das dann am Browser eingespielt worden sein muss.

Wie die Authentisierung stattzufinden hat, wird am Firmen-Gateway konfiguriert, wo auch in gewohnter Weise die weitere Parametrisierung zur Rechtestruktur für den Zugriff auf das Firmennetzwerk erfolgt.

Das Aussehen der Login-Seite kann firmenspezifisch gestaltet werden.

Die von NCP vorgegebenen Eingabefelder (für Passwort und Benutzername) müssen allerdings beibehalten werden.

Nach der erfolgreichen Authentisierung öffnet sich im Browser eine Menü-Seite (Portal), über die der Anwender aus einer (über das VPN-Gateway zu konfigurierenden Liste) die gewünschte Anwendung auswählen kann.

Je nach gewählter Anwendung wird (für den Anwender im Hintergrund) vom VPN-Gateway eine Verbindung hergestellt (z.B. zu Web-Server, Terminal-Server, File-Server) und die entsprechende Applikation über die Browser-Oberfläche gestartet.

VLAN

VLAN (Virtuelles LAN) ist neben GRE und VPN eine weitere Art der Tunnelweiterleitung für die Mitglieder einer bestimmten Domain-Gruppe. Ein VLAN wird nur dazu eingerichtet, die IP-Pakete der definierten Gruppe (zu einem anderen VLAN-fähigen Gateway) weiterzuleiten. (Eine SSL VPN-Weiterleitung im VLAN ist nur unter Windows-Betriebssystemen möglich.)

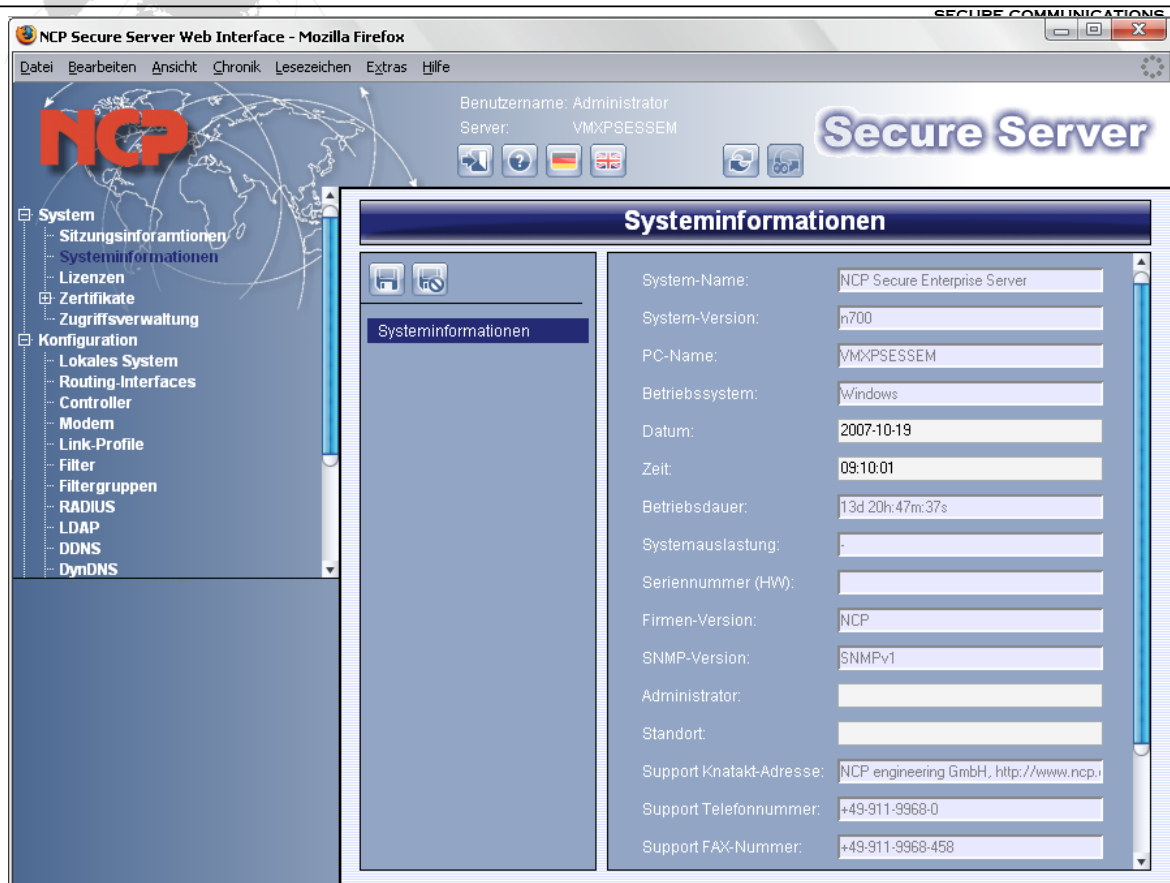
Das VLAN wird als Routing-Schnittstelle auf einem LAN-Adapter ins Firmennetz aufgesetzt. Pro LAN-Adapter können maximal 256 VLANs definiert werden. Von welcher Domain-Gruppe welches VLAN genutzt wird, wird dabei über die VLAN ID festgelegt.

Zur Konfiguration eines VLANs am LAN-Adapter (unter "Routing Interfaces") klicken Sie im Parameterfeld "VLAN" auf "Hinzufügen".

Web-Interface

Administration und Konfiguration des NCP Secure Enterprise Servers können unabhängig vom Betriebssystem über einen Web-Browser erfolgen.

Das Web-Interface des Secure Server Managers ist im Standardlieferungsumfang des Secure Enterprise Servers 7.0 enthalten und ist nach dessen Installation betriebsbereit. Das Web-Interface des Secure Enterprise Servers wird über einen Browser aufgerufen, indem Sie die Internet-Adresse oder URL in Form von Hostname oder IP-Adresse mit der nachfolgenden Port-Nummer 20112 in die Adressleiste eingeben. Zum Beispiel: <https://hostname:20112>



Einschränkung der maximalen Bandbreite

Mit diesem Parameter kann die maximal nutzbare Bandbreite pro Teleworker in kBits/s festgelegt werden. Damit ist unabhängig von der Verbindungsart der entfernten Clients die zentralseitig verfügbare Bandbreite für alle Benutzer gleichmäßig zuordenbar. Es ist zu differenzieren, ob die Bandbreite für ausgehenden (Tx) oder eingehenden (Rx) Datenverkehr genutzt wird. Zu beachten ist, dass die Zentrale die Bandbreite unabhängig von der Richtung des Datenaufkommens zur Verfügung stellt. Ist die Bandbreite ausgeschöpft, kann kein weiterer Datenverkehr stattfinden (die Bandbreitenbeschränkung kann nur für TCP-Anwendungen eingerichtet werden).

Die maximale Bandbreite ist auf drei Ebenen einstellbar:

- linkspezifisch unter "Link-Profil / Line-Management"
(gilt nur für den jeweiligen Benutzer)
- gruppenspezifisch unter "Domain-Gruppen / Allgemein"
(gilt für alle Benutzer der jeweiligen Gruppe)
- global für dieses VPN-Gateway unter "Lokales System / Restriktionen"
(gilt für alle Benutzer)

Auf allen drei Ebenen kann eine unterschiedliche maximale Bandbreite eingestellt werden. Dem aktuell ins Firmennetz eingewählten Benutzer wird immer nur die Bandbreite gestattet, die die höchste Priorität hat. Dabei hat die linkspezifische Konfiguration Priorität vor der gruppenspezifischen und diese wiederum vor der globalen.

Erweiterung der IPSec Optionen

Dieses Feature ermöglicht die Konfiguration von: DPD-Intervall, PFS-Gruppe und die Verwendung der erweiterten Authentisierung (XAUTH) pro Link-Profil. Hier die Optionen:

- Benutze XAUTH für ausgehende Verbindungen
Wird für eine ausgehende Verbindung "IPSec-Tunneling" genutzt, so kann die Authentisierung über Extended Authentication (XAUTH Protokoll, Draft 6) erfolgen.
- DPD-Intervall
DPD (Dead Peer Detection) wird automatisch im Hintergrund ausgeführt, sofern dies die Gegenstelle unterstützt. Mit DPD (Dead Peer Detection) wird die Gegenstelle aktiv (nach eingestelltem Zeitintervall in Sekunden) unabhängig vom tatsächlichen Nutzdatenverkehr "angepingt" und der Tunnel abgebaut, wenn keine Antwort erfolgt oder der Timeout abgelaufen ist (unabhängig vom Datenaufkommen). Mit einem größeren Intervall werden weniger häufig Pakete geschickt, die die Erreichbarkeit der Gegenstelle überprüfen und damit das Datenaufkommen verringert.
- PFS-Gruppe
Mit Auswahl einer der angebotenen Diffie-Hellman-Gruppen wird für die ausgehende IPSec-Verbindung festgelegt, ob ein kompletter Diffie-Hellman-Schlüsselaustausch (PFS, Perfect Forward Secrecy) in Phase 2 zusätzlich zur SA-Verhandlung stattfinden soll. Standard ist "keine".

Erweiterung der IP-Pools

Die Anzahl möglicher IP-Pools wurde auf maximal 256 pro Gruppe erweitert.

Die Darstellung unter "Routing Interfaces / Secure Server Adapter" und "Domain-Gruppen" erfolgt nun in einer Liste. Die Pool-Nummer kann als Zahl im Link-Profil unter "Routing" angegeben werden. Bei Einwahl auf älteren Secure Servern wird die bisherige Ansicht angezeigt.

Erweiterte Zertifikats-Unterstützung

Mit dieser Version werden auch Zertifikaten mit einer Schlüssellänge bis zu 4096 Bits unterstützt.

Erweiterung von RADIUS-Attributen

RADIUS Access Attribute

Zusätzliches Attribut im RADIUS Access Request des RADIUS Clients:

TUNNEL-CLIENT-ENDPOINT (ID 66) Öffentliche IP-Adresse des Initiators

RADIUS Accounting Attribute

Innerhalb der RADIUS Accounting Start Message wird zusätzlich übergeben:

TUNNEL-CLIENT-ENDPOINT (ID 66) (type IPADDRESS), welches die öffentliche IP-Adresse des Initiators enthält.

FRAMED-IP-ADDRESS (ID 8) (type IPADDRESS), welches die private (VPN) IP-Adresse enthält, die dem Initiator zugewiesen wurde.

NAS-PORT-TYPE (ID 61) (type INTEGER), welches den Wert der vom Client benutzten Verbindungsart enthält. Die Werte der Verbindungsarten sind wie folgt definiert:

ISDN	0 ISDN
DIGITAL MODEM	1 digitales Modem
V110	2 V.110 über ISDN
SYNC	3 sync. Modem
ASYNC	4 async. Modem
LAN	8 LAN
XDSL	10 XDSL
RAS	12 externer Dialer (MS)
ATM	14 ATM
IPASS	15 externer Dialer (IPASS)
MSPPTP	16 MS PPTP
GPRS/UMTS	18 GPRS/UMTS
PPC	19 Pocket PC Connection Manager
WLAN	20 WLAN

RADIUS Authentication Attribute

Alternativ zum lokalen System oder einer Domain-Gruppe ist es möglich, über RADIUS in einem Link-Profil den Management Server zu zuweisen. Dafür wurden die RADIUS Authentisierungs-Attribute erweitert:

```
ATTRIBUTE NCPS-MgmServer1 172 ipaddr SEM1 IP Address
ATTRIBUTE NCPS-MgmServer2 173 ipaddr SEM2 IP Address
```

RADIUS-Konfiguration für ausgehende Verbindungen

Mit dieser Funktion kann das zugehörige Link-Profil zu einer Ziel-IP-Adresse eines Clients vom RADIUS Server abgefragt werden. Diese Funktion ist nur mit dem Secure Enterprise Management gegeben. Ist zusätzlich zu dieser Funktion auch "LDAP-Konfiguration für ausgehende Verbindung" gesetzt, so wird die LDAP-Konfiguration herangezogen.

Weiterleitung für Management-Pakete

Management-Pakete für Benutzer einer Gruppe, für die eine Weiterleitung (GRE, VPN oder VLAN) konfiguriert ist (Domain-Gruppen / Allgemein), werden dann nicht weitergeleitet,

wenn der in der Domain-Gruppe angelegte Management Server die gleiche IP-Adresse besitzt wie der im lokalen System angelegte (Lokales System / DNS/WINS).

Sind Management Server mit unterschiedlichen IP-Adressen im lokalen System (Lokales System / DNS/WINS) und in einer Domain-Gruppe (Domain-Gruppen / Allgemein) definiert, so wird bei einer Management-Anfrage die eingestellte Weiterleitung (Domain-Gruppen / Allgemein) genutzt.

Hinweise:

Das Lizenzmodell für den SSL VPN-Server

Die 30-Tage Vollversion (Testversion) des NCP Secure Enterprise Servers wird mit dem Server Manager, 5 IPSec-Tunnel und 5 SSL VPN-Tunnel ausgeliefert. Ein SSL VPN-Tunnel entspricht einem Concurrent User. In der Testversion verfügt der SSL VPN-Server über alle Module, also Web Proxy, Endpoint Security und Port Forwarding.

Bei Lizenzierung des SSL VPN-Servers mit allen Modulen (Endpoint Security und Port Forwarding) werden die Test-Konfigurationen ebenfalls komplett übernommen.

Wird der SSL VPN-Server ohne Endpoint Security lizenziert, so wird zwar die zugehörige Konfiguration übernommen, die Wirksamkeit der Endpoint Security jedoch ausgeschaltet.

Wird der SSL VPN-Server ohne Port Forwarding lizenziert, so wird die zugehörige Konfiguration übernommen, die konfigurierten Anwendungen werden dem SSL VPN-Benutzer in der Web-Oberfläche jedoch nicht angeboten.

Wird der SSL VPN-Server nicht lizenziert, sondern ausschließlich der IPSec VPN-Server, dann verlieren die SSL VPN-Tunnel und die zugehörige Konfiguration bzw. die Concurrent User der Testversion ihre Funktionalität. D. h. nach der Lizenzierung des IPSec VPN-Gateways entfällt die SSL VPN-Funktionalität.

Eine 30-Tage Vollversion des IPSec VPN-Servers wird lizenziert und zur unbegrenzten Vollversion freigeschaltet, indem im Menü des Server Managers unter "System / Lizenz" der Aktivierungsschlüssel und die Seriennummer eingetragen werden.

Die Lizenzierung des SSL VPN-Servers erfolgt im Menü des Server Managers unter "System /SSL/VPN-Lizenz". Die Seriennummer muss dabei der Seriennummer des IPSec VPN-Servers entsprechen, das mit einem neuen, dazu passenden Aktivierungsschlüssel um den SSL VPN-Server erweitert wird.

Dieser Aktivierungsschlüssel variiert je nach erworbener Modul-Lizenz und wird immer mit dem Lizenzschlüssel für das IPSec VPN-Server kombiniert.

Im Lizenz-Fenster kann abgelesen werden, ob diese Version eine Vollversion oder eine Testversion ist und wie lange letztere noch gültig ist. Der Aktivierungsschlüssel kann geändert werden. Dies ist dann nötig, wenn Sie eine Tunnelerweiterung vorgenommen haben.

Neue Features von Version 6.11 zu Version 6.0

VRRP-Unterstützung

Kommt im Backup-Fall der Secondary Server im Failsafe-Modus zum Einsatz, so müssen bei Einsatz des VRRP keine Routing-Anpassungen des Default Routers mehr vorgenommen werden, da beide Gateways, die im Failsafe-Modus arbeiten, über eine gemeinsame IP-Adresse

angesprochen werden können. Voraussetzung für den Einsatz des VRRP (Virtual Router Redundance Protocol) ist die Konfiguration eines HA-Systems im Failsafe-Modus.

Die beiden VPN Gateways stehen innerhalb einer DMZ und besitzen je einen LAN-Adapter in Richtung Internet und einen in Richtung internes Firmennetz.

Sowohl die LAN-Adapter der beiden Gateways in Richtung Internet, als auch die LAN-Adapter in Richtung internes Firmennetz bekommen eine gemeinsame virtuelle IP-Adresse und eine gemeinsame VRRP ID. (Siehe dazu die Parameter: Benutze VRRP, VRRP ID, Virtuelle IP-Adresse)

VLAN-Unterstützung

VLAN (Virtuelles LAN) ist neben GRE und VPN eine weitere Art der Tunnelweiterleitung. Die VLAN-ID bestimmt, über welchen LAN-Adapter (unter "Routing Interfaces") die Pakete eines remote VPN-Benutzers an seine Domain-Gruppe weitergeleitet werden. Die VLAN-ID kann Werte von 1 bis 4095 annehmen. Zur Konfiguration am LAN-Adapter klicken Sie im Parameterfeld "VLAN" auf "Hinzufügen" und tragen eine beliebige VLAN-ID ein. Die gleiche VLAN-ID muss auch in der entsprechenden Domain-Gruppe unter "Allgemein / Weiterleitung" eingetragen werden. (Auf einem LAN-Adapter können max. 256 VLAN-IDs eingetragen werden.) Die MAC-Adresse sollte auf der voreingestellten Nullstellung belassen werden. Die VLAN ID muss gleich konfiguriert werden am LAN-Adapter und in der entsprechenden Domain-Gruppe.

In der Domain-Gruppe stellen Sie unter "Subsystem" den "Routing-Modus" auf "RIP" und tragen die LAN IP-Adresse des VLAN (vom Administrator zu bestimmen) sowie die IP-Adresse des Master Router 1 (Default Router) ein. Zudem muss in der Domain-Gruppe unter "Allgemein" die Art der Weiterleitung mit der VLAN-ID festgelegt werden. Tragen Sie dazu die gleiche VLAN-ID ein, die unter "VLAN" am entsprechenden LAN-Adapter konfiguriert wurde. Achten Sie außerdem darauf, dass die Weiterleitungsarten GRE und VPN für diese Gruppe nicht genutzt werden. (Siehe dazu die Parameter: VLAN-ID, MAC-Adresse)

Freie Port-Wahl für die IPSec-Kommunikation mit UDP

Sind beispielsweise an der zentralen Firewall die Standard-Ports für die IPSec-Kommunikation bereits für andere IPSec-Lösungen freigeschaltet (IPSec mit UDP -> Port 4500, für IPSec ohne UDP -> Port 500), lässt sich für die NCP IPSec-Lösung mit dieser Option ein beliebig anderer Port für die IPSec-Kommunikation definieren. Voraussetzung ist, dass UDP (User Datagram Protocol) Encapsulation genutzt wird. Global wird der Port definiert unter "Konfiguration / Lokales System / VPN / Alternativer IKE-Port". Dieser Port wird mit UDP Encapsulation sowohl für die IKE-Verhandlung als auch für die IPSec-Verhandlung genutzt und muss in der Client-Konfiguration im Telefonbuch unter "IPSec-Optionen / Benutze UDP Encapsulation" ebenso konfiguriert sein. Ebenso muss dieser Port an der Firewall freigeschaltet werden.

Gruppenspezifischer Pre-Shared Key für IPSec

Ist der Pre-Shared Key nicht benutzerspezifisch im Link-Profil konfiguriert (siehe -> Link-Profile / Security), so wird unter „Allgemein/Domain-Gruppen“ der hier eingegebene gruppenspezifische Pre-Shared Key für die IPSec-Verbindung herangezogen.