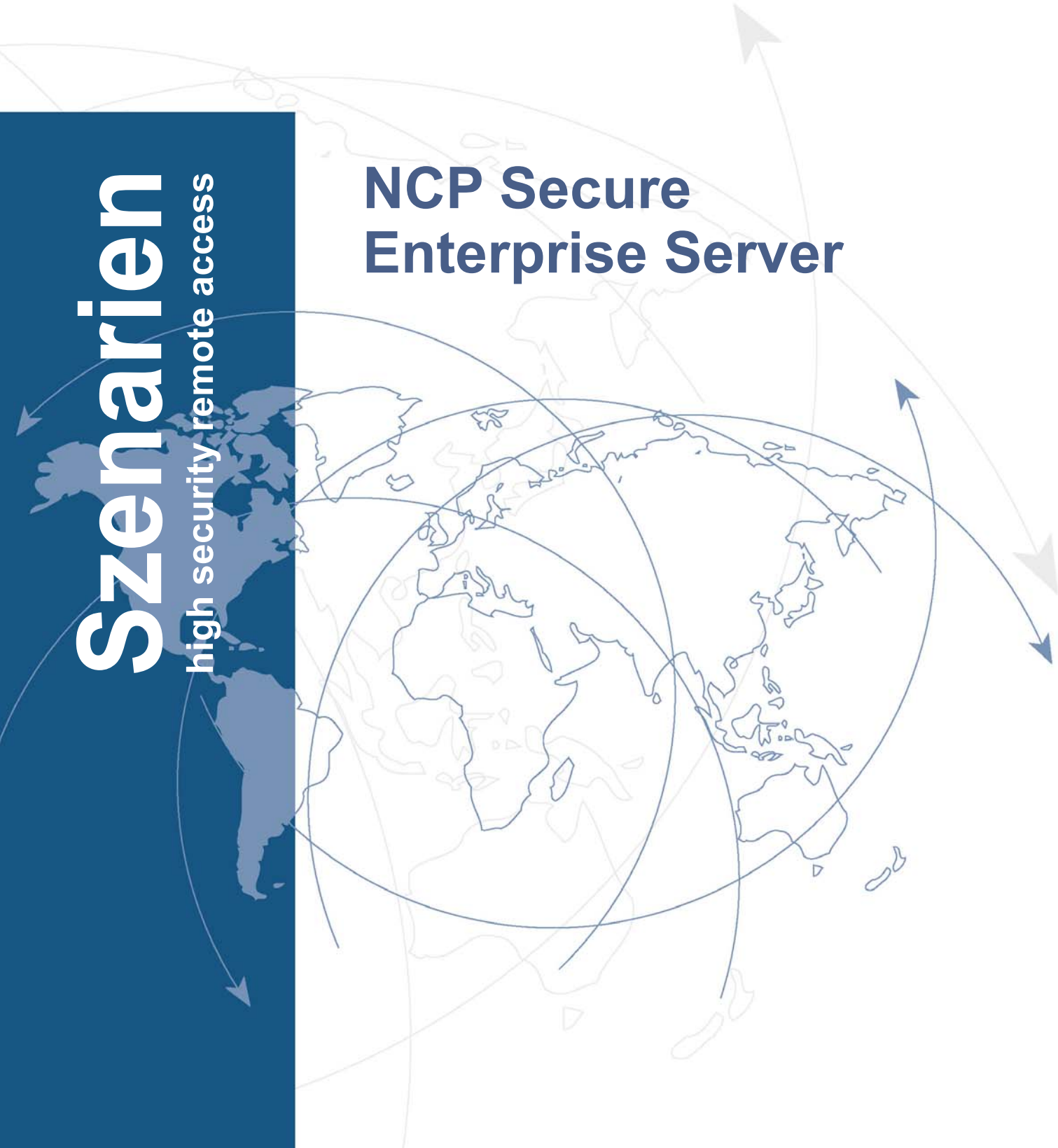
NCP
SECURE COMMUNICATIONS

Szenarien

high security remote access

NCP Secure Enterprise Server



Secure Enterprise Server

Szenarien

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com

Copyright

Sie erreichen unsere NCP Experten unter folgenden Hotlines:

Kunden mit Hotline Service Vertrag
Sie erhalten sofortigen Support unter der vertraglich angegebenen Rufnummer.
Ihnen steht das komplette Serviceportfolio zur Verfügung.

Kunden ohne Hotline Service Vertrag
Sie können wählen zwischen:
Kostenpflichtige Service-Rufnummer 09001996800 (-,80 Euro / Minute)
E-Mail an support@ncp-e.com oder Telefax an 0911 99 68 458
(ohne feste Reaktionszeiten)

Dienstleistungsauftrag (Berechnung nach Aufwand)
mit festen Reaktionszeiten und Zusatzservices.
Bitte nutzen Sie zur Anfrage das NCP Service-Formular von der Website
http://www.ncp-e.com/de/service-support/support.html

Sie möchten mehr über den NCP Hotline Service Vertrag wissen?
Bitte senden Sie eine E-Mail an:
vertrieb@ncp-e.com

Szenarien

Diese Dokumentation beschreibt Einsatzmöglichkeiten des VPN Gateways in verschiedenen Netzwerkumgebungen.

Weitere Informationen zu Ausbaustufen und Produktvarianten erhalten Sie auf der NCP Website: http://www.ncp-e.com

Sichere End-to-End-Kommunikation ohne offizielle IP-Adresse

Die Zielsetzung der Unternehmen und Organisationen, Corporate Networks immer kostengünstiger gestalten zu wollen ohne auf Vertrauenswürdigkeit und Vertraulichkeit zu verzichten, hat Virtuelle Private Netze (VPNs) in den Mittelpunkt von Netzwerkplanungen rücken lassen.

In Internet-VPNs (auch IP-VPNs genannt) ist jeder Kommunikationspartner grundsätzlich nur über eine öffentliche (offizielle) IP-Adresse erreichbar, die ihm vom Internet Service Provider (ISP) bei jeder Einwahl zugeordnet wird. Die Internetzugänge mit festen IP-Adressen als Voraussetzung für einen Verbindungsaufbau über IP sind verhältnismäßig teuer. Deshalb wird mit günstigen Internetzugängen ohne feste IP-Adresse gearbeitet, d.h. der Benutzer bekommt bei jedem Verbindungsaufbau in das Internet eine andere IP-Adresse zugewiesen. Das Auffinden eines solchen Partners erfordert besondere Mechanismen, die von der eingesetzten VPN-Lösung erbracht werden müssen.

Die Leistungsmerkmale **Lockruf** und **DynDNS** (Dynamic Domain Name Server) bieten alle auf diese Kommunikationsbedürfnisse abgestimmten Funktionalitäten. Auf diese Weise ist ein hochsicherer, performanter Datenverkehr via Internet gewährleistet, auch ohne feste IP-Adressen der Kommunikationspartner.

Lockruf

Der Lockruf ermöglicht, die Kommunikationsgegenstelle über den Kommunikationswunsch zu informieren, ohne dass diese Online ist.

Liegen z. B. Daten in der Firmenzentrale für einen entfernten Anwender vor, so wählt das zentrale Gateway die externe Gegenstelle (Client oder Gateway) an. Die Anwahl erfolgt ohne Verbindungskosten zu verursachen direkt über ISDN mittels “Anklopfen im D-Kanal” d.h. die Rufnummer wird signalisiert. Die Gegenstelle etabliert nach erfolgreicher Überprüfung der Rufnummer selbsttätig einen VPN-Tunnel zum anrufenden Gateway (automatischer Rückruf). Nach erfolgreich durchgeführten Security-Verhandlungen können nun Daten hochsicher, End-to-End zwischen dem zentralen Gateway und dem entfernten Anwender übertragen werden.

Lockruf-Konfiguration

Der Lockruf wird vom zentralen Gateway aus angestoßen, indem z.B. ein Ping an die IP-Adresse der Remote-Seite abgesetzt wird. Auf der Remote-Seite wird die im ISDND-Kanal signalisierte Rufnummer vom Gateway überprüft. Stimmt die gesendete Rufnummer mit der konfigurierten überein, wird ein automatischer Rückruf ausgeführt.

Die relevanten Konfigurationsparameter heißen **Rufnummer für CLI** (Calling Line Identification) und **Rückrufmodus**. Sie werden mittels Web-Interface für ein zu definierendes Link-Profil gesetzt. Die “Rufnummer für CLI” ist ein exklusives ISDN-Leistungsmerkmal und wird im Link-Profil unter **Authentisierung** konfiguriert. Der Rückrufmodus wird im Link-Profil unter **Verbindungssteuerung** eingestellt.

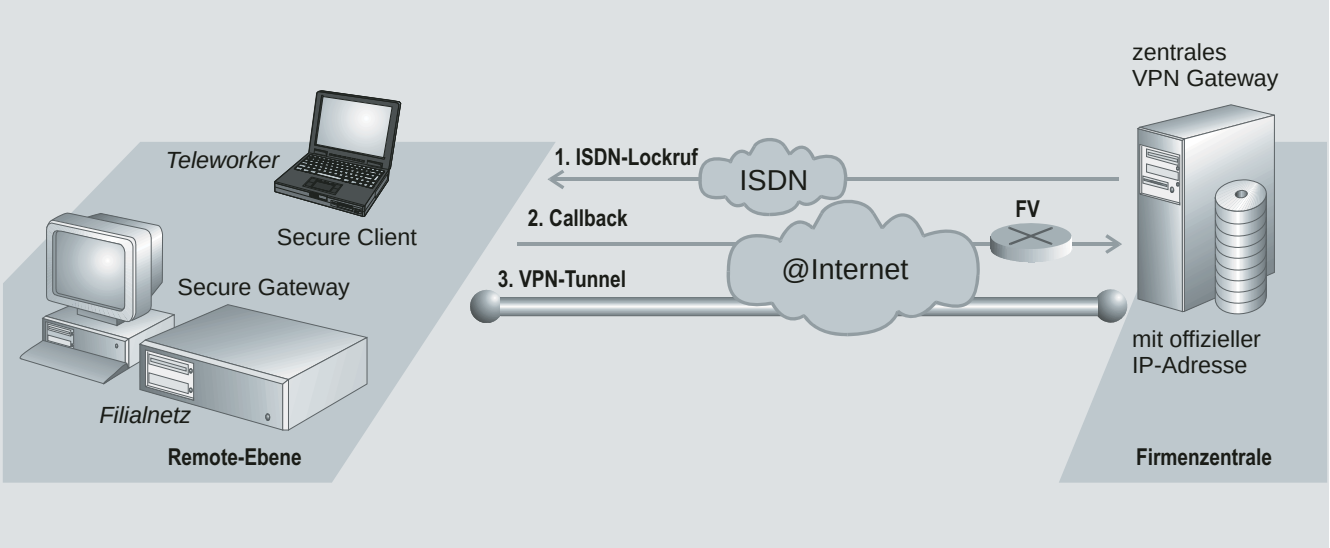


Abb.oben: Dial Out mit Lockruf (Firmenzentrale verfügt über eine feste IP-Adresse)
Ablauf des Verbindungsaufbaus: Nachdem das Gateway einen Lockruf via ISDN an die Remote-Ebene abgesetzt hat (1), erfolgt ein Verbindungsaufbau (Rückruf / Callback) an die vorkonfigurierte feste IP-Adresse des Gateways (2), womit gleichzeitig ein VPN-Tunnel aufgebaut wird (3).

Dynamic DNS

Da die IP-Adresse des zentralen Gateways im Beispiel nicht bekannt ist, wird mit dem Hostnamen statt einer TEP IP-Adresse gearbeitet. Der Benutzer muss lediglich im Klartext den Namen des Zielsystems eingeben, die Umsetzung in die entsprechende IPAdresse übernimmt ein DNS-Server. Die im Internet befindlichen DNS-Server sind für alle statischen DNS-Namen (feste IP-Adressen) nicht aber für dynamische IP-Adressen vorgesehen. Für dynamische (wechselnde) IP-Adressen kommen in diesem Fall DynDNS-Server zum Einsatz.

Versucht A eine Verbindung zu einem Partner B via Internet herzustellen, kontaktiert er den zunächst den DNS Server des ISP und fragt nach der IP-Adresse von B. Ist keine feste IP-Adresse vorhanden, befragt der ISP den DynDNS-Server nach der derzeit gültigen IP-Adresse von B. Sobald er diese hat, wird sie an A übermittelt, der dann eine direkte Verbindung zu B aufbauen kann. Im Unterschied zum Lockruf muss der gewünschte Kommunikationspartner immer online sein, also über eine Flatrate verfügen, um erreichbar zu sein.

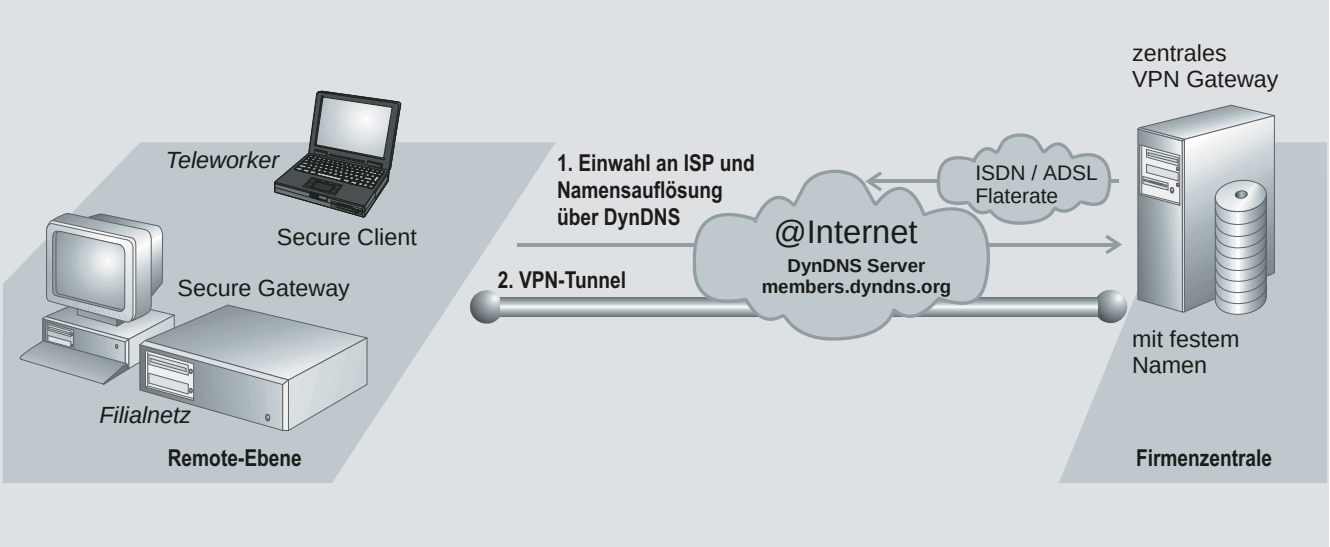


Abb.oben: Dial In mit DynDNS: Firmenzentrale verfügt über keine feste IP-Adresse
Ablauf des Verbindungsaufbaus: Der feste Name (DNS-Name) des zentralen Gateways ist am DynDNS Server registriert, dem mittels eines DynDNS Clients die jeweils aktuelle IP-Adresse (vom ISP) übermittelt wird. Der DNS-Name ist auf der Remote-Seite anstatt einer IP-Adresse konfiguriert. Bei der Einwahl der Remote-Seite am ISP erfolgt eine Namensauflösung (1), womit die Remote-Seite die gerade aktuelle IP-Adresse des zentralen Gateways erhält und den VPN-Tunnel dorthin aufbauen kann (2).

DynDNS-Konfiguration

Da das VPN Gateway vom ISP bei jeder erneuten Einwahl eine andere IP-Adresse erhält, kann die eindeutige Identifikation durch den Secure Client nicht mehr über eine fest konfigurierte IP-Adresse erfolgen. Auf Seiten des Clients wird nun statt der (festen) IP-Adresse fur den Tunnel-Endpunkt (siehe Client-Parameter, **Tunnel-Parameter**) der beim DynDNS Service Provider hinterlegte Name des Gateways eingetragen (DNS Name). Der DNS-Name wird in das Feld **Gateway (Tunnel-Endpunkt)** eingetragen.

Zur Abfrage der aktuellen IP-Adresse des Gateways findet nun vor dem Tunnelaufbau vom Client zum Gateway ein DNS Request statt, über den eine Auflösung des DNS-Namens erfolgt. Damit erhält der Client die jeweils aktuelle IP-Adresse des Gate-

ways, und der Tunnelaufbau zum Gateway kann erfolgen.

Beachten Sie bitte, dass eine Verbindung vom Client zum Gateway natürlich nur stattfinden kann, solange das Gateway eine Verbindung zum Internet unterhält (z. B. über DSL Flatrate). Beachten Sie außerdem, dass eine Nutzung von DynDNS nicht möglich ist, wenn der Client fur seinen Link die **Einwahl über Windows-DFÜ** nutzt.

Konfiguration am Server

Die Verbindung vom Gateway zum ISP wird als ausgehender Link konfiguriert. Der Wert fur den Parameter **DNS Name [Link-Profile]** (DynDNS-Hostname), der im Link-Profil unter **Routing** eingegeben wird, ist der Name des Gateways, der auch bei der Registrierung des Gateways beim DynDNS Service Provider und am Client in den Profil-Einstellungen unter **Tunnel-Parameter** eingegeben wurde (z. B. test.dyndns.org; siehe unten).

Unter **Lokales System / DynDNS** wird der Zugang zum Dynamic DNS Server konfiguriert, indem dessen Server-Name Hostname DynDNS Server (z. B. members.dyndns.org) und die Zugangsdaten, die bei der Registrierung als Benutzername (User ID) und Passwort verwendet wurden, eingegeben werden. Die Funktion **Benutze DynDNS** wird aktiv geschaltet.

Automatische Einrichtung für den DynDNS Client

Nach den eingegebenen Werten, inklusive der vom ISP zugewiesenen IP-Adresse, wird die Batch-Datei NCPDDNS.BAT automatisch wie folgt generiert und gestartet:

```
rem the input to this batchfile is as follows
rem ncpddns members.dyndns.org test test 172.16.15.52 test.dyndns.org
rem %1 = members.dyndns.org : This is the Name of the DDNS provider.
rem %2 = test               : This is the UserID to the DDNS provider.
rem %3 = test               : This is the Password to the DDNS provider.
rem %4 = 172.16.15.52       : This is the IPAddress to be assigned.
rem %5 = test.dyndns.org    : This is the Name of the IP address above.

rem The NCP DDNS client is called by default
rem 1. -h DynDNSServer
rem 2. -u UserID
rem 3. -w Password
rem 4. -i IPAddress
rem 5. -n DNSName
rem -p Port               Default HTTP:80, HTTPS:443
rem -x Proxy Ip Address   Default none
rem -y Proxy Port         Default 80
rem -s Use HTTPS

e:\win2000s\ncprtr\ncpdnscl -h %1 -u %2 -w %3 -i %4 -n %5 -s
```

Die Batch-Datei enthalt alle nötigen Parameter für den NCP-DynDNS Client. Wird ein anderer DynDNS Client verwendet, so kann die Batch-Datei abgeändert werden.

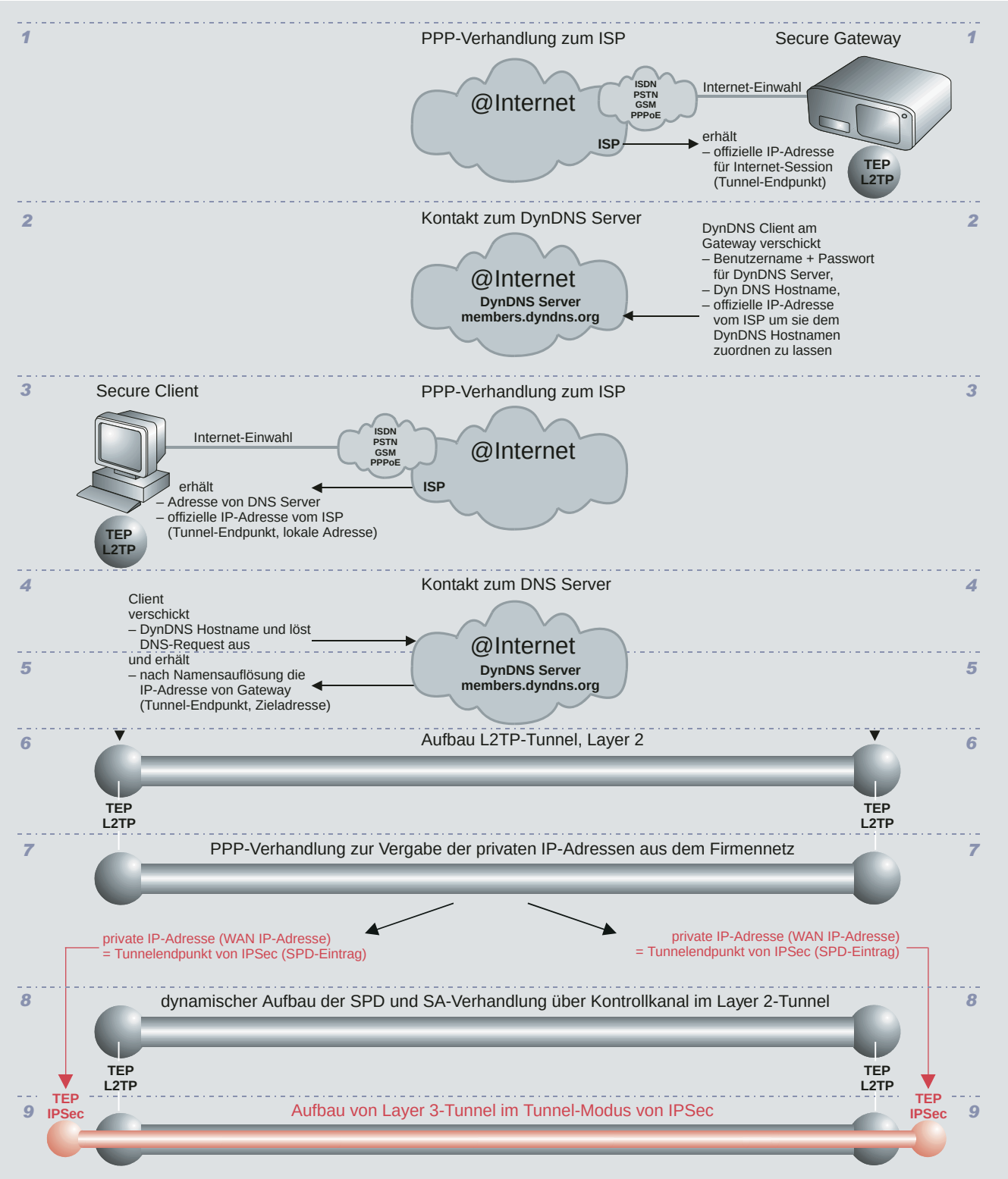


Abb. oben: Austausch der IP-Adressen unter Einsatz von DynDNS

Bereits vor der Einwahl des Clients ins Internet (Phase 3) muss sich das Ziel-Gateway im Internet eingewählt haben, um die Verhandlungen mit dem ISP und dem DynDNS Server abschließen zu können. Das heißt, nur wenn beide Teilnehmer online sind, kann auch ein erfolgreicher DNS-Request (Phase 4) mit Namensauflösung (Phase 5) stattfinden und die Verbindung vom Client zum Ziel-Gateway aufgebaut werden. Mit dem dazu etablierten L2TP-Tunnel (Phase 6) wird die sichere End-to-End-Kommunikation eingeleitet – im abgebildeten Fall mit IPSec over L2TP.

Managed VPNs

Eine Alternative zu selbstunterhaltenen VPNs bilden so genannte “Managed VPNs”, bei denen Einrichtung, Betrieb und Administration der kompletten VPN-Security durch einen Dienstleister erbracht wird. Diese Managed Security Service Provider (MSSP) oder Application Service Provider (ASP) bilden quasi eine Relaisstation zwischen den entfernten Anwendern und der Firmenzentrale. MSSPs verfügen immer über eine feste IP-Adresse und sind demzufolge standardmäßig erreichbar. Die Verbindungen werden sowohl bei Remote Access als auch bei Dial Outs mittels der Lockruf-Funktionalität durch den MSSP etabliert.

Versucht A eine Verbindung zu einem Partner B via Internet herzustellen, wählt er das Gateway den MSSP an. Dieses erkennt den Verbindungswunsch und aktiviert mittels Lockruf den Aufbau des VPN Tunnels von Partner B zum MSSP. Nunmehr kann Partner A und B über den weitergeleiteten Tunnel (Tunnel-Forwarding) kommunizieren.

Zur Konfiguration von Managed VPNs

Datenpakete von Mitgliedern einer Domain-Gruppe können vom zentralen VPN Gateway, das bei einem Application Service Provider betrieben wird, über Tunnel an das entfernte Ziel-Gateway weitergeleitet werden. Dazu wird für die entsprechende Domain-Gruppe im Parameterfeld **Allgemein** ein jeweils zu konfigurierendes Link-Profil für eine ausgehende Verbindung zugeordnet, über welches der Tunnel zum gewünschten Ziel-Gateway hergestellt (bzw. initiiert) wird.

Verfügt das Ziel-Gateway nicht über eine feste IP-Adresse, so erfolgt via ISDN vom ASP Gateway ein Lockruf an das Ziel-Gateway, womit ein Tunnelaufbau vom Ziel-Gateway zum ASP initiiert wird.

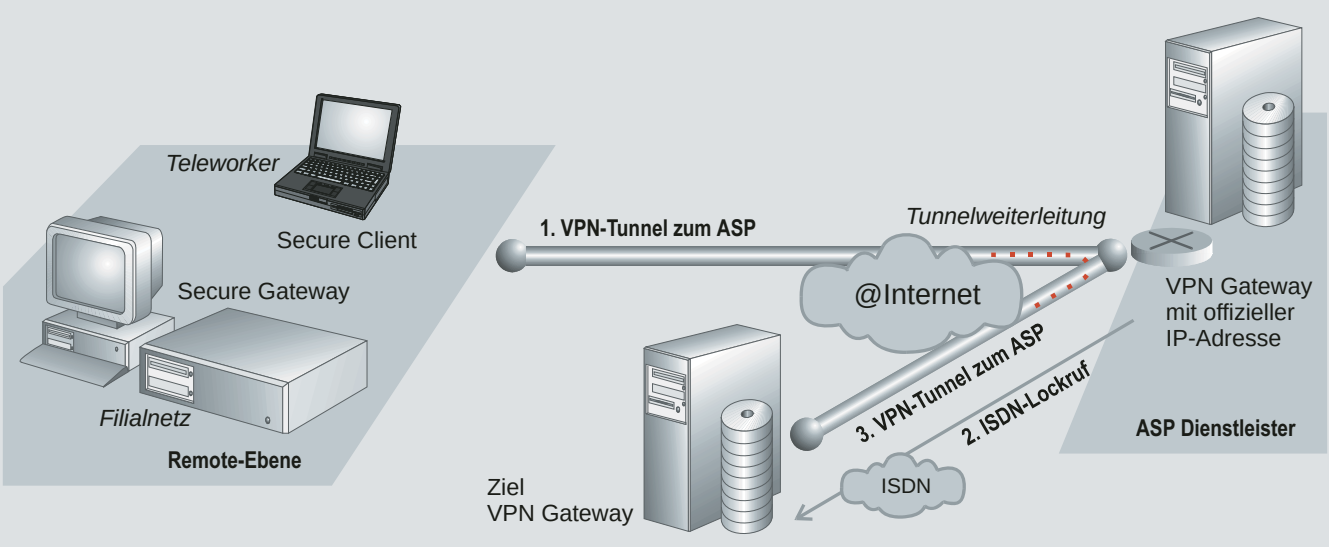


Abb.oben: Tunnelweiterleitung (Tunnel-Forwarding) über Service Provider (ASP, MSSP)
Ablauf des Verbindungsaufbaus: Ein Benutzer aus der Remote-Ebene wählt sich beim Dienstleister über Internet ein und baut einen VPN-Tunnel zu dessen offizieller IP-Adresse auf (1). Das VPN Gateway des Dienstleisters erkennt die Zugehörigkeit des Remote-Teilnehmers zu einer vorkonfigurierten Domain-Gruppe und setzt einen Lockruf via ISDN an das zu dieser Gruppe gehörige Ziel-Gateway ab (2). Vom Ziel-Gateway wird daraufhin ein Rückruf (Call-back) über das Internet an den Dienstleister ausgeführt und damit ein Tunnel zu dessen fester IP-Adresse aufgebaut (3). Damit ist eine Tunnelweiterleitung von der Remote-Ebene zum Ziel-Gateway hergestellt.

Szenarien in Internet-VPNs

Differenzierungskriterien für die Nutzung der Leistungsmerkmale:
– Anschlusslage der Kommunikationspartner: Wählleitung oder Festverbindung
– Kommunikationsrichtung : Remote Access (Dial In) und/oder Dial Out

Art / öffentl. Netze	Teleworker / Filiale	Firmenzentrale	Bemerkungen
Dial In	Einwahl in das Firmennetz		
Dial In	ISDN	ISDN / Flatrate	DynDNS
Dial In	ISDN	ADSL / Flatrate	DynDNS
Dial In	ADSL	ADSL / Flatrate	DynDNS
Dial In	Modem	ISDN / ADSL / Flatrate	DynDNS
Dial In	GSM, GPRS, WLAN	ISDN / ADSL / Flatrate	DynDNS
Dial In / Dial Out	Auswahl aus dem Firmennetz / Einwahl in das Firmennetz		
Dial In / Dial Out	ISDN	Festverbindung	Lockruf
Dial In / Dial Out	ADSL	Festverbindung	Lockruf
Dial In / Dial Out	ISDN	ISDN / Flatrate	DynDNS / Lockruf
Dial In / Dial Out	ISDN	ADSL / Flatrate	DynDNS / Lockruf
Dial In / Dial Out	Managed Security Services durch Dienstanbieter		

Dial-Backup-Funktion für kleine Gateways

Mit der Dial-Backup-Funktion wird beim Ausfall einer Verbindung (z.B.) über PPPoE automatisch eine Backup-Leitung über ISDN geschaltet.

Für gewöhnlich sind an einem kleinen Gateway zur Anbindung einer Filiale (Client Gateway) an das zentrale Firmennetz zwei Links konfiguriert. Ein Link ist der Tunnel-Link (TL), der andere ist der Provider-Link (PL).

Die Default Route wird über den TL gesetzt und eine Host Route zum Tunnel-Endpunkt (TEP) über den PL. Wird zentralseitig ein HA-Server eingesetzt, werden Host Routen zu den HA-Servern (HAEP1, HAEP2) über den PL gesetzt. Die Routing-Tabelle sieht dann so aus:

Zur Konfiguration

– Konfiguration eines Tunnel-Links;
– Konfiguration des PL1; der Name für PL1 ist frei wählbar, z.B. “Provider”;
– Konfiguration des PL2-Backup-Links; der Name für einen Backup-Link beinhaltet den Namen des Links für den der Backup-Link konfiguriert wird und bekommt zusätzlich “_backup” angehängt, z.B. “Provider_backup”.

```
Network Address    NetMask           Gateway
0.0.0.0            0.0.0.0           TL
TEP                255.255.255.255   PL
HAEP1              255.255.255.255   PL
HAEP2              255.255.255.255   PL
```

Um die Backup-Funktion nutzen zu können, wird ein zweiter Provider-Link, PL2, neben PL1 definiert. Solange die Verbindung über den ersten Link funktioniert, sieht die Routing-Tabelle wie folgt aus:

```
Network Address    NetMask           Gateway
0.0.0.0            0.0.0.0           TL
TEP                255.255.255.255   PL1
HAEP1              255.255.255.255   PL1
HAEP2              255.255.255.255   PL1
```

Ist es nicht möglich eine Verbindung über PL1 herzustellen oder bricht die Verbindung über PL1 ab, so wird der Backup-Mechanismus aktiviert. Der Backup-Mechanismus baut eine Verbindung über PL2 auf und ändert die Routen wie folgt ab:

```
Network Address    NetMask           Gateway
0.0.0.0            0.0.0.0           TL
TEP                255.255.255.255   PL2
HAEP1              255.255.255.255   PL2
HAEP2              255.255.255.255   PL2
```

Über PL1 wird nun alle 5 Sekunden versucht, eine Verbindung aufzubauen. Sobald dies gelingt, wird die Verbindung über PL2 abgebaut und die Routen zurück über PL1 gesetzt. Diese Art des Backup-Mechanismus hat keinen Einfluss auf den Tunnel, der beibehalten wird. Das zentrale VPN Gateway sieht lediglich verschiedene Tunnel-Endpunkte am Client Gateway.