NCP
SECURE COMMUNICATIONS

Sicherer mobiler Zugriff in Ihr Unternehmen – warum SSL VPN nicht das Allheilmittel ist

Ein Vergleich verschiedener VPN-Technologien

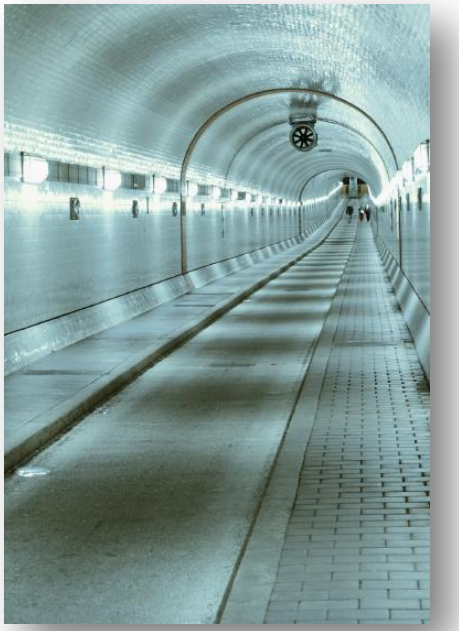
Überblick

- Überblick VPN Technologien
- SSL VPN Sicherheitsrisiken
- IPsec VPN Sicherheitsmerkmale
- Aufdeckung von SSL VPN Mythen
- Lösungen für sicheres SSL VPN
- Vergleich SSL VPN mit IPsec VPN
- Handlungsempfehlungen für den Mittelstand
- NCP – Partner / Referenzen

© NCP engineering GmbH

Überblick VPN Technologien

- Transparenter Tunnel
  - PPTP: Unter Anderem von Microsoft entwickelt. Stark verbreitet. Sicherheit hängt vom verwendeten Passwort ab.
    Gravierendes Sicherheitsproblem in MS-CHAPv2
  - L2TP: Layer 2-Tunnelung ohne Verschlüsselung
    - IPsec over L2TP
    - SSL over L2TP (L2Sec)
    - L2TP over IPsec: Bietet die Tunnelung auf Layer 2 Ebene (multiprotokollfähig) und wird in Kombination mit IPsec (Verschlüsselung) eingesetzt
  - Open VPN u.a.: Layer 2 oder 3-Tunnelung in Kombination mit SSL zur Verschlüsselung, Open Source



© NCP engineering GmbH

Überblick VPN Technologien

- IPsec: Layer 3-Tunnelung, Verschlüsselung und Authentisierung des IP-Protokolls; IPsec wurde für Site-to-Site Verbindungen entwickelt

  - Schwächen der Vergangenheit:
    - Pre-shared key für alle IPsec-Clients identisch (Main Mode)
    - Keine Adresszuweisung (IP-Adresse, DNS, WINS) innerhalb der IKE-Phasen spezifiziert => IKE config mode
    - Fehlende Authentifizierungsmethoden => XAUTH
    - Keine Unterstützung für IP-NAT => NAT-Traversal

  - Heute, herstellerübergreifender Standard:
    - IPsec mit IKEv2: Zusammenfassung aller relevanten IKE-Erweiterungen zu einem einheitlichen Standard und Straffung des Verbindungsaufbaus; Definition grundsätzlich zur Verfügung stehender Verschlüsselungs- und Hashwert-Algorithmen (z.B. kein DES); Abschaffung von Main Mode und Aggressive Mode; individueller Pre-shared key pro Anwender
      ▶ bessere Interoperabilität

© NCP engineering GmbH

Überblick VPN Technologien

- Applikations-basiert
  - SSL-basiert: Entwicklung 1994 von Netscape; Verschlüsselung auf Applikationsebene, zur sicheren Kommunikation für Webbrowser entwickelt; aktueller Stand: SSL 3.0 bzw. TLS 1.0 (seit 1999), TLS 1.1, 1.2 kaum verbreitet
  - SSL VPNs meist dreistufig:
    1. Zugriff mit Webbrowser auf Webapplikationen
       Umschreiben des HTML- und Javascript Quellcodes; Problem mit Flash und Java-Applets
       => Kompliziert und fehleranfällig
    2. Anbindung lokaler Applikationen über SSL VPN Tunnel
       Nicht für beliebige Applikationen einsetzbar, hoher Konfigurationsaufwand; Client-Rechner muss Grundvoraussetzungen erfüllen (Java, ActiveX, …)
    3. Transparenter Tunnel – SSL FAT Client
       Installation mit Administratorrechten notwendig; aus Performance-Gründen wird oft IPsec als Protokoll verwendet
    4. Diverse Erweiterungen … Sandbox-Technologie, Virenscanner, …

© NCP engineering GmbH

SSL VPN Sicherheitsrisiken

- Phishing
  - Gefahr grundsätzlich vorhanden, da Anmeldung über Webbrowser
  - Zugriff auf manipulierte DNS-Server, z.B. innerhalb Hotspots oder durch Viren („DNS-Changer“)
- Webbrowser als grundsätzliches Sicherheitsrisiko falls veraltete Version genutzt wird
  - TLS 1.0 oder älter ist anfällig für Man-in-the-Middle-Angriffe (BEAST: Browser Exploit Against SSL/TLS)
  - Gefahr sofern der Zertifikatsaussteller kompromittiert wurde (Comodo, DigiNotar, Gemnet, … in 2011)
- Fremde, unsichere Zugangshardware
  - Ausspähen von Zugangsdaten; fremde Hardware ist immer ein potenzielles Risiko! Gefahr durch Trojaner, Keylogger etc.
  - Zurücklassen sicherheitsrelevanter Daten
    - Webbrowser-Cache
    - Mailanhänge die lokal gespeichert wurden

© NCP engineering GmbH

IPsec VPN Sicherheitsmerkmale

- IKE zum sicheren Schlüsselaustausch beim Verbindungsaufbau
- ESP stellt die Authentisierung, Integrität und Vertraulichkeit (Verschlüsselung) innerhalb IPsec sicher. Es ist nicht anfällig für IP Spoofing, SYN Flooding und IP Hijacking
- Die Kombination aus IKE und ESP wird seit Jahrzehnten geprüft und für sicher befunden
- Zertifikate als Maßnahme gegen Man-in-the-Middle Angriffe
- Hardware-Zertifikate zur Authentisierung des Endgerätes

Vorteile:

- Zentrale Sicherheits-Richtlinien gelten auch für das Remote-Gerät
- Benutzer-Anmeldung an Active Directory möglich
- Jeglicher Benutzerzugriff auf das Internet erfolgt über das Firmennetz und die zentrale Firewall

© NCP engineering GmbH

Aufdeckung von SSL VPN Mythen

- „SSL VPN nutzt SSL-Protokoll“
  - Für den Fall des transparenten Netzwerkzugriffs weichen zahlreiche SSL VPN-Hersteller gern auf IPsec aus!

- „SSL VPN ist viel einfacher als IPsec VPN“
  - Nur im einfachsten Fall: Zugriff auf Web-Applikationen – Kompatibilität ist nicht immer gegeben
  - OTP-Lösungen zur sicheren Authentisierung auf fremder Hardware nötig
  - Komplizierte Zusatzlösung für den Zugriff auf fremder Hardware nötig, z.B. Sandbox

- „SSL VPN ist clientless“
  - Marketinglüge
    - … sobald transparenter Netzwerkzugriff im Spiel
    - … sobald Kapselung/Sandbox der Anwendersession im Spiel

© NCP engineering GmbH

Lösungen für sicheres SSL VPN

- Keine Verwendung unbekannter Hardware für sicherheitskritische Anwendungen/Daten
- Verwendung geprüfter Webbrowser
- Starke Authentisierung mittels Zertifikat, Hardware-Token oder OTP-Lösung

© NCP engineering GmbH

Vergleich SSL VPN mit IPsec VPN

- Der technische Aufwand, um den gleichen Leistungsumfang und hohen Sicherheitslevel mit SSL VPN (auf fremder Hardware) im Vergleich zu firmeneigener Hardware und IPsec VPN zu erreichen, ist immens und fehleranfällig.

- SSL VPN kann für bestimmte, nicht besonders sicherheitskritische Anwendungen zur Ergänzung eingesetzt werden.

- Der Remote-Arbeitsplatz bedarf meist eines transparenten Netzwerkzuganges in das Firmennetz
  - Firmeneigene Hardware mit Festplattenverschlüsselung, Firewall, Virenschutz und IPsec Client

© NCP engineering GmbH

Handlungsempfehlungen für den Mittelstand

Auswahlkriterien

Welchen Anwendungen, welches Sicherheitsbedürfnis habe ich?

- Hohe Verfügbarkeit und Skalierbarkeit der Gateways (SSL oder IPsec) gegeben?
- Wird starke Authentisierung unterstützt / mit angeboten?
- Technologie zur Überwindung von IPsec-Barrieren beim Internetzugang vorhanden?

Wie kommt der Anwender sicher in das Internet?

- Internet Connector und Firewall als Teil der Lösung?
- Umgebungssensitive Firewall, sichere Hotspot-Anmeldung, WLAN und 3G/4G-Unterstützung vorhanden?

Inbetriebnahme, Betrieb und Integration der Remote Access Lösung in die eigene Firmen-IT

- Zentrales Management von Clients und Gateways sowie einfacher Client-Rollout; Standardschnittstellen vorhanden?

© NCP engineering GmbH

NCP – Partner / Referenzen

Partner








Referenzen
















© NCP engineering GmbH

Vielen Dank für Ihre Aufmerksamkeit!

Referent	Dipl.-Ing. Swen Baumann, Product Manager
E-Mail	Swen.Baumann@ncp-e.com
Telefon	0911 / 99 68 0
Internet	www.ncp-e.com