-Technical Whitepaper -

Hochtechnologie für virtuell private Netzwerke

high technologie for virtual private network solutions

msm net ingenieurbüro meissner

Am Porstendorferweg 4
D 07570 Niederpöllnitz

Inhaltsverzeichnis

1.Vorwort

Das vorliegene „technical whitepaper“ wendet sich an technisch versierte Entscheidungsträger und an Systemadministratoren. Es stellt kurz und übersichtlich wichtige technische Kennziffern dar. Von diesen Übersichten ausgehend kann schnell eine Evaluierung zu möglichen Aufbauvarianten und Systenintegrationen erfolgen.
Wir bieten jedem interessierten Leser einen vertiefenden Dialog an. Im nachfolgenden Absatz können Sie sich über die enormen Skalierungsmöglichkeiten informieren.

2. Allgemeine technische Möglichkeiten

Mit den VPN Lösungen von „msm net ingenieurbüro meissner“ können beliebige VPN - Netzwerkstrukturen realisiert werden. Es können unter Nutzung des Internet klassische Stern- und Maschennetzwerke sowie Kombinationen realisiert werden. Die Umsetzung kann mit statischen und/oder dynamischen IP - Adressen in beliebiger Kombination erfolgen.

Von diesen Fakten ausgehend können also VPN im stationären als auch im mobilen Bereich realisiert werden. Alle beliebigen Kombinationen können durch vorhandene Administrationstools von einer zentralen Stelle administriert werden.

Für die technische Umsetzung gelten in der Regel sehr unterschiedliche Hardwareanforderungen. Die technischen Lösungen von „msm net ingenieurbüro meissner“ erschließen eine enorme Bandbreite. Für die Realisierung werden konsequent Standard- HW-Komponenten aus dem PC Bereich verwendet.

Je nach technischen Anforderungen können sich sehr einfache (ohne Festplatte, CD-ROM und FD) aber auch sehr anspruchsvolle Lösungen (Mehrprozessorsysteme ...) ergeben.

Durch unser modulares Konzept, ist auch die technische Anbindung an das Internet als Transportmedium sehr flexible gestaltbar.

Selbstverständlich ist jeder VPN Router mit einer Firewall ausgestattet.

3. Technische Daten der VPN Software

Kategorie	Details
Betriebssystem	Linux
Hardware Systemplattform	PC Komponenten, skalierbar nach projektbezogenen Anforderungen. Minimallösung: ohne Festplatte, CDROM und FD mit notwendigen Interfaces
Anzahl möglicher VPN Verbindungen	Begrenzt durch eingesetzte Hardware
Authentifizierungsverfahren	-MD5 - SHA - SHA2-256 - SAH2-512
Mögliche Verschlüsselungsverfahren	-3DES - AES 128 - AES 192 - AES 256 - Blowfish 128 - CAST 128 - Twofish - Serpent
DH Group Bitlänge	-768 -1024 - 2048 - 3072 - 4096 - 6144 - 8192

VPN Verbindungsverfahren	- IPSEC - PPTP - L2TP
Mögliche Tunnelverfahren	- GRE - IP over IP
IP Adressen	- IPv4 und IPv6 - statisch - dynamisch
Autom. Verbindungstrennung	konfigurierbar
Autom. Schlüsselaktualisierung	Konfigurierbar
Zertifikat Verwaltung	- CA ROOT Zertifikate - Authentifizierungs Zertifikate - CRL, Zertifikatssperrlisten, OSCP - Cryptosmartcard Anwendung
Authendifizierungsverfahren	- X509 Zertifikate (auch Cryptosmartcard) - PSK
Logdateien	-Konfigurierbar und per e-mail zustellbar -zentrale Logfileablage und automatisierte Auswertung
Systemredundanz	Redundanzsteuerung für die Nutzung des Übertragungsmeduim und der Partneradressierung (mittels OSPF)
Möglicher Datendurchsatz	Begrenzt durch verwendete Verfahren und durch Hardware

4. Basis RFC's der VPN Software

Overview RFCs
2401 Security Architecture for the Internet Protocol
2411 IP Security Document Roadmap

Basic protocols
2402 IP Authentication Header
2406 IP Encapsulating Security Payload (ESP)

Key management
2367 PF_KEY Key Management API, Version 2
2407 The Internet IP Security Domain of Interpretation for ISAKMP
2408 Internet Security Association and Key Management Protocol (ISAKMP)
2409 The Internet Key Exchange (IKE)
2412 The OAKLEY Key Determination Protocol
2528 Internet X.509 Public Key Infrastructure

Details of various things used
2085 HMAC-MD5 IP Authentication with Replay Prevention
2104 HMAC: Keyed-Hashing for Message Authentication
2202 Test Cases for HMAC-MD5 and HMAC-SHA-1
2207 RSVP Extensions for IPSEC Data Flows
2403 The Use of HMAC-MD5-96 within ESP and AH
2404 The Use of HMAC-SHA-1-96 within ESP and AH
2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
2410 The NULL Encryption Algorithm and Its Use With IPsec
2451 The ESP CBC-Mode Cipher Algorithms
2521 ICMP Security Failures Messages

Older RFCs which may be referenced
1321 The MD5 Message-Digest Algorithm
1828 IP Authentication using Keyed MD5
1829 The ESP DES-CBC Transform
1851 The ESP Triple DES Transform
1852 IP Authentication using Keyed SHA

Related RFCs
1750 Randomness Recommendations for Security
1918 Address Allocation for Private Internets
1984 IAB and IESG Statement on Cryptographic Technology and the Internet
2144 The CAST-128 Encryption Algorithm

5. Projektorientierte Problemlösungen

Für die Planung und Realisierung eines VPN müssen alle technischen Belange von bestehenden Netzwerken sowie deren technische Anbindung an das Internet und die mobile Kommunikation des Aussendienstes berücksichtigt werden.

Aus diesem Grund ist es von besonderer Bedeutung, das zuerst eine IST-Analyse über alle zu integrierenden Teile vorgenommen wird. Von dieser IST-Analyse ausgehend kann eine klare Zieldefinition mit allen umzusetzenden Massnahmen und Anforderungen erfolgen.

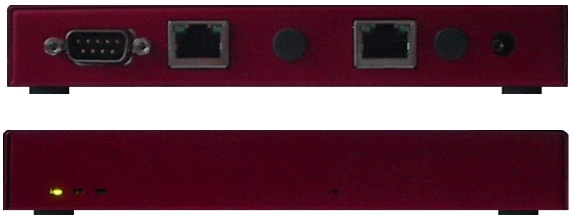
Für die Realisierung Ihrer VPN bieten wir Ihnen folgende Leistungen an:

- Beratungs-, Planungs- und Projektierungsleistungen zur Schaffung von VPN im internationalen und nationalen Umfeld
- Erstellung eines Betriebskonzeptes für VPN - Netzwerke
- Erstellung eines Mengengerüstes für die Bestimmung der Hardwareanforderungen
- Installation, Konfiguration, und Inbetriebnahme von Hard- und Software und Komponenten des VPN
- Überwachung und Auswertung von Protokolldateien
- regelmäßige Sicherheitsüberprüfungen
- Remote und Vorort Service und Wartung
- Einweisung und Schulung lokaler Administratoren

Durch die Nutzung unserer Produkte ist es möglich eine beliebige Anzahl von lokalen Netzwerken und Aussendienstmitarbeitern in einem VPN über das Internet zu vernetzen.

Für weiterführende Informationen stehen wir Ihnen jederzeit zur Verfügung.

6. VPN Router Varianten

Mini-VPN-Router	
	Die Mini-VPN-Router sind in einem sehr stabilen Aluminiumgehäuse mit einer Größe von (B x T x H) 15,5 x 15,5 x 2,5 cm realisiert. mögliche Interface: 2 x 10/100 Mbit Datendurchsatz: ca. 8Mbit bei 3DES-MD5-2048

Midi-VPN-Router	
	Midi-VPN-Router können als standalone oder als 19“ Variante (mit 22 oder 45 cm Tiefe) realisiert werden. mögliche Interface: 2x 10/100 Mbit, ADSL, ISDN Datendurchsatz: ca. 35 Mbit bei 3DES-MD5-2048

Maxi-VPN-Router	
	Maxi-VPN-Router werden als 19“ Variante (mit 45 cm Tiefe) und auf Nachfrage auf einer Serverplattform realisiert werden. mögliche Interface: 2x 10/100/1000 Mbit Datendurchsatz: über 200 Mbit bei 3DES-MD5-2048

Midi-HC-VPN-Router	
	Midi-HC-VPN-Router nutzen bei AES-Verschlüsselung und SHA-Authentifizierung die Padlockengine des VIA C7 Prozessors. mögliche Interface: 2x 10/100/1000 Mbit, TP, SC, ST Datendurchsatz: ca. 11 Mbyte bei AES128-SHA128-2048 in einer 100Mbit Netzwerkumgebung ca. 25 Mbyte bei AES128-SHA128-2048 in einer 1000 Mbit Netzwerkumgebung

Maxi-HC-VPN-Router	
	Maxi-HC-VPN-Router nutzen bei AES-Verschlüsselung und SHA-Authentifizierung die Padlockengine des VIA C7 Prozessors. mögliche Interface: 2x 10/100/1000 Mbit, TP, SC, ST Datendurchsatz: ca. 11 Mbyte bei AES128-SHA128-2048 in einer 100Mbit Netzwerkumgebung ca. 110 Mbyte bei AES128-SHA128-2048 in einer 1000 Mbit Netzwerkumgebung

Spezielle Schnittstellenanforderungen können auf Nachfrage realisiert werden.

Optionale Ausstattung	Mini-Router	Midi-Router	Maxi-Router
Cryptosmartcart Applikation	✔	✔	✔
Hardware Kryptografie (nur Geräte ohne VIA C7 Prozessor)	✔	✔	✔

Durch den Einsatz von Hardware-Kryptografie können sehr hohe Sicherheitsanforderungen bei gleichzeitiger Performancesteigerung realisiert werden.

7. Service- und Wartungsdienstleistungen

„msm net ingenieurbüro meissner“ bietet zu all seinen Produkten umfassende Service und Wartungsdienstleistungen an.
Diese Service- und Wartungsdienstleistungen sind gestaffelt nach Ruf- und garantierten Fehlerbeseitigungszeiten und werden im Rahmen von Wartungsverträgen angeboten.

8. Training, Schulung und Beratung

Für das effektive Erreichen Ihrer Unternehmensziele sind qualifizierte Mitarbeiter eine wesentliche Voraussetzung. Gern schulen wir Ihre Mitarbeiter zu folgenden Themenkomplexen:

- VPN Administration
- Außendienst- und Servicenetzwerke,
- e-mail - Anwendungen,
- System- und Netzwerkadministration,
- Internet und Informationsbeschaffung und
- Datensicherheit.

9. Kontaktdaten

Anschrift

msm net ingenieurbüro meissner

Am Porstendorferweg 4

D - 07570 Niederpöllnitz

Kommunikation

Telefon : +49 (0) 36607 60567

Fax : +49 (0) 36607 60577

Handy: +49 (0) 0170 24190 25

e-mail : service@msm-net.de

Internet : www.msm-net.de