

VPN-Technologien

**Alternativen und Bausteine einer erfolgreichen
Lösung**

von

Dipl.-Inform. Andreas Meder

Inhaltsverzeichnis**INHALTSVERZEICHNIS** **I**

1	<u>ERSTER ÜBERBLICK</u>	1-1
1.1	Begriffsklärung	1-1
1.2	VPN-Techniken	1-2
1.3	Layer-2-VPNs	1-3
1.4	MPLS	1-4
1.5	IP-basierte VPNs	1-8
1.6	Inhaltsüberblick	1-10
2	<u>GRUNDLAGEN VON VERSCHLÜSSELUNGSTECHNIKEN</u>	2-11
2.1	Motivation	2-12
2.2	Allgemeine Begriffe, Prinzipien und Beispiele	2-14
2.2.1	Definitionen und Begriffe	2-14
2.2.2	Historische Kryptosysteme	2-16
2.2.3	Qualität von Kryptosystemen	2-22
2.3	Symmetrische Kryptosysteme	2-28
2.3.1	Prinzip und grundlegende Mechanismen symmetrischer Kryptosysteme	2-28
2.3.2	DES	2-30
2.3.3	3DES	2-40
2.3.4	IDEA	2-41
2.3.5	RC4	2-42
2.3.6	AES	2-43
2.4	Asymmetrische Kryptosysteme	2-47
2.4.1	Funktionsprinzip asymmetrischer Kryptosysteme	2-47
2.4.2	Grundlagen von Public-Key-Systemen	2-49
2.4.3	Schlüssellängen und Beispiele asymmetrischer Kryptosysteme	2-50
2.5	Hybride Verfahren	2-52
2.6	Digitale Signaturen	2-54
2.6.1	Authentizität und Integrität von Nachrichten	2-54
2.6.2	Prinzip digitaler Unterschriften	2-54

4.2.2	Dial-In-Komponente	4-112
4.2.3	Tunnelkomponente	4-113
4.2.4	Authentifizierungskomponente	4-114
4.2.5	Verschlüsselungskomponente	4-116
4.2.6	Autorisierungskomponente	4-117
4.2.7	Die „optimale“ Lösung	4-118

5 AUTHENTIFIZIERUNG 5-120

5.1	Methoden und Werkzeuge	5-120
5.1.1	Identitätsmerkmale und deren Überprüfung	5-120
5.1.2	Authentifizierungswerkzeuge	5-122
5.1.3	Authentifizierungsprotokolle	5-123
5.2	RADIUS – die universelle Schnittstelle	5-125
5.3	Grenzen konventioneller Ansätze	5-127
5.4	One Time Passcodes	5-132
5.4.1	Einmal-Verschlüsselung	5-133
5.4.2	Challenge-Response-Token	5-135
5.4.3	Zeitabhängige Passcodes	5-139
5.4.4	Mehrfach-Hash	5-144
5.4.5	Anforderungen an die verwendeten Schlüssel	5-146
5.4.6	Grenzen und Einschränkungen	5-147
5.5	Security Server – Auswahl und Einsatz	5-150
5.6	Benutzerauthentifizierung in IPSec-basierten VPNs	5-152

6 VPN-PRODUKTE – DER MARKT 6-154

6.1	Technische Lösungsansätze	6-155
6.2	Marktbeispiele	6-159
6.3	Virtual Private Network Consortium	6-163
6.3.1	Ziele des VPNC	6-163
6.3.2	Mitglieder-Übersicht	6-164
6.3.3	Interoperabilität und Konformität	6-165
6.4	Der Weg zur „maßgeschneiderten“ Lösung	6-169

7	<u>DESIGN UND ORGANISATION VON VPNS</u>	7-170
7.1	Einsatzaspekte	7-170
7.1.1	Identitätsverifikation	7-170
7.1.2	Performance	7-172
7.1.3	RAS-Integration	7-172
7.1.4	Sicherheit gegenüber dem Trägernetz	7-173
7.1.5	Rahmenbedingungen	7-176
7.2	Architekturen	7-178
7.2.1	Integrierter VPN-Anschluss	7-179
7.2.2	Separater VPN-Anschluss	7-182
7.2.3	Präferenzen	7-185
7.3	Ausfallsicherheit	7-186
7.3.1	Der Local Loop als Ansatzpunkt	7-186
7.3.2	Redundanzmaßnahmen	7-188
7.3.3	Redundanz-Ebene der Gesamtlösung	7-193
7.4	Quality of Service	7-201
7.5	VPNs auf Firewallbasis	7-202
7.6	Sicherer Betrieb von VPNs	7-203
7.6.1	Betrieb reiner VPN-Gateways	7-203
7.6.2	Betrieb komplexer Firewall/VPN-Lösungen	7-203
7.7	Schlüsselmanagement	7-205
7.7.1	Wozu braucht man eine Public Key Infrastructure?	7-206
7.7.2	Zertifikate	7-206
7.7.3	PKI-Komponenten	7-207
7.7.4	CA-Modelle	7-208
7.7.5	Zertifizierungsstellen	7-210
8	<u>SICHERE VPNS MIT WINDOWS-BORDMITTELN?</u>	8-212
8.1	Bestandteile einer Windows 2000 VPN-Lösung	8-212
8.1.1	Routing and Remote Access Service (RRAS)	8-212
8.1.2	Internet Authentication Service (IAS)	8-219
8.1.3	Public Key Infrastructure (PKI)	8-221
8.1.4	Smart-Card-Anmeldung	8-229
8.2	Positionierung des VPN-Servers	8-236

8.3	Interoperabilität mit Produkten von Drittherstellern	8-238
8.4	Fazit	8-240
9	<u>SSL-VPNS – KONKURRENT ODER PARTNER FÜR IPSEC?</u>	9-241
9.1	SSL und VPNs	9-242
9.1.1	Die Idee	9-243
9.1.2	HTTPS und SSL	9-243
9.1.3	Funktionsweise gängiger SSL-VPN-Lösungen	9-244
9.1.4	OpenVPN als Alternativansatz	9-249
9.1.5	Problemfelder bei SSL-VPNs	9-250
9.1.6	Der Markt	9-252
9.1.7	Vergleich und Fazit	9-253
10	<u>FALLSTUDIE – EIN PROJEKTBEISPIEL</u>	10-255
10.1	Rahmenbedingungen und Projektanforderungen	10-255
10.2	Technische Realisierung	10-256
10.3	Organisation des Betriebs	10-262
10.3.1	Inhalt	10-262
10.3.2	Rahmenbedingungen	10-262
10.3.3	Personal	10-263
10.3.4	Betriebsaufgaben	10-263
10.3.5	Dienstregelungen	10-264
10.4	Ausblick auf die Fortentwicklung des Netzes	10-265
11	<u>FAZIT</u>	11-267
ANHANG		A-269
A	Anbieter von Authentifizierungswerkzeugen (Auszug)	A-269
B	Mathematische Grundlagen ausgewählter asymmetrischer Kryptosysteme	B-270
B.1	RSA	B-270
B.2	Diffie-Hellman	B-271
C	Auflösungen aus Kapitel 2.4.2	C-272
D	Konfigurationsbeispiele	D-273
D.1	Checkpoint VPN-1	D-273

D.2 Enterasys XSR

D-285

ABBILDUNGSVERZEICHNIS **288**

TABELLENVERZEICHNIS **292**

INDEX **293**

ABKÜRZUNGEN **299**