VPN Basis-Interoperabilität

Secorvo White Paper

Version 1.0
Stand 29. Januar 2003

Stefan Gora, Hans-Joachim Knobloch, Claus Stark, Christian Knoblauch

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455

E-Mail info@secorvo.de
Internet http://www.secorvo.de

Inhaltsübersicht

Abkürzungen

3DES	Triple-DES
AH	Authentication Header
DES	Data Encryption Standard
DNS	Domain Name Service
ESP	Encapsulating Security Payload
HMAC	Hashed Message Authentication Code
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
IPSRA	IP Security Remote Access
ISO/OSI	International Standardization Organization – Open Systems Interconnect
ITSEC	Information Technology Security Evaluation Criteria
JFK	Just fast keying
PKI	Public Key Infrastructure
LAN	Local Area Network
L2TP	Layer2 Tunneling Protocol
MBit	Megabit
MS	Microsoft
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
POP3	Post Office Protocol
PPTP	Point to Point Tunneling Protocol
QoS	Quality of Service
RFC	Request for Comments („Internet Standard“)
SA	Security Association
SHA-1	Secure Hash Algorithm (NIST Standard)
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

1 Zusammenfassung

Virtuelle Private Netzwerke (VPN) sind heute die Standard-Methode, um Geschäftsstellen, Niederlassungen, Heimarbeitsplätze und Außendienstmitarbeiter sicher, d.h. über verschlüsselte und integritätsgesicherte Verbindungen in die Netzwerkinfrastruktur des Unternehmens zu integrieren.

Wenn ein Unternehmen seine IT-Infrastruktur für seine Kunden und Geschäftspartner öffnen möchte oder beispielsweise im Rahmen von Firmenübernahmen oder der Umorganisation des Unternehmens unterschiedliche IT-Netzwerke miteinander gekoppelt werden müssen, spielt daher das Thema VPN-Interoperabilität oft eine wichtige Rolle. Die drängendste Frage richtet sich hierbei oft auf die eingesetzten Produkte: *„Kann zwischen den VPN-Gateways der Hersteller X und Y ein sicherer Tunnel betrieben werden?“* Secorvo hat diese Frage für verbreitete VPN-Gateways im eigenen Testlabor exemplarisch untersucht. Die Ergebnisse der ersten Untersuchung sind in diesem Whitepaper zusammengefasst.

Begonnen wurden die Untersuchungen zur VPN-Interoperabilität mit einer grundlegenden Testreihe zur Basis-Interoperabilität von VPN-Gateways. Dieser Begriff beschreibt dabei die Interoperabilität von VPN-Gateways auf der kleinstmöglichen gemeinsamen Basis. Hier sollte zwischen beliebigen VPN-Gateways *stets* eine sichere Verbindung herstellbar sein. Wie genau diese kleinste gemeinsame Basis aussieht, und ob in der Praxis der sichere Verbindungsaufbau zwischen verschiedenen Produkten auch tatsächlich möglich ist, wurde exemplarisch an acht verschiedenen VPN-Gateways untersucht.

Die VPN-Hardware-Lösungen von sechs Herstellern – Astaro F1, Cisco PIX 515, Cisco VPN 3015 Concentrator, Genua GenuGate, Nokia IP 650, Nortel Contivity Extranet 100, Nortel Contivity Extranet 600 und Watchguard Firebox 1000 – wurden für den gemischten Einsatz bei LAN-to-LAN-Kopplungen paarweise getestet. Der Schwerpunkt lag auf der Untersuchung, ob oder mit welchen Einschränkungen ein VPN-Betrieb möglich ist. Hierzu wurden einige grundlegende Testszenarien entworfen. In diesem Whitepaper werden die Testvorgaben, der Ablauf und die Ergebnisse ausführlich vorgestellt und diskutiert.

Die Tests wurden von Herrn Christian Knoblauch im Rahmen seiner Diplomarbeit zum Thema „VPN-Interoperabilität“ in Zusammenarbeit mit den Autoren bei der Secorvo Security Consulting GmbH im Security Testlabor durchgeführt.

Unser Dank gilt den Herstellern und Partnerfirmen, die uns hierfür ihre VPN-Geräte zur Verfügung gestellt und der Veröffentlichung der Testergebnisse zugestimmt haben. Eine vollständige Liste der Hersteller findet sich in Anhang A.

Eine kompakte Darstellung des VPN-Tests und seiner Ergebnisse wurde in der Zeitschrift iX, Ausgabe 10/2002 publiziert [GoKnSt02], die ausführlichere Diskussion mit Darstellung der Grundlagen ist in der Diplomarbeit von Christian Knoblauch enthalten [Kno02].

2 Motivation

VPN-Lösungen haben sich bereits seit Jahren in der betrieblichen IT-Kommunikation fest etabliert, um z.B. dezentrale Firmenniederlassungen und Außendienst-Mitarbeiter kostengünstig und sicher an die Netzwerkinfrastruktur der Zentrale anzubinden. Hierbei treten i.d.R. keine größeren Interoperabilitätsprobleme auf, wenn auf VPN-Geräte eines einzigen Herstellers zurückgegriffen wird.

Mittlerweile kann man jedoch nicht mehr in allen Fällen von einem solchen homogenen Szenario ausgehen, denn neben den eigenen Mitarbeitern und Filialen wird zunehmend auch Kunden, Geschäftspartnern oder auch Behörden der direkte Zugriff auf ausgewählte Firmenressourcen im Intranet zur Verfügung gestellt: Zulieferer wollen sich direkt in die „Supply Chain“ der Produktion einklinken, Behörden wollen direkt auf die Forschungsergebnisse der Produktzulassung zugreifen, und mit zunehmender Zahl der Abteilungs- und Firmenfusionen werden zuvor fremde Netzwerke zusammengeschmolzen. In solchen Szenarien kann nicht mehr vorausgesetzt werden, dass die eingesetzten VPN-Produkte identisch sind und geschützte Verbindungen zwischen ihnen problemfrei aufgebaut werden können. Hier spielt die Interoperabilität der VPN-Geräte eine zentrale Rolle: Wie standardkonform wurden VPN-Standards wie IPsec in den Produkten tatsächlich umgesetzt, und was ist der (kleinste) gemeinsame Nenner, um einen sicheren Verbindungsaufbau zwischen ihnen zu ermöglichen?

Ein typisches Szenario der Nutzung von VPNs in der betrieblichen IT-Kommunikation aus der täglichen Praxis wird in Abbildung 1 skizziert: Die Firmenzentrale stellt Ressourcen für ihre Mitarbeiter und Filialen, aber auch für Kunden und Geschäftspartner bereit. Die sichere Anbindung erfolgt auf verschiedene Weise, beispielsweise über Gateway-to-Gateway- und Remote-Access-VPNs.

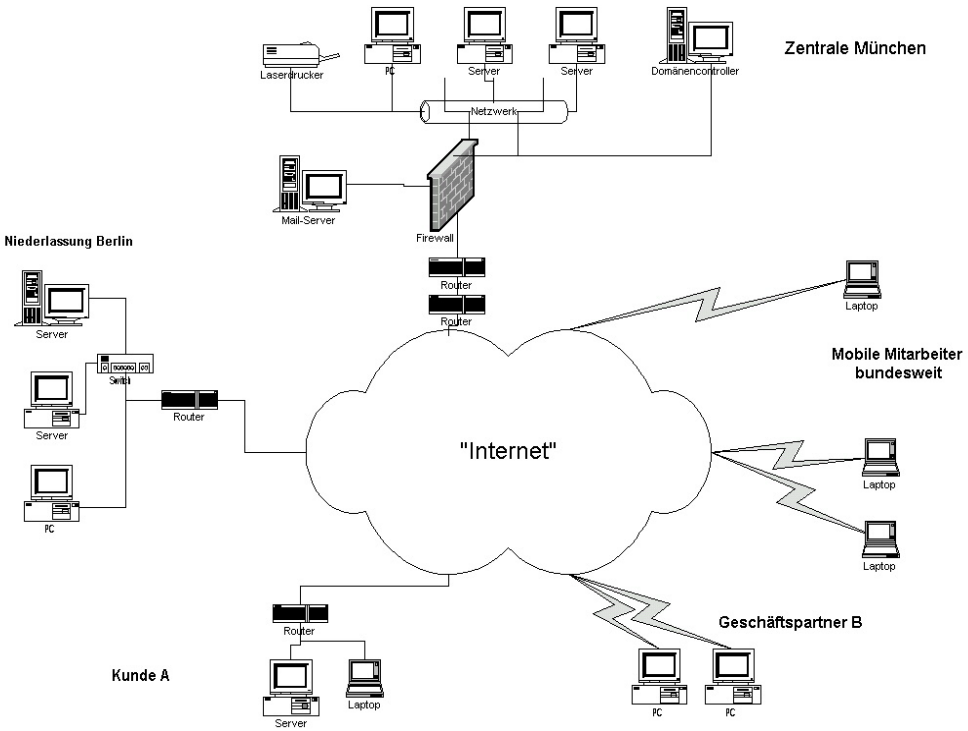

Abbildung 1: Ein typisches Szenario für die Internetnutzung eines Unternehmens

Der Schwerpunkt dieses Whitepapers liegt auf den *„Gateway-to-Gateway"-Verbindungen*: Dem Aufbau sicherer Verbindungen zwischen zwei voneinander getrennten LANs über öffentliche Kommunikationsnetze wie das Internet mittels VPN-Gateways. Dabei soll nicht ein spezifisches Produkt untersucht werden, welches in allen Teilnetzen gleichermaßen verwendet wird; für diesen Fall wird die volle Funktionsfähigkeit, Sicherheit und Interoperabilität der Geräte des VPNs à priori unterstellt.

Der Fokus dieser Untersuchung liegt auf der Frage, ob sichere IPsec-Verbindungen auch zwischen VPN-Gateways verschiedener Hersteller möglich sind, oder ob es Einschränkungen zu beachten gilt. Kann vorhandene Hardware verschiedener Hersteller weiterverwendet werden, spart dies die Kosten für Neubeschaffungen. Mittelbar können Folgekosten wie die Mitarbeiterschulung und zusätzliche Administrationskosten eingespart werden. Es kann sich also lohnen, sich mit dem Betrieb eines heterogenen VPN-Netzwerks auseinander zu setzen.

3 Grundlagen

Dieses Grundlagenkapitel beschreibt knapp und bündig, was in diesem Whitepaper unter dem Begriff „VPN" verstanden wird und auf welche Standards und Parameter bei der Auswahl der Geräte und Konfigurationsoptionen zurückgegriffen wird. Technisches Basiswissen wird nicht vermittelt – hierzu sei auf die in Kapitel 7 angegebene Referenzliteratur verwiesen.

3.1 Anforderungen an ein Virtual Private Network

Ein virtuelles privates Netzwerk (VPN) ist nach Definition des VPN Konsortiums [VPNC02] – eines Interessenverbands der VPN-Industrie – ein „privates Netzwerk, das öffentliche Telekommunikationsinfrastruktur nutzt und dabei die *Privatsphäre* der geführten IT-Kommunikation der Teilnehmer wahrt". Diese Vertraulichkeits- und Integritätsanforderung kann von Dritten wie z.B. den Netzprovidern garantiert werden („trusted VPN"), oder aber durch die Teilnehmer selbst mit Hilfe kryptographischer Protokolle sichergestellt werden („secure VPN"). Neben diesen genannten unterscheidet das VPN Konsortium noch zwei weitere VPN-Typen („hybrid VPN" und „provider-provisioned VPN").

Unter VPN wird im Weiteren ein „secure VPN" verstanden, das von den Teilnehmern selbst betrieben wird. Ein VPN muss dabei folgende Sicherheitsdienste für die Teilnehmer erfüllen:

- Teilnehmer-Authentisierung: Jeder Teilnehmer (Gateway oder Client) muss sich im Netz eindeutig identifizieren und sicher authentisieren, da sonst ein gezielter Verbindungsaufbau zwischen VPN-Teilnehmern unmöglich ist.
- Sicherstellung der Vertraulichkeit der IT-Kommunikation: Die IT-Kommunikation, die über öffentliche Telekommunikationseinrichtungen geführt wird, kann vertrauliche Informationen enthalten. In diesem Falle muss das VPN durch Verschlüsselung des Datenverkehrs eine unberechtigte Kenntnisnahme der Daten durch Dritte verhindern und so die Vertraulichkeit sicherstellen.
- Sicherstellung der Integrität der IT-Kommunikation: Die IT-Kommunikation, die über öffentliche Telekommunikationseinrichtungen geführt wird, kann sensible Informationen enthalten, die nicht verändert werden dürfen. In diesem Falle muss das VPN durch integritätssichernde Verfahren des Datenverkehrs die Datenintegrität so sicherstellen, dass nicht autorisierte Veränderungen erkannt werden. Eng verknüpft mit der Integritätssicherung ist die Datenauthentizität, die üblicherweise mit denselben

Verfahren erreicht wird. Dabei wird sichergestellt, dass die empfangenen Daten auch tatsächlich vom angegebenen Absender stammen.

Die Sicherstellung des *QoS* eines VPNs („Quality of Service“, u.a. Bandbreite und Netzverfügbarkeit) ist ebenfalls ein wichtiges Thema, spielt aber im Rahmen der folgenden Betrachtungen keine Rolle.

3.2 Unterschiedliche VPN-Typen

VPNs lassen sich weiter klassifizieren nach dem Typus der abzusichernden Verbindung. Hier lassen sich grundsätzlich folgende drei Typen unterscheiden (siehe Abbildung 2):

- Host-to-Host-VPN: Eine gesicherte Verbindung zwischen zwei beliebigen End-Systemen („Ende-zu-Ende-Sicherheit“). Dies können beispielsweise Peer-Verbindungen zwischen verschiedenen Servern sein.
- Host-to-Gateway-VPN: Eine gesicherte Verbindung zwischen einem End-System (z.B. einem PC eines Außendienstmitarbeiters) und einem VPN-Gateway. Dieser Typ tritt i.d.R. bei Remote Access-Szenarien auf.
- Gateway-to-Gateway-VPN: Eine gesicherte Verbindung zwischen zwei VPN-Gateways. Dieser Typ wird verwendet, um zwei oder mehrere Teilnetze miteinander zu verbinden. Über die sichere Verbindung zwischen den Gateways können die End-Systeme der verbundenen Teilnetze miteinander kommunizieren.

Der Fokus dieser Untersuchung liegt auf dem Gateway-to-Gateway-VPN.

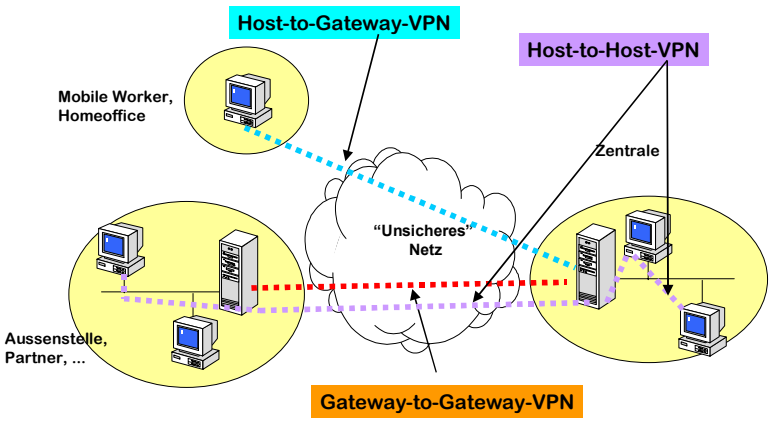

Abbildung 2: Verschiedene VPN-Typen

3.3 Der VPN-Standard IPsec

IPsec (*Internet Protocol Security*) ist ein Standard für Netzwerk-Sicherheitsdienste auf ISO/OSI-Schicht 3, der „IP-Schicht“ von TCP/IP.

IPsec auf Basis des aktuellen RFCs 2401 und darauf aufbauender Standards [KeAt98a/b/c] hat sich bei den Herstellern von VPN-Gateways durchgesetzt und kann als „der“ VPN-Standard schlechthin angesehen werden. Eng verbunden mit IPsec ist IKE (*Internet Key Exchange*), der Standard für die Teilnehmerauthentisierung und den Schlüsselaustausch [HaCa98, Maug98]. IKE und IPsec kommen i.d.R. gemeinsam zum Einsatz, obwohl beide Standards offen für andere Kombinationen sind. Beispielsweise kann IKE grundsätzlich auch für den Schlüsselaustausch zwischen Anwendungen verwendet werden und IPsec prinzipiell

auch auf andere Schlüsselaustauschverfahren zurückgreifen. Im Folgenden wird die verbreitete Kombination IPsec/IKE vorausgesetzt.

IPsec/IKE stellt im wesentlichen Sicherheitsdienste zur Geräte-Authensierung (IKE) und zur Sicherstellung der Vertraulichkeit (IPsec-Protokoll ESP), der Integrität und der Authentizität (IPsec-Protokolle ESP und AH) der übertragenen Daten zur Verfügung. Weitere Sicherheitsfunktionen sind integriert (z.B. zur Abwehr von Denial-of-Service-Angriffen), werden aber im Rahmen dieses Whitepapers nicht explizit betrachtet.

Die Standardisierung von IPsec und IKE ist – ungeachtet der starken Verbreitung – noch lange nicht abgeschlossen. Die vorhandenen Standards haben Schwächen, die ihre Einsatzmöglichkeiten beschränken (siehe u.a. die kritischen Kommentare in [FeSc00, Perl00, Shie00], bzw. die Arbeiten der IETF-Arbeitsgruppe „IP Security Remote Access“ IPSRA). Ihre Fortentwicklung ist in vieler Hinsicht – u.a. geringere Komplexität des Schlüsselmanagements, NAT-Kompatibilität [Abo02] und Realisierungsmöglichkeiten von Remote Access – sehr wünschenswert. Mit den Internet Drafts zu IKEv2 [Har02], JFK („just fast keying“, [Aie02]) und zu Son-of-IKE [Mad02] wurde bereits heftig über einen möglichen IKE-Nachfolger diskutiert. Der Ausgang dieser Diskussionsprozesse ist zur Zeit ungewiss.

Die vorliegende Untersuchung basiert auf den aktuellen IKE-Standard (RFC 2409) und dem IPsec-Standard ESP (RFC 2406).

3.4 Authentisierung der VPN-Endsysteme

In einem VPN müssen die einzelnen Endsysteme – VPN-Hosts und -Gateways – sicher authentisiert werden, um den Aufbau nicht-zulässiger Verbindungen zu erkennen und abzuwehren. IKE als Schlüsselaustauschverfahren für IPsec unterstützt mehrere Verfahren zur Authentisierung der Endsysteme in einem VPN:

- Pre-Shared-Key-Verfahren: Das einfache und deswegen wohl beliebte und sehr weit verbreitete Authentisierungsverfahren ist die Vorab-Vereinbarung eines gemeinsamen Geheimnisses (des „Pre-Shared-Keys“) zwischen je zwei beteiligten Endsystemen, mit denen sich die Geräte gegenseitig authentisieren können. Dies ist im Regelfall ein gemeinsames Passwort (mit all den Sicherheitsproblemen beim Umgang mit Passworten und ihrer sicheren Verteilung). Für einfache VPN-Szenarien – wie sie in diesem Whitepaper unterstellt werden – ist dieser Ansatz für die sichere Endsystemauthentisierung ausreichend. Für größere Zahlen beteiligter Endsysteme hingegen steigt die Anzahl möglicher Kommunikationspaare jedoch schnell erheblich[1], so dass die Vereinbarung von Pre-Shared-Keys unpraktikabel wird[2].
- Public-Key-basierte Verfahren: Auf einem etwas komplexeren Ansatz basieren sog. Public-Key-Verfahren, die ebenfalls von IKE unterstützt werden. Das Endsystem authentisiert sich durch die Vorlage eines (für vertrauenswürdig zu erachtenden) öffentlichen Schlüssels bzw. Zertifikats und den Nachweis des Besitzes des dazugehörigen privaten Schlüssels. Diese Verfahren erlauben ein sehr hohes Sicherheitsniveau hinsichtlich der Teilnehmerauthentisierung, sind aber relativ komplex,

---

1 Bei einem voll vermaschten Netzwerk wächst die Zahl der zu verwaltenden Keys quadratisch mit der Zahl der Endsysteme: bei fünf Geräten sind es zehn Keys, bei zehn Geräten 45, bei 100 Geräten schon 4.950.

2 Von der Verwendung eines einzigen (oder weniger) Pre-Shared-Keys im gesamten VPN wird aus Sicherheitsgründen dringend abgeraten.

da i.d.R. eine PKI („Public Key Infrastruktur“) erforderlich ist. Dieser Ansatz ist dann attraktiv, wenn man mit sehr vielen und wechselnden Kommunikationspartnern zu tun hat und komplexere VPN-Szenarien realisiert[3].

- **Kerberos:** Ein Sonderstellung nimmt die VPN-Authentisierung mittels Kerberos ein, da dieses Verfahren im aktuellen IKE-Standard nicht vorgesehen ist, es aber in den aktuellen Microsoft-Betriebssystemen (Windows 2000 und Windows XP) als default Option vorgesehen ist. Für reine Windows-Domänen ohne VPN-Lösungen anderer Hersteller ist dieser Ansatz sicherlich interessant, soll in dieser Untersuchung aber nicht verfolgt werden.

Die vorliegende Untersuchung beschränkt sich auf den weitverbreiteten Pre-Shared-Key-Ansatz. Dies ist akzeptabel, wenn nur wenige statische VPN-Verbindungen zu betreiben sind, was speziell für Gateway-to-Gateway-VPNs typisch ist.

3.5 VPN-Interoperabilität

Interoperabilität im Kontext von Virtual Private Networks heißt, dass sichere VPN-Verbindungen zwischen beliebigen VPN-Gateways unterschiedlicher Hersteller aufgebaut und betrieben werden können. Was aber bedeutet VPN-Interoperabilität konkret? Was sind geeignete Bewertungskriterien um festzustellen, ob zwei VPN-Gateways zueinander interoperabel sind oder nicht?

Interoperabilität setzt Standardkonformität voraus. Das heißt, dass die Vorgaben, die in den relevanten Standards gemacht werden, im Produkt korrekt umgesetzt sind. Alle obligatorischen Funktionen und Parameter müssen, optionale dürfen implementiert werden. In der Praxis ist dies aus unterschiedlichen Gründen jedoch nicht immer gegeben. Beispielsweise sieht der IPsec-Standard obligatorisch „DES“ als Verschlüsselungsverfahren für ESP vor; in der aktuellen IPsec-Implementierung von Linux (FreeS/WAN) aber wird DES aus Sicherheitsgründen (DES gilt inzwischen als schwaches Verschlüsselungsverfahren) explizit nicht mehr realisiert. Darüber hinaus sind Standards bisweilen unscharf definiert, so dass die vorhandenen Freiheitsgrade bei der Implementierung der Standards von den Produktherstellern sehr unterschiedlich ausgelegt werden können. Das verursacht gelegentlich große Interoperabilitätsprobleme.

Standardkonformität alleine reicht aber nicht aus, um volle Interoperabilität zu gewährleisten. Die IPsec-Standards besitzen sehr viele Optionen, die i.d.R. in den Produkten nicht immer alle implementiert werden (und auch nicht implementiert werden müssen). Realisieren zwei VPN-Gateways beispielsweise disjunkte IPsec-konforme Optionen, ist ein Verbindungsaufbau zwischen ihnen unter Verwendung dieser Optionen nicht möglich.

Volle Interoperabilität ist praktisch nicht erreichbar, denn das hieße, dass alle Variationen von VPN-Verbindungen zwischen zwei beliebigen VPN-Gateways aufgebaut werden können, mit beliebigen Protokollen und Parametern. Allein aufgrund der in der Praxis häufig sehr unterschiedlichen IPsec- und IKE-Implementierungen ist eine volle Interoperabilität zwischen zwei beliebigen VPN-Gateways sehr unwahrscheinlich.

Was aber auf jeden Fall erwartet werden darf, ist *Basis-Interoperabilität*: eine gesicherte IT-Kommunikation unter möglichst geringen Voraussetzungen und Anforderungen an die einzelnen VPN-Gateways. Basis-Interoperabilität in diesem Sinne wird in diesem Whitepaper

---

3 Bei einer geringeren Anzahl an Endsystemen können auch Zertifikate eines kommerziellen Anbieters („Trust Center“) genutzt werden.

praktisch untersucht. Dabei wird sie möglicherweise auf Kosten des erreichbaren Sicherheitsniveaus erkauft werden. Ob dieses Niveau ausreichend ist oder nicht, muss stets von Fall zu Fall individuell bewertet werden.

4 Der Test-Aufbau

Der für die Tests verwendete Aufbau sollte zum einen möglichst einfach sein, sich andererseits aber an realistischen Randbedingungen orientieren.

4.1 Test-Szenario

Auf Basis des IPsec-Protokolls sollten paarweise möglichst viele Kombinationen verschiedener VPN-Gateways hinsichtlich des Aufbaus einer sicheren VPN-Verbindung untersucht werden. Die Fragestellung, wie sich ein VPN mittels Produkten von drei oder mehr verschiedenen Herstellern aufbauen ließe, war nicht Gegenstand der Untersuchung.

Es standen insgesamt acht Produkte für den Test zur Verfügung, d.h. es konnten maximal 28 (n*(n-1) / 2 Möglichkeiten) unterschiedliche Produktkombinationen getestet werden. Tests zwischen identischen Produkten wurden nicht durchgeführt, da Interoperabilität hier unterstellt werden kann.

Aufgrund der eingeschränkten Verfügbarkeit einzelner Testgeräte konnten nicht alle 28 Produktkombinationen untersucht werden. Von den acht zur Verfügung gestellten Geräten wurden sechs intensiv getestet; zwei Geräte standen nur für einen kurzen Zeitraum zeitgleich mit den weiteren Geräten zur Verfügung und konnten daher nur eingeschränkt berücksichtigt werden.

Für jede untersuchte Produktkombination wurden die beiden folgenden Einzeltests durchgeführt:

- Verbindungs-Test: Ist ein gesicherter Verbindungsaufbau und -betrieb zwischen den beiden VPN-Gateways möglich? Für folgende Anwendungen wurden untersucht, ob eine VPN-Verbindung aufgebaut und gehalten werden konnte:
  - Ping
  - Webserver-Zugriff
  - E-Mail-Versand zum Mailserver
  - Windows 2000 Domänenanmeldung
  - Dateifreigabe (Filesharing)
- Ausfall-Test: Wie reagieren die beiden VPN-Geräte bei Störungen der gesicherten Verbindung (z.B. durch Abschalten eines VPN-Geräts)? Wird die VPN-Verbindung wieder hergestellt, oder bleibt die Verbindung unterbrochen?

Für den Basis-Interoperabilitätstest wurde ein „kleinster gemeinsamer Nenner“ mit den folgenden Einschränkungen und Vorgaben definiert:

- Fokus auf IPsec: Als VPN-Protokoll wurde die aktuelle und inzwischen sehr weit verbreitete Security-Protokollfamilie IKE/IPsec verwendet. Andere VPN-Protokolle wie PPTP, L2TP und weitere wurden nicht untersucht.
- Nur Verbindungen zwischen VPN-Gateways: Der Fokus dieser Untersuchung lag auf Verbindungen zwischen dedizierten VPN-Gateways. Remote Access-Szenarien

zwischen VPN-Clients und Gateways und VPN-Verbindungen zwischen Hosts wurden nicht untersucht.

- Preshared Key für die Geräte-Authentisierung: Für die Authentisierung der VPN-Gateways wurde als kleinster gemeinsamer Nenner das „Preshared Key“-Verfahren gewählt. Die Authentisierung auf der Basis einer Public Key Infrastruktur (PKI) wurde aufgrund ihrer Komplexität nicht weiter untersucht.
- Eingeschränkte IPsec-Parameterauswahl: Als Verschlüsselungsverfahren für ESP wurde 3DES festgelegt. Zwar wird vom IPsec-Standard als schwächstes Verfahren DES vorgesehen, das alle VPN-Gateways mindestens beherrschen sollten. Da DES jedoch keine hinreichend hohe Sicherheit mehr bietet, wurde den Tests aus Sicherheitsgründen 3DES zu Grunde gelegt.
  In der Praxis sind durch die Verwendung des sicheren 3DES keine Probleme aufgrund der Rechenleistung der VPN-Geräte zu erwarten. Insbesondere stehen i.d.R. skalierbare Lösungen und Beschleunigungskarten zur Verfügung, bei denen die Ver- und Entschlüsselung mit hohem Durchsatz in Hardware erfolgt.
  Es wurde nur das ESP Protokoll eingesetzt, das AH Protokoll ohne Verschlüsselung wurde nicht betrachtet.
- Nur eine VPN-Verbindung zur Zeit: Es wurde bei jeder Produktkombination nur eine einzige Verbindung zwischen zwei VPN-Gateways aufgebaut. Die Untersuchung multipler Verbindungen zu einem oder mehrerer VPN-Gateways gleichzeitig wurde nicht untersucht. Aufgrund vorhergehender Untersuchungen ergeben sich durch diese Vorgehensweise bei gleichen Hersteller-Paarungen keine wesentlichen Einschränkungen hinsichtlich der Aussagekraft der Tests. Allerdings sollte in der Praxis vor einer größeren Investition die Interoperabilität der auszuwählenden Produkte bei mehreren gleichzeitigen VPN-Verbindungen überprüft werden.
- Einheitlicher Adressraum: Es wurde im Test ein einheitlicher IP-Adressraum über beide Teilnetze angenommen. Beide Gateways waren direkt an das Koppelnetz („Internet“) angeschlossen. Die NAT-Problematik brauchte daher nicht betrachtet werden.
- Einfaches WAN ohne Routing: Im Test wurde ein sehr einfaches WAN-Transportmedium nachgebildet, das beiden VPN-Zugängen das gleiche Subnetz zur Verfügung stellt. Auch hier wurde durch vorhergehende Untersuchungen nachgewiesen, dass diese Wahl des Transportnetzes keine Einschränkung der Aussagekraft der Tests bedeutet.
- Identifikation der Teilnehmer über IP-Adressen**:** Im Test erfolgte die Identifikation der VPN-Gateways ausschließlich über ihre IP-Adressen. In der Praxis kann die Identifikation z.B. auch über Geräte- oder DNS-Namen erfolgen.

Viele dieser Einschränkungen zielen darauf ab, überhaupt eine sichere Verbindung zwischen den VPN-Gateways herzustellen und mögliche sekundäre Probleme zu vermeiden.

4.2 Technischer Laboraufbau

Das Testszenario sieht vor, eine LAN-to-LAN VPN-Anbindung von einer Zweigstelle (Branch Office) zur Hauptniederlassung (Headquarter) zu simulieren. Technisch betrachtet wird die Verbindung zweier IP-Subnetze über ein WAN getestet. Um den Verkehr im simulierten Internet beobachten zu können, wurde über einen Hub ein weiterer PC mit Sniffersoftware angeschlossen.

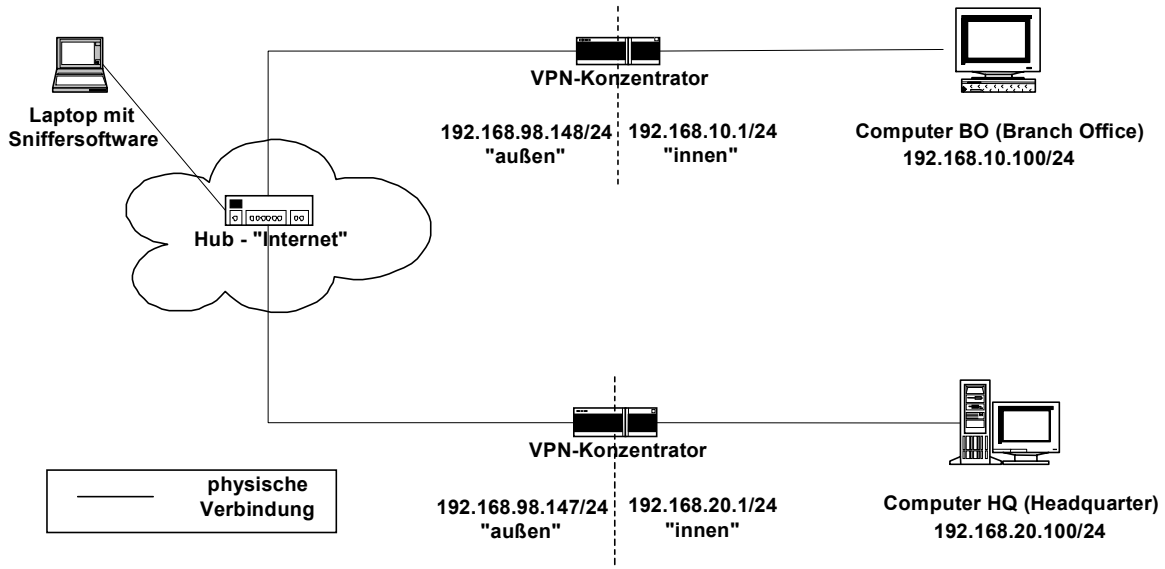

Abbildung 3: Test-Szenario im Labor

4.3 Festlegung der Gateway und Tunnelparameter:

Folgende Parameter wurden entsprechend ihrer Bedeutung in der Praxis für das IKE und IPsec Protokoll bestimmt.

Einstellungen IKE:

- Verschlüsselung mit 3DES
- Integritätsschutz mit HMAC-SHA-1
- Authentisierung mit Pre-Shared Key (Passwort: „testtest“)
- Schlüsselaustausch mit Diffie-Hellman Group 2 (1024 Bit)
- SA-Lifetime 86.400 Sekunden (24 Stunden), keine Begrenzung der Lebenszeit nach Datenvolumen
- Identifizierung über IP-Adresse

Einstellungen IPsec:

- ESP im Tunnelmodus
- Verschlüsselung mit 3DES
- Integritätsschutz mit HMAC-SHA1
- Schlüsselaustausch mit Diffie-Hellman Group 2 (1024 Bit)
- Anwendung von PFS (Perfect Forwarding Secrecy mit Diffie-Hellman Group 2)
- SA-Lifetime 28800 Sekunden (8 Stunden), keine Begrenzung der Lebenszeit nach Datenvolumen

3DES ist zur Zeit der von den meisten Geräten unterstützte Verschlüsselungsalgorithmus und wird auch von den meisten Anwendern eingesetzt. ESP im Tunnelmodus bietet den

höchst möglichen Schutz durch das komplette Einkapseln des originalen IP-Pakets. Die SA-Lifetimes, SHA1 und Diffie-Hellman Group 2 sind empfehlenswerte Standardeinstellungen.

4.4 Softwareauswahl und Installation der HQ/BO-Computer

4.4.1 Softwareauswahl

Für die Testumgebung wurde eine gängige und praxisnahe Mischung von Betriebssystemen verwendet: ein Windows 2000 Server (Headquarter, System-HQ) als Domänencontroller und eine Windows NT 4 Workstation (Branch-Office, System-BO). Viele Unternehmen migrieren von Windows NT zu Windows 2000, so dass beide Betriebssysteme in der Praxis oft gemischt anzutreffen sind. Zwischen den beiden Windows-Systemen wurde eine Domänenanmeldung über das VPN simuliert.

Auf jedem der Rechner wurde ein Webserver betrieben. Der Windows 2000 Server enthält standardmäßig den IIS-Webserver. Auf dem NT Rechner wurden ein Apache-Webserver (Windows Version) und zusätzlich noch ein Mailserver installiert, um Verbindungen vom System-HQ zum System-BO testen zu können. Durch diese Verteilung der Serverdienste konnte die VPN-Verbindung in beide Richtungen getestet werden.

Auf beiden Windows-Systemen wurden standardmäßig die Dienste zum Filesharing mit installiert. Somit konnte ohne zusätzliche Software auch Filesharing durch den VPN-Tunnel getestet werden.

An dieser Stelle sei explizit darauf hingewiesen, dass es sich bei der Testumgebung um eine Laborinstallation handelt, die man im „real life“ nicht in dieser Form einsetzen sollte. Auf Dienstetrennung, Sicherheitskonfiguration der Server etc. wurde explizit nicht geachtet, um den Aufwand der Testumgebung gering und den Aufbau möglichst einfach zu halten. Ziel der Untersuchung war die Interoperabilität der VPN-Gateways zu testen und nicht das Sicherheitsniveau der als Testumgebung benötigten Softwareinstallationen.

Gerätename	**Betriebs-system**	**Anwendungen**	**Rolle**
Host Headquarter	Win2000	- Webbrowser (MS IE 5) - Webserver (MS IIS 5) - Mailclient (MS Outlook)	Der Host Zentrale repräsentiert das Teilnetz der Zentrale.
Host Branch Office	Win NT 4	- Webbrowser (ME IE 5) - Webserver (Apache v1.3.23) - POP3 / SMTP-Mailserver (SLmail v1.1)	Der Host Niederlassung repräsentiert das Teilnetz einer Niederlassung.
Hub		-	Mit dem Hub wird das „Internet“ simuliert, das die beiden Teilnetze Zentrale und Niederlassung miteinander verbindet.
Sniffer	Suse Linux 7.2	tcpdump (Version 3.4a6) im promiscous -Mode	Mit dem Sniffer wird der Verbindungsaufbau beobachtet und überprüft, ob Datenpakete verschlüsselt oder unverschlüsselt übermittelt werden.

Tabelle 1: Basiskonfiguration des Testaufbaus

4.5 Testdurchführung

Die folgende Tabelle gibt eine Übersicht über die durchgeführten Einzeltests:

	Test	Kurzbeschreibung
Basistest: Ist ein Verbindungsaufbau möglich?		
1	Ping	Ping-Anfragen zwischen den Hosts
2	Client-Server-Verbindung	Aufbau einer HTTP-Verbindung zwischen Webclient- und Webserver
3	Mailversand	Versand einer E-Mail vom Mailclient zum Mailserver via SMTP, bzw. Abruf von Mail vom Mailserver via POP3
4	Domänenanmeldung	Anmeldung eines Benutzers auf der NT 4.0 Workstation an der Windows 2000 Domäne des Headquarter
5	Dateifreigabe	Gegenseitiger Zugriff über das Netzwerk auf freigegebene Verzeichnisse und Dateien
Ausfalltests: Wie verhalten sich die VPN-Gateways bei Geräteausfall?		
6	Ausfall des sendenden VPN GWs „Headquarter“	s.u.
7	Ausfall des sendenden VPN GWs „Branch Office“	s.u.
8	Ausfall des empfangenden VPN GWs „Headquarter“	s.u.
9	Ausfall des empfangenden VPN GWs „Branch Office“	s.u.

Tabelle 2: Übersicht über die Einzeltests

Alle Einzeltests zwischen je zwei VPN-Gateways wurden isoliert durchgeführt.

4.5.1 Der Basistest

Ping zwischen den Testgeräten

Der Ping-Test soll sicher stellen, dass ein IPsec-Tunnel zwischen beiden Geräten aufgebaut werden kann. Wenn der Ping-Befehl erfolgreich abgesetzt wurde und im simulierten Internet nur verschlüsselte Daten mit dem Sniffer zu sehen sind, gilt die VPN-Verbindung (IPsec Tunnel) als erfolgreich zustande gekommen.

Häufig war zu beobachten, dass die ersten ein bis fünf Pings fehlschlagen, weil erst der IPsec-Tunnel aufgebaut werden musste. Danach funktionierte Ping problemlos. Dies kann z.B. durch die Option „-t“ („Ping 192.168.20.100 –t“) sichtbar gemacht werden, durch die fortlaufend Ping-Anfragen gesendet werden.

Zeigt der Sniffer unverschlüsselte Ping-Pakete zwischen den VPN-Geräten, so ist es möglich, dass aufgrund der Ping-Pakete kein Tunnel aufgebaut wird, sondern die Pakete wegen einer Fehlkonfiguration des Routings oder der NAT-Umwandlung unverschlüsselt ins Netz geraten.

Anfragen Webserver

Vom BO Computer wurde mit dem installierten Browser auf den IIS-Webserver des HQ Computers zugegriffen. Über den Sniffer lässt sich prüfen, ob die angezeigten Daten tatsächlich vom Webserver und nicht (ohne Netzwerkkommunikation) aus dem Browsercache des BO Computers kommen. Dabei kann mit der Tastenkombination Strg-F5

beim Internet Explorer sichergestellt werden, dass eine Webseite komplett neu vom Webserver angefordert wird.

Im umgekehrten Fall wurde vom HQ Computer der Apache-Server des BO Computers angefragt. Mit Hilfe des Sniffers wurde wieder geprüft, ob die angezeigten Daten auch wirklich vom Webserver kommen.

E-Mail

Im nächsten Versuch wurde mit Outlook eine E-Mail erstellt und an eine beliebige E-Mail-Adresse abgesendet. Der Versand wird mit dem „Senden und Empfangen“ Button ausgelöst. Der korrekte Login am E-Mail-Server und Eingang der Mail konnten im Protokoll des Mailservers überprüft werden. Ob die Datenübertragung tatsächlich in verschlüsselter Form statt fand, wurde mit dem Sniffer überprüft.

Domänenanmeldung

Der aktuelle Benutzer des BO Computers wurde abgemeldet. Beide VPN-Geräte wurden gebootet, um eine evtl. bestehende Verbindung zwischen den Geräten abzubauen. Wenn der Anmeldebildschirm von Windows NT erschien, wurden Benutzer- und Domänenname und das zugehörige Passwort eingegeben. Nach dem Klicken des OK-Buttons sollte eine neue Verbindung aufgebaut werden und verschlüsselter Datenverkehr zwischen den VPN-Geräten auf dem Sniffer zu sehen sein. Ob der Benutzer wirklich auf dem HQ Server angemeldet war, konnte über das „net user“ Kommando auf der Konsole des HQ Servers festgestellt werden.

Schlug die Anmeldung über VPN fehl, so erschien auf der NT Workstation in einer Dialogbox die Meldung, dass der Domänencontroller nicht gefunden wurde.

Verzeichnisfreigaben

Mit dem Windows Explorer wurde getestet, ob sich auf beiden Rechnern die Verzeichnisfreigabe des jeweils anderen Rechners als Netzlaufwerk mit dem Freigabenamen „Test“ verbinden ließ. Anschließend wurden mit dem Windows Explorer beliebige Dateien zwischen den Rechnern transferiert.

Fast alle VPN-Gateways bieten die Möglichkeit, einzusehen, wie viele Kilobyte Datenvolumen durch einen Tunnel übertragen wurden. Wenn eine Datei zwischen den Rechnern kopiert wird, liefert der Anstieg des Volumenzählers einen Beleg für die Übertragung.

Bei vielen Geräten sind auch Hitcounter des IPsec-Verkehrs einsehbar und geben eine weitere Möglichkeit zu überprüfen, ob die IP-Pakete durch den Tunnel geschickt wurden. Diese Hitcounter zählen mit, wie oft die Regel, die besagt, dass ein Paket durch einen IPsec-Tunnel geschickt werden soll, auf ein weiterzuleitendes IP-Paket zugetroffen hat. Ein Kopieren einer Datei erzeugt entsprechenden IP-Verkehr, was ein Hochzählen der Hitcounter zur Folge hat.

Falls Hitcounter und Volumenzähler nicht hochzählen, liegt wahrscheinlich keine Verschlüsselung der Daten vor und die Daten werden geroutet. Mit dem Sniffer kann die Verschlüsselung der übertragenen Daten überprüft werden.

4.5.2 Der Ausfalltest: Gehen Verbindungen verloren?

Der Ausfalltest sollte zeigen, wie sich zwei VPN-Geräte verhalten, wenn eines der Geräte durch Abschalten, Reboot, Stromausfall oder Hardwaredefekt /Austausch ausfällt und später wieder den Betrieb aufnimmt.

Um festzustellen, wie sich ein Gerät in einer bestimmten Situation verhält, ist es wichtig festzulegen, welches Gerät versucht die Verbindung aufzubauen, und welches den Ausfall simuliert. Hierdurch ergeben sich vier Kombinationsfälle.

Der Test wurde so definiert, dass der Computer des aufbauenden Gerätes permanent Ping-Anfragen an den Computer der Gegenstelle schickt:

- Ist das HQ VPN GW das aufbauende Gerät, so schickt der HQ Computer permanent Ping Anfragen an den BO Computer.
- Ist das BO VPN GW das aufbauende Gerät, so schickt der BO Computer permanent Ping Anfragen an den HQ Computer.

Folgende Tabelle zeigt die Kombinationsmöglichkeiten der Geräte:

Ausfallgerät	Aufbauendes/ sendendes Gerät	Erklärung
HQ VPN GW	HQ VPN GW	HQ VPN GW wird abgeschaltet. Es versucht gleich nach dem Booten eine Verbindung zum BO VPN GW aufzubauen, da der HQ Computer fortlaufend versucht, Ping Pakete an den BO Computer zu schicken.
BO VPN GW	BO VPN GW	BO VPN GW wird abgeschaltet. Es versucht gleich nach dem Booten eine Verbindung zum HQ VPN GW aufzubauen, da der BO Computer fortlaufend versucht, Ping Pakete an den HQ Computer zu schicken.
HQ VPN GW	BO VPN GW	HQ VPN GW wird abgeschaltet. Der BO Computer sendet vor und nach dem Abschalten immer weiter Ping-Pakete an den HQ-Rechner, um so eine Verbindung zwischen BO VPN GW und HQ VPN GW aufrechtzuerhalten bzw. umgehend wieder aufzubauen.
BO VPN GW	HQ VPN GW	BO VPN GW wird abgeschaltet. Der HQ Computer sendet vor und nach dem Abschalten immer weiter Ping-Pakete an den BO-Rechner, um so eine Verbindung zwischen HQ VPN GW und BO VPN GW aufrechtzuerhalten bzw. umgehend wieder aufzubauen.

Tabelle 3: Kombinationsmöglichkeiten von BO VPN GW und HQ VPN GW

Im nachfolgenden Kapitel wird an Stelle des Begriffs „Security Association“ (SA) der Verständlichkeit wegen synonym der Begriff „Verbindung“ verwendet. In der folgenden Darstellung bezeichnet „Gegenstelle“ immer das nicht ausgefallene VPN Gerät.

Eine „gleichseitige“ Kombination (HQ-HQ, BO-BO) zeigt das Verhalten der Gegenstelle, wenn zu dieser eine neue Verbindung (SA) aufgebaut wird, ohne die alte Verbindung ordnungsgemäß zu beenden.

Mögliche Ergebnisse sind:

- Die Gegenstelle merkt, dass vom „alten“ Partner eine neue Verbindung aufgebaut wird und verwirft die nicht mehr gültige.

- Die Gegenstelle baut neben der alten einfach eine neue Verbindung auf. Die alte Verbindung (SA) verfällt nach einer Idle-Time oder dem Ablauf der SA-Lifetime.
- Die Gegenstelle merkt durch einen dead-peer detection Mechanismus, dass der alte Verbindungspartner ausgefallen ist und löscht die SA.

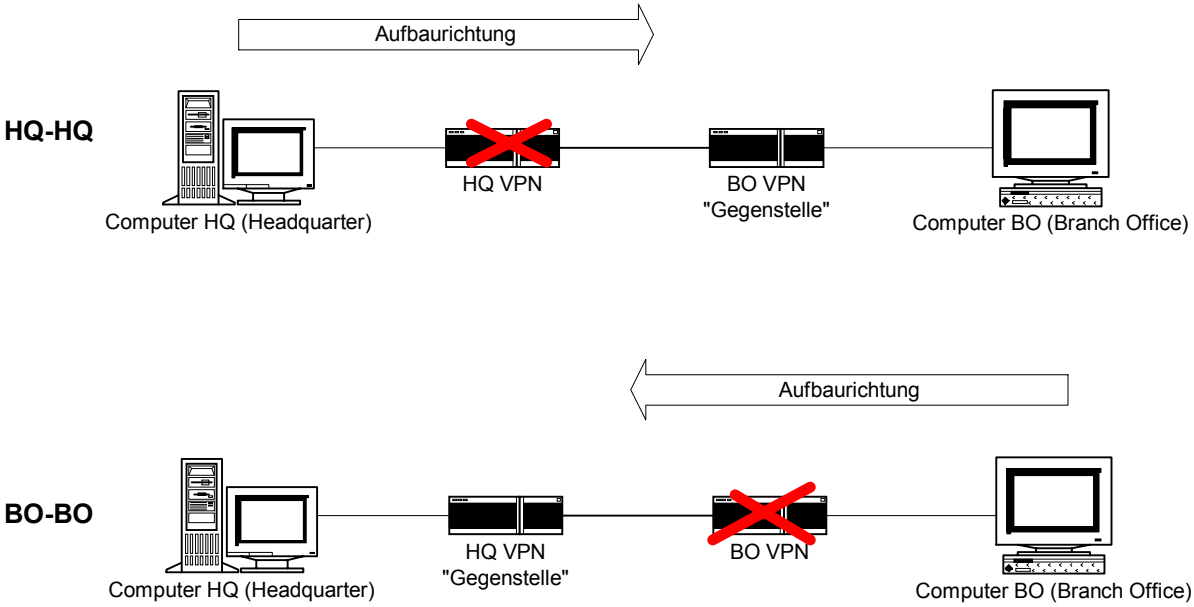

Abbildung 4: Gleichseitiger Verbindungsaufbau und Ausfall

Eine „ungleichseitige“ Kombination (BO-HQ, HQ-BO) zeigt das Verhalten der Gegenstelle, wenn sie selbst Daten an eine nicht mehr existierende Verbindung schickt und auch das Verhalten des ausgefallenen und wieder neu gestarteten Gerätes, welches Daten zugeschickt bekommt, für die keine gültige SA besteht.

Mögliche wünschenswerte Systemreaktionen sind:

- Die Gegenstelle merkt durch einen „Dead-Peer Detection Mechanismus“, dass der alte Verbindungspartner ausgefallen ist. Diese Mechanismen sind nicht als Standard definiert und werden von den Herstellern auf jeweils eigene Weise implementiert.
- Die ausgefallene Seite teilt der Gegenstelle mit, dass für die ankommenden Pakete keine gültige SA existiert, daraufhin wird eine neue SA ausgehandelt und ein neuer Tunnel aufgebaut.
- Die Gegenstelle merkt, dass lange keine Antwort vom Verbindungspartner mehr gekommen ist und erklärt die Verbindung für beendet.

Mögliches unerwünschtes Systemverhalten ist:

- Die ausgefallene Seite hat keine gültige SA für die eintreffenden Pakete der Gegenstelle und lehnt diese einfach ab. Dieser Fall ist völlig konform zum gültigen Standard, da in diesem keine weiteren Mechanismen für das Vorgehen definiert sind.

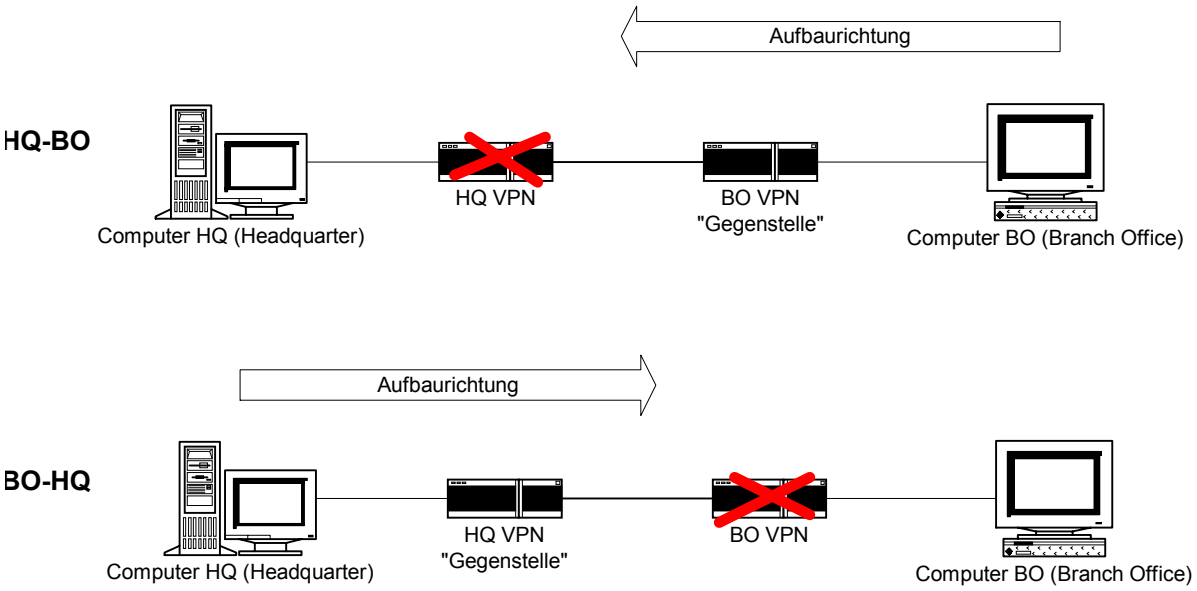

Abbildung 5: Ungleichseitiger Verbindungsaufbau und Ausfall

Praktische Durchführung eines Ausfalltests

Die praktische Durchführung wird am Beispiel HQ (ausfallend) und BO (sendend) erläutert.

1. Vom BO Computer werden permanent Ping Anfragen an den HQ Computer geschickt. Dies wird auf der Konsole mit dem Kommando „Ping 192.168.20.10 –t“ durchgeführt.
2. Sobald die Meldung „Antwort von 192.168.20.10 ....“ kommt, besteht eine VPN-Verbindung zwischen den Geräten.
3. Nun wird das HQ Gerät für ein paar Sekunden abgeschaltet. Im Konsolen-Fenster des BO Computers erscheint nun die Meldung „Zeitüberschreitung der Anforderung“. Der Ping erreicht sein Ziel nicht mehr, da die VPN-Verbindung unterbrochen ist.
4. Wenn das HQ Gerät wieder gebootet wird, lässt sich mit dem Sniffer der Datenverkehr auf der Netzleitung beobachten. Auch in den Log-Dateien und mit den Traffic-Monitoren der VPN-Geräte kann man beobachten, was auf den Geräten passiert.

Mögliche Verhaltensweisen im konkreten Beispiel sind:

- Das HQ VPN GW lehnt alle IPsec-Pakete auf Grund der fehlenden SA ab.
- Das HQ VPN GW teilt dem BO VPN GW mit, dass keine SA existiert (IKE Notify Messages).
- BO merkt, dass lange keine Antwort vom HQ gekommen ist und bricht die Verbindung ab.
- Eine „Dead-Peer Detection“ Einrichtung auf dem BO VPN GW hat den Ausfall des HQ VPN GWs bemerkt und die alte Verbindung abgebaut (somit wird BO eine neue aufbauen können).

Eine Verfälschung des Tests tritt dann auf, wenn für den Testfall die Verbindung von BO zum HQ aufgebaut werden soll, tatsächlich aber vom HQ zum BO aufgebaut wird. Ein Grund

hierfür kann z.B. sein, dass das Protokoll NetBIOS überprüft, ob verbundene Laufwerke noch existieren und damit den Aufbau der Verbindung anstößt. Durch Beobachtung der tatsächlichen Richtung des IPsec-Verbindungsaufbaus mit einem Sniffer wurden solche Verfälschungen erkannt und der Test erforderlichenfalls wiederholt.

4.6 Festgestellte Fehlergruppen und Probleme

Bei der Durchführung der Tests traten verschiedene Ursachen für Fehler und Probleme auf, wie z.B.:

Connectivity Probleme

- Zugang zur Managementkonsole
- Physische Connectivity
- Routing Connectivity
- Inbound/Outbound Filter
- Andere Regeln (NAT, Access Control Listen)

Fehler bei IKE und IPsec Einstellungen

- Falsche Proposals
- Lifetime

Sonstige Problemquellen

- Komplexität der Einstellungen
- Seiteneffekte (DNS, NetBIOS usw.)
- Geräteeigenheiten (Reboot erforderlich usw.)
- Unterschiedliche Terminologie der Hersteller (Missverständnisse bei nicht standardisierten Ausdrücken)
- Voreinstellungen

Um Probleme bei der Fehlersuche schneller einkreisen zu können, hilft es, die oben angeführten Gruppen systematisch zu durchlaufen.

5 Ergebnisse und Bewertung

Die gute Nachricht vorweg: Bei allen untersuchten Produktkombinationen konnte im Basistest eine sichere VPN-Verbindung aufgebaut werden. Die schlechte Nachricht: Sie konnte nicht immer aufrecht erhalten werden. Die einzelnen Untersuchungsergebnisse werden in der folgenden Tabelle zusammengefasst:

	Cisco VPN Concentrator 3000	Cisco PIX Firewall 515	Watchguard Firebox 1000	Nortel Networks Contivity 100	Nortel Networks Contivity 600	GenuGate	Astaro	Nokia IP 650
Cisco VPN Concentrator 3000								
Cisco PIX Firewall 515	OK							
Watchguard Firebox 1000	E	E						
Nortel Networks Contivity 100	E	E	E					
Nortel Networks Contivity 600	OK	E	OK	E				
GenuGate	NG	NG	NG	NG	NG			
Astaro	N	E	E	E	E	NG		
Nokia IP 650	NG	NG	NG	NG	NG	NG	NG	

Tabelle 4: Ergebnisse des Ausfalltests

Legende zu Tabelle 4:

- OK: Nach dem Ausfall eines Gerätes ist der Aufbau einer Verbindung in allen vier Fällen ohne Einschränkungen möglich.
- E: Der Aufbau einer Verbindung ist nach dem Ausfall eines Gerätes nur noch mit Einschränkungen möglich.
- N: Ein Verbindungsaufbau ist nach dem Ausfall eines Gerätes nicht mehr möglich.
- NG: Basistest erfolgreich, Ausfalltests wurden nicht durchgeführt.

Zwischen allen acht getesteten Geräten konnte stets ein sicherer IPsec Tunnel aufgebaut werden. Die getesteten VPN-Geräte haben somit alle den Basistest bestanden.

Allerdings verhielten sich die Geräte im Ausfalltest recht unterschiedlich, lediglich bei drei Gerätepaaren konnte nach einem Geräteausfall in allen Fällen wieder automatisch ein Tunnel aufgebaut werden. Alle anderen getesteten Gerätepaare konnten die Verbindung nach einem Ausfall nicht in allen vier Ausfallszenarien – teilweise in keinem davon – wieder aufbauen (siehe Tabelle 4).

Der Grund für dieses unterschiedliche Verhalten liegt in der unterschiedlichen Implementierung von „keep-alive“-Mechanismen in den Geräten. Manche der Geräte haben neben den die Lebenszeit der SA beschränkenden Lifetime- und Volumenzählern noch eigene lebenszeitbeschränkende Mechanismen. Diese bauen eine Verbindung ab, wenn sich eine Gegenstelle lange nicht gemeldet hat oder auf Anfragen nicht reagiert.

Auch die Interpretation von sogenannten „IKE-Notify Messages“ (Fehlermeldung im IKE Protokoll) ist sehr unterschiedlich. Nur bei sehr wenigen Geräten konnte man aus den Logdateien entnehmen, dass die Geräte auf IKE-Notify Messages reagierten.

Auf Grund der unterschiedlichen Verhaltensweisen bewegt sich die Qualität der Zusammenarbeit der einzelnen Geräte nach einem Ausfall zwischen sehr gut und mangelhaft. Wie gut zwei Geräte zusammenarbeiten, liegt nicht daran, wie viel Funktionalität ein Gerät enthält, sondern wie gut die Funktionalitäten der Geräte miteinander operieren.

6 Empfehlungen und Ausblick

In den durchgeführten Tests konnte bei einer einfachen Basiskonfiguration zwischen allen getesteten Geräten Interoperabilität festgestellt werden, denn es konnten jeweils IPsec-Tunnel aufgebaut werden.

Jedoch haben die Ausfalltests gezeigt, dass sich die Geräte schon bei einfachen, in der Praxis vergleichsweise häufig zu erwartenden Betriebsstörungen sehr uneinheitlich verhalten können. Ein definiertes Verhaltens zweier beliebig kombinierten Geräte ist nicht gegeben, unter anderem auch, weil die relevanten Standards keine Festlegungen zum Störungsverhalten enthalten. Möglichkeiten der Abhilfe werden derzeit in der IPsec-Arbeitsgruppe der IETF diskutiert. Wird das Verhalten der Geräte bei Störungsfällen künftig vom Standard mit abgedeckt und konform implementiert, so werden die IPsec Implementierungen wie auch die Verbindungen zwischen zwei Gegenstellen stabiler und sicherer werden.

Aus den praktischen Anforderungen eines Unternehmens kann die Forderung abgeleitet werden, dass sich die Geräte nach Störungen automatisch wieder synchronisieren sollen. Ist dies durch die Geräte nicht gegeben, müssen zumindest organisatorische Prozesse definiert werden, wie von Hand oder skriptgesteuert die Verbindung wieder angestoßen werden kann. Besonders kritisch müssen Fälle betrachtet werden, in denen der Ausfall der VPN-Verbindung möglicherweise nicht zeitnah bemerkt wird und sich daraufhin Folgeschäden wie z.B. inkonsistente Datenbanken und fehlende Datensicherungen ergeben können.

Die anhand der Tests gewonnenen Ergebnisse zeigen, dass zwischen verschiedenen VPN-Geräten eine Basis-Interoperabilität vorliegt. Es darf erwartet werden, dass zwei beliebige VPN-Gateways zumindest einen IPsec-Tunnel erfolgreich aufbauen können. Im konkreten Einzelfall bleibt jedoch der mögliche Funktionsumfang, das Gerätemanagement und das Verhalten der Geräte im Störungsfall genau zu prüfen.

Ein weiterer Hinderungsgrund für den Einsatz heterogener VPN-Netze in der Praxis dürfte der erhöhte Aufwand bei der Administration sein. Sofern verschiedene Managementsysteme für die Produkte der jeweiligen Hersteller verwendet werden müssen, erhöht dies natürlich den Betriebsaufwand. Man muss diesen Aufwand und die dadurch entstehenden Kosten aber stets in Relation zur Neuanschaffung einer homogenen VPN-Landschaft setzen. Über den Aufwandsaspekt hinaus können sich durch uneinheitliche Managementsysteme für verschiedene Produkte eines heterogenen VPNs auch leichter Konfigurationsfehler ergeben, die sich auf die Sicherheit auswirken. Daher ist zu empfehlen, die Sicherheit von VPNs regelmäßig zu überprüfen, z.B. durch Sniffer und automatisierte Tools.

7 Referenzen und Internet-Quellen

[Abo02] Aboba, B. (2002): *IPsec-NAT Compatibility Requirements*, Internet Draft

[Aie02] Aiello, W. et al (2002): *Just Fast Keying (JFK)*, Internet Draft draft-ietf-ipsec-jfk-04.txt

[ENX] ENX – *European Network Exchange* (www.enxo.com)

[FeSc00] Ferguson, N.; Schneier, B. (2000): *A Cryptographic Evaluation of IPsec*, http://www.counterpane.com/ipsec.html

[GoKnSt02] Gora, S.; Knoblauch, C.; Stark, C. (2002): *Schönwetter-Connection – Verglichen: Interoperabilität von VPN-Gateways*, erschienen in: iX – Magazin für professionelle Informationstechnik, Heft 10, S. 92-95

[HaCa98] Harkins, D.; Carrel, D. (1998): *The Internet Key Exchange (IKE)*, RFC 2409

[Har02] Harkins, D. et al (2002): *Proposal for the IKEv2 Protocol*, Internet Draft draft-ietf-ipsec-ikev2-02.txt

[KeAt98a] Kent, S.; Atkinson, R. (1998): *Security Architecture for the Internet Protocol*, RFC 2401

[KeAt98c] Kent, S.; Atkinson, R. (1998): *IP Authentication Header*, RFC 2402

[KeAt98b] Kent, S.; Atkinson, R. (1998): *IP Encapsulating Security Payload (ESP)*, RFC 2406

[Kno02] Knoblauch, C. (2002): *VPN-Interoperabilitätstest*, Diplomarbeit an der Fachhochschule Heidelberg, Fachbereich Wirtschaftsinformatik

[Mad02] Madson, C. (2002): *Son-of-IKE Requirements*, Internet Draft draft-ietf-ipsec-son-of-ike-protocol-reqts-01.txt

[Maug98] Maughan, D. et al (1998): *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408

[Perl00] Perlman, R.; Kaufman, C. (2000): *Key Exchange in IPsec – Analysis of IKE*, in: IEEE Internet Computing, December 2000

[Shie00] Shieh S.;Ho, F.; Huang Y.; Luo, J. (2000): *Network Address Translators – Effects on Security Protocols and Applications in the TCP/IP Stack*, in: IEEE Internet Computing, December 2000

[VPNC02] VPN Consortium (2002): *VPN Technologies – Definitions and Requirements*, Whitepaper (verfügbar unter: www.vpnc.org)

RFCs und aktuelle Internet Drafts sind verfügbar über die Webseite der Internet Engineering Task Force (IETF): http://www.ietf.org/html.charters/ipsec-charter.html

Anhang A: Übersicht über Hersteller und Produkte

Der Markt für VPN-Gateways ist vielschichtig. Neben einigen großen Herstellern bieten eine Vielzahl von kleinen Unternehmen VPN-Produkte an. Für die Tests sollte eine möglichst repräsentative Auswahl getroffen werden. Daher wurde anhand folgender beiden Kriterien eine Selektion vorgenommen:

- Marktanteil des Produkts bzw. Herstellers am VPN-Markt
- Besonderheiten des Produkt-Ansatzes (z.B. OpenSource-Basis, Sicherheits-Evaluierung etc.)

Folgende Geräte standen im Testzeitraum zur Verfügung:

Hersteller	Untersuchte Produkte (Version)	Anmerkung	Kontakt
Astaro AG	F1 Security Linux (2.0)	Linux-basierte Lösung	www.astaro.de
Cisco Systems GmbH	VPN 3015 Concentrator (3.5) PIX 515 Firewall (6.1.(3))		www.cisco.de
Genua Gesellschaft für Netzwerk- und UNIX-Administration mbH	GeNUGate (3.2)	Evaluiert nach ITSEC E3 hoch, Lösung basiert auf FreeBSD	www.genua.de
Nokia GmbH	IP 650 (FW1-NG Build 51012)	Hardware-Variante des Produkts VPN-1 von Check Point	www.nokia.de
Nortel Networks Deutschland GmbH	Contivity Extranet 100 Contivity Extranet 600 (4.05)		www.nortelnetworks.de
Watchguard Technologies	Firebox 1000 (5.0)		www.watchguard.com

Tabelle 5: Im Test berücksichtigte Hersteller und Produkte