Weiterführende Aufgabenstellungen bei VPN-Systemen

In diesem Kapitel werden einige weiterführende Aufgabenstellungen behandelt, die mit dem Betrieb von VPN-Systemen verbunden sind. Dazu gehören die Verfügbarkeit der Netzwerkdienste, mögliche Realisierungsformen von VPN-Systemen ...

13.1 Verfügbarkeit

Der Anwender muss sich darauf verlassen können, dass die Services, die er für die Erledigung seiner Aufgaben benötigt, »immer« verfügbar sind. Dies betrifft alle Komponenten, die ein VPN-System ausmachen, aber auch die Verfügbarkeit des Netzes, insbesondere der Kommunikationsverbindungen über das Internet.

Inwieweit Organisationen (ASPs) in der Lage sind, »Quality of Service« im Internet zu garantieren, hängt wesentlich davon ab, ob die Internet Provider (ISPs) dies zukünftig global anbieten können.

Bezüglich der Verfügbarkeit der Komponenten des VPN-Systems muss ein Verfügbarkeitskonzept erarbeitet werden. Dementsprechend müssen die wichtigsten Komponenten in einem VPN-System redundant ausgelegt werden. Außerdem ist Loadbalancing notwendig, damit eine angemessene Verfügbarkeit realisiert werden kann, um den für die Anwendung notwendigen Grad an »Quality of Service« zu erreichen /Harl2000/.

Aus der Sicht des Anwenders müssen Mindestanforderungen im Bereich »Quality of Service« garantiert werden, damit das Risiko der Nichtverfügbarkeit sinnvoll abgeschätzt werden kann.

13.2 Redundanzsysteme

Um beim Ausfall eines VPN-Gateways die Verfügbarkeit des Netzwerks nicht zu gefährden, werden üblicherweise Redundanzsysteme eingereichtet. Hierzu gibt es verschiedene Möglichkeiten, die im Folgenden erläutert werden.

13.2.1 Parallele VPN-Gateways

Werden zwei VPN-Gateways parallel geschaltet, erhält jeder VPN-Gateway die Verbindungsregeln des parallel geschalteten Geräts. Alle anderen Daten – wie IP-Adresse und Schlüssel – differieren. Diese Betriebsart kann zur Lastverteilung zwischen zwei oder mehreren VPN-Gateways, angewendet werden, die beispielsweise zwischen zwei Netzen positioniert sind.

13.2.2 Passives Redundanzsystem

Ein passives Redundanzsystem dient dazu, ein defektes VPN-Gateway auszutauschen, ohne dass Verzögerungen durch die Personalisierung des neuen Geräts entstehen. Dies ist besonders dann von Vorteil, wenn das zentrale Sicherheitsmanagement-System sich an einem anderen Ort befindet als das ausgefallene VPN-Gateway.

Das »passive Redundanzgerät« wird in der Regel wie jedes andere Gerät personalisiert, aber als »passiv redundant« erfasst. Anschließend wird dieses Gerät wird nicht im Netz installiert, sondern als Ersatzgerät am jeweiligen Einsatzort gelagert. Wenn das im Netz befindliche VPN-Gateway ausfällt, kann es schnell gegen das Redundanzgerät ausgetauscht werden.

13.2.3 Aktives Redundanzsystem

In einem aktiven Redundanzsystem sind üblicherweise zwei parallel geschaltete VPN-Gateways (ein »aktives« und ein »redundantes« Gerät) über ein Kabel miteinander verbunden. Bei Ausfall des »aktiven VPN-Gateways« übernimmt das Redundanzgerät selbstständig dessen Funktion. Abbildung 13.1 verdeutlicht den Aufbau eines aktiven Redundanzsystems.

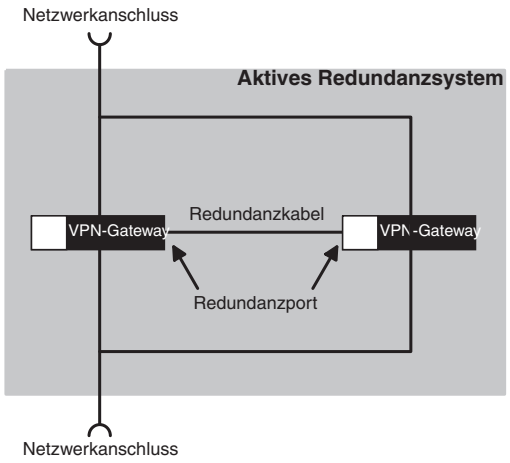

Abb. 13.1: Aktives Redundanzsystem

13.2.4 Redundanzsystem im »Spanning Tree«

Um die Verfügbarkeit eines Netzwerks zu erhöhen, werden in manchen Systemen zwei oder mehrere Switches parallel integriert. Das daraus resultierende Problem der »Schleifenbildung« wird durch ein Protokoll umgangen, das zwischen zwei Kommunikationspartnern einen eindeutigen Weg durch einen dieser Switches bzw. durch alle im Netzwerk befindlichen Switches berechnet. Der Weg wird in regelmäßigen Abständen überprüft und bei einem Ausfall eines Switches wird dieser aus dem Baum entfernt.

Diesen das Netzwerk umfassenden Baum bezeichnet man als »Spanning Tree«, das Protokoll zur Berechnung des Baums als »Spanning Tree Protocol«.

Abbildung 13.2 zeigt, wie ein Redundanzsystem aus zwei VPN-Gateways in eine derartige Netzwerkstruktur integriert werden kann. Die Switches bestimmen mithilfe des »Spanning Tree Protocols«, über welches VPN-Gateway der Netzwerkverkehr geleitet wird.

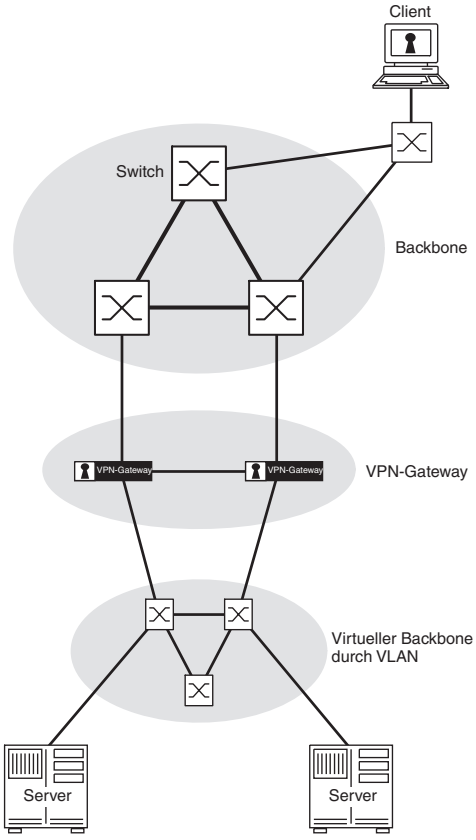

Abb. 13.2: VPN-Redundanzsystem im »Spanning Tree«

13.3 Realisierungsformen für VPN-Gateways

Es gibt unterschiedliche Möglichkeiten, eine VPN-Funktionalität zur Verfügung zu stellen. Die gängigsten Realisierungen bestehen darin, die VPN-Funktionalität in einem Router zu integrieren oder als separate Sicherheitskomponente anzubieten.

13.3.1 VPN-Realisierung im Router

Viele Router, die für die Sicherung der Netze verwendet werden sollen, bieten heute VPN-Funktionalität an. Die in solchen Geräten integrierten Sicherheitsfunktionalitäten sind hinreichend für interne Anwendungen, die nicht besonders sicherheitsrelevant sind, und bieten für diese Fälle eine preiswertere Lösung als separate Sicherheitskomponenten.

Router mit VPN-Funktionalitäten haben jedoch einige Schwächen:

- Die meisten Router bieten, weil sie keine Sicherheitsprodukte sind, nur eine unzureichende Administration der Sicherheitsfunktionen an. Weil das Security Management fehlt, werden dabei immer wieder Fehleinstellungen gemacht, die Sicherheitslöcher verursachen können.
- Router haben in der Regel nur unvollständige Protokollierungsmöglichkeiten und keinen Alarmierungsmechanismus für sicherheitsrelevante Ereignisse.
- Router sind schlecht gegen Angriffe gerüstet, die auf die Sicherheitsmechanismen selber gerichtet sind. Es fehlen Schutzmaßnahmen gegen solche Angriffe, so dass oft die Möglichkeit besteht, von außen über Management-Funktionen die VPN-Funktionalitäten auszuschalten oder das Regelwerk zu ändern.
- In der Praxis nimmt die Performance bei einigen Routern so stark ab, dass die eigentlichen Routing-Aufgaben nicht in der erforderlichen Geschwindigkeit durchgeführt werden können.
- Ein neuer Router, der für diese Aufgabe erst angeschafft werden muss, ist teurer als eine separate Sicherheitskomponente.
- Oft liegt die Verantwortung für den Betrieb der Router in einem anderen Bereich (andere Abteilung oder andere Firma, zum Beispiel Netzdienstanbieter), was die Einhaltung der Sicherheitspolitik schwierig bis unmöglich machen kann.

13.3.2 VPN-Gateways als separate Sicherheitskomponenten

VPN-Gateways als separate Sicherheitskomponenten haben die Hauptaufgabe, die vertrauenswürdige Kommunikation über eine unsichere Netzwerkverbindung zu ermöglichen.

Diese Realisierungsform von VPN-Produkten bietet mehrere wesentliche Vorteile:

- VPN-Gateways können die sicheren Designkriterien leichter erfüllen als Router, weil sie keine zusätzliche Software für andere Aufgabenstellungen benötigen.
- Mit separaten VPN-Gateways wird eine klare Abgrenzung zwischen Kommunikations- und Sicherheitsanforderungen geschaffen.
- VPN-Gateways bieten in der Regel ein separates Sicherheitsmanagement, das auch zentral für die Verwaltung mehrerer VPN-Gateways verwendet werden kann. Dadurch kann eine einheitliche und kontrollierbare Sicherheitspolitik einfach umgesetzt werden.
- Separate Sicherheitskomponenten sind flexibler als Router mit VPN-Funktionalität, weil sie unabhängig von anderen Funktionalitäten sind.

Aber auch die Nachteile separater VPN-Gateways sollen nicht verschwiegen werden:

- VPN-Gateways sind oft teurer als Software-Erweiterungen im Router.
- Die Integration einer zusätzlichen Hardwarekomponente – hier: eines VPN-Gateway – reduziert prinzipiell die Verfügbarkeit der Netzdienste.

13.4 Verwaltung großer VPN-Netzwerke

Bei großen VPN-Netzwerken kommt der Frage, wie eine optimale Konfiguration des Regelwerks durchgeführt werden kann, eine besondere Bedeutung zu. Das folgende Beispiel zeigt, wie komplex das Regelwerk in einem solchen Fall sein kann und wie mithilfe eines zentralen Sicherheitsmanagements sowie »virtueller Komponenten« die Administration wesentlich vereinfacht werden kann.

Abbildung 13.3 zeigt ein großes Netzwerk, das mithilfe von VPN-Gateways abgesichert werden soll. Das VPN-Netzwerk besteht aus 10 IP-Netzwerken [N] mit jeweils 45 Subnetzwerken [S]. Jedes Subnetzwerk soll durch ein VPN-Gateway geschützt werden, insgesamt werden 450 VPN-Gateways eingesetzt. Die Kommunikation zwischen allen Netzwerken bzw. Subnetzwerken soll nur in verschlüsselter Form erlaubt sein.

Wie groß ist die Anzahl der benötigten Regeln [R]?

Aus der Sicht eines VPN-Gateways muss für jedes vorhandene Subnetz (d.h. für jedes andere VPN-Gateway) eine Regel eingetragen werden (z.B. »Subnetz_X darf mit Subnetz_Y in verschlüsselter Form kommunizieren«). Die Summe aller notwendigen Regeln für alle VPN-Gateways wird mit der folgenden Formel berechnet:

$$\mathbf{R}_1 = S*(S-1)/2 = 450*(450-1)/2 = \mathbf{101\ 025}$$

R: Anzahl der Regeln
S: Anzahl der Subnetze

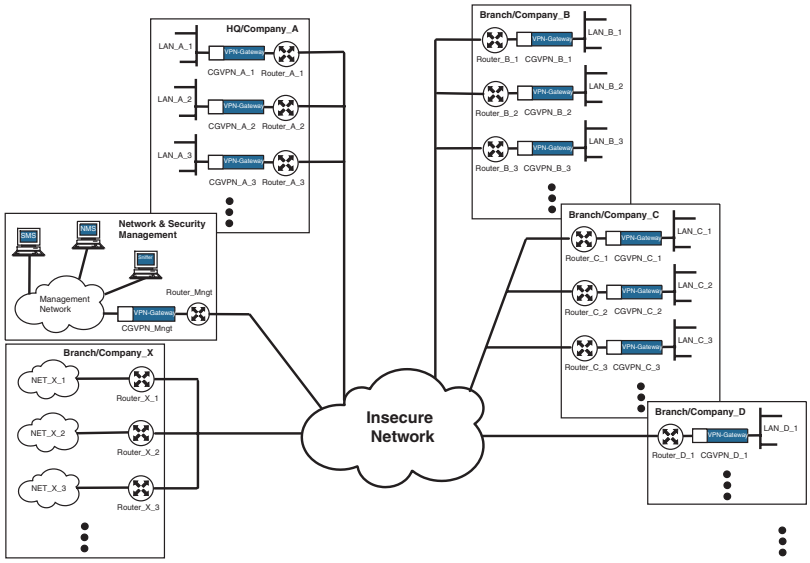

Abb. 13.3: Beispiel für ein großes VPN-Netzwerk

Die Einrichtung und Pflege eines solchen Gesamtnetzwerks mit 101.025 Regeln ist sehr komplex. Abbildung 13.4 verdeutlicht die Komplexität des notwendigen Regelwerks.

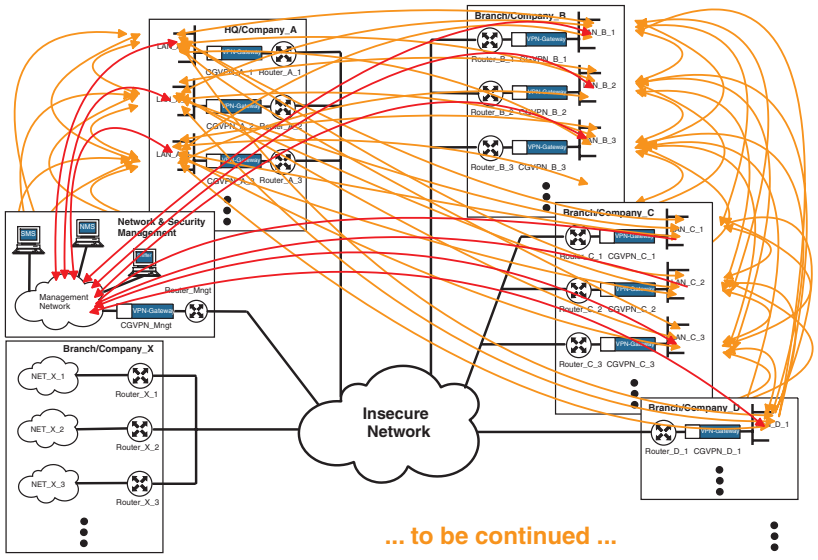

Abb. 13.4: Komplexität des Regelwerks in einem großen VPN-Netzwerk

Welche Alternativen gibt es, um die Anzahl der Regeln zu reduzieren?

Im Folgenden wird beschrieben, mit welchen Hilfsmitteln die Komplexität des Regelwerks minimiert werden kann. Dazu werden im zentralen Sicherheitsmanagement »virtuelle Komponenten« definiert, die die Formulierung von Regeln vereinfachen.

Voraussetzung dafür ist, dass im Sicherheitsmanagement die Möglichkeit, solche »virtuellen Komponenten« zu verwenden, herstellerseitig vorgesehen ist.

- **»Virtual Box«:**
  Die »Virtual Box« ist ein Hilfsmittel, mit dem alle Bestandteile eines IP-Netzwerks N in der Darstellung als ein Objekt zusammengefasst werden können.
  - »Virtual Boxes« dienen der Bildung von Gruppen in der Topologie.
  - Im zentralen Management werden 10 solcher »Virtual Boxes« eingerichtet.
  - Diese sind nicht mit Funktionen verknüpft (d.h., ihnen werden keine Regeln zugewiesen).
  - Ihre Bezeichnung beginnt mit »V_<sector id>«.
  - Wenn möglich, sollten ihre IP-Adressen besonders gekennzeichnet werden, damit die Administration vereinfacht wird.
  - Ort ist »virtual«.

Abb. 13.5: Symbol für eine »Virtual Box«

- **»Dummy Box«:**
  Die »Dummy Box« ist ein (ebenfalls virtuelles) Hilfsmittel, mit dem die Netzwerke aus der Sicht der Endgeräte in den Subnetzen als ein Objekt zusammengefasst werden können.
  - »Dummy Boxes« werden niemals konfiguriert oder installiert.
  - Im zentralen Management werden 10 solcher »Dummy Boxes« eingerichtet. Dies ergibt den Vorteil, dass man die 10 IP-Netzwerke über je einen IP-Adressbereich ansprechen kann, anstatt die jeweils 45 Subnetze einzeln anzusprechen.
  - »Dummy Boxes« werden in virtuellen Verbindungen (Verbindungsregeln) verwendet (z.B. »LAN_A zum S_NET_A«).
  - Ihre Bezeichnung beginnt mit »D_<sector id>«, wobei nur reale Sektoren verwendet werden dürfen.

- Wenn möglich, sollten die IP-Adressen besonders gekennzeichnet werden, damit die Administration vereinfacht wird.
- Ort ist »virtual«.

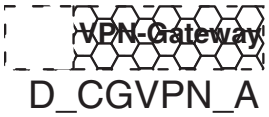

Abb. 13.6: Symbol für eine »Dummy Box«

- **»Super Net«:**
  - »Super Nets« dienen der logischen Gruppierung von Sektornetzwerken.
  - Im zentralen Management werden 10 solcher »Super Nets« eingerichtet, die jeweils den IP-Adressbereich der 45 Subnetze eines IP-Netzwerkes N abbilden.
  - »Super Nets« werden in virtuellen Verbindungen genutzt.
  - Ihre Bezeichnung beginnt mit »S-<sector id>-«.
  - Die Organisationseinheit ist <sector id>, z.B. S_NET_A für Supersektor von A.
  - Um einen Sektor zu beschreiben, sollen so wenige »Super Nets« wie möglich verwendet werden.

Abb. 13.7: Symbol für ein »Super Net«

In Abbildung 13.8 wird aufgezeigt, wie das Gesamtbild des VPN-Netzwerks mithilfe von »virtuellen Komponenten« beschrieben werden kann.

Wie groß ist die Anzahl der benötigten Regeln [R] bei Verwendung »virtueller Komponenten«?

Aus der Sicht eines VPN-Gateways muss für jedes vorhandene »Super Net« eine Regel eingetragen werden (z.B. »Subnetz_X darf mit dem Super Net in verschlüsselter Form kommunizieren«).

Wird das VPN-Netzwerk aus dem oben genannten Beispiel (10 IP-Netzwerke [N] mit jeweils 45 Subnetzwerken [S], insgesamt 450 VPN-Gateways, Kommunikation zwischen allen Netzwerken bzw. Subnetzwerken nur in verschlüsselter Form erlaubt) mithilfe virtueller Komponenten eingerichtet, errechnet sich die Summe aller benötigten Regeln folgendermaßen:

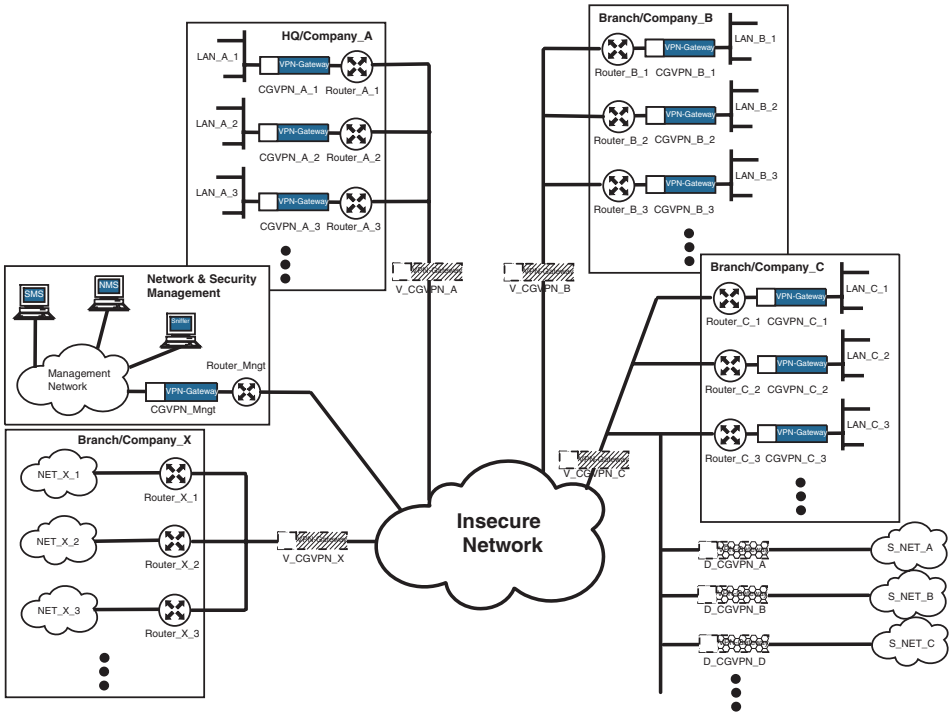

Abb. 13.8: Beschreibung eines großen VPN-Netzwerks mithilfe »virtueller Komponenten«

$\mathbf{R_2}$ = S*N = 450*10 = **4 500**

Ergebnis:

R_1/R_2 = 0,044 = **4,4 %**

Vergleicht man die beiden Varianten, so reduziert sich in diesem Beispiel die Anzahl der notwendigen Regeln bei Verwendung »virtueller Komponenten« auf nur 4,4 % gegenüber der ersten Variante.

Abbildung 13.9 verdeutlicht die Komplexität des Regelwerks. Mit einem zentralen Sicherheitsmanagement, das das oben beschriebene Verfahren unterstützt, und den Hilfsmitteln »Virtual Boxes«, »Dummy Boxes« und »Super Nets« kann die Anzahl der notwendigen Regeln deutlich reduziert werden. Auch komplexe VPN-Netzwerke können auf diese Weise einfacher verwaltet werden.

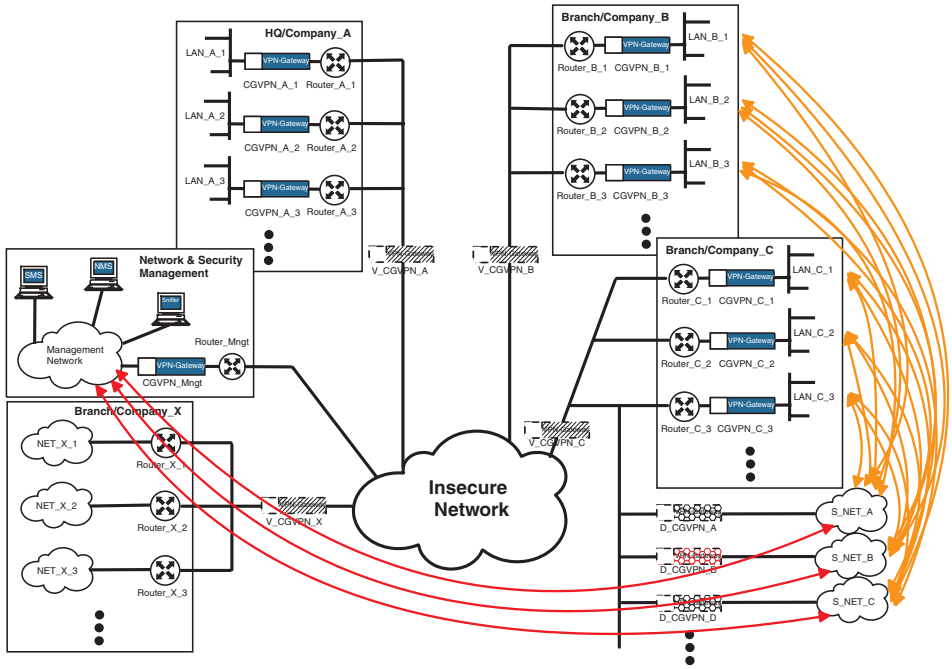

Abb. 13.9: Durch »virtuelle Komponenten« reduzierte Komplexität des Regelwerks

13.5 Zukünftige Entwicklungen bei VPN-Systemen

VPN-Systeme werden sich, wie auch die Kommunikationsanwendungen selbst, in Zukunft weiterentwickeln. In diesem Abschnitt werden schlaglichtartig einige heute schon absehbare Entwicklungen beschrieben.

Innovationen im Bereich der Internet-Anwendungen

Der Bereich der Internet-Anwendungen entwickelt sich ständig weiter. Dementsprechend müssen neue Wege gefunden werden, die VPN-Systeme schnell, dynamisch und ohne Sicherheitsverluste den neuen Anforderungen anzupassen.

Zunahme von Geschwindigkeit und Schutzbedarf

Immer mehr Geschäftsprozesse werden über Kommunikationssysteme abgewickelt. Der Umfang der ausgetauschten Informationen steigt damit stetig. Deshalb werden in naher Zukunft höhere Bandbreiten benötigt, die sich je nach Einsatzzweck unterscheiden werden: Für öffentliche Anschlüsse werden sie zunächst bei 34 bzw. 155 MBit/s, später bei 622 MBit/s liegen, im lokalen Bereich mit Fast Ethernet bei 100 MBit/s, bei Gigabit Ethernet bis zu 1 GBit/s. Um derart hohe Datendurchsätze bewältigen zu können, müssen VPN-Systeme entsprechende Geschwindig-

keiten erbringen. Zugleich wird die Menge der übertragenen und verarbeiteten Informationen mit hohem bis sehr hohem Schutzbedarf steigen.

Damit die zukünftigen Anforderungen an Geschwindigkeit und Schutzbedarf erfüllt werden können, müssen Konzepte erarbeitet werden, wie beispielsweise IPSec-Funktionalitäten optimiert und sicher in Hardwarekomponenten integriert werden können.

Sicherheit als Dienstleistung

Um Sicherheit als Dienstleistung anbieten zu können, wird neben Clustering und Loadbalancing zur Steigerung der Übertragungsraten auch eine Steigerung der Verfügbarkeit von VPN-Systemen (High Availability) erforderlich sein.

Secure Multicast and Group Communication

Eine Herausforderung für VPN-Systeme stellt aus heutiger Sicht unter anderem das Thema »Secure Multicast and Group Communication« dar. Eine Vielzahl neuer Anwendungen, die in Zukunft auch durch VPN-Systeme abgesichert werden sollen (z. B. Multimedia-Anwendungen wie Video-Konferenzen), basieren auf Multicast-Kommunikation (»one-to-many«).

Integratives zentrales Management aller Sicherheitsmechanismen

Damit ein Höchstmaß an Sicherheit garantiert werden kann, wird es in Zukunft immer wichtiger sein, dass unterschiedliche Sicherheitsmechanismen in ein Gesamtsystem mit einem zentralen Sicherheitsmanagement integriert werden können.

Universelle Identifikations- und Authentikationsverfahren

Auf Grundlage des Signaturgesetzes wird in Europa eine Sicherheitsinfrastruktur aufgebaut, die zum Vorbild einer weltweiten Regelung werden könnte. Diese Infrastruktur macht Zertifikate (»elektronische Ausweise«) mit öffentlichen Schlüsseln für alle verfügbar und sorgt für eine eindeutige Identifikation aller Beteiligten. Die Zertifikate der Teilnehmer sind bei den öffentlichen Zertifizierungsinstanzen (TrustCenter) zugänglich und können durch eine einfache Abfrage überprüft werden.

Damit ist es möglich, ein einheitliches Identifikations- und Authentikationsverfahren unter anderem für VPN-Systeme, Rechnersysteme, den Zugang zu Gebäuden etc. zu verwenden. Mit der Chipkarte, über die jeder Teilnehmer dieser Infrastruktur verfügt, kann die Identifikation und Authentikation gegenüber den verschiedenen Systemen durchgeführt werden, wodurch sich wesentliche Vereinfachungen erreichen lassen.

Interoperabilität (IPSec, PKI usw.)

Da die Notwendigkeit sicherer Kommunikation zwischen unterschiedlichen Organisationen immer weiter zunimmt, müssen die bestehenden Interoperabilitätsprobleme dringend gelöst werden. Aus technischer Sicht muss dazu die Kompatibilität der verwendeten Standards (z. B. IPSec) sowie der Sicherheits-Token (z. B. Smart-Cards für unterschiedliche Anwendungen) sichergestellt werden. Zunehmend ist auch die Kompatibilität der Sicherheitsmanagement-Systeme von Bedeutung, damit Sicherheitskomponenten verschiedener Hersteller im Verbund betrieben werden können. In organisatorischer Hinsicht ist die Interoperabilität zwischen verschiedenen Public-Key-Infrastrukturen ein wesentlicher Faktor.

Einen pragmatischen Lösungsansatz auf der technischen Ebene zeigt die Spezifikation »ISIS-MTT«. Auf der organisatorischen Ebene verfolgt die Initiative »European Bridge-CA« das Ziel, eine »Brücke des Vertrauens« zwischen verschiedenen PKIs weltweit herzustellen. Dazu definiert sie Mindestanforderungen an die Policy und die eingesetzte Technik, die eine sichere Kommunikation über organisatorische Grenzen hinweg erlauben.