Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

BSI-Standards zur Internet-Sicherheit (ISi-S)

Version 2.1 vom 26.08.2014

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände findet man auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de Internet

Bundesamt für Sicherheit in der Informationstechnik

ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Nahezu alle Institutionen sind inzwischen auf eine funktionierende IT-Infrastruktur angewiesen. Aus den meisten Arbeitsbereichen sind PCs und andere IT-Geräte nicht mehr wegzudenken. Neben den direkt sichtbaren Geräten wie Arbeitsplatz-PCs, Druckern oder Datei-Servern, gehören zu einem lokalen Netz (LAN) noch viele weitere Komponenten, die oft nur im Hintergrund bleiben, jedoch wichtige Basisdienste für den reibungslosen Betrieb zur Verfügung stellen.

In der Regel soll das eigene LAN mit dem Internet verbunden werden, um Dienste wie WWW und E-Mail nutzen zu können. Der Schritt das eigene Netz ans Internet anzuschließen geht jedoch mit vielen Risiken einher, da man sein eigenes Netz von außen angreifbar macht. Eine Beschränkung und Kontrolle der ein- und ausgehenden Verbindungen ist daher unerlässlich.

Diese Studie gibt Empfehlungen zur Strukturierung des eigenen Netzes und zum Aufbau eines Sicherheits-Gateways, um die Gefährdungen für das Netz durch eine Internet-Anbindung überschaubar zu halten. Die dazu notwendigen Grundlagen, Techniken und Protokolle werden in den Abschnitten 2 und 4 erläutert. Abschnitt 3 stellt ausführlich ein Thema dar, das in den kommenden Jahren viel an Bedeutung gewinnen wird: IPv6.

Der Wechsel von IPv4 zu IPv6 betrifft sowohl den Aufbau des eigenen LAN als auch die Anbindung an das Internet:

- Im internen Netz ermöglicht IPv6 einen sehr viel strukturierteren Aufbau.
- Die Internet-Anbindung muss mittelfristig sowohl mit IPv4 als auch IPv6 erfolgen.
- Werden eigene Dienste im Internet angeboten, so müssen diese auch über IPv6 erreichbar gemacht werden.

Die Einführung von IPv6 erfordert Einarbeitung und personelle Ressourcen. Insbesondere der in der Übergangszeit in einigen Bereichen notwendige Parallelbetrieb und die Pflege der Filterregeln im Sicherheits-Gateway verursacht zusätzliche Aufwände.

Abschnitt 5 stellt eine sichere Grundarchitektur für ein lokales Netz mit Internet-Anbindung vor. Dabei sind die neuen Möglichkeiten, die IPv6 bietet, bereits berücksichtigt. Hinweise zur Auswahl, zur Konfiguration und zum Betrieb der in der Grundarchitektur verwendeten Komponenten finden sich im Abschnitt 6.

Die vorgestellte Grundarchitektur wird in Abschnitt 7 den Gefährdungen gegenüber gestellt, denen ein Netz ausgesetzt ist. Viele dieser Gefährdungen lassen sich durch die Grundarchitektur auf ein vertretbares Maß reduzieren. Häufig verbleibt jedoch ein Restrisiko, dem bei besonderen Anforderungen an den Schutzbedarf mit zusätzlichen Maßnahmen begegnet werden kann. Solche Varianten der Grundarchitektur werden ebenfalls in Abschnitt 7 aufgeführt.

2 Grundlagen Rechnernetze

Dieser Abschnitt umreißt die grundlegenden Protokolle, Dienste und Technologien, die zur Beschreibung einer sicheren Grundarchitektur für lokale Netze mit Internet-Anbindung und den damit einhergehenden Gefährdungen relevant sind.

2.1 Netzprotokolle

Das Internet-Protokoll (IP) ist das grundlegende Kommunikationsprotokoll in modernen Rechnernetzen. Es ist Teil einer umfassenderen Protokollfamilie. Das TCP/IP-Referenzmodell, benannt nach den beiden vorherrschenden Protokollen der IP-Familie, beschreibt den Aufbau und das Zusammenwirken dieser Protokolle und gliedert sie in vier aufeinander aufbauende Schichten. Tabelle 1 zeigt die vier Protokollschichten des TCP/IP-Referenzmodells und deren Entsprechungen im OSI-Schichtenmodell, einem feineren, von der ISO standardisierten siebenschichtigen Modell.

TCP/IP-Referenz-modell	*Funktion*	*OSI-Schichtenmodell*	*Beispiele*
Anwendungs-schicht	umfasst alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten und anwendungsspezifische Daten austauschen	Schicht 5-7	HTTP, SMTP
Transport-schicht	stellt eine Ende-zu-Ende-Verbindung zwischen Prozessen her. Das wichtigste Protokoll dieser Schicht ist das Transmission Control Protocol (TCP) für das zuverlässige Übermitteln von Datenströmen.	Schicht 4	TCP, UDP
Internet-Schicht	zuständig für die Weitervermittlung von Datenpaketen zwischen den Netzknoten und die Wegewahl (Routing). Die Aufgabe dieser Schicht ist es, zu einem empfangenen Paket das nächste Zwischenziel zu ermitteln und das Paket dorthin weiterzuleiten. Kern dieser Schicht ist das Internet-Protokoll (IP).	Schicht 3	IPv4, IPv6
Netzzugangs-schicht	im TCP/IP-Referenzmodell spezifiziert, enthält jedoch keine Protokolle der TCP/IP-Familie, sondern fasst die verschiedenen Techniken zur Datenübertragung zusammen (z. B. Ethernet, FDDI, WLAN)	Schicht 1-2	Ethernet

Tabelle 1: TCP/IP-Referenzmodell und OSI-Schichtenmodell in der Gegenüberstellung

2.1.1 Grundlegende Netzprotokolle

Die Kommunikation im Internet wird maßgeblich von wenigen, grundlegenden Protokollen bestimmt. Im Folgenden werden diese Protokolle mit ihren wesentlichen sicherheitsrelevanten Eigen-

schaften kurz vorgestellt. Abbildung 2.1 zeigt im Überblick, wie sich die Protokolle in das TCP/IP-Referenzmodell einordnen.

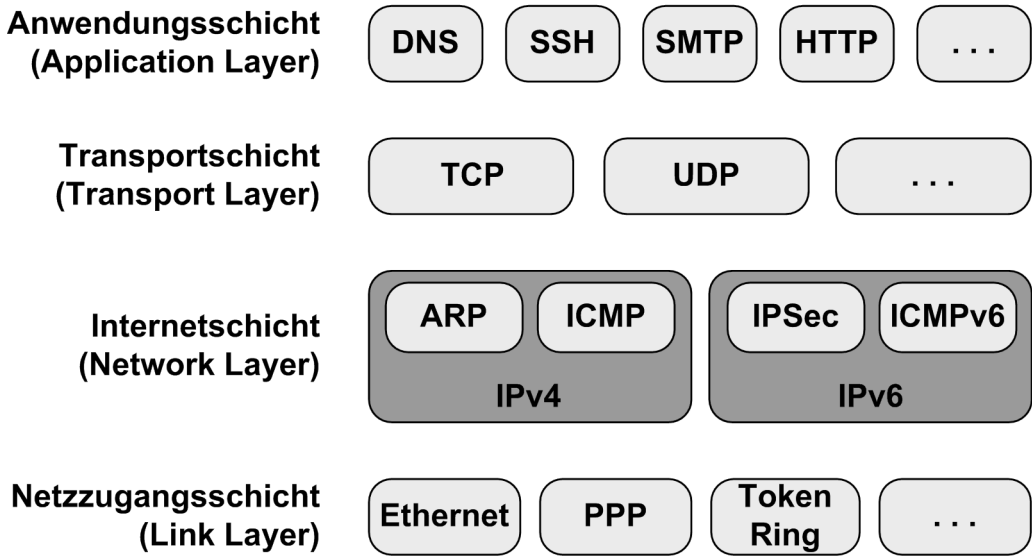

Abbildung 2.1: Protokollschichten nach dem TCP/IP-Model

ARP

Das Address Resolution Protocol dient der Abbildung von Adressen der Internet-Schicht (IP-Adressen) auf Adressen der Netzzugangsschicht (MAC-Adressen). Dazu wird ein ARP Request für die gewünschte IP-Zieladresse als Broadcast auf der Netzzugangsschicht ausgesendet. Das angesprochene Gerät in der Broadcast-Domäne beantwortet die Anfrage mit einem ARP Response, der die gesuchte MAC-Adresse enthält. Unbeteiligte Geräte in der gleichen Broadcast-Domäne aktualisieren anhand der mitgelesenen ARP-Nachrichten ihre lokale Adress-Zuordnungstabelle (ARP Table).

ARP-Nachrichten sind unverschlüsselt und ungesichert. Daher kann ein Angreifer falsche ARP-Nachrichten streuen, um fehlerhafte Adresszuordnung zu erzwingen. Er kann so Protokollnachrichten der Internet-Schicht fehlleiten oder abfangen.

Bei IPv6 wird ARP durch einen neuen Mechanismus namens Neighbor Discovery ersetzt (siehe Abschnitt 3.5.3).

IPv4/IPv6

Das Internet Protocol Version 4 (IPv4) ist ein paketvermittelndes Protokoll der Internet-Schicht für die Punkt-zu-Punkt- oder Punkt-zu-Mehrpunkt-Übermittlung von Daten zwischen Rechnern ohne vorherigen Verbindungsaufbau. Es bildet die Grundlage der Internet-Datenkommunikation. IPv4 verfügt nicht über Verlässlichkeits- oder Flusssteuerungsmechanismen, sondern überlässt den Schutz vor Verlust, Duplizierung oder Vertauschung von Paketen der Transportschicht.

Die Kopfdaten eines IP-Pakets enthalten Quell- und Zieladresse. Dies ermöglicht eine ursprungs- oder zielbezogene Filterung von IP-Verkehr.

Das Internet Protocol Version 6 (IPv6) ist die Nachfolgeversion von IPv4 und wird dieses ablösen. Die Grundlagen von IPv6 sind ausführlich in Abschnitt 3 beschrieben. Eine Erweiterung, die IPv6 mit sich bringt, ist IPSec, das aber ebenfalls für IPv4 verfügbar ist.

IPSec

Internet Protocol Secure ist der Sammelbegriff für die Sicherheitserweiterungen des Internet-Protokolls zum Schutz der übertragenen Daten vor dem Verlust von Vertraulichkeit, Integrität und Authentizität. Die Sicherungsdienste von IPSec werden durch zwei zusätzliche Header realisiert. Der *Authentication Header* (AH) schützt die Nutzdaten sowie invariante Kopfdaten des IP-Pakets gegen Verfälschung. Der *Encapsulating Security Payload Header* (ESP) dient der Verschlüsselung der Nutzdaten. Zur Absicherung von IP-Datagrammen können AH und ESP Header einzeln oder gemeinsam verwendet werden. Gesicherte Kommunikation ist in den beiden Betriebsarten Transport Mode (ungeschützte Kopfdaten) oder Tunnel Mode (geschützte Kopfdaten) mit unterschiedlichen kryptografischen Algorithmen möglich.

Darüber hinaus umfasst IPSec auch Methoden für den Austausch von Protokollparametern und Schlüsseln (Internet Key Exchange, IKE). Verbindungsparameter der Kommunikations-Endpunkte werden als Security Association (SA) ausgehandelt und verwaltet.

ICMP

Das Internet Control Message Protocol transportiert Fehler- und Diagnose-Informationen für IPv4 und in der neueren Version auch für IPv6. Es wird auch zur Steuerung von TCP- und UDP-Verbindungen genutzt.

ICMP ist ein verbindungsloses Protokoll, das mittels IP-Datagrammen übertragen wird. Es verfügt über keinerlei Mechanismen zur Authentisierung, Verschlüsselung oder Integritätssicherung, daher sind ICMP-Nachrichten leicht angreifbar. Durch Einschleusen bestimmter ICMP-Nachrichten kann ein Angreifer die Verfügbarkeit der IP-Kommunikation gefährden oder die Struktur eines Netzes ausspähen.

ICMP-Nachrichten lassen sich anhand ihres Nachrichtentyps unterscheiden und selektiv sperren. Da Paketfilter ICMP oft nur zustandslos behandeln, ist eine genaue Filterung komplexer ICMP-Transaktionen zum Schutz gegen Angriffe allerdings nur eingeschränkt möglich.

Bei IPv6 kommt ICMP eine größere Bedeutung zu als bei IPv4 (siehe Abschnitt 3.5.1).

TCP

Das Transmission Control Protocol ist ein verbindungsorientiertes Protokoll der Transportschicht. Durch Transportquittungen und Flusskontrolle gewährleistet es eine korrekte, vollständige, duplikatfreie und reihenfolge-erhaltende Übertragung von Daten zwischen Diensten der Anwendungsschicht. Quell- und Zielanwendung sind in den Kopfdaten eines TCP-Pakets durch die IP-Adresse und TCP-Portnummer des jeweiligen Kommunikationspartners bezeichnet.

TCP ist unverschlüsselt und hat keine Mechanismen zur Authentisierung oder Integritätssicherung. TCP-Sequenznummern bieten (schwachen) Schutz gegen eine Unterwanderung des Protokolls durch Außenstehende. Der Verbindungsaufbau (Drei-Wege-Handshake), der jeder Datenübertragung vorausgehen muss, ermöglicht eine zustandsbehaftete, gerichtete und anwendungsbezogene Filterung von TCP-Verbindungen anhand der im Paket-Header enthaltenen TCP-Flags, IP-Adressen und Portnummern. Unvollständige Drei-Wege-Handshakes binden beim Empfänger Ressourcen und können daher gezielt als Mittel für Angriffe auf die Verfügbarkeit eines Systems genutzt werden.

Ganz grundsätzlich kann eine TCP-Verbindung verschiedene Zustände haben. Dabei können auch inaktive, eigentlich geschlossene Verbindungen noch Ressourcen auf dem Rechner verbrauchen (z.B. Zustand `TIME-WAIT`, `FIN_WAIT`). Diese Eigenschaft wird u.a. bei DoS-Attacken verwendet.

UDP

Das User Datagram Protocol ist ein verbindungsloses Protokoll der Transportschicht. Anders als TCP sieht es weder Transportquittungen noch andere Mechanismen zur Sicherung der Übertragung vor. Die Kontrolle darüber wird der Anwendung überlassen. Der Header enthält wie bei TCP zwei Portnummern, die eine Zuordnung zu Diensten der Anwendungsschicht ermöglichen. Der Aufwand zur Verarbeitung eines Datenpakets ist bei UDP geringer als bei TCP. Der Effizienzgewinn wird jedoch durch mehrere Nachteile erkauft, wie etwa eine höhere Wahrscheinlichkeit für Paketverluste.

UDP ist unverschlüsselt und bietet keine Mechanismen zur Authentisierung oder Integritätssicherung. UDP-Datagramme lassen sich anhand ihrer IP-Quell- und -Zieladresse sowie anhand der UDP-Portnummern anwendungsbezogen filtern. Eine zustandsbehaftete Filterung ist aufgrund der verbindungslosen Funktionsweise nur mittels dynamischer Zeitfenster realisierbar.

SSL/TLS

Transport Layer Security (TLS) ist ein verbindungsorientiertes Protokoll für die authentisierte, integritätsgesicherte und vertrauliche Übertragung von Daten. TLS bietet eine anwendungsunabhängige, sichere Transportverbindung, basierend auf verschiedenen Verschlüsselungsalgorithmen mit unterschiedlicher Stärke. Es dient vor allem als sicheres Transportprotokoll für HTTP, aber auch zur sicheren Übertragung anderer TCP-basierter Protokolle (z. B. POP3, IMAP). Transport Layer Security Version 1.0 ist die standardisierte, leicht modifizierte Version von seinem Vorgängerprotokoll Secure Socket Layer (SSL) in der Version 3.0.

TLS ermöglicht das Aushandeln von Sitzungsparametern, insbesondere die Festlegung der Kryptoverfahren und Sitzungsschlüssel sowie den Austausch von Authentisierungszertifikaten. Bei unzureichender Prüfung der Server- oder Client-Zertifikate besteht jedoch die Gefahr von Man-in-the-Middle-Angriffen.

Der Sitzungsschlüssel wird durch ein Schlüsselaustauschprotokoll ausgehandelt. Bei TLS sind unter anderem RSA und Diffie-Hellman (DH) üblich. Der Vorteil des Diffie-Hellman-Schlüsseltausch ist, dass der Sitzungsschlüssel nie übertragen werden muss. Dadurch kann ein Angreifer den Inhalt der Nachrichten selbst dann nicht entschlüsseln, wenn er die gesamte Kommunikation abhört.

Eine weitere Eigenschaft von Schlüsselaustauschprotokollen ist *Perfect Forward Secrecy*. Diese Eigenschaft stellt sicher, dass eine aufgezeichnete Kommunikation im Nachhinein nicht entschlüsselt werden kann. Dies wird über Diffie-Hellman-basierte Verfahren erreicht, bei denen flüchtige (engl. ephemeral) Parameter verwendet werden (DHE). Eine Liste kryptografischer Verfahren, die Perfect Forward Secrecy unterstützen, findet sich in der Technischen Richtlinie des BSI zu TLS [TR-TLS].

Tabelle 2 gibt einen Überblick über die zuvor beschriebenen Protokolle und deren Sicherheitseigenschaften.

Protokoll	*Sicherheitseigenschaften*			*Referenz*
	Authentisierung	*Integri-täts-Sicherung*	*Verschlüsselung*	
ARP	-	-	-	[RFC 826]
IPv4	-	-	-	[RFC 791]
IPv6	x (mittels IPSec)	x (mittels IPSec)	x (mittels IPSec)	[RFC 2460]
IPSec	x	x	x	[RFC 4301]
ICMP	-	-	-	[RFC 792]
TCP	-	-	-	[RFC 793]
UDP	-	-	-	[RFC 768]
TLS 1.1, 1.2	x	x	x	[RFC 4364], [RFC 5246]

Tabelle 2: Grundlegende Netzprotokolle und ihre Sicherheitseigenschaften

2.1.2 Basis-Dienste und grundlegende Netzmanagement-Protokolle

DHCP

Das Dynamic Host Configuration Protocol ist ein verbindungsloses Protokoll der Anwendungsschicht, um Rechnern dynamisch IP-Adressen und weitere Konfigurationsparameter (z. B. Subnetz-Maske, Standard-Gateway, zuständiger DNS-Server) zuzuweisen. Es ermöglicht die Integration neuer Rechner in ein Netz ohne besondere Konfigurationsvorbereitungen. Dazu fragt der DHCP Client per Broadcast an Port 67/UDP nach Konfigurationsinformationen. Jeder erreichbare DHCPServer sendet seinen Konfigurationsvorschlag als Broadcast an Port 68/UDP. Der Client wählt eine der Antworten aus und quittiert diese, alle übrigen DHCP-Angebote verfallen.

DHCP für IPv4 bietet keine Mechanismen für Authentisierung, Integritätssicherung oder Verschlüsselung. DHCPv6 für IPv6 über Port 546/UDP und Port 547/UDP ermöglicht hingegen Authentisierung, Integritätssicherung und Replay-Erkennung zur gesicherten Kommunikation, ist jedoch ebenfalls unverschlüsselt. Falsche DHCP-Nachrichten können zu Störungen bei den angeschlossenen Clients führen, zum Beispiel durch die Verbreitung falscher Routing- bzw. DNS-Informationen. Dadurch kann die Kommunikation umgelenkt, verhindert oder verfälscht werden. Böswillige Clients können durch wiederholte DHCP-Anfragen Adressreservierungen anhäufen, um durch Verknappung freier IP-Adressen die Verfügbarkeit des Netzes für andere Rechner zu beeinträchtigen.

Im manuellen DHCP-Modus ist eine statische Zuordnung von IP-Adressen zu MAC-Adressen der DHCP-Clients möglich, um nicht autorisierten Clients einen Zugang zu erschweren. Im dynamischen Modus bietet die zeitlich befristete Zuweisung von IP-Adressen Schutz gegen das böswillige Horten von Adressen.

DNS

Das Domain Name System ist ein verteilter Dienst der Anwendungsschicht, der die Zuordnung von alphanumerischen Adressnamen zu numerischen Adressen (z. B. www.bsi.bund.de zu 194.95.177.86) verwaltet und zwischen den beiden Adressformaten übersetzt. Ursprünglich für die

Abbildung von Domain-Namen auf IP-Adressen konzipiert, kann DNS auch für andere Verzeichnisse verwendet werden, etwa zur Verwaltung von IP-Telefonnummern.

DNS bildet einen hierarchischen Namensraum, der durch eine entsprechende Hierarchie von DNS-Servern verwaltet wird. Der Namensraum ist in Zonen unterteilt. Jede Zone bildet einen unabhängigen Administrationsbereich mit einem verantwortlichen Name Server (DNS Primary). Das DNS-Protokoll nutzt Port 53/TCP für den Datenaustausch zwischen DNS-Servern (Zonentransfer). Für DNS-Anfragen nutzen Clients ein verbindungsloses Protokoll über Port 53/UDP. Alternativ ist auch Port 53/TCP nutzbar, dies ist jedoch ungebräuchlich.

Der verantwortliche DNS Primary gibt an nachgeordnete Server DNS-Informationen mit beschränkter Gültigkeitsdauer (Time to Live, TTL) weiter. Diese hierarchisch gestaffelten Server puffern DNS-Datensätze, wobei jedoch nicht alle Server die TTL korrekt beachten. Kann ein Server die Anfrage eines Clients nicht lokal auflösen, leitet er die Anfrage an übergeordnete DNS-Server weiter.

Das DNS-Protokoll ist ungesichert. Es bietet nur die Filtermöglichkeiten von TCP bzw. UDP. Falsche DNS-Informationen können genutzt werden, um in die Rolle fremder Server zu schlüpfen oder den Kommunikationsaufbau zu stören. Vorschläge für eine kryptografische Sicherung der DNS-Kommunikation existieren, sind aber noch wenig verbreitet. Inzwischen hat sich die Sicherheits-Erweiterung DNSSEC (DNS Security Extensions) [RFC 4033] etabliert, so dass im Internet Mechanismen zur Authentisierung und Integritätssicherung des DNS-Protokolls bestehen.

Mittels DANE (DNS-Based Authentication of Named Entities) [RFC 6698] besteht zudem die Möglichkeit Zertifikate für Web- und E-Mail-Server im DNS zu hinterlegen oder bestimmte Trust Anchors zu definieren. Voraussetzung für DANE ist, dass die Domain per DNSSEC signiert ist. So können Angriffe, die auf kompromittierten Zertifikaten beruhen, ausgeschlossen werden.

NTP

Das Network Time Protocol ist ein verbindungsloses Protokoll der Anwendungsschicht zum Synchronisieren von Rechnern in IP-Netzen. Als Trägerprotokoll auf Transportschicht dient UDP. Die Protokollversion NTPv4 ist in [RFC 5905] spezifiziert. Das Protokoll basiert auf einer Hierarchie von Zeitservern; die ranghöchsten Server (Stratum 1) nutzen in der Regel eine hochgenaue externe Zeitquelle (z. B. DCF77). NTP-Clients passen ihre lokale Uhr in Phase und Frequenz an die Synchronisationssignale des Servers an und erzielen damit eine Synchronisationsgenauigkeit im Millisekunden-Bereich.

NTP-Instanzen können in den Betriebsarten Client (nur Synchronisationsempfänger), Server (beantwortet nur Synchronisationsanfragen von Clients), Peer (gegenseitige Peer-Synchronisation) oder Broadcast (periodisches, ungefragtes Aussenden von Synchronisationsinformation) betrieben werden. Eine Filterung von NTP-Nachrichten ist auf Basis der UDP-Quell- und -Zieldresse sowie anhand des Betriebsmodus möglich. NTP bietet Mechanismen zur Sicherung der Integrität und der Authentizität der Protokollnachrichten. Eine Störung des Protokolls könnte die Synchronisation aufheben, was z. B. eine Logdatenauswertung oder das Erkennen abgelaufener Schlüssel oder Zertifikate erschwert.

SNMP

Das Simple Network Management Protocol ist ein verbindungsloses Protokoll der Anwendungsschicht. Es dient dem Austausch von Konfigurations- und Zustandsinformationen zwischen SNMP-Agents (Client) und Netzmanagement-Systemen (Server). Agent bezeichnet die SNMP-Instanz auf dem überwachten Gerät, die in einer hierarchischen Management Information

Base (MIB) Geräteparameter verwaltet. Der SNMP-Manager kann MIB-Einträge mittels Anfragen an den Agenten (über Port 162/UDP) auslesen oder aktualisieren. Darüber hinaus kann ein Agent auch ungefragt spontane Meldungen (sogenannte Traps) an Port 162/UDP des Managers senden.

SNMPv1 und SNMPv2c bieten nur rudimentären Zugriffsschutz durch sogenannte Community Strings, jedoch keinerlei Mechanismen zur Authentisierung, Integritätssicherung oder Verschlüsselung der SNMP-Nachrichten. SNMPv2p und SNMPv2u sind experimentelle, in der Praxis nicht gebräuchliche Protokollversionen. SNMPv3 unterstützt Authentisierung, Verschlüsselung und Integritätssicherung mittels Keyed-Hash Message Authentication Code (HMAC-MD5, HMAC-SHA) sowie eine rollenbasierte Zugriffskontrolle. Eine Filterung des Protokolls ist anhand der UDP-Quell- und Zieladressen möglich.

RADIUS

Der Remote Authentication Dial-in User Service ist ein Dienst zur Authentisierung, Autorisierung und zum Abrechnen (Accounting) von Client-Zugriffen auf IT-Systeme mittels eines zentralen Servers. Darüber hinaus kann RADIUS einem Client bei der Anmeldung allgemeine Konfigurationsparameter zuteilen. Um einen Zugriff zu erhalten, sendet der Client auf der Anwendungsschicht seine relevanten Zugangsdaten (z. B. Benutzer-Kennung, Passwort-Hash, Portnummer) an einen RADIUS-Server. Der Server vergleicht die Angaben mit hinterlegten Zugriffskriterien; gegebenenfalls fordert er vom Client eine erneute Authentisierung (Challenge-Response-Verfahren). Bei positiver Überprüfung erhält der Client die Zugriffsberechtigung mit den dazu erforderlichen Konfigurationsparametern.

Das RADIUS-Protokoll für die Client-Server-Kommunikation ist ein verbindungsloses Protokoll der Anwendungsschicht. Es nutzt auf der Transportschicht den Server-Port 1812/UDP. RADIUS-Nachrichten werden im Grundsatz unverschlüsselt übertragen, nur kritische Parameter sind verschlüsselt. Für Client-Anfragen (Access Requests) bietet das Protokoll weder Authentisierung noch Integritätssicherung, die Antworten des RADIUS-Servers sind jedoch authentisiert und gegen Verfälschung geschützt. Bei schlecht gewählten Client- oder Authentisierungs-Passwörtern besteht die Gefahr sogenannter Wörterbuch-Angriffe, sofern ein Angreifer die RADIUS-Kommunikation mitlesen kann.

SSH/SCP/SFTP

Secure Shell basiert auf einem verbindungsorientierten Protokoll der Anwendungsschicht, das authentisierte, integritätsgesicherte und verschlüsselte Verbindungen zwischen zwei Rechnern herstellt. Das Protokoll unterstützt diverse Verschlüsselungsalgorithmen, Authentisierungsverfahren und Schlüsselformate. Auf Transportschicht wird die Verbindung zu Port 22/TCP des Zielrechners aufgebaut.

Das grundlegende SSH-Protokoll dient zur Realisierung verschiedener Anwendungsdienste:

- Secure Shell (SSH) als sicherer Ersatz für ungesicherte Dienste wie etwa Telnet, rlogin, oder rsh;
- Secure Copy (SCP) als Ersatz für unverschlüsseltes rcp;
- SSH File Transfer Protocol[1] (SFTP) als Ersatz für unverschlüsseltes FTP.

Darüber hinaus ermöglicht das SSH-Protokoll die Übertragung beliebiger TCP/IP-Verbindungen in einem verschlüsselten Kommunikationskanal (z. B. Port Forwarding, X11 Forwarding).

1 Achtung: SFTP darf nicht mit dem weniger sicheren Secure FTP verwechselt werden. SFTP verschlüsselt bei einem Dateitransfer sowohl den Steuerkanal als auch die Nutzdaten, während bei Secure FTP lediglich der Steuerkanal mittels SSH-Protokoll verschlüsselt wird, der Nutzdatenkanal jedoch nicht.

Version 1 des SSH-Protokolls (SSH-1) enthält Sicherheitsschwächen, die mit SSH-2 behoben wurden.

Telnet

Das Teletype Network ermöglicht eine verbindungsorientierte, bidirektionale, zeichenbasierte Kommunikation zwischen sogenannten Network Virtual Terminals. Das Telnet-Protokoll wird vor allem zur Realisierung des Telnet-Dienstes genutzt, der den Zugriff auf eine Kommando-zeilen-Schnittstelle des Zielrechners ermöglicht. Der Telnet-Dienst ist über Port 23/TCP erreichbar.

Das Telnet-Protokoll überträgt Nutzdaten mit eingestreuten Steuerzeichen unverschlüsselt und ungesichert. Der Telnet-Dienst authentisiert den Client zwar über Benutzer-Kennung und Passwort, überträgt diese Information jedoch unverschlüsselt. Generell sollte diese Anwendung nicht mehr verwendet werden, da meist eine bessere Alternative (z. B. SSH-2) verfügbar ist.

FTP/TFTP

Das File Transfer Protocol ist ein verbindungsorientiertes Client-Server-Protokoll für den einfachen Austausch von Dateien zwischen zwei Rechnern. FTP verwendet getrennte Übertragungskanäle für die Sitzungssteuerung (Port 21/TCP des Servers) und die Nutzdatenübertragung (im Active Mode Port 20/TCP des Servers). Man unterscheidet zwei Betriebsarten: Im Modus *active* eröffnet der Server die Nutzdatenverbindung von Port 20/TCP aus, was den Schutz des Servers erleichtert. Im Modus *passive* eröffnet der Client die Nutzdatenverbindung zu einem vom Server vorgegebenem Port, was den Schutz des Clients vereinfacht.

FTP selbst verfügt über keinerlei Schutzmechanismen. Der darauf basierende FTP-Dienst fordert bei Sitzungseröffnung in der Regel eine Benutzer-Kennung und ein Passwort zur Authentisierung auf der Anwendungsschicht. Wegen der textbasierten, ungesicherten Übertragung der Nachrichten bietet der Dienst jedoch keinen sicheren Schutz gegen Angriffe. In unsicheren Netzen sollte daher eine sichere Alternative (z. B. SFTP, SCP) verwendet werden.

Das Trivial File Transfer Protocol (TFTP) ist eine einfachere, verbindungslose Protokollalternative über Port 69/UDP für das Lesen und Schreiben von Dateien. Es dient hauptsächlich der Übertragung von Software-Konfigurationen auf Netzkomponenten. Da der TFTP-Dienst keinerlei Authentisierung oder Verschlüsselung vorsieht, darf er nur in sicheren Netzen verwendet werden und nur dann, wenn keine sichere Alternative verfügbar ist.

Die Filterung von FTP/TFTP ist anhand der Transportschicht-Parameter möglich. FTP-Verbindungen können zusätzlich anhand des Betriebsmodus selektiert werden.

syslog/syslog-ng

Syslog ist ein verbindungsloses, textbasiertes Anwendungsprotokoll zur Übertragung von Log-Meldungen an einen syslog-Server. Der Server ist über Port 514/UDP erreichbar. Das ursprüngliche Protokoll wurde mehrfach erweitert und ist in verschiedenen Implementierungen verbreitet. Das Nachrichtenformat des Protokolls ist daher uneinheitlich. Typische Attribute einer Nachricht sind Datum, Zeitstempel, Facility (Typ der meldenden Komponente), Priorität sowie ein frei wählbarer Meldungstext.

Syslog-ng ist eine weitverbreitete syslog-Implementierung mit einigen Erweiterungen, die wahlweise auch die Nutzung von TCP als Transportprotokoll ermöglicht.

Das syslog-Protokoll bietet keine Mechanismen zur Authentisierung oder Verschlüsselung. Wegen der ungesicherten Übertragung sollte syslog nur in sicheren Management-Netzen (out-of-band)

eingesetzt oder in einem verschlüsselten Übertragungskanal getunnelt werden, um es vor Ausspähen und Manipulation zu schützen. Derzeit sind Standardisierungsbestrebungen für sichere syslog-Varianten im Gange [Syslog], entsprechende Protokolle sind aber noch nicht etabliert.

Tabelle 3 gibt einen Überblick über die beschriebenen Protokolle und deren Sicherheitseigenschaften.

Protokoll	*Port*	*Sicherheitseigenschaften*			*Referenz*
		Authentisierung	*Integritäts-Sicherung*	*Verschlüsselung*	
DHCP	67/UDP 68/UDP	-	-	-	[RFC 2131]
DHCPv6	546/UDP 547/UDP	x	x	-	[RFC 3315]
DNS	53/UDP 53/TCP	-	-	-	[RFC 1034]
NTPv4	123/UDP	x	x	-	[RFC 5905]
SNMPv1, SNMPv2c	161/UDP 162/UDP	x (Community String)	-	-	[RFC 1157]
SNMPv3	161/UDP 162/UDP	x	x	x	[RFC 3410]
RADIUS	1812/UDP 1813/UDP	x (nur Server Response)	x (nur Server Response)	x (ausgewählte Attribute)	[RFC 2865]
SSH, SCP, SFTP	22/TCP	x	x	x	[RFC 4250]
Telnet	23/TCP	-	-	-	[RFC 854]
FTP	21/TCP 20/TCP	-	-	-	[RFC 959]
TFTP	69/UDP	-	-	-	[RFC 1350]
Syslog, syslog-ng	514/UDP 514/TCP	-	-	-	[RFC 5424]

Tabelle 3: Sicherheitseigenschaften der grundlegenden Dienste und Netzmanagement-Protokolle

2.1.3 Routing-Protokolle

Routing bezeichnet die Wegewahl in vermaschten Kommunikationsnetzen. Routing-Protokolle dienen dem Austausch von Erreichbarkeitsinformationen zwischen verschiedenen Routern. Das Verbreiten nicht autorisierter, gefälschter oder replizierter Routing-Informationen gefährdet die Funktionsfähigkeit der Internet-Schicht oder ermöglicht einem Angreifer, Datenpakete zum Ausspähen oder Manipulieren gezielt in seinen Einflussbereich umzuleiten. Darüber hinaus ermöglichen Routing-Protokolldaten Rückschlüsse auf die Struktur eines Netzes. Daher müssen Routing-Protokolle gegen Eindringen, Verfälschen und Ausspähen geschützt werden.

Um die Eignung von möglichen Routen zu bewerten, gibt es verschiedene Metriken. In die Bewertung kann sowohl die Weglänge als auch die Verbindungsgüte und die Kommunikationslast entlang der Route einfließen. Beim statischen Routing basiert die Wegewahl auf voreingestellten,

unveränderlichen Erreichbarkeitsinformationen. Beim dynamischen Routing versuchen die Router, ihre Erreichbarkeitsinformationen gemäß den beobachteten Übertragungsbedingungen zu aktualisieren, um ihre Wegewahl an Veränderungen im Netz anzupassen.

Das Internet ist in unabhängige administrative Bereiche untergliedert, die einer individuellen Routingstrategie unterliegen und nach außen als kohärente „Routing-Insel“ mit einheitlichen Routing-Eigenschaften gegenüber ihren Nachbarn erscheinen. Diese Bereiche werden auch *Autonome Systeme* genannt.

Intradomain-Routing

Intradomain-Routing bezeichnet Routing im Inneren eines einzelnen Autonomen Systems. Hierbei kommen sogenannte Interior-Gateway-Protocols (IGP) zum Einsatz. Im Vordergrund steht hier meist die technisch effiziente Nutzung des Netzes, also eine Wegewahl entlang kürzester Pfade. Typische IGP-Repräsentanten sind zum Beispiel:

- OSPF: Open Shortest Path First ist ein verbindungsloses Protokoll direkt oberhalb der Internet-Schicht (IP-Protokollnummer 89). Die Protokollnachrichten sind durch ein Klartextpasswort oder einen schlüsselabhängigen Hash-Code authentisiert und integritätsgesichert. Unter IPv6 ist eine Authentisierung und Verschlüsselung mittels IPSec möglich.
- IS-IS: Das Intermediate-System-to-Intermediate-System-Protokoll wurde ursprünglich als ISO-Standard für die Verwendung mit dem Connectionless Network Protocol (CLNP) entworfen, kann aber auch auf der Internet-Schicht aufsetzen (IP-Protokollnummer 124). IS-IS ist weniger aufwendig als OSPF. Die Protokollnachrichten sind unverschlüsselt, werden aber durch einen schlüsselabhängigen Hash-Code authentisiert und integritätsgesichert.
- RIP: Das Routing Information Protocol ist ein verbindungsloses Protokoll über Port 520/UDP, das die Wegegüte (unter IP) allein anhand der Anzahl der Netzknoten zwischen Ursprung und Ziel bewertet (Hop Count). Die Protokollversion 1 verfügt über keinerlei Authentisierungsmechanismen, Version 2 nutzt Klartext-Passwörter oder einen schlüsselabhängigen Hash-Code zur Integritätssicherung und Authentisierung. RIP ist weniger empfehlenswert als OSPF oder IS-IS (es garantiert z. B. keine Schleifenfreiheit). In einfachen, wenig gefährdeten Netzen ist RIPv2 allerdings eine leichter administrierbare und weniger ressourcenintensive Alternative zu den aufwendigeren Routing-Protokollen.
- IGRP/EIGRP: Das Interior Gateway Routing Protocol ist ein Cisco-proprietäres Protokoll, das inzwischen durch den weiterentwickelten Nachfolger, das Enhanced Interior Gateway Routing Protocol, abgelöst wurde. EIGRP nutzt auf Transportschicht das Reliable Transport Protocol (RTP, IP-Protokollnummer 88). EIGRP-Pakete werden durch schlüsselabhängige Hashcodes authentisiert und integritätsgesichert, nicht aber verschlüsselt.

Abgesehen von OSPF in Kombination mit IPSec sind die genannten Protokolle trotz Authentisierung potenziell durch Replay-Angriffe verwundbar.

Interdomain-Routing

Interdomain-Routing bezeichnet Routing über mehrere Autonome Systeme hinweg. Es verwendet sogenannte Exterior Gateway-Protokolle (EGPs). Da Interdomain-Routing das Routing zwischen verschiedenen Diensteanbietern regelt, liegt der Fokus beim Interdomain-Routing meist auf einer möglichst profitablen Nutzung des Netzes. Dazu teilt ein Autonomes System seinen Nachbarn jeweils nur ausgesuchte Informationen gemäß einer zuvor vereinbarten Routing-Strategie mit (Policy-basiertes Routing). Ein lokaler Administrator muss sich in der Regel nur insoweit mit Interdomain-Routing befassen, als die sogenannten Edge Router an der Grenze des Autonomen

Systems Routing-Informationen zwischen IGP und EGP austauschen müssen. Routing über mehrere Autonome Systeme hinweg administriert im Allgemeinen der Internet-Diensteanbieter.

Im Internet ist der de-facto-Standard für Interdomain-Routing heute BGP. Das Border Gateway Protocol Version 4 (BGPv4) ist ein verbindungsorientiertes Protokoll zum Austausch von Informationen über die Erreichbarkeit von IP-Präfixen (Netzen) und Autonomen Systemen. Dies ermöglicht unter anderem die Rekonstruktion der Verbindungstopologie der Autonomen Systeme, die Eliminierung zyklischer Routen, das Aggregieren von Routen sowie die Durchsetzung spezifischer Routing-Strategien (Policies) für ein Autonomes System. Das Protokoll nutzt eine Transportverbindung über Port 179/TCP. BGP-Nachrichten können durch eine kryptografische Prüfsumme authentisiert und integritätsgesichert werden. Die Datenpakete sind jedoch unverschlüsselt und der Empfänger ist nicht authentisiert. Dies birgt die Gefahr von Replay-Angriffen und des Ausspähens der Netztopologie. In [RFC 4272] werden die potenziellen Schwachstellen von BGPv4 im Detail erörtert.

BGP wird auch innerhalb des Autonomen Systems zwischen den Edg*e-Rou*tern verwendet, um die extern gelernten Pfadinformationen weiterzugeben. Dies nennt man iBGP (Internal BGP). Dies ist notwendig, da eine Weitergabe der BGP-Pfadinformationen von den IGP-Protokollen nicht unterstützt wird.

Tabelle 5 gibt einen Überblick über die zuvor beschriebenen Protokolle und deren Sicherheitseigenschaften.

Protokoll	***Port***	***Sicherheitseigenschaften***			***Referenz***
		Authentisierung	***Integri-täts-Sicherung***	***Ver-schlüsselung***	
OSPFv2, OSPFv3	-	x	x	IPSec für OSPFv3	[RFC 2328] [RFC 5340]
IS-IS	-	x	x	-	[RFC 1142]
RIPv1	520/UDP	-	-	-	[RFC 1058]
RIPv2	520/UDP	x	x	-	[RFC 2453]
EIGRP	-	x	x	-	Cisco proprietär
BGPv4	179/TCP	x	x	-	[RFC 4271]

Tabelle 4: Sicherheitseigenschaften der wichtigsten Routing-Protokolle

2.1.4 Protokolle zur Vermeidung redundanter Netzpfade

Um die Verfügbarkeit zu erhöhen, sollten Kommunikationsnetze über redundante physische Verbindungspfade zwischen den Netzknoten verfügen. Dabei sollte aber möglichst immer nur einer der Pfade genutzt werden, um Paketverdopplungen und Reihenfolge-Vertauschungen zu vermeiden. Zu diesem Zweck konstruieren Spanning-Tree-Protokolle in geswitchten Netzen auf der Netzzugangsschicht einen aufspannenden Baum für das Kommunikationsnetz, also eine schleifen- und redundanzfreie logische Netztopologie. Die gebräuchlichsten Protokolle sind:

- STP: Das Spanning Tree Protocol verwendet Bridge Protocol Data Units (BPDU) auf der Netzzugangsschicht. Zunächst bestimmt STP per Multicast einen Wurzelknoten, von wo aus hierarchisch ein aufspannender Baum konstruiert wird. Die Wurzel sendet periodische Alive-BPDUs. Wenn solche Nachrichten ausbleiben, gehen die Baumknoten davon aus, dass der

Spannbaum defekt ist. Dies löst eine automatische Rekonfiguration aus. Die Rekonfigurationsphase kann 30 Sekunden oder länger dauern. Während dieser Zeit ist kein Nutzdatenverkehr möglich. Daher ist STP anfällig für Angriffe auf die Verfügbarkeit durch gefälschte Rekonfigurations-BPDUs.

- RSTP: Das Rapid Spanning Tree Protocol arbeitet sehr ähnlich wie STP, nutzt aber ein erweitertes BPDU-Format, um Spannbaum-Defekte schneller zu erkennen und auch während einer Baumrekonfiguration noch Nutzdatenverkehr zu ermöglichen. Dies ermöglicht Rekonfigurationszeiten von weniger als einer Sekunde.
- MSTP: Das Multiple Spanning Tree Protocol fasst mehrere Virtuelle LANs zu Instanzen zusammen und bildet pro Instanz nur einen aufspannenden Baum. Dadurch erzielt MSTP einen verbesserten Lastausgleich zwischen Virtual LANs.

Darüber hinaus existieren weitere proprietäre Protokolle, zum Beispiel das Per VLAN Spanning Tree (PVST) Protokoll.

Die verschiedenen Varianten der Spanning Tree Protokolle nutzen BPDUs ohne Authentisierung, Integritätssicherung oder Verschlüsselung. Böswillige Clients können mittels BPDU-Manipulation oder -Unterdrückung leicht Netzausfälle provozieren oder unberechtigt in VLANs eindringen, um Nutzdatenverkehr abzuhören oder zu verfälschen. Um dies zu verhindern, können BPDUs an Endgeräte-Ports blockiert werden, was ein Eindringen von Anwendungsrechnern in Spanning-Tree-Protokolle unterbindet.

Tabelle 6 gibt einen Überblick über die zuvor beschriebenen Protokolle und deren Sicherheitseigenschaften.

Protokoll	***Sicherheitseigenschaften***			***Referenz***
	Authentisierung	***Integritäts-Sicherung***	***Verschlüsselung***	
STP	-	-	-	IEEE 802.1d
RSTP	-	-	-	IEEE 802.1w
MSTP	-	-	-	IEEE 802.1s

Tabelle 5: Sicherheitseigenschaften von Protokolle zur Vermeidung redundanter Netzpfade

2.1.5 Redundanzprotokolle

Redundanzprotokolle dienen dazu, mehrere physische Router zu einer Gruppe zusammenzuschließen, die im Netz als ein logischer virtueller Router mit einer (virtuellen) MAC- und IP-Adresse wahrgenommen wird. Ein Gruppenmitglied ist der Master der Redundanzgruppe, die übrigen Gruppenmitglieder fungieren als Backup-Systeme. Das Redundanzprotokoll sorgt dafür, dass ein Ausfall des Masters erkannt wird und ein Reservesystem dessen Rolle unter der gleichen MAC- und IP-Adresse übernimmt (dynamic fail-over). Die beiden gebräuchlichsten Redundanzprotokolle sind das Virtual Router Redundancy Protocol (VRRP) und das Hot Standby Router Protocol (HSRP).

VRRP realisiert ein verbindungsloses Election-Protokoll über IP-Multicasts (IP-Adresse 224.0.0.18), um einen eindeutigen Master innerhalb der Redundanzgruppe zu bestimmen. Frühere VRRP-Versionen [RFC 2338] verfügten über Mechanismen zur Authentisierung. Im neueren [RFC 5798] (früher auch [RFC 3768]) wurden diese Protokoll-Optionen aufgrund von Protokollschwierigkeiten jedoch wieder gestrichen.

HSRP ist eine Cisco-proprietäre Version des VRRP mit ähnlicher Funktionsweise. HSRP wird jedoch über Port 1985/UDP abgewickelt. Das Protokoll unterstützt Authentisierung und Integritätssicherung mittels eines Klartextpassworts oder seines schlüsselabhängigen Hashcodes.

Um ein Eindringen in Redundanzprotokolle zu unterbinden, sollten Protokollnachrichten an Nutzdatenports gänzlich blockiert oder anhand ihrer IP-Adresse (sowie der Portnummer bei HSRP) gefiltert werden.

Tabelle 8 gibt einen Überblick über die zuvor beschriebenen Protokolle und deren Sicherheitseigenschaften.

Protokoll	***Sicherheitseigenschaften***			***Referenz***
	Authentisierung	***Integri-täts-Sicherung***	***Verschlüsselung***	
VRRP	nur ältere VRRP-Version [RFC 2338]	nur ältere VRRP-Version [RFC 2338]	-	[RFC 5798]
HSRP	x	x	-	[RFC 2281] Cisco proprietär

Tabelle 6: Sicherheitseigenschaften von Redundanzprotokollen

2.2 Technologien und Komponenten im LAN

Ein Local Area Network (LAN) ist ein Rechnernetz, das sich über einen begrenzten Raum erstreckt. LANs kommen in Firmen und Behörden, aber auch immer häufiger im privaten Bereich zum Einsatz. Lokale Netze sind als feste Installation dort zu finden, wo mehrere Rechner über geringe Entfernungen an einem bestimmten Ort dauerhaft vernetzt werden sollen.

2.2.1 LAN-Technologien

Die Netzzugangsschicht heutiger LANs basiert meist auf der Ethernet-Technik, die andere LAN-Technologien (z. B. Token Bus, Token Ring, ATM) zunehmend in Nischenanwendungen zurückgedrängt hat (z. B. FDDI für hohe Verfügbarkeitsansprüche).

Nach dem ursprünglichen Funktionsprinzip eines Ethernets senden Teilnehmer ihre Datenpakete über ein gemeinsames Busmedium. Der Bus bildet eine sogenannte Kollisionsdomäne, denn gleichzeitiges Senden mehrerer Busteilnehmer verursacht Signalüberlagerungen („Kollisionen“). Solche Kollisionen werden in Kauf genommen, aber erkannt (sogenanntes Carrier Sense Multiple Access/Collision Detection, CSMA/CD).

Die Kollisionsdomäne dient gleichzeitig der Realisierung von Broadcasts auf der Netzzugangsschicht. Ein Broadcast kann aber darüber hinaus auch in weiteren Kollisionsdomänen verbreitet werden (Broadcast-Domäne). Jede Broadcast-Domäne umfasst somit eine oder mehrere Kollisionsdomänen. Große Kollisionsdomänen bedingen selbst bei Punkt-zu-Punkt-Nachrichten Abhörgefahren und begrenzen den Durchsatz auf der Netzzugangsschicht. Große Broadcast-Domänen sind diesbezüglich nur bei Punkt-zu-Multipunkt-Übertragungen kritisch.

Sogenannte Switched Ethernets vermeiden Kollisionen durch gezielte physische Segmentierung des Ethernet-Busses und durch Entkopplung der Endgeräteanschlüsse: Anstatt mehrere Rechner am gleichen Bus anzuschließen, wird nur ein Endgerät pro Switch-Port betrieben. Da in diesem Fall

keine Kollisionen auftreten können, kann auf die Kollisionserkennung und damit das CSMA-Protokoll verzichtet werden (wird dann Full-Duplex statt Half-Duplex genannt). Die Bandbreite steht damit sowohl Sender als auch Empfänger voll zur Verfügung (z.B. 200 Mbit statt 100 Mbit). Dies minimiert die Kollisionsdomäne, was die Kommunikationsleistung und Vertraulichkeit des Netzes verbessert, für sich allein allerdings noch keinen sicheren Schutz gegen Ausspähen bietet.

2.2.2 Koppelelemente

Die sichere Kollisionserkennung (CSMA/CD-Prinzip) erfordert eine Längenbeschränkung des Ethernet-Busses. Zur Überbrückung größerer Distanzen können mehrere Bus-Segmente mit einem Repeater zu einer gemeinsamen Kollisionsdomäne zusammengeschlossen werden. Der Repeater sorgt dabei auf der Netzzugangsschicht für eine elektrische Signalaufbereitung. Ein Multiport-Repeater, der eine sternförmige Kopplung von Ethernet-Segmenten ermöglicht, wird Hub genannt.

Eine Bridge ist ein „intelligenter Repeater“, der eingehende Datenpakete nur an den Ausgangs-Port weiterleitet, falls sich der Empfänger im entsprechenden Ethernet-Segment befindet; ein Datenaustausch innerhalb eines Segments wird gegenüber dem anderen Segment jedoch abgeschirmt. Dies zerlegt die gemeinsame Broadcast-Domäne in zwei Kollisionsdomänen, was den Durchsatz und die Abhörsicherheit des Netzes verbessert, ohne die logische Verbindungstopologie einzuschränken. Ein Multiport-Bridge für den Zusammenschluss mehrerer Kollisionsdomänen zu einer Broadcast-Domäne, wird Switch genannt.

Switches, Switched Ethernets und Virtual LANs

Aufgrund sinkender Preise und wachsender Ansprüche sind heute überwiegend Gigabit-Switche gebräuchlich, während Repeater, Hubs und Bridges eher selten eingesetzt werden. Einfache Switche (sogenannte Layer-2-Switche[2]) agieren nur auf der Netzzugangsschicht und unterstützen in der Regel nur die grundlegenden Management-Funktionen. Sogenannte Layer-3-Switches verwerten auch Protokollinformationen der Layer-3-Schicht und ermöglichen so auch IP-Routing sowie IP-Paketfilterung.

Mit zunehmender Größe einer Broadcast-Domäne steigt trotz physischer Segmentierung auch in einem Switched Ethernet die Kommunikationslast durch Broadcasts und Multicasts. Daher unterstützen moderne Switches die Aufteilung eines physischen Switches in mehrere logische Segmente, um sogenannte Virtual LANs (VLANs) zu realisieren.

Ein VLAN realisiert eine logische Netzstruktur auf einer physischen LAN-Topologie, um funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz zu verbinden. Jedes VLAN bildet eine eigene Broadcast-Domäne. VLAN-Teilnehmer können andere VLANs nicht auf der Netzzugangsschicht erreichen (logische Segmentierung).

Ein gebräuchlicher VLAN-Standard ist IEEE 802.1q. Um Ethernet-Datenpakete eindeutig einem VLAN zuzuordnen, wird der Paket-Header vom ersten Switch in der Übertragungskette um ein VLAN-Tag erweitert. VLAN-Switches übermitteln die so gekennzeichneten Datenpakete untereinander über spezielle Trunk Ports. Erst bei der Zustellung des Pakets an einen Endgeräte-Port entfernt der letzte Switch auf dem Kommunikationspfad das VLAN-Tag2 und liefert die Daten als gewöhnliches Ethernet-Paket aus. Um zu verhindern, dass ein Angreifer mit falschen VLAN-Tag2s in fremde VLANs eindringen kann, sind Pakete mit VLAN-Tag2s an Endgeräteports filterbar.

2 Traditionell richtet sich die Namensgebung nach der Protokollschicht des OSI-Schichtenmodells, auf dem ein Switch operiert (vgl. Tabelle 1). Layer 2 bezeichnet hier also einen Teil der Netzzugangsschicht (Schicht 1) des TCP/IP-Referenzmodells.

Wegen diverser Sicherheitsrisiken, etwa der Bedrohung durch manipulierte VLAN-Tags, sind VLANs dennoch nicht zur Trennung von Sicherheitszonen im Netz geeignet (siehe Abschnitt 5.1.2). Zur sicheren Trennung ist vielmehr mindestens eine physische Segmentierung auf der Layer-3-Schicht erforderlich, das heisst die Entkopplung durch einen Paketfilter.

Router

Ein (IP-)Router ist ein Vermittlungsrechner, der Netze auf IP-Ebene koppelt und Wegewahlentscheidungen anhand von IP-Protokollschicht-Informationen trifft. Router trennen Netze auf der Netzzugangsschicht und begrenzen daher die Broadcast-Domäne eines Ethernets.

Router unterstützen meist auch Transportschicht-Attribute (z. B. TCP Flags oder Portnummern: sogenanntes Policy Routing) sowie Paket-Filterung auf Basis dieser Attribute. Moderne Kombi-Geräte vereinen die Funktion von Switch, Router und IP-Paketfilter.

2.2.3 Drahtlose lokale Netze

Funknetze ermöglichen den schnellen Aufbau von lokalen Kommunikationsnetzen ohne aufwendige Verkabelung. Dies erleichtert die redundante Auslegung des Netzes mittels unabhängiger Funkkreise. Außerdem unterstützen Funknetze einen Ortswechsel der Netzteilnehmer, bis hin zu einem Wechsel der Funkzelle (Roaming) ohne Verbindungsunterbrechung.

Funkübermittlung hat inhärent eine Broadcast-Charakteristik, daher kann der Kreis der potenziellen Empfänger nur grob mittels Reichweiten-Begrenzung durch geringe Sendeleistung oder durch den Einsatz von Antennen mit Richtfunk-Charakteristik eingegrenzt werden. Da die Wirkung solcher Maßnahmen in der Regel schwer abschätzbar ist, sind Funksignale stark abhörgefährdet. Das Netzzugangsprotokoll ist grundsätzlich offen für beliebige Teilnehmer in Reichweite, daher sind Funknetze anfällig für Eindringlinge. Zudem sind Funksignale störanfällig, die Übertragung lässt sich jedoch kaum gegen Störeinflüsse abschirmen. Eine weitere Schwäche besteht darin, dass Funknetz-Teilnehmer anhand ihrer MAC-Adresse leicht wiederzuerkennen und durch Funkpeilung zu orten sind, was das Erstellen von Bewegungsprofilen einzelner Nutzer ermöglicht.

Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität drahtloser Kommunikation sind also prinzipiell besonders gefährdet. Da physische Schutzmaßnahmen kaum verfügbar sind, ist zur sicheren Nutzung ein logischer Schutz durch Kryptografie auf oder oberhalb der Netzzugangsschicht unverzichtbar.

Die Nutzung drahtloser Netzsegmente kann auch das Konzept eines zentralen Sicherheits-Gateways für die Kommunikationverbindungen zwischen LAN und Internet untergraben, denn Funkkommunikation bietet eine potenzielle Hintertür zur Umgehung des Gateways. Daher wird der Einsatz drahtloser Netze in sicherheitskritischen Anwendungsumgebungen grundsätzlich nicht empfohlen. Soweit unverzichtbar, sollten Funknetz-Segmente in einer eigenen Sicherheitszone hinter einem Sicherheits-Gateway gekapselt werden. Detailliertere Hinweise zur sicheren Nutzung drahtloser lokaler Netze bieten [TR-S-WLAN] sowie [ISi-WLAN].

WLAN

Mit Wireless Local Area Network werden drahtlose Netze bezeichnet, die auf der mit [IEEE 802.11] bezeichneten Familie von Standards basieren. Die WLAN-Spezifikation umfasst einen funkbasierten Übertragungsstandard und eine Protokollfamilie auf der Netzzugangsschicht.

WLAN dient meist zur Erschließung von Gebäuden oder zur drahtlosen Anbindung benachbarter LAN-Segmente. Der Ad-hoc-Betriebsmodus ermöglicht eine Datenübertragung von Teilnehmer zu

Teilnehmer ohne Basisstation und ohne Weiterleitung (single hop); im Infrastruktur-Modus kommunizieren die Funknetz-Teilnehmer sternförmig mit einer Basistation (Access Point) als Vermittler.

Der WLAN-Standard operiert mit geringer Sendeleistung für Reichweiten in einer Größenordnung von 100 Metern. Dabei teilt WLAN sein Frequenzband mit anderen lizensierungsfreien Funkstandards im sogenannten ISM-Band (z. B. Bluetooth [IEEE 802.15.1], ZigBee [IEEE 802.15.4]), was wechselseitige Störungen bedingen kann. Einige Protokollvarianten bieten Verschlüsselung, Integritätssicherung und Authentisierung auf der Netzzugangsschicht (z. B. [IEEE 802.11i], WPA2). Beim Einsatz von WLAN-Verschlüsselungstechniken ist jedoch darauf zu achten, dass ältere Standards nur unzureichenden Schutz bieten. So ist zum Beispiel Wired Equivalent Privacy (WEP) ein leicht kompromittierbares Verschlüsselungsverfahren, das auf keinen Fall verwendet werden sollte.

Alternativ zu einer Verschlüsselung auf der Netzzugangsschicht ist aber auch eine Verschlüsselung auf der Internet-Schicht möglich: So kann ein Virtuelles Privates Netz (z. B. mittels IPSec, siehe Abschnitt 4.2) über ein unverschlüsseltes WLAN eingerichtet werden.

WiMAX

Worldwide Interoperability for Microwave Access ist ein breitbandiger, funkbasierter Übertragungsstandard nach [IEEE 802.16] und bezeichnet eine Protokollfamilie auf der Netzzugangsschicht mit Reichweiten im Kilometerbereich. WiMAX wird meist zum Aufbau von Zugangsnetzen (Access-Bereich) verwendet und dient vor allem der Erschließung der „letzten Meile“. Einige WiMAX-Varianten ermöglichen auch Funkzellenwechsel während einer Verbindung [IEEE 802.16e] oder Bandbreitengarantien (QoS).

WiMAX-Clients (Subscriber Stations) sind mittels X.509-Zertifikaten authentisierbar, Basisstationen hingegen (IEEE 802.16e Amendment) nur mittels Extensible Authentication Protocol (EAP). WiMAX unterstützt eine Nutzdatenverschlüsselung mittels AES, jedoch ist im Standard keine Verschlüsselung der Steuerdaten vorgesehen. Zur besseren Absicherung der Kommunikationsverbindung kann wahlweise auch ein Virtuelles Privates Netz über unverschlüsseltes WiMAX betrieben werden.

2.2.4 Drahtlose Client-Kommunikation

Neben WLAN im Ad-hoc-Modus gibt es noch weitere drahtlose Übertragungsstandards, die eine Teilnehmer-zu-Teilnehmer-Verbindung ermöglichen. Dadurch werden weitere Möglichkeiten zum Ausspähen von Teilnehmern oder ungewollte Hintertüren in ein LAN eröffnet, sofern der Teilnehmer während der drahtlosen Verbindung auch mit dem drahtgebundenen LAN verbunden ist. Ähnliches gilt für Datenkommunikation über Mobilfunknetze (z. B. GPRS, UMTS) bei Endgeräten, die zugleich auch eine LAN-Verbindung besitzen. Stellvertretend seien hier zwei weitverbreitete Standards genannt.

Bluetooth

Bluetooth [IEEE 802.15.1] ist ein Funkstandard zur drahtlosen Vernetzung von Geräten im Nahbereich. Wie WLAN nutzt Bluetooth das ISM-Band, daher sind wechselseitige Störungen möglich. Für Bluetooth sind verschiedene Reichweiten-Klassen für Übertragungsstrecken zwischen 10 und 100 Metern definiert.

Das Protokoll unterstützt PIN-basierte Authentisierung und eine optionale Verschlüsselung der Verbindung. Bei schwacher PIN kann durch Abhören der Paarung und Authentisierung der Verbindungsschlüssel berechnet werden. Schlecht geschützte Endgeräte (mit bspw. Standard-PIN oder Implementierungsfehlern) sind durch Ausspähen gefährdet. Bluetooth-Angriffe können etwa dazu dienen, Tastatureingaben abzufangen oder die persönlichen Daten auf dem Mobiltelefon eines Nutzers (z. B. die Adress- und Kalender-Informationen) auszulesen. Weiterführende Informationen können der Broschüre *Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte* [DRAHT-KOM] entnommen werden.

IrDA

Der IrDA-Standard der Infrared Data Association beschreibt eine Familie von Kommunikationsprotokollen für den Austausch von Daten mittels infrarotem Licht über kurze Strecken von bis zu etwa einem Meter. IrDA-Schnittstellen sind vor allem in Laptops, PDAs, Mobiltelefonen und PC-Druckern verbreitet. IrDA bietet keine besonderen Schutzmechanismen auf der Protokollebene. Der einziger Schutz besteht in der geringen Sendereichweite und in der Abstrahlfokussierung, die eine direkte Sichtverbindung erforderlich macht, um in IrDA-Verbindungen einzudringen.

3 IPv6-Grundlagen

Dieser Abschnitt soll den Leser mit den grundsätzlichen Unterschieden zwischen IPv4 und IPv6 vertraut machen.

3.1 Einordnung in den TCP/IP-Protokollstapel

Das Internet Protocol, Version 6, kurz IPv6, ergänzt den TCP/IP-Protokollstapel (engl. „TCP/IP Stack“) um ein neues Protokoll in der Internet-Schicht (engl. Network Layer Protocol), parallel zum traditionellen Internet Protocol, Version 4, kurz IPv4. Abbildung 3.1 zeigt den um IPv6 erweiterten TCP/IP-Protokollstapel.

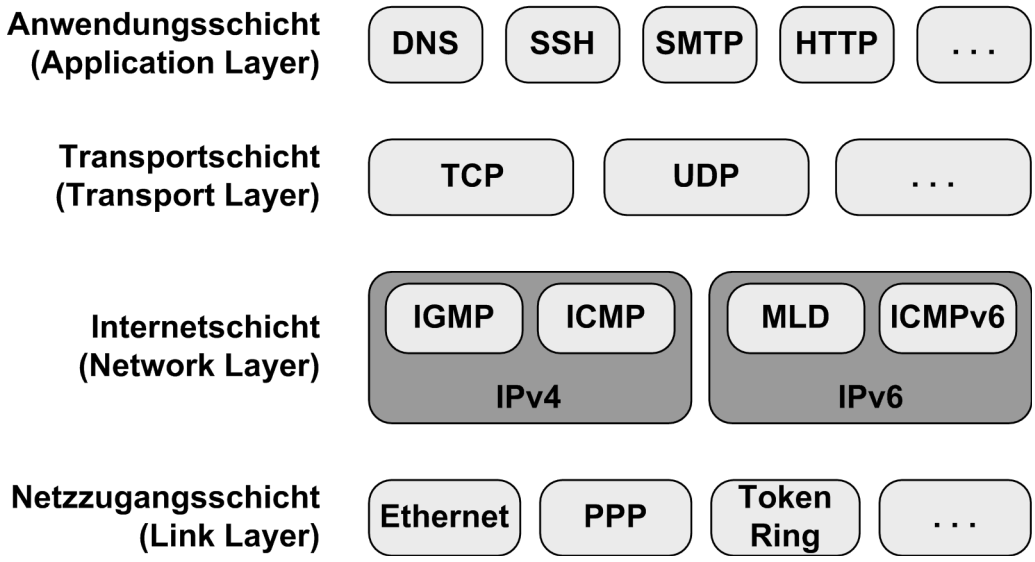

Abbildung 3.1: TCP/IP-Protokollstack

Schon an dieser Stelle sind einige grundlegende Eigenschaften von IPv6 zu erkennen:

- Die Protokolle der anderen Schichten sind im Wesentlichen unverändert geblieben. Lediglich an den Schnittstellen zur Internet-Schicht waren geringfügige Anpassungen notwendig, die aber bis auf eine Ausnahme – die Adressvergabe bei PPP (Point-to-Point Protocol) – nur innerhalb des Protokollstapels als solchem relevant und nach außen nicht sichtbar sind.
- IPv4 und IPv6 lassen sich parallel betreiben. Während der gesamten Spezifikation ist konsequent sichergestellt worden, dass die Möglichkeit des parallelen Betriebs von IPv4 und IPv6 innerhalb eines Subnetzes, eines Rechners und über eine einzelne Netzwerkschnittstelle (engl. Network Interface Card (NIC) oder kurz Interface) gewährleistet ist.
  Die Möglichkeit, IPv4 und IPv6 parallel zu betreiben, erlaubt es, in einer existierenden Umgebung IPv6 schrittweise einzuführen. Ein „harter“ Wechsel von IPv4 nach IPv6 ist weder notwendig noch sinnvoll.
- Bei der Portierung IPv4-basierter Software nach IPv6 müssen nur Zugriffe aus der Anwendung direkt auf die Internet-Schicht, insbesondere beim Umgang mit IP-Adressen, angepasst werden. Sind Anwendungen in einer Hochsprache geschrieben, die von IP-Adressen abstrahiert und stattdessen die Verwendung von Host-Namen unterstützt, ist existierende Software im Allgemeinen ohne jede Anpassung IPv6-fähig.

3.2 Grundlegende Terminologie

IPv6 führt einige grundlegende neue Begriffe und Begriffsdefinitionen ein, die zum Verständnis notwendig sind.

Für die Adressvergabe und das dynamische Routing ist die Unterscheidung zwischen Routern und Nicht-Routern relevant:

Node: Ein Gerät, das IPv6 „spricht“.

Router: Ein Node, der Pakete annimmt, dessen IP-Zieladresse nicht seine eigene ist – typischerweise, um das Paket weiterzuleiten.

Host: Ein Node, der kein Router ist. Für Hosts, und damit in typischen Umgebungen die Mehrzahl aller Nodes, gibt es besonders einfache Mechanismen zur Netzwerkkonfiguration.

Im Zusammenhang mit Netzen als solchen tauchen immer wieder die Begriffe Link und Site auf:

Link: Ein Subnetz oder eine Menge von Nodes, die sich alle direkt ohne zwischengeschaltete Router untereinander erreichen können.

Site: Für die Zwecke dieser Studie ist eine Site (deutsch etwa „Standort“) ein Teil des Internets, innerhalb dessen Adressen genutzt werden, die nicht über die Grenzen dieser Site hinaus geroutet werden.

3.3 Adressen

Der Auslöser für die Entwicklung von IPv6 war ursprünglich die sich abzeichnende Knappheit von IPv4-Adressen. Trotzdem wurde nicht einfach der Adressraum von IPv4 vergrößert, sondern es wurde eine Reihe weiterer, teils grundlegender Änderungen eingebracht, die sich nachträglich nicht direkt in IPv4 integrierbar waren.

Ein Beispiel für eine solche grundlegende Änderung ist der Verzicht auf die von IPv4 bekannten Broadcasts. Stattdessen wird bei IPv6 Multicast verwendet, das praktikabel auch über Subnetzgrenzen hinweg eingesetzt werden kann. Dies ist auch aus Sicht der Netzwerksicherheit bedeutsam.

3.3.1 Netzwerkschnittstellen und Adressen

Das Design von IPv6 sieht vor, dass einer Netzwerkschnittstelle mehrere, gleichberechtigte Adressen zugewiesen werden. Dies vereinfacht den Wechsel von IP-Adressen im laufenden Betrieb und die Konfiguration individueller Adressen für jeden auf einem Server angebotenen Dienst. Außerdem ist diese Eigenschaft Voraussetzung dafür, dass die in Abschnitt 3.3.4 vorgestellten Scopes sinnvoll genutzt werden können. Diese helfen wiederum, die Sicherheit von IPv6 gegenüber IPv4 schon im Design in mehreren zentralen Punkten zu verbessern.

3.3.2 Adresslänge

IPv6-Adressen sind 128 Bits (=16 Bytes) lang. In dem dadurch entstehenden dünn besiedelten (engl. *sparsely populated* oder kurz *sparse*) Adressraum werden Maßnahmen zu dessen effizienten Nutzung, angefangen bei Variable Length Subnet Masks (VLSM) bis hin zur Network Address Translation (NAT), überflüssig und fallen als potenzielle Fehlerquellen weg.

3.3.3 Adress- und Prefixnotation

Anders als IPv4-Adressen werden IPv6-Adressen hexadezimal notiert. Dabei werden Blöcke von jeweils zwei Bytes (genauer: Oktette), also vier Hexadezimalziffern (Nibbles) bzw. sechzehn Bits durch Doppelpunkte voneinander getrennt:

fe80:0000:0000:0000:020c:29ff:fe47:110a

Um die Notation etwas zu verkürzen, dürfen zunächst führende Nullen weggelassen werden. Ein Block mit dem Wert 0, oft als *Nullblock* bezeichnet, darf als eine einzelne Null geschrieben werden. Die Beispieladresse darf also auch als

fe80:0:0:0:20c:29ff:fe47:110a

geschrieben werden.

In vielen Fällen enthalten IPv6-Adressen eine ganze Folge von Nullblöcken. Um die Adressdarstellung weiter zu verkürzen, darf eine dieser Folgen, typischerweise die längste, durch einen doppelten Doppelpunkt abgekürzt werden. Die obige Adresse darf also notiert werden als:

fe80::20c:29ff:fe47:110a

Adresspräfixe werden, ähnlich wie bei IPv4, als Adresse notiert, der hinter einem angehängten Schrägstrich die Anzahl der relevanten Bits (in dezimaler Schreibweise) folgt:

2001:db8:2010:0:20c:29ff:fe47:110a/34

ist das Präfix, das allen Adressen von

2001:db8::

bis

2001:db8:3fff:ffff:ffff:ffff:ffff:ffff

gemeinsam ist. Die Definition, dass vor dem Schrägstrich eine vollständige Adresse angegeben wird, ist in Verbindung mit der Doppel-Doppelpunktnotation wichtig. Die Schreibweisen fe80::/64 und fe80::1/64 meinen das gleiche, nämlich immer das Prefix fe80:0000:0000:0000. Für ein Prefix fe80:0000:0000:0001 wäre die kürzeste mögliche Schreibweise fe80:0:0:1::/64.

Allgemeine („nichtmonotone“) Netzmasken (engl. Netmask) wie beispielsweise 192.0.2.66/253.0.240.26, die bei IPv4 erlaubt sind, unterstützt IPv6 nicht.

3.3.4 Scopes

Die Verwendung global eindeutiger und gerouteter Adressen ist nicht immer zweckmäßig. IPv6 unterstützt deshalb sogenannte *Scopes*, (etwa *Sichtbarkeitsbereiche*, *Gültigkeitsbereiche* oder *Reichweiten*), die festlegen, in welchem Teil des IPv6-Internets eine Adresse die gleiche Bedeutung hat. Jeder Adresse ist implizit ein Scope zugeordnet. Die wichtigsten Scopes sind:

Global Scope: Adressen mit diesem Scope sind global eindeutig, entsprechend den global gerouteten Adressen von IPv4.

Site-Local Scope: Adressen mit Site-Local Scope sind das IPv6-Äquivalent der RFC1918-Adressen (10.0.0.0/8, 172.16.0.0/12 und 192.168.0.0/16). Sie werden im Internet nicht geroutet.

Link-Local Scope: Diese Adressen gelten innerhalb eines einzelnen Subnetzes und werden darüber hinaus nicht geroutet. Sie entsprechen annähernd den Zeroconf-Adressen von IPv4 (169.254.0.0/16), werden aber für andere Aufgaben eingesetzt.

Interface-Local Scope: Diese Adressen gelten nur innerhalb der Netzwerkschnittstelle. Typisches Beispiel ist die Loopback-Adresse.

Darüber hinaus gibt es noch weitere Scopes, die ausschließlich in Verbindung mit gerouteten Multicasts zur Verfügung stehen.

3.3.5 Unicast-Adressen

Genau wie bei IPv4 sind Unicast-Adressen „normale“ Adressen, die nur einer einzelnen Netzwerkschnittstelle zugewiesen werden können.

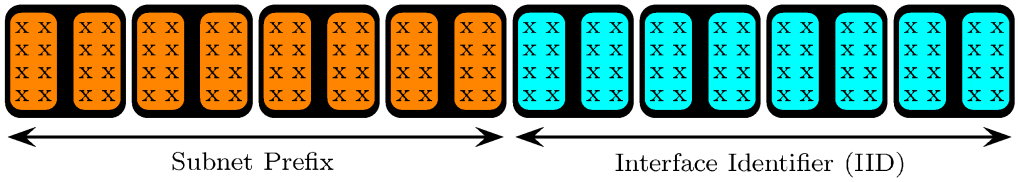

Abbildung 3.2: IPv6 Unicast Adressen

IPv6-Unicast-Adressen bestehen aus zwei Hälften: Dem Subnet Prefix, als Gegenstück zum Network Part einer IPv4-Adresse, und der Interface ID als Gegenstück zum Host Part. Beide Hälften sind laut [RFC 4291] und [RFC 4193] immer 64 Bits lang. Lediglich Adressen aus dem Bereich ::/3, der für spezielle Aufgaben reserviert ist, dürfen von diesem Aufbau abweichen.

Globale Adressen (aktuell aus 2000::/3): Globale (oder global geroutete) Adressen bezeichnen durch das gesamte Internet hindurch eindeutig die gleiche Netzwerkschnittstelle.

Bei ihnen ist das Subnet Prefix unterteilt in ein *Global Routing Prefix* und eine *Subnet ID*. Das Global Routing Prefix wird vom Provider zugeteilt. Die Subnet ID wird lokal innerhalb der Site vergeben.

In der Regel wird Endkunden, die selbst kein ISP sind, ein /48- Prefix als Global Routing Prefix zugewiesen. Selbst privaten Endkunden stehen damit normalerweise $2^{16} = 65536$ Subnetze zur Verfügung. Manche Provider vergeben an private Endkunden lediglich ein /56-Präfix. Dies entspricht $2^{8} = 256$ Subnetzen.

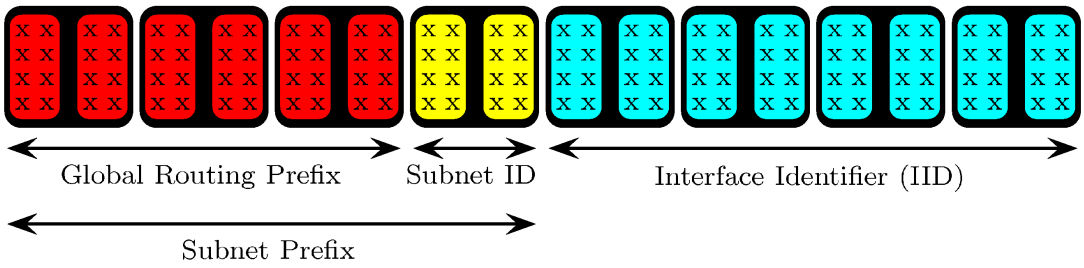

Abbildung 3.3: IPv6 globale Unicast-Adresse

Unique-Local-Adressen (fd00::/8): Für Site-interne Zwecke sind Unique-Local-Adressen (ULA) gedacht ([RFC 4193]). Sie haben Site-Local Scope und werden von Providern nicht geroutet. Aus dem Adressbereich darf sich jede Site ein zufällig gewähltes /48-Prefix generieren und dann nach eigenem Ermessen für Site-interne Zwecke verwenden.

Unique-Local-Adressen entsprechen den privaten Adressen von IPv4 nach [RFC 1918].

In älteren Texten zu IPv6 findet man gelegentlich noch den Adressbereich fec0::/10, die ursprünglichen Site-Local-Adressen, die ebenfalls Site-Local Scope haben. Sie sollten nicht mehr verwendet werden; wo sie bereits benutzt werden, sollten sie durch die funktional äquivalenten Unique-Local-Adressen ersetzt werden.

Link-Local-Adressen (fe80::/10): Jede IPv6-fähige Netzwerkschnittstelle muss eine Link-Local-Adresse aus dem Adressbereich fe80::/64 einrichten, bevor weitere Adressen mit größerem Scope konfiguriert werden. Als Interface ID dieser Link-Local-Adresse wird typischerweise die MAC-Adresse der Netzwerkschnittstelle verwendet. Ist diese kürzer als 64 Bit, zum Beispiel bei Ethernet, wird sie nach einem festgelegten Verfahren auf 64 Bits erweitert. Auch wenn ein komplettes /10-Präfix für Link-Local-Adressen reserviert ist, wird nur der Bereich fe80::/64 tatsächlich genutzt.

Link-Local-Adressen haben Link-Local Scope und lassen sich damit nur innerhalb eines Subnetzes verwenden. Damit entsprechen sie prinzipiell den Zeroconf-Adressen 169.254/16 bei IPv4. Sie dienen aber nicht primär zur Kommunikation zwischen Anwendungen, sondern internen Zwecken des TCP/IP-Protokollstapels. Weil sie bei jeder Netzwerkschnittstelle immer zur Verfügung stehen, können Mechanismen zur Konfiguration gerouteter Adressen (mit globalem oder Site-Local Scope) bereits auf Link-Local-Adressen zurückgreifen, womit diese Mechanismen deutlich einfacher werden als bei IPv4. Die Einschränkung, dass Link-Local-Adressen nicht zwischen Subnetzen geroutet werden, wird konsequent dazu genutzt, Funktionalitäten wie ICMP Redirects abzusichern, die nur innerhalb eines Subnetzes angewendet werden; durch die Beschränkung auf Link-Local-Adressen sind diese Mechanismen grundsätzlich nicht mehr über Subnetzgrenzen hinweg anzugreifen, so dass gegenüber IPv4 viele Angriffsszenarien wegfallen.

Die Loopback-Adresse (::1): Die Loopback-Adresse erfüllt die gleiche Funktion wie 127.0.0.1 für IPv4. Anders als alle anderen Unicast-Adressen ist sie nicht in Subnet Prefix und Interface ID unterteilt. Implementierungen ordnen ihr typischerweise aus pragmatischen Überlegungen heraus eine Präfixlänge von /128 zu. Jeder IPv6-fähige Node muss diese Adresse einrichten.

3.3.6 Multicast-Adressen

Multicast-Adressen sind dazu gedacht, IP-Pakete effizient an mehrere Empfänger (engl. *Listener* oder *Subscriber*) zu verteilen. Dazu können beliebig viele Netzwerkschnittstellen eine Multicast-Adresse *abonnieren* (engl. *subscribe*) oder einer Multicast-Gruppe *beitreten* (engl. *join*).

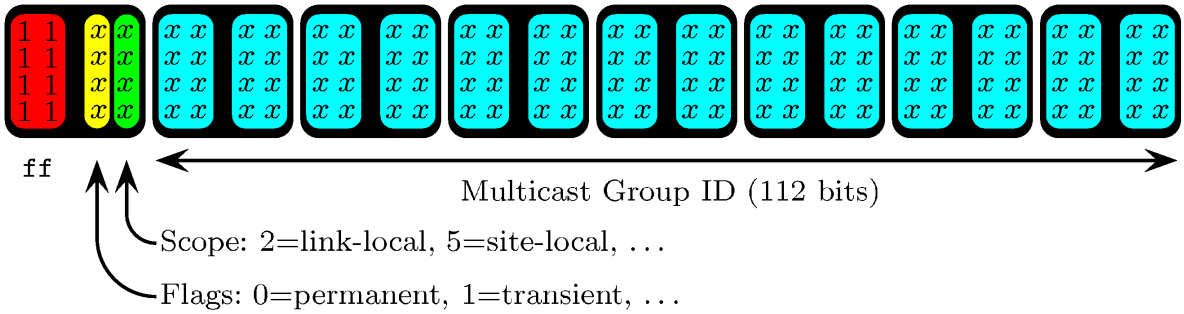

Abbildung 3.4: IPv6-Multicast-Adresse

Für Multicast-Adressen ist der Adressbereich ff00::/8 reserviert. Alle Multicast-Adressen haben den in Abbildung 3.4 gezeigten Aufbau.

Die ersten beiden Ziffern der Adresse haben immer den Wert ff. Die dritte Ziffer der Adresse, das *Flags Field* gibt an, um was für eine Art von Multicast-Adresse es sich handelt, die vierte den Scope der Adresse. Die restlichen 112 Bits heißen Multicast ID.

Gültige Werte für den Scope sind:

1	Interface-Local Scope	6, 7	(unbenannt, zur lokalen Verwendung)
2	Link-Local Scope	8	Organization-Local Scope
4	Admin-Local Scope	9 – d	(unbenannt, zur lokalen Verwendung)
5	Site-Local Scope	e	Global Scope

Die Werte 0, 3 und f sind von der IANA (Internet Assigned Numbers Authority) reserviert. Der Admin-Local Scope ist der *„kleinste* Scope*, der explizit konfiguriert werden muss, statt sich aus der physischen Anbindung oder anderer, nicht Multicast-bezogener Konfiguration zu ergeben“* ([RFC 4291], Seite 14). Der Organization-Local Scope ist gedacht für Organisationen mit mehreren Sites, zwischen denen Multicast-Pakete geroutet werden sollen. Die unbenannten Scopes 6, 7 und 9 bis d können nach Bedarf vergeben werden.

Der Inhalt des Flags Field zeigt an, ob eine Adresse von der IANA offiziell vergeben ist (Wert 0), ob sie „transient“, also vorübergehend lokal zugewiesen ist (Wert 1) oder spezielle Eigenschaften hat, die vor allem für das Multicast-Routing relevant sind (Werte 3 und 7).

Die Multicast ID, also die letzten 112 Bytes der Adresse, dienen zur Unterscheidung der Multicast-Gruppen. Anders als bei Unicast lassen sich Multicasts nur über ihre Multicast-Adresse abonnieren, Port-Nummern werden nicht berücksichtigt.

Wichtige Multicast-Adressen sind:

ff02::1	Die All-Nodes Link-Local Multicast Address (alle Nodes in einem Subnetz)
ff02::2	Die All-Routers Link-Local Multicast Address (alle Router in einem Subnetz)
ff02::1:ff00:0/104	Die Solicited-Node Multicast Addresses (Adressen, die für Neighbor Discovery benutzt werden)

3.3.7 Anycast

Ähnlich wie Multicast-Adressen können Anycast-Adressen mehrere Listener haben. Ein Paket, das als Zieladresse eine Anycast-Adresse hat, wird aber nur einem einzigen Listener zugestellt, nicht allen.

Für Anycast sind keine eigenen Adressbereiche festgelegt; stattdessen werden Adressen aus den Unicast-Adressbereichen für Anycast benutzt, so dass die Gegenseite, die mit einer Anycast-Adresse kommuniziert, weder die Adresse als Anycast-Adresse noch den tatsächlichen Empfänger des Pakets erkennen kann.

Anycast-Adressen sind dazu gedacht, redundante Umgebungen aufzubauen. Stehen alle Anycast-Listener in einem Subnetz, beschränkt sich die Konfiguration darauf, auf den Listenern die zusätzliche Anycast-Adresse als solche zu konfigurieren. In komplexeren Umgebungen existieren mehrere räumlich getrennte Subnetze, die das gleiche Subnet Prefix benutzen. In diesem Fall muss beim Ausfall aller Listener in einem Subnetz gezielt in das dynamische Routing eingegriffen werden, um Pakete in ein anderes Subnetz mit noch funktionierenden Listenern weiterzuleiten.

Eine Funktionalität, die Anycast prinzipbedingt nicht leisten kann, ist eine Lastverteilung zwischen den Listenern in einem Subnetz: Bei typischen Implementierungen werden von einem Router immer alle Pakete an eine Anycast-Adresse dem selben Rechner innerhalb des Subnetzes geschickt.

Einige Interface IDs sind fest für Anycast-Adressen definiert:

0:0:0:0	Die Subnet-Router Anycast Address ([RFC 4291]).
dfff:ffff:ffff:fffe	Mobile IPv6 Home Agent Anycast ([RFC 2526]).
dfff:ffff:ffff:ff80 – dfff:ffff:ffff:ffff	Von IANA reserviert.

3.4 Der Aufbau von IPv6-Paketen

Der Aufbau von IPv6-Paketen folgt einem Ansatz, der sich grundlegend von IPv4 unterscheidet.

Wie Abbildung 3.5 zeigt, bildet den Anfang jedes IPv6-Pakets der *Base Header*. Er enthält im Wesentlichen nur Platz für Daten, die bei jedem IP-Paket tatsächlich benötigt werden. Anders als ein IPv4-Header hat er eine feste Größe von 40 Bytes. Die Header-Optionen von IPv4 sind ersetzt worden durch *Extension Headers*, die dem Base Header bei Bedarf nacheinander angehängt werden.

Abbildung 3.5: Paketaufbau bei IPv6

Während bei IPv4-Paketen die Header-Optionen auf insgesamt 60 Bytes begrenzt sind, kann IPv6 deutlich mehr Informationen in den Extension Headers unterbringen; die Größe eines einzelnen Extension Headers ist auf 8 kByte beschränkt, für alle Extension Header zusammen gibt es keine Größenbeschränkung.

3.4.1 Base Header

Abbildung 3.6 zeigt den Aufbau des Base Headers. Wie bei IPv4 enthält er in den ersten vier Bits die Versionsnummer des IP-Pakets. Der Flow Label ist ein neues Feld, das zur Bandbreiten-reservierung genutzt werden kann; Details folgen in Abschnitt 3.10.2. Die *Payload Length* gibt an, wie viele Bytes dem Base Header insgesamt folgen.

Das Feld Internet *Header Length* von IPv4 fällt weg. Alle Felder, die IPv4 für die Fragmentierung in jedem Paket mitführt, sind in einen Extension Header ausgelagert worden. Auf eine Header-Prüfsumme hat man verzichtet, weil deren Aufgabe in der Netzzugangs- (engl. Link Layer) und Transportschicht (engl. Transport Layer) wahrgenommen wird.

Einige Felder sind umbenannt worden: Aus *Type of Service* (ToS) ist *Traffic Class* (TC) geworden, *Protocol* wurde in *Next Header* umbenannt und *Time to Live* (TTL) heißt bei IPv6 *Hop Limit* (HL).

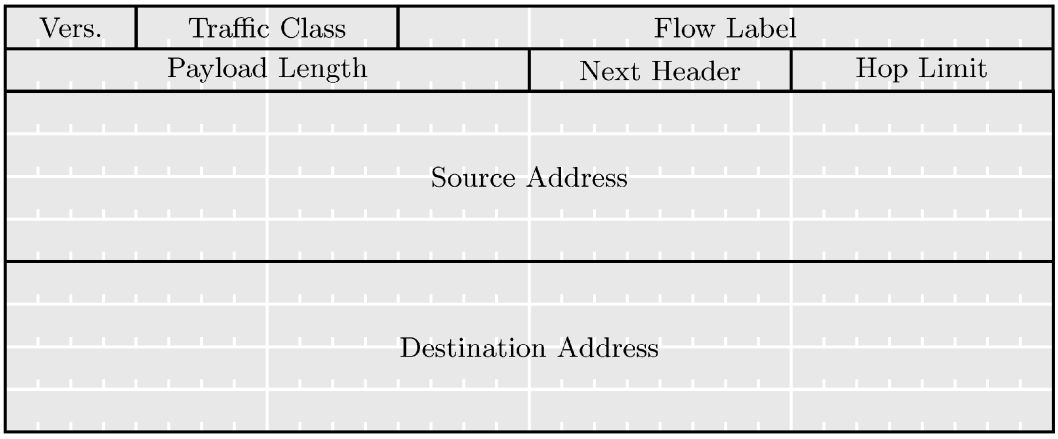

Abbildung 3.6: Der Base Header eines IPv6-Paketes.

3.4.2 Extension Header

Auch bei der Definition der Extension Headers hat man sich von IPv4 gelöst. Detaillierte Informationen finden sich in [RFC 2460], [RFC 2675] und [RFC 2711].

Neben grundlegenden Funktionen wie der Fragmentierung von IPv6-Paketen, die in Abschnitt 3.5.4 beschrieben wird, verwenden auch neue Funktionalitäten wie IPsec (siehe Abschnitt 3.10.1) und Mobile IPv6 (siehe Abschnitt 3.10.3) Extension Headers.

Extension Header dürfen in beliebiger Reihenfolge und in beliebiger Anzahl vorkommen, auch wenn [RFC 2460] eine Reihenfolge und eine Häufigkeit vorschlägt. Durch diese Freiheitsgrade kommt es regelmäßig zu Problemen beim Parsen von Extension Headern, insbesondere dann, wenn nicht alle Extension Header im Paketfragment enthalten sind (siehe hierzu [RFC 7112]).

Ein weiteres Problem mit Extension Headern ist, dass sie oftmals gefiltert werden. Dabei ist zwischen einer Filterung auf Empfängerseite und auf dem Transportweg zu unterscheiden. Eine Filterung beim Empfänger kann gewollt sein – beispielsweise aufgrund von Sicherheitsrichtlinien. Der Empfänger hat hier Einfluss auf die korrekte Zustellung der Pakete. Werden die Pakete bereits auf dem Transportweg gefiltert, so können weder Sender noch Empfänger die korrekte Zustellung beeinflussen. Aktuellen Untersuchungen zufolge treten Filterungen von Extension Header auf dem Transportweg häufig auf, obwohl dies in den Standards nicht empfohlen wird (siehe RFC 7045]).

Seit der Spezifizierung von IPv6 in [RFC 2460] wurden einige neue Erweiterungen definiert und andere überholt. Dadurch ist es für Hersteller von Netzkomponenten oftmals schwierig, mit Extension Headern umzugehen. [RFC 6564] definiert ein einheitliches Format für neue Erweiterungen und entschärft damit die Situation etwas. Andererseits wirft dieser Ansatz ein neues Problem auf, das man aktuell durch die Spezifikation eines universellen Extension Header für IPv6 zu lösen versucht. Derzeitig sind folgende Extension Header definiert:

Protokollnummer	*Beschreibung*	*Referenz*
0	Hop-By-Hop Option	[RFC 2460]
43	Routing Header	[RFC 2460], [RFC 5095]
44	Fragment Header	[RFC 2460]
50	Encapsulating Security Payload	[RFC 4303]
51	Authentication Header	[RFC 4302]
60	Destination Options	[RFC 2460]
135	Mobility Header	[RFC 6275]
139	Host Identity Protocol	[RFC 5201]
140	Shim6 Protocol	[RFC 5533]
253	Reserviert für Testzwecke	[RFC 3692], [RFC 4727]
254	Reserviert für Testzwecke	[RFC 3692], [RFC 4727]

Tabelle 7: Übersicht der aktuell spezifizierten Erweiterungs Header

3.5 Geänderte IP-interne Mechanismen

Wie beim Aufbau der IPv6-Header hat man bei der Spezifikation der IPv6-internen Protokolle und Mechanismen, insbesondere rund um ICMPv6, die Gelegenheit genutzt, einige historisch bedingte Altlasten zu bereinigen, die bei IPv4 nicht mehr nachträglich zu korrigieren waren.

3.5.1 Internet Control Message Protocol, Version 6 (ICMPv6)

Der grundlegende Aufbau von ICMP hat sich beim Wechsel von ICMP für IPv4 nach ICMPv6 nicht geändert. Viele der von IPv4 her bekannten ICMP-Typen und -Codes sind übernommen worden, lediglich die Nummerierung der Typen und Codes hat sich durchgehend geändert, was in einigen Fällen die Konfiguration von Paketfiltern erleichtert.

Weiter legt [RFC 4443] fest, dass eine Reihe von sicherheitskritischen ICMPv6-Paketen von einer Link-Local-Adresse und mit einem Hop Limit von 255 kommen müssen. Erfüllen sie diese Bedingung nicht, müssen sie von einem RFC-konformen Empfänger verworfen werden. Damit wird auch ohne Paketfilter verhindert, dass zum Beispiel ICMP Redirects von außen in ein Subnetz eingeschleust werden.

Schließlich ist der Funktionsumfang von ICMPv6 gegenüber ICMPv4 deutlich erweitert worden. ICMPv6 ersetzt insbesondere das Address Resolution Protocol (ARP), das bei IPv4 „unterhalb“ der Internet-Schicht agiert und deshalb von manchen Paketfiltern nicht berücksichtigt wird.

3.5.2 Multicast Listener Discovery (MLD)

Analog zum Internet Group Management Protocol (IGMP) für IPv4 verwendet IPv6 Multicast Listener Discovery (MLD), um Multicast-Router und Multicast-fähige Switches über aktuelle Listener zu informieren.

MLD ist kein eigener Protokolltyp, sondern benutzt mehrere MLD-spezifische ICMPv6-Typen. Es gibt zwei Versionen von MLD: MLDv1, nach [RFC 2710], ist weitgehend an IGMPv2 angelehnt,

recht einfach im Aufbau und funktional in einigen Punkten eingeschränkt. MLDv2, nach [RFC 3810], ist komplexer, bietet aber einige Funktionen, mit denen sich geroutetes Multicast besser nutzen lässt.

Aktuelle Implementierungen auf der Client-Seite nutzen teils MLDv1, teils MLDv2, so dass beide Versionen unterstützt werden müssen. Multicast-Router und -Switches, die MLD unterstützen, sind typischerweise in der Lage, beide Versionen zu verstehen und nutzen zu können. Switches, die MLD nicht verstehen, leiten alle Multicast-Pakete wie Broadcasts an alle Ports weiter.

3.5.3 Neighbor Discovery (ND)

Durch die Einführung der Link-Local-Adressen wurde es möglich, das Address Resolution Protocol (ARP) durch ein ICMPv6-basiertes Verfahren zu ersetzen.

Bei diesem Verfahren, Neighbor Discovery (ND), werden Neighbor Solicitation (NS) genannte ICMPv6-Pakete an spezielle Multicast-Adressen, die Solicited-Node Multicast Addresses, geschickt. Diese Adressen haben die Form ff02::1:ff*xx*:*xxxx*, wobei die drei letzten Bytes durch die drei letzten Bytes der gesuchten IPv6-Adresse ersetzt werden. Als Absenderadresse für diese Anfragen wird die Link-Local-Adresse der jeweiligen Netzwerkschnittstelle genutzt. Im Datenteil des Pakets wird die IPv6-Adresse, deren zugehörige MAC-Adresse gesucht wird, in voller Länge übermittelt.

Die Antwort, Neighbor Advertisement (NA) genannt, benutzt als Absender- und Zieladressen Unicast-Adressen mit Link-Local Scope.

Das Ergebnis der Neighbor Discovery wird im Neighbor Discovery Cache abgelegt, der analog zum ARP-Cache bei IPv4 die Zuordnung von IPv6-Adressen zu MAC-Adressen speichert.

Neighbor Discovery entlastet große Subnetze, in denen das Broadcast-basierte ARP zu einer unnötigen Grundlast auf allen angeschlossenen Rechnern führt. Bei enorm großen Subnetzen (z. B. bei Sensornetzen) kann es dennoch zu einer hohen Grundlast führen. Möglichkeiten diese Grundlast zu reduzieren werden aktuell noch diskutiert. Des Weiteren ist Neighbor Discovery unabhängig vom benutzten Netzzugangsprotokoll: Während ARP nur über IEEE-802-basierte Netze funktioniert, wird Neighbor Discovery grundsätzlich über alle Netzzugangsprotokolle verwendet.

Einträge im Neighbor Discovery Cache werden nach Ablauf einer „Lifetime“ nicht einfach gelöscht, sondern nur als „veraltet“ (engl. stale) markiert. Soll an eine solche Adresse ein Paket geschickt werden, wird abhängig vom Inhalt des Pakets entweder zur Überprüfung eine Neighbor Solicitation als Unicast an die letzte bekannte MAC-Adresse geschickt oder das auslösende Paket versuchsweise an die letzte bekannte MAC-Adresse geschickt und auf eine Antwort gewartet. Erst wenn das fehlschlägt, wird der Cache-Eintrag gelöscht und eine neue Anfrage an die Solicited-Node Multicast Address geschickt. Dieses Verfahren wird Neighbor Unreachability Detection (NUD) genannt.

Damit Neighbor Discovery funktioniert, müssen die ICMPv6-Typen für Neighbor Discovery von eventuellen Paketfiltern zugelassen – aber nicht weiter geroutet – werden. Weil diese Pakete nur mit Link-Local-Adressen funktionieren und das Hop Limit auf 255 gesetzt werden muss, können Neighbor-Discovery-Pakete nicht von außerhalb eines Subnetzes eingeschleust werden.

Die Spezifikation der Neighbor Discovery ([RFC 4861]) beschreibt noch eine Reihe anderer ICMPv6-Typen, die den gleichen grundsätzlichen Paketaufbau wie Neighbor Discoveries und Neighbor Solitications verwenden. Die Bezeichnung Neighbor Discovery wird deshalb sowohl für den hier vorgestellten Mechanismus als auch für alle in diesem RFC genannten Pakete und Mechanismen verwendet.

3.5.4 Minimum MTU, Fragmentierung und Path MTU Discovery

Unterschiedliche Netzzungangstechnologien erlauben unterschiedliche maximale Paketgrößen, die in den Frames der jeweiligen Netzzugangstechnologie transportiert werden können. Die maximale Paketgröße innerhalb eines Subnetzes wird als Maximum Transmission Unit (MTU) bezeichnet.

Bei IPv6 hat man festgelegt, dass die MTU mindestens 1280 Bytes groß sein muss.

Pakete, die zu groß sind, um über ein Subnetz in einem einzelnen Frame transportiert zu werden, müssen in mehrere Fragmente zerlegt werden, spezielle Pakete, die vom Empfänger vor der Weiterverarbeitung wieder zu einem einzelnen, unfragmentierten Paket zusammengesetzt werden. Während IPv4 dazu in jedem IP-Header die notwendigen Informationen mitführt, obwohl sie selten benötigt werden, verwendet IPv6 einen separaten Extension Header.

Es kann passieren, dass ein Router ein großes Paket auf einer Netzwerkschnittstelle mit großer MTU empfängt und es über eine Netzwerkschnittstelle weiterleiten muss, dessen MTU kleiner als das Paket ist. In diesem Fall sendet der Router an den Absender des Pakets ein ICMPv6-Paket mit dem Typ `Packet Too Big` (Paket zu groß) und fordert ihn damit auf, das Paket in kleinere Fragmente zerlegt noch einmal zu senden. Das Verfahren wiederholt sich, bis der Absender des Pakets die minimale MTU auf der Strecke zum Empfänger, die Path MTU, kennt. Anschließend sendet er alle Pakete an den Empfänger in der geringst möglichen Anzahl von Fragmenten.

Dieses Verfahren heißt Path MTU Discovery (pMTUd). Mit IPv6 wird ausschließlich per Path MTU Discovery fragmentiert, Router fragmentieren weiterzuleitende Pakete nicht.

Nachteil der Path MTU Discovery ist, dass die entsprechenden ICMPv6-Pakete nicht gefiltert werden dürfen. Paketfilter, die diese ICMPv6-Pakete filtern, führen zu Störungen, deren Ursache nur schwierig zu finden ist.

3.6 Adresskonfiguration

Durch den Überfluss an Adressen, die Einführung von Link-Local-Adressen und die Verwendung mehrerer Adressen pro Netzwerkschnittstelle ergeben sich gegenüber IPv4 einige teils grundlegende Änderungen an den Mechanismen zur Adresskonfiguration.

3.6.1 Interface IDs

Sobald eine IPv6-Netzwerkschnittstelle an ein Subnetz angeschlossen wird, konfiguriert sie zunächst eine Interface ID.

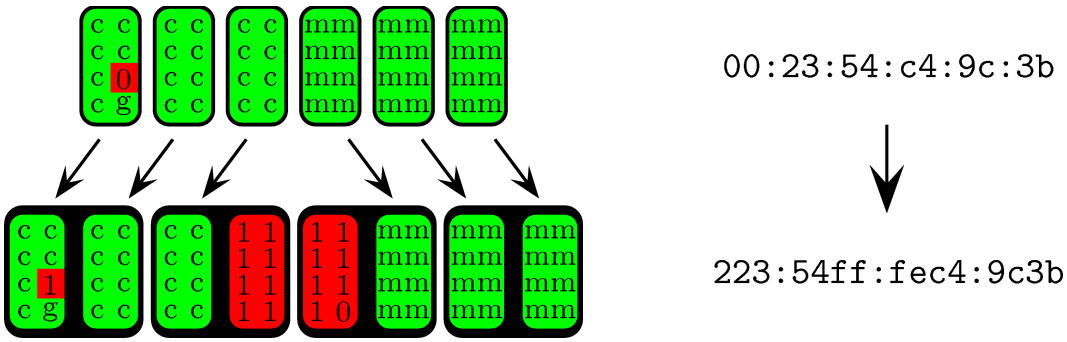

Abbildung 3.7: Berechnung der Interface ID aus einer Ethernet-Adresse

Insbesondere in IEEE-802-basierten Netzen wie Ethernet oder WLAN, in denen durch die MAC-Adresse eine global eindeutige 48 Bit lange Adresse zur Verfügung steht, wird diese zur Konstruktion der Interface ID herangezogen. Dazu wird das siebte Bit im ersten Byte von 0 auf 1 gesetzt, also das erste Byte um zwei erhöht. Dieses Bit bestimmt, ob eine Adresse global eindeutig ist oder nicht, und hat in den MAC-Adressen von Ethernet-Karten immer den Wert 0. Außerdem werden nach den ersten drei Bytes der MAC-Adresse die zusätzlichen Bytes FF und FE eingefügt. Abbildung 3.7 fasst die Umformung noch einmal zusammen.

Andere Netzzugangsprotokolle verwenden teils andere Mechanismen, um aus der MAC-Adresse eine Interface ID zu berechnen; Anhang A von [RFC 4291] spezifiziert weitere Umrechnungsverfahren.

Bei manchen Netzzugangsprotokollen steht keine MAC-Adresse zur Verfügung. In diesen Fällen ist es den jeweiligen Implementierungen überlassen, entweder die MAC-Adresse einer anderen Netzwerkschnittstelle im Rechner zu verwenden, eine *Node ID* genannte eindeutige Rechnernummer (CPU- oder im ROM eingebrannte Seriennummer) als Grundlage zur Berechnung der Interface ID heranzuziehen oder schließlich eine manuelle Konfiguration der Interface ID zu verlangen.

Manche Implementierungen erlauben es, die Interface ID auch dann explizit zu konfigurieren, wenn sie aus einer MAC-Adresse oder ähnlichem berechnet werden kann.

Wegen etwaiger datenschutzrechtlicher Probleme wird zurzeit diskutiert, ob die Generierung der Interface ID aus der MAC-Adresse als überholt und ein anderes Verfahren als Standard deklariert werden soll.

Aktuelle Versionen von Microsoft Windows verwenden bereits jetzt nicht die MAC-Adresse der Netzwerkschnittstelle zur Berechnung der Interface ID, sondern generieren beim Start des Betriebssystems einmalig eine zufällige Interface ID nach [RFC 4941] (Privacy Extensions, siehe auch Abschnitt 3.6.7). Optional kann auch die Verwendung des oben genannten Verfahrens auf Basis der MAC-Adresse eingestellt werden.

[RFC 7217] beschreibt ein Verfahren zur Generierung einer zufälligen Adresse pro Subnetz. Dadurch sind Geräte im stationären Einsatz immer unter der gleichen Adresse zu erreichen, wechseln im mobilen Betrieb jedoch regelmäßig ihre Adresse.

Die folgenden Abschnitte zeigen, wie die Interface ID anschließend zur Konfiguration von IP-Adressen verwendet wird. Aus der Ableitung der ID aus der MAC-Adresse folgen in manchen Konstellationen unerwünschte Sicherheitsimplikationen, denen durch die Einrichtung von zusätzlichen IP-Adressen mit temporärer, zufällig gewählter Interface ID Rechnung getragen wird. Die Details dieses Verfahrens werden in Abschnitt 3.6.7 vorgestellt.

3.6.2 Link-Local-Adressen

Sobald eine Netzwerkschnittstelle in Betrieb genommen wird, richtet sie als Erstes eine Link-Local-Adresse ein, indem sie das Subnetz-Prefix fe80::/64 mit der Interface ID kombiniert.

Diese Link-Local-Adresse ist Voraussetzung dafür, dass eine Reihe IP-interner Mechanismen funktioniert. Potenziell gefährliche Mechanismen, die nur innerhalb eines Subnetzes verwendet werden, setzen wie schon in Abschnitt 3.5.3 für die Neighbor Discovery beschrieben, die Verwendung von Link-Local-Adressen voraus und verhindern so, dass bösartige Pakete von außerhalb des Subnetzes eingeschleust werden.

Sobald eine Netzwerkschnittstelle eine Link-Local-Adresse konfiguriert hat, können weitere Adressen mit größerem Scope, also Site-Local oder globalem Scope, hinzukonfiguriert werden.

Anders als bei IPv4 werden neue Adressen zu den existierenden hinzugefügt, statt sie zu überschreiben.

3.6.3 Duplicate Address Detection (DAD)

Wenn eine Netzwerkschnittstelle eine Adresse konfiguriert, führt sie als Erstes eine Duplicate Address Detection durch, um sicherzustellen, dass kein anderes Gerät im gleichen Subnetz bereits diese Adresse verwendet. Dazu verwendet sie eine besondere Variante der Neighbor Discovery.

Die Netzwerkschnittstelle, die eine neue Adresse bekommen soll, sendet eine Neighbor Solicitation an die zugehörige Solicited-Node Multicast Address. Als Absenderadresse benutzt sie dabei die spezielle Adresse ::, die Unspecified Address. Benutzt ein anderes Geräte bereits die gewünschte Adresse im Subnetz, dann antwortet es mit einem Neighbor Advertisement an die All-Nodes Link-Local Address ff02::1, die auch das anfragende Gerät schon empfängt, ohne bereits eine funktionierende Adresse zu haben. In diesem Fall weiß das anfragende Gerät, dass die Adresse bereits belegt ist, loggt einen Fehler und nimmt die Adresse nicht in Betrieb. Das Gerät, das die gewünschte Adresse schon verwendet, wird nicht im Betrieb gestört.

3.6.4 Statische Adresskonfiguration

Genau wie bei IPv4 auch können Adressen explizit im Gerät konfiguriert werden. Insbesondere auf Routern und Servern ist dies die empfohlene Vorgehensweise.

Auch bei diesen Adressen muss das Gerät wieder eine Duplicate Address Detection durchführen, bevor es die Adresse endgültig in Betrieb nimmt.

3.6.5 Stateless Address Autoconfiguration

IPv6 unterstützt mit der Stateless Address Autoconfiguration (abgekürzt meist SAC, SAA, SLAAC oder Autoconf) ein Verfahren, das den großen Adressraum, die immer und überall verfügbaren Link-Local-Adressen und das allgemein unterstützte Multicast innerhalb eines Subnetzes ausnutzt. Dazu werden zwei ICMPv6-Typen (*Router Solicitation* und *Router Advertisement*) verwendet, die ausschließlich in Verbindung mit Adressen mit Link-Local Scope verwendet werden.

Dieses Verfahren basiert darauf, dass Router prinzipbedingt wissen müssen, welche Präfixe in den an sie angeschlossenen Subnetzen verwendet werden. Hosts suchen mit einem *Router Solicitation* (RS) genannten ICMPv6-Paket an die All-Router Link-Local Multicast Address ff02::2 alle im Subnetz angebundenen Router. Die Router antworten mit einem *Router Advertisement* an die All-Nodes Link-Local Multicast Address ff02::1, mit dem sie über die Subnetz-Präfixe für das Subnetz informieren, sich als potenzieller Defaultrouter zu erkennen geben und bei Bedarf weitere Informationen über das Subnetz an die Hosts übermitteln.

Hosts kombinieren nun ihre Interface IDs mit allen erhaltenen Präfixen zu neuen, gerouteten Unicast-Adressen mit Site-Local- oder globalem Scope und führen dabei mit ihnen wieder eine Duplicate Address Detection durch. Außerdem richten sie alle vorhandenen Router als Defaultrouter ein.

Router schicken periodisch unaufgefordert (engl. unsolicited) weitere Router Advertisements an die All-Nodes Link-Local Multicast Address, um die existierende Konfiguration immer wieder zu bestätigen und Änderungen der Netzwerkkonfiguration an die Hosts weiterzureichen. Die Hosts nehmen diese Informationen auf und aktualisieren ihre eigene Konfiguration entsprechend.

Nur Hosts dürfen Autoconfiguration für ihre Netzwerkeinstellungen verwenden. Gängige Implementierungen unterscheiden Router von Hosts daran, ob das Forwarding (Weiterleiten) von

Paketen eingeschaltet ist und verwenden per Default auf Hosts Autoconfiguration. Auf Routern müssen also Adressen statisch konfiguriert werden (theoretisch ist dies auch per DHCP möglich). Auch auf Servern werden typischerweise feste IP-Adressen konfiguriert. Ob die Autoconfiguration auf Servern noch zum Einrichten des Routings benutzt werden soll oder nicht, kann im Einzelfall entschieden werden.

Per Autoconfiguration lassen sich noch weitere Parameter an die Hosts weiterleiten, von der MTU im Subnetz über die Timing-Parameter der Neighbor Discovery bis zur Präferenz der Defaultrouter. Außerdem kann der Host darüber informiert werden, ob Adressen oder andere Informationen im Subnetz per DHCP bereitgestellt werden. Das Verfahren ist in [RFC 4861] und [RFC 4862] spezifiziert. [RFC 4191] führt darüber hinaus mehrere Erweiterungen ein, mit der Router ihre Priorität als Defaultrouter und weitere, spezifischere Routen mitteilen können.

Autoconfiguration ist nicht in der Lage, Geräte im DNS einzutragen, wie es DHCP-Server können. In Windows-basierten Umgebungen mit Active Directory erfüllen proprietäre Mechanismen diese Aufgabe.

3.6.6 Adressvergabe per DHCP (Dynamic Host Configuration Protocol)

Wie auch bei IPv4 lässt sich weiterhin das Dynamic Host Configuration Protocol (DHCP) für die dynamische Adresskonfiguration verwenden. Auch Kombinationen mit der Stateless Address Autoconfiguration sind möglich: manche Hosts unterstützen DHCP nur, wenn sie per Autoconfiguration darüber informiert werden, dass die Adresskonfiguration per DHCP erfolgt. Die Implementierungen verschiedener Betriebssysteme verhalten sich jedoch – insbesondere bei Randfällen wie z. B. einem Wechsel von SLAAC zu DHCP – sehr unterschiedlich (siehe auch [DHCP/SLAAC]).

Details zu DHCP für IPv6, auch über die Adressvergabe hinaus, folgen in Abschnitt 3.7.1.

3.6.7 Dynamisch wechselnde Interface IDs

Die Verwendung der MAC-Adresse zur Erzeugung der Interface ID, und damit mit Hilfe von Autoconfiguration der gerouteten IP-Adressen, führt zu einer Reihe von Sicherheits- und Datenschutzproblemen.

Um diesen entgegenzuwirken, wurde in [RFC 3041] und seinem Nachfolger [RFC 4941] unter der Bezeichnung *Privacy Extensions* ein optionaler Mechanismus spezifiziert, der eine zweite, zufällig generierte Interface ID verwendet. Mit ihr werden weitere Adressen mit den per Autoconfiguration erhaltenen Präfixen generiert. Die zufällige Interface ID wird periodisch nach einer konfigurierbaren Zeit, per Default alle 24 Stunden, und jedes Mal, wenn die Netzwerkschnittstelle neu hochgefahren wird, neu generiert.

Alle gängigen Implementierungen unterstützen dieses Verfahren. Microsoft Windows Vista und 7 haben es per Default eingeschaltet, bei anderen muss es erst in der Konfiguration aktiviert werden.

Folgende Punkte sind bei Verwendung dieser Adressen zu beachten:

- sie eignen sich zum höheren Schutz der Privatsphäre und zur Verhinderung von Profiling,
- beim Einsatz von dieser Adressart müssen Paketfilter auf Subnetzgrenzen ausgerichtet werden, einzelne Endgeräte lassen sich nicht zuordnen, da feste Adressen fehlen,
- beim Auswerten von Logdaten und bei der Fehlersuche muss auf die wechselnde Zuordnung von Adressen zu Geräten geachtet werden.

In der Grundarchitektur (siehe Abschnitt 5) ist eine Verwendung von Adressen nach [RFC 4941] oder [RFC 7217] nicht vorgesehen, da sich die damit verbundenen höheren Aufwendungen für Einrichtung, Betrieb und Fehlersuche nicht rechtfertigen lassen. Sinnvoll ist dieses Verfahren primär bei Geräten, deren Identität nach außen hin nicht durch ein mehrstufiges Sicherheits-Gateway (engl. Security-Gateway) verschleiert wird.

3.7 Hilfsprotokolle

Auch bei IPv6 werden einige zentrale Funktionen, die zur Netzinfrastruktur gehören, in der Anwendungsschicht implementiert. Aufgrund dieser Rolle ist es sinnvoller, sie im Zusammenhang mit der Internet-Schicht zu behandeln als zusammen mit „normalen“ Anwendungsprotokollen.

3.7.1 DHCP (Dynamic Host Configuration Protocol)

Das Dynamic Host Configuration Protocol (DHCP) für IPv6 ist gegenüber seinem IPv4-Vorläufer funktional im Wesentlichen unverändert geblieben. Intern ist es allerdings deutlich überarbeitet worden. Dabei konnte auf eine Abwärtskompatibilität zu BOOTP verzichtet werden, weil BOOTP für IPv6 nicht spezifiziert ist.

Für DHCP-Anfragen wird die Link-Local-Adresse verwendet, da diese Adresse bereits vorher von der Netzwerkschnittstellt konfiguriert sein muss. DHCP-Anfragen werden nicht als Broadcast ins Subnetz geschickt, sondern an die dafür reservierte Multicast-Adresse ff02::1:2.

Wie bei IPv4 muss in jedem Subnetz ein DHCP-Server oder -Relay stehen, weil ein Client möglicherweise noch zum Zeitpunkt der DHCP-Anfrage nur eine Link-Local-Adresse hat. Die Relays können explizit mit der Unicast-Adresse des Servers konfiguriert werden. Wenn auf der Strecke zwischen Relay und Server Multicast-Routing zur Verfügung steht, kann auf die Konfiguration der speziellen Unicast-Adressen verzichtet werden, wenn der Server auf die dazu vorgesehene Multicast-Adresse ff05::1:3 (mit Site-Local Scope) hört und das Relay die Anfragen an diese Multicast-Adresse weiterleitet.

Auch der Aufbau der DHCP-Pakete ist grundlegend überarbeitet und vereinheitlicht worden. Die Protokolldetails sind in [RFC 3315] spezifiziert. In Abgrenzung zum Stateless DHCP, das im folgenden Abschnitt vorgestellt wird, findet man für DHCP mit Adressvergabefunktionalität oft die Bezeichnung Stateful DHCP.

3.7.2 Stateless DHCP

Sollen Adressen per Stateless Address Autoconfiguration, aber zusätzliche Informationen wie DNS-Domain und -Server per DHCP eingerichtet werden, kann man auf einen großen Teil der DHCP-Funktionalität verzichten.

Deshalb definiert [RFC 3736] eine reduzierte DHCP-Variante unter dem Namen *Stateless DHCP*, in der auf alle Funktionen zur Adressvergabe und -verwaltung verzichtet wurde. Durch diese Reduzierung entfällt die Notwendigkeit im DHCP-Server den Status der vergebenen Adressen zu speichern. Damit fallen auf Speicherverbrauch zielende Angriffe weg und aufwendige Fail-over-Szenarien, die den Status erhalten, werden überflüssig.

3.7.3 DNS (Domain Name System)

Die Erweiterung des DNS um IPv6-Unterstützung beschränkt sich im Wesentlichen darauf, einen neuen Record Type für IPv6-Adressen in den Forward Zones und eine neue Pseudo-Domain für die Reverse Zones einzuführen. Das DNS-Protokoll als solches, wie es zwischen Clients und Servern eingesetzt wird, ist unverändert geblieben.

Zur Auflösung von DNS-Namen in IPv6-Adressen wurden in [RFC 1886] für die Forward Zones zusätzliche Resource Records vom Typ `AAAA` (gesprochen *Quad-A*) definiert. IPv4- und IPv6-Adressen finden sich zusammen in der gleichen Forward Zone.

Beispiel: www.example.com. AAAA 2001:db8:2010:1::1

Die Reverse Zones für IPv6-Adressen sind nach [RFC 3596] unterhalb der neuen Pseudo-Domain „ip6.arpa." (analog zu „in-addr.arpa." für IPv4) angesiedelt. In dieser Domain wird der gleiche PT" Record Type verwendet wie bei der Rückwärtsauflösung von IPv4. Die Darstellung einer IPv6-Adresse als DNS-Name im durch [RFC 1886] spezifizierten sogenannten *Nibble Format* besteht aus den einzelnen Ziffern der Adresse in umgedrehter Reihenfolge, gefolgt von der Pseudo-Domain „ip6.arpa.", also für das obige Beispiel als

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.1.0.2.8.b.d.0.1.0.0.2. 7200 IN PTR www.example.com.

3.8 Unicast-Routing

Im Hinblick auf das Routing von Unicast-Paketen hat sich mit IPv6 gegenüber IPv4 auf den ersten Blick wenig geändert. Neben einer Reihe von Detailänderungen, die das Routing vereinfachen, führt aber insbesondere die Stateless Address Autoconfiguration zu einigen Veränderungen.

3.8.1 Routing-Tabelle und Destination Cache

Die Routing-Tabellen für IPv6 ähneln von Ihrem Aufbau her denen von IPv4. Analog zum ARP Cache bei IPv4 wird wie schon in Abschnitt 3.5.3 beschrieben im Neighbor Discovery Cache die Zuordnung von IPv6- und MAC-Adressen vorgehalten. Darüber hinaus sieht IPv6 noch einen zusätzlichen Destination Cache vor, der den Neighbor Discovery Cache konzeptionell erweitert: Im Destination Cache wird für Ziele, die nicht direkt innerhalb eines gemeinsamen Subnetzes erreichbar sind, die MAC-Adresse des nächsten Routers abgelegt. Abhängig von der jeweiligen Implementierung können Neighbor und Destination Cache zwei getrennte oder auch eine gemeinsame Struktur sein.

Der Destination Cache dient darüber hinaus dem Zweck, dynamische Host-Routen zu verwalten, die per ICMPv6 Redirect kommuniziert werden. Er übernimmt damit Aufgaben, die bei klassischen IPv4-Implementierungen Teil der Routing-Tabelle sind.

3.8.2 Statisches Routing

Wie bei IPv4 ist es möglich, in den Routing-Tabellen Einträge statisch zu konfigurieren. Auch bei IPv6 bedeutet ein statisch konfiguriertes Routing, dass entweder bei Ausfall eines Routers das Routing manuell umkonfiguriert werden muss oder redundante Router und Router-Redundanzprotokolle wie HSRP oder VRRP verwendet werden müssen, um bei Ausfall eines Routers den Betrieb sicherzustellen.

3.8.3 Autoconfiguration, Neighbor Unreachability Detection und ICMPv6 Redirects

Die Stateless Address Autoconfiguration stellt alle notwendigen Mechanismen bereit, um die Routing-Tabellen auf Hosts automatisch zu pflegen.

Wie schon in Abschnitt 3.6.5 beschrieben, richten Hosts mit eingeschalteter Autoconfiguration automatisch Defaultrouten auf die gefundenen Router ein. Die Router können in ihren Router Advertisements angeben, ob und mit welcher Priorität sie als Defaultrouter verwendet werden wollen.

Mit Hilfe der Neighbor Unreachability Detection erkennt ein Host, wenn der aktuell verwendete Defaultrouter ausfällt. In diesem Fall wählt es einen neuen Defaultrouter aus. In vielen praktisch relevanten Fällen werden damit Router-Redundanzprotokolle wie HSRP oder VRRP überflüssig. Um einen schnellen Fail-over zu erreichen, kann es unter Umständen noch hilfreich sein, mit den Router Advertisements die Timing-Parameter für die Neighbor Unreachability Detection anzupassen.

Sind außerdem die Erweiterungen der Autoconfiguration nach [RFC 4191] bereits implementiert, können mit den Router Advertisements zusätzliche Routen an die Hosts übermittelt werden. Aktuell ist diese Funktionalität aber nur eingeschränkt nutzbar, weil erstens nicht alle routerseitigen Implementierungen in der Lage sind, Routen aus dem dynamischen Routing in die Router Advertisements zu übernehmen und zweitens auch auf Host-Seite nicht alle Implementierungen diese Erweiterungen unterstützten.

Auch ohne diese Erweiterungen funktionieren allerdings schon ICMPv6 Redirects. Mit ihnen kann ein Router einen Host darüber informieren, dass zu einer gegebenen Zieladresse eine bessere Route zur Verfügung steht als über den sendenden Router. Der Host richtet daraufhin dynamisch eine Host-Route für das Ziel ein. Die zwingend vorgeschriebene Verwendung von Link-Local-Adressen für ICMPv6 Redirects verhindert dabei, anders als bei IPv4, Angriffe mit Hilfe von ICMPv6 Redirects über Subnetzgrenzen hinweg.

3.8.4 Dynamisches Routing zwischen Routern

Beim dynamischen Routing zwischen Routern haben sich einige wichtige Details geändert, auch wenn die Routing-Protokolle als solche im Wesentlichen unverändert von IPv4 übernommen wurden.

Das Routing Information Protocol, Version 2 (RIPv2) ist in [RFC 2080] unter dem Namen RIPng und Open Shortest Path First, Version 2 (OSPFv2) in [RFC 5340] als OSPFv3 für IPv6 spezifiziert. In beiden Fällen hat man gegenüber den IPv4-Varianten auf Authentisierungsmechanismen in der Annahme verzichtet, dass es sinnvoller sei, für diesen Zweck IPsec zu verwenden. Abschnitt 3.10.1 geht näher auf die Probleme dieses Ansatzes ein. Einige Implementierungen verhindern außerdem, dass ein Routing-Protokoll auf einem Host aktiviert wird. Passives Routing, in dem ein Host seine Routing-Tabelle durch „Mithören“ des Routing-Protokolls aktualisiert, wird damit unmöglich.

Neben RIPng und OSPFv3 unterstützt auch das Cisco-proprietäre Enhanced Interior Gateway Routing Protocol (EIGRP) seit 2006 IPv6.

Für das dynamische Routing zwischen Providern und bei der redundanten Anbindung auf Basis von Provider-unabhängigen Adressen (engl. Provider-Independent Addresses oder PI Addresses) kommt auch für IPv4 als externes Routing-Protokoll typischerweise das Border Gateway Protocol, Version 4 (BGP4) zum Einsatz. Dazu unterstützt BGP4 gemäß [RFC 4760] das Routing beliebiger Protokolle im Rahmen seiner Multiprotocol Extensions.

3.9 Multicast-Routing

Ähnlich wie beim Unicast-Routing dient beim Multicast-Routing zur Kommunikation zwischen Hosts und Routern ein anderes Protokoll als zur Router-Router-Kommunikation. Zwischen Hosts und Multicast-Routern wird wie in Abschnitt 3.5.2 beschrieben die Multicast Listener Discovery (MLD) verwendet, zwischen Routern verschiedene Varianten von Protocol Independent Multicasts (PIM).

3.9.1 Multicast-Routing-Tabellen

Die zentrale Datenstruktur, die für das Multicast-Routing benutzt wird, ist eine Multicast-Routing-Tabelle. Anders als bei Unicast benutzen nur Multicast-Router diese Tabellen, um zu entscheiden, welche Multicast-Pakete sie von wo nach wo weiterleiten müssen. Hosts verwenden teilweise die gleiche Datenstruktur, verwalten damit aber nur, welche Multicasts von den Prozessen auf dem Host aktuell bezogen werden.

Während Unicast-Routing-Tabellen in jeder Zeile einem Adresspräfix typischerweise entweder eine Ziel-Netzwerkschnittstelle oder die Adresse des nächsten Routers zuordnen, enthält eine Multicast-Routing-Tabelle in jedem Eintrag eine Liste aller Netzwerkschnittstellen, an die passende Pakete weitergeleitet werden.

3.9.2 Protocol-Independent Multicast (PIM)

Alle Multicast-Routing-Protokolle für IPv6 benutzen einen gemeinsamen Protocol Type, *Protocol-Independent Multicast* (PIM). Jedes PIM-Paket enthält ein vier Bit großes Feld, das den Typ des PIM-Pakets identifiziert. Die PIM-basierten Protokolle benutzen getrennte PIM-Typen und sind für unterschiedliche Anwendungsszenarien gedacht.

Das einfachste Multicast-Routing-Protokoll für IPv6 ist *Protocol-Independent Multicast – Dense Mode*, abgekürzt PIM-DM, gemäß [RFC 3973]. Es verteilt zunächst alle Multicast-Pakete im gesamten Netz. Zusätzlich können Multicast Router aber ihren unmittelbaren Nachbarn mit speziellen PIM-Paketen mitteilen, wenn sie für die Multicast-Pakete, die sie erhalten, keine weiteren Listener haben. Mit diesen *Prune Messages* (deutsch etwa *Stutz-Nachrichten*) werden dann allmählich Multicast-Pakete nur noch in die Subnetze weitergeleitet, in denen sie tatsächlich verlangt werden. Dieses Verfahren funktioniert nur dann sinnvoll, wenn die Masse der Multicast-Gruppen in annähernd alle Subnetze weitergeleitet werden muss – deshalb auch der Name Dense Mode (deutsch etwa „dicht besiedelter Modus“). Damit ist es hauptsächlich für sehr kleine Umgebungen mit wenigen Subnetzen und für spezielle Anwendungszwecke wie in manchen Rechen-Clustern geeignet.

In größeren Umgebungen wird deshalb statt PIM-DM das deutlich komplexere *Protocol-Independent Multicast – Sparse Mode* (PIM-SM) nach [RFC 2362] verwendet. Es liefert Multicast-Pakete nur dorthin aus, wo sie auch tatsächlich verlangt werden. Es benutzt für jede Multicast-Gruppe einen speziellen Multicast-Router, den Rendezvous Point (RP), von dem aus sämtliche Multicast-Pakete an diese Gruppe zentral verteilt werden. PIM-SM ist in [RFC 2362] spezifiziert, weitergehende Funktionen in [RFC 3569], [RFC 3956] und [RFC 3446]. PIM-SM ist ein vergleichsweise robustes und einfach zu handhabendes Protokoll, aber seine Interna sind deutlich komplexer als hier dargestellt, so dass zu weiterführenden Themen und insbesondere zur Fehlersuche eine Lektüre der Spezifikationen und/oder geeigneter Sekundärliteratur unvermeidlich ist.

3.9.3 Skalierbarkeit und Ressourcenbedarf

Multicast-Routing ist auch in Verbindung mit IPv6 keine Technologie, die beliebig durch das Internet hindurch eingesetzt werden kann. Innerhalb einer Site lässt sich Multicast-Routing allerdings sinnvoll und vergleichsweise problemlos einsetzen.

3.10 Neue Funktionalitäten

Gemäß der RFCs bringt IPv6 eine Reihe interessant erscheinender neuer Funktionalitäten mit, die sich aber bei genauerem Hinsehen als problematisch oder unpraktikabel herausstellen.

3.10.1 IP Security (IPsec)

Von Anfang an war bei IPv6 vorgesehen harte kryptografische Verschlüsselung und Authentisierung zu integrieren. Dazu sind unter dem Sammelbegriff IPsec zusätzliche Extension Header und Schlüsselaustauschverfahren spezifiziert worden, die es erlauben, Pakete in der Internet-Schicht zu verschlüsseln und/oder zu authentisieren. Das Verfahren wurde erfolgreich und ohne funktionale Verluste nach IPv4 „rückportiert“, wo es für viele Implementierungen als optionale Erweiterung zur Verfügung steht.

Grundsätzlich verhält sich IPsec unabhängig von der IP-Version immer gleich, sodass eine detaillierte Erläuterung an dieser Stelle entfallen kann. Durch den Wegfall von NAT sind die Protokolle und Implementierungen von IPSec für IPv6 einfacher als bei IPv4. Es gibt aber einige wesentliche Unterschiede zwischen IPv4 und IPv6.

Anders als bei IPv4 ist IPsec gemäß [RFC 4305] zwingender Bestandteil aller RFC-konformen IPv6-Implementierungen. In der Aktualisierung der Spezifikation ([RFC 6434], Dezember 2011) wurde diese Forderung jedoch gelockert. IPSec wird nun nicht mehr zwingend gefordert, sondern lediglich empfohlen (in der RFC-Terminologie SHOULD statt MUST).

Dennoch setzen manche Protokolle, wie zum Beispiel die in Abschnitt 3.8.4 bereits erläuterten Routing-Protokolle, voraus, dass IPsec zur Verfügung steht.

Aufgrund der international immer noch weitverbreiteten Beschränkungen für Verwendung, Im- und Export von harter Verschlüsselung haben eine Reihe von Herstellern IPsec überhaupt nicht oder ohne die als Minimum im Standard vorgeschriebenen harten Verschlüsselungsalgorithmen (und damit nur mit dem leeren Null-Algorithmus) implementiert.

Der Einsatz von IPsec bedingt zusätzlichen Rechenaufwand, den die Verschlüsselungsalgorithmen erfordern, und erhöht damit die Verwundbarkeit gegenüber Denial-of-Service-Angriffen.

Ein weiteres fundamentales Problem aller verwendeten kryptografischen Verfahren ist, dass asymmetrische Verfahren nur zum Austausch symmetrischer Schlüssel verwendet werden, die dann wiederum zur Verschlüsselung und/oder Authentisierung der IP-Pakete dienen. Wenn Multicast-Pakete verschlüsselt oder authentisiert werden sollen, müssen alle Absender und Listener den gleichen Schlüssel haben. Damit kann aber jeder Absender oder Listener erfolgreich „authentisierte“ Pakete versenden, deren Source-Adresse nicht seine eigene ist.

3.10.2 Quality of Service (QoS)

Mit IPv6 hat man versucht, den TCP/IP-Protokollstapel um Funktionalitäten zu erweitern, mit denen er dem Echtzeit-orientierten Design klassischer Telefonnetze näher kommt und die unter dem Namen *Integrated Services* (IntServ) zusammengefasst werden. Im Base Header jedes IPv6-Pakets

gibt es ein Flow Label genanntes Feld, mit dem IPv6-Datenströme (Flows) von einem Absender zu einem Empfänger identifiziert werden können. Mit dem Resource Reservation Protocol (RSVP) ist es dann möglich, für einzelne Flows auf dem Pfad vom Absender zum Empfänger Bandbreite auf den Routern zu reservieren.

IntServ setzt voraus, dass das Routing zwischen Absender und Empfänger unveränderlich ist, und verträgt sich deshalb nicht mit dynamischem Routing. Der Verwaltungsaufwand auf den einzelnen Routern, die über jedes einzelne Paket den zugehörigen Flow ermitteln und dann Buch führen müssen, ist immens. Außer in wenigen, sehr speziellen und für einen spezifischen Anwendungszweck angelegten Netzen ist damit IntServ praktisch nicht nutzbar, selbst wenn Router IntServ durchgängig implementieren sollten.

Als pragmatische Alternative unterstützt IPv6 genau wie auch IPv4 unter dem Namen *Differentiated Services* (DiffServ) die Markierung von Paketen zur bevorzugten Behandlung durch Router. Dieses bewährte Verfahren passt deutlich besser in das Design des TCP/IP-Protokollstapels. Das IPv6-Äquivalent zum ToS-Feld im IPv4-Header ist das Traffic-Class-Feld (TC). Abgesehen von der Umbenennung unterscheiden sich ToS- und TC-Feld nicht voneinander.

3.10.3 Mobile IPv6

Mobile IPv6 [RFC 3775] ist eine optionale Protokollerweiterung, mit der mobilen Geräten trotz wechselnder Netzanbindung eine feste IPv6-Adresse zugeordnet werden kann. Auch wenn sich die Netzanbindung eines solchen mobilen Gerätes ändert, bleiben existierende TCP-Verbindungen erhalten.

Zunächst funktioniert Mobile IPv6 wie ein Virtual Private Network (VPN), allerdings nicht unbedingt mit der VPN-typischen Verschlüsselung: Sämtlicher Verkehr von und zum VPN-Client, der hier *Mobile Node* heißt, wird über einen VPN-Server geroutet, den *Home Agent*. Damit hat Mobile IPv6 alle Sicherheitsprobleme, die auch von mobilen VPN-Clients her bekannt sind.

Darüber hinaus unterstützt Mobile IPv6 unter der Bezeichnung *Route Optimization* auch noch einen weitergehenden Mechanismus, mit dem der Mobile Node Geräte, die mit ihm eine Verbindung aufbauen oder unterhalten, den sogenannten *Correspondent Nodes*, über seine aktuelle „tatsächliche“ IP-Adresse informieren kann. Wenn Route Optimization eingeschaltet ist, wird die Kommunikation zwischen Mobile Node und Correspondent Nodes im Wesentlichen ohne den Umweg über den Home Agent abgewickelt.

Wie in [RFC 4487] dokumentiert, schließen sich der Einsatz von Route Optimization und von Sicherheits-Gateways faktisch gegenseitig aus. Außerdem lässt sich Route Optimization trivial dazu missbrauchen, den aktuellen Aufenthaltsort des Mobile Node in Form seiner aktuellen „tatsächlichen“ Adresse zu ermitteln.

Aufgrund dieser noch ungelösten, im Design verankerten Sicherheitsprobleme ist für die hier betrachteten Szenarien vom Einsatz von Mobile IPv6 über das Internet oder andere ungeschützte Netze dringend abzuraten, wenn nicht erhebliche anwendungsspezifische Sicherungsmaßnahmen zusätzlich eingesetzt werden. Auch der interne Einsatz innerhalb eines geschlossenen Netzes setzt Sicherungsmaßnahmen voraus, die in diesem Leitfaden jedoch nicht betrachtet werden.

3.11 IPv4/IPv6-Interoperabilität

Wie schon in Abschnitt 3.1 deutlich wurde, funktionieren IPv4 und IPv6 unabhängig voneinander, eine „automatische“ Kommunikation zwischen beiden gibt es nicht. Wenn reine IPv4-Geräte mit reinen IPv6-Geräten kommunizieren sollen, muss eine Brücke zwischen beiden Seiten geschlagen werden (siehe Abbildung 3.8).

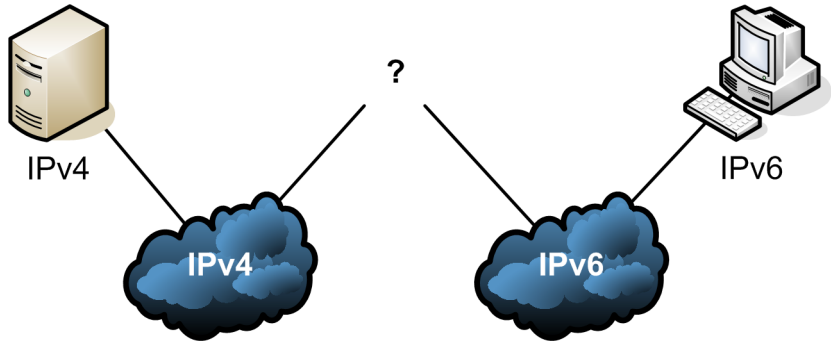

Abbildung 3.8: Verbindung zwischen IPv4 und IPv6

3.11.1 Dual-Stacked Server

Die pragmatischste Lösung des Interoperatibilitätsproblems ist, eine der beiden Seiten *Dual-Stacked* zu betreiben. Dieses Vorgehen ist insbesondere dann sinnvoll, wenn die Anzahl der Geräte auf beiden Seiten deutlich voneinander abweicht, also typischerweise einige wenige Server einer großen Zahl von Clients gegenüberstehen.

Das Verfahren hat eine Reihe von Vorteilen, mit denen es allen anderen Ansätzen überlegen ist: Es benötigt keine zusätzliche Hardware, verursacht den geringst möglichen zusätzlichen Aufwand bei der Systemadministration, bringt nur minimale zusätzliche potenzielle Fehlerquellen mit sich und funktioniert mit allen Anwendungsprotokollen. Im Dual-Stack Betrieb sind Server sowohl über IPv4 als auch über IPv6 erreichbar. Daher sind auch beide Protokollstapel angreifbar.

Damit dieser Ansatz funktioniert, ist es allerdings notwendig, die Dual-Stacked betriebenen Systeme selbst administrativ zu kontrollieren. Außerdem muss die darauf eingesetzte Software in der Lage sein, sowohl IPv4 als auch IPv6 zu unterstützen, ohne dass es dabei zu Performance- oder Stabilitätsproblemen kommt. Dieser Ansatz ist insbesondere für interne Zwecke geeignet.

3.11.2 Anwendungsspezifische Proxys und Application Level Gateways (ALGs)

Ist es unmöglich, den eigentlichen Server Dual-Stacked zu betreiben, ist in vielen Fällen der einfachste Weg, um die Verbindung zwischen IPv4 und IPv6 herzustellen, ein anwendungsspezifischer Proxy. Dazu wird zunächst ein weiterer Rechner Dual-Stacked mit IPv4 und IPv6 angebunden, auf ihm wird die Proxy-Software installiert und gestartet. Alle Clients werden so konfiguriert, dass sie für das Anwendungsprotokoll den Proxy benutzen. Die Proxy-Software ist typischerweise nicht speziell dafür geschrieben, als Proxy zwischen IPv4 und IPv6 eingesetzt zu werden; sie muss nur sowohl IPv4 als auch IPv6 unterstützen.

Ein typisches Beispiel für einen anwendungsspezifischen Proxy ist ein Mail Relay oder Mail Forwarder, der per SMTP Mails annimmt und weiterleitet. Solange er Dual-Stacked angebunden ist, erfüllt er ohne weitere Konfiguration auch die Rolle des Proxys zwischen IPv4 und IPv6. Die

Mehrheit der heute üblichen Mail Transport Agents (MTAs) unterstützt IPv6 und lässt sich damit auch als Proxy benutzen. Auch für Webserver lässt sich dieses Verfahren nutzen.

Insbesondere bei der externen Anbindung durch ein mehrstufiges Sicherheits-Gateway stehen in vielen Fällen anwendungsspezifische Proxys als Application Level Gateways (ALGs) innerhalb der Sicherheits-Gateways zur Verfügung.

Der Einsatz eines Anwendungs-Proxys setzt voraus, dass erstens das Protokoll überhaupt proxytauglich ist und zweitens eine anwendungsspezifische Proxy-Software zur Verfügung steht. Treffen diese beiden Voraussetzungen zu und ist es außerdem unmöglich, wie in Abschnitt 3.11.1 beschrieben, den eigentlichen Server Dual-Stacked zu betreiben, dann ist dieses Vorgehen zu bevorzugen: Es ist in vielen Fällen der wirtschaftlichste Ansatz, funktioniert typischerweise stabil und eventuell im Betrieb auftretende Probleme sind im Allgemeinen gut lösbar.

3.11.3 Transparente Proxys (Transport Layer Translator)

Es gibt Protokolle, die nicht Proxy-tauglich sind (zum Beispiel Skype oder Protokolle, die Ende-zu-Ende verschlüsseln), sodass keine anwendungsspezifischen Proxys für sie zur Verfügung stehen. Insbesondere wenn nur eine kleine, im Vorfeld bekannte Anzahl von Zielgeräten angesprochen werden soll, kann es sinnvoll sein, transparente Proxys einzusetzen.

Im einfachsten Fall ist ein transparenter Proxy ein *TCP-Relay*, das per IPv6 Verbindungen annimmt und diese dann unverändert per IPv4 an das eigentliche Ziel durchreicht. Der Vorteil transparenter Proxys ist, dass die eingesetzte Anwendung nicht proxytauglich sein muss.

3.11.4 Dual-Stacked Clients

Gelegentlich ist keines der bisher genannten Verfahren anwendbar. In diesen Situationen bleibt der Ausweg, Clients Dual-Stacked zu betreiben.

Dieser Ansatz ist prinzipiell unkritisch, führt aber typischerweise zu deutlichem zusätzlichem Aufwand in der System- und Netzwerkadministration und damit zu Folgekosten; außerdem ist die Fehlersuche in Dual-Stacked Netzen tendenziell aufwendiger, sodass dieser Ansatz die Zuverlässigkeit der betroffenen Geräte reduzieren kann.

Um diese Nachteile zu kompensieren, kann es hilfreich sein, statt verteilter Clients mit Dual-Stack zentralisiert Terminal-Server oder eine Gruppe virtueller Clients auf einem entsprechenden Server zu betreiben.

3.11.5 Protocol Translation (NAT-PT, NAT64)

Ein weiteres Verfahren versucht, diese Einschränkungen transparenter Proxys (nicht alle Protokolle lassen sich damit unterstützen, siehe Abschnitt 3.11.3) zu überwinden, indem es in das DNS-Protokoll eingreift. Die transparenten Proxys des Abschnitts 3.11.3 werden dabei durch eine Familie von Mechanismen ersetzt, die unter der Bezeichnung Protocol Translation zusammengefasst werden.

Zunächst werden dabei die transparenten Proxys durch eine Art „erweitertes NAT“ ersetzt, bei dem nicht mehr alleine IPv4-Adressen und Portnummern ausgetauscht werden, sondern ganze IPv4-Header gegen IPv6-Header und umgekehrt. Damit übernimmt dieser Ansatz auch alle Probleme, die aus der IPv4-Welt von NAT bekannt sind. Als Beispiel hierfür kann die Veränderung der Paketlängen durch Austausch von Adressen und Headern dienen, der bei IPv4 durch zusätzliche Fragmentierung unter Inkaufnahme von Performanceverlusten gelöst werden kann. Bei IPv6 ist

dieses Problem nicht standardkonform lösbar, da keine Fragmentierung auf dem Transportweg erlaubt ist.

Anders als bei NAT reicht es aber nicht, anhand von Paketen, die auf dem Gateway ankommen, dynamisch einen entsprechenden State Table (Übersetzungstabelle) zu pflegen. Vielmehr muss ein IPv6-Client, der einen IPv4-Server erreichen will, schon bei seiner DNS-Anfrage nach dem IPv4-Server eine vom Gateway vergebene IPv6-Adresse erhalten, für die ein entsprechender Eintrag im State Table eingerichtet wird.

Damit Protocol Translation funktioniert, müssen sämtliche DNS-Anfragen des Clients über das Gateway umgeleitet werden. Durch den Eingriff des Gateways ins DNS kann es zu verschiedensten Problemen kommen, die in [RFC 4966] ausführlich diskutiert werden und die Grund genug waren, das ursprüngliche NAT-PT als *Historic* zu erklären und von seiner Verwendung dringend abzuraten.

Derzeitig existiert eine Spezifikation für NAT64 [RFC 6146], das in Kombination mit DNS64 [RFC 6147] die oben beschriebene DNS-Probleme beherrschbar macht. Dennoch sollte in produktiven Umgebungen nach Möglichkeit auf den Einsatz verzichtet werden. Eventuelle Ausnahmen von dieser Regel setzen eine detaillierte Analyse der besonderen Bedingungen und der möglichen Auswirkungen auf die Sicherheit und den produktiven Betrieb der Umgebung voraus.

Mit 464XLAT [RFC 6877] steht ein Verfahren zur Verfügung, das in reinen IPv6-Umgebungen zur Bereitstellung von IPv4 genutzt werden kann. Es ist zu erwarten, dass diese Art der Protocol Translation insbesondere im Mobilfunkumfeld Verbreitung finden wird.

3.12 Tunnel

Neben der Interoperabilitätsthematik, bei der die Endpunkte unterschiedliche IP-Versionen „sprechen“, kommt es immer wieder zu der Situation, dass zwar die Endpunkte die gleiche IP-Version benutzen, aber Teile des Netzes zwischen den beiden diese IP-Version nicht unterstützen.

Aktuell ist die gängigste Variante dieses Problems, dass Endpunkte IPv6 verwenden, aber auf Teilen des Netzes dazwischen nur IPv4 geroutet wird. In der Zukunft, wenn IPv4 zur Altlast geworden ist und nicht mehr durchgehend geroutet wird, muss man auch mit der umgekehrten Variante rechnen. Um die Kommunikation zwischen den Endpunkten trotzdem zu ermöglichen, werden Tunnel verwendet.

3.12.1 Grundprinzipien und Terminologie

Abbildung 3.9 zeigt ein typisches Tunnelszenario. Der Absender ganz links schickt ein IPv6-Paket an den Empfänger ganz rechts. Das Paket wird zunächst wie gewohnt durch die linke Netzwolke

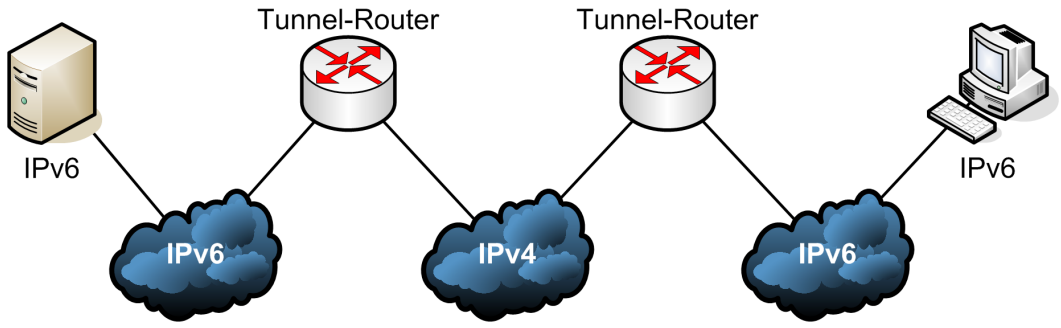

Abbildung 3.9: Tunnelszenario

geroutet, bis es den Tunneleingangspunkt (engl. Tunnel Entry Point) erreicht. Weil die mittlere Netzwolke nur IPv4 unterstützt und deshalb das Paket nicht routen kann, „verpackt“ der Tunneleingangspunkt das gesamte IPv6-Paket als Nutzdaten (engl. Payload) in ein IPv4-Paket, das zum Tunnelausgangspunkt (engl. Tunnel Exit Point) geroutet werden kann, und schickt es durch die mittlere Netzwolke. Wenn der Tunnelausgangspunkt dieses „getunnelte“ Paket erhält, entnimmt er das ursprüngliche IPv6-Paket aus den Nutzdaten und routet es wie gewohnt per IPv6 durch die rechte Netzwolke bis zum Empfänger. Solche Verfahren können genutzt werden, um IPv6-Inseln einzubinden, die nur über eine IPv4-Anbindung verfügen.

Durch das Verpacken von einem Paket in einem anderen haben sich für die Header die Bezeichnungen innerer Header für den Header des ursprünglichen Pakets und äußerer Header für den vom Tunneleingangspunkt erzeugten Header etabliert.

Im einfachsten Fall, wie im oben dargestellten Beispiel, wird IP in IP verpackt. Für alle Kombinationen von IPv4 und IPv6 sind die Details, wie das Verpacken zu geschehen hat, spezifiziert. Je nach Implementierung ist es damit auch problemlos möglich, IPv4 in IPv4 oder IPv6 in IPv6 zu tunneln – auch wenn derartige Konstruktionen eher nur in Ausnahmefällen sinnvoll sind.

Neben den IP-in-IP-Tunneln ist es auch möglich, IP in andere Protokolle wie beispielsweise in UDP zu verpacken. Speziell in Kombination mit UDP oder TCP als äußerem Protokoll ist es möglich, auch durch NAT-Gateways hindurch einen Tunnel zu betreiben.

Abgesehen von den inneren und äußeren Protokollen unterscheiden sich Tunnelmechanismen in der Art, wie der Tunneleingangspunkt die äußere Zieladresse eines Pakets, also die Adresse des Tunnelendpunkts, bestimmt. Insbesondere wenn IPv6 über IPv4 getunnelt werden soll, gibt es für unterschiedliche Anwendungsszenarien eine recht unübersichtliche Auswahl von Varianten.

Weil die Kommunikation zwischen Endpunkten nur in seltenen Ausnahmefällen ausschließlich in einer Richtung erfolgt, werden Tunnel oft als gegenläufiges Tunnelpaar eingerichtet. Deshalb wird ein solches Tunnelpaar oft zusammen als Tunnel und die beiden Tunnelanfangs- und Endpunkte als Tunnelrouter bezeichnet. Insbesondere bei der Konfiguration und Fehlersuche führt das gelegentlich zu Verwirrung und Missverständnissen; gerade in diesen Situationen ist es wichtig, immer beide Richtungen als eigenständige Tunnel zu berücksichtigen.

Im Folgenden werden die wichtigsten Tunnel kategorisiert und kurz erläutert. Eine ausführlichere Übersicht findet sich in [RFC 7059]. Allgemeine Sicherheitsaspekte für IP-Tunnel sind in [RFC 6169] zusammengefasst.

3.12.2 Produktiv nutzbare Tunnel

Der bevorzugte Ansatz, IPv6 über IPv4 zu tunneln, ist die Verwendung *konfigurierter (6in4-)Tunnel* (engl. configured (6in4) tunnel), bei denen der Tunneleingangspunkt mit der IP-Adresse des Tunnelendpunkts explizit konfiguriert wird. Diese Tunnel werden typischerweise als bidirektionales Tunnelpaar konfiguriert. Sie sind in [RFC 4213] standardisiert und sollten ohne nennenswerte Kompatibilitätsprobleme auch zwischen Produkten unterschiedlicher Hersteller funktionieren.

Allgemein ist es möglich, beliebige IP-Versionen durch konfigurierte (IP-in-IP-)Tunnel zu transportieren. Langfristig werden vermutlich konfigurierte 4in6-Tunnel dazu verwendet werden müssen, für Altsysteme IPv4-Konnektivität über reine IPv6-Netze bereitzustellen.

Neben IP-in-IP-Tunneln gibt es die in [RFC 2784] spezifizierte Alternative der *Generic Routing Encapsulation* (GRE). Dieser generische Tunnelmechanismus funktioniert grundsätzlich wie ein IP-in-IP-Tunnel, ist aber nicht alleine auf IP-Protokolle beschränkt. Für diese zusätzliche Flexibili-

tät belegt GRE in jedem Paket acht Bytes mit zusätzlichen Informationen, hat also einen etwas größeren Overhead als IP-in-IP-Tunnel.

GRE-Tunnel sind wichtig, wenn die verwendeten Implementierungen auf den Tunnelroutern in Verbindung mit GRE-Tunneln eine bessere Performance liefern als mit IP-in-IP-Tunneln. Bei Performance-Problemen mit IP-in-IP-Tunneln sind GRE-Tunnel deshalb eine akzeptable Alternative.

3.12.3 Produktiv nutzbare tunnel-ähnliche Mechanismen

In manchen Fällen ist es möglich, tunnel-ähnliche Mechanismen, die schon aus anderen Gründen eingesetzt werden, zusätzlich auch als Tunnel zu benutzen.

Manche VPN-Lösungen erlauben es, neben IPv4 auch IPv6 durch das VPN zu transportieren. Insbesondere die Anbindung von mobilen Geräten, wie Notebooks von Außendienstmitarbeitern, erfolgt typischerweise über VPN-Lösungen, wie in [ISi-Fern] beschrieben. Statt zunächst ein reines IPv4-VPN aufzusetzen, um dann jedes dieser Geräte über einen Tunnel mit einer IPv6-Anbindung zu versorgen, sollten die Möglichkeiten der verwendeten VPN-Lösung genutzt werden. Unterstützt das verwendete VPN den Transport von IPv6 nicht, muss im Einzelfall entschieden werden, ob es sinnvoller ist, die VPN-Lösung auszutauschen oder über die existierende VPN-Lösung einen Tunnel zu betreiben.

In manchen Fällen hat sich der Einsatz von VPN-Lösungen als Tunnelersatz auch deshalb bewährt, weil viele VPN-Lösungen in der Lage sind, durch NAT-Gateways hindurch einen Tunnel aufzubauen, was bei IP-in-IP-Tunneln zusätzliche Konfigurationen auf dem NAT-Gateway voraussetzt, die oft aus technischen oder organisatorischen Gründen nicht möglich sind.

Bei der Beschaffung und Konfiguration der VPN-Lösung muss auch IPv6 betrachtet werden. Dies gilt selbst dann, wenn intern nur IPv4 eingesetzt wird, da es im Außeneinsatz zu unerwünschten Effekten kommen kann (siehe auch Gefährdung 7.5.9).

LISP [RFC 6830] dient nicht, wie ein VPN, zur Verbindung zweier Knoten oder Netze, sondern ist vielmehr eine Routing-Variante. Dabei wird zwischen der Identität und dem Aufenthaltsort unterschieden. Somit kann ein Gerät auch beim Wechsel in ein anderes Netz eindeutig adressiert werden.

3.12.4 Ungeeignete Tunnel

Neben den bisher vorgestellten Tunnelvarianten gibt es mehrere andere Ansätze, die aus verschiedenen Gründen für den produktiven Einsatz nicht geeignet sind:

- 6to4-Tunnel nach [RFC 3056] verwenden ein hochgradig asymmetrisches Routing, das eine zuverlässige Fehlerdiagnose und -behebung unmöglich macht.
- 6rd-Tunnel nach [RFC 5569] sind für den Einsatz innerhalb des Netzes eines Internetserviceproviders (ISP) konzipiert und erlauben nur die Anbindung eines einzelnen Subnetzes.
- 6over4-Tunnel nach [RFC 2529] setzen ein funktionierendes IPv4-Multicast-Routing voraus und binden nur einzelne Hosts per Tunnel an.
- 6a44 nach [RFC 6751] ist ein experimentelles Protokoll. Es wurde entwickelt um die Probleme mit Teredo (siehe Abschnitt 3.12.5) zu beseitigen. So wird der Tunnel beispielsweise nicht zu einem Microsoft-Relay sondern zu einem Relay beim ISP aufgebaut. Auf den Einsatz von 6a44 sollte dennoch verzichtet werden, da es auf dem gleichen Prinzip wie Teredo basiert.
- 6bed4 ist noch nicht in einem RFC spezifiziert, soll jedoch eine direkte bidirektionale Verbindung zwischen zwei Hosts ermöglichen. Dabei soll auch UDP zum Einsatz kommen, um die Kommunikation über NAT-Gateways zu ermöglichen.

- SEAL ist ein weiteres experimentelles Protokoll, das noch nicht abschließend spezifiziert ist. SEAL führt einen zusätzlichen Layer zwischen innerem Paket und äußerem Header ein, um insbesondere die MTU-Problematik zu lösen.

3.12.5 Sicherheitskritische Tunnel

Zwei weitere Tunnelmechanismen haben sich nicht nur als ungeeignet für den produktiven Einsatz, sondern aus verschiedenen Gründen als Sicherheitsproblem herausgestellt. Beide zeichnen sich dadurch aus, dass insbesondere Microsoft Windows ab Vista beim Starten in einer reinen IPv4-Umgebung versucht, mit einem dieser Tunnel-Mechanismen eine IPv6-Anbindung ins Internet aufzubauen.

- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) nach [RFC 5014] versucht, den unqualifizierten DNS-Namen `isatap` aufzulösen und, wenn es auf diese Anfrage IPv4-Adressen erhält, dorthin einen Tunnel aufzubauen.
- Teredo nach [RFC 4380] versucht, einen UDP-basierten Tunnel zu teredo.ipv6.microsoft.com auf UDP-Port 3544 aufzubauen. Weil Teredo über UDP tunnelt, ist es in der Lage, auch NAT-Gateways zu durchdringen.

Insbesondere bei mobilen VPN-Clients stellen diese Mechanismen eine erhebliche Gefahr dar und müssen konsequent abgeschaltet werden.

4 Grundlagen Internet-Anbindung

Eine Anbindung an das Internet ist heute Stand der Technik für nahezu alle lokalen Netze. Ohne diese funktionieren viel Prozesse und Abläufe in Verwaltung und Fertigung nicht mehr oder nur sehr eingeschränkt.

Eine Internet-Anbindung birgt jedoch grundsätzliche Risiken. Unter Sicherheitsaspekten ist daher eine Abwägung erforderlich, ob eine Internet-Anbindung des gesamten LANs überhaupt erforderlich ist und ob der Nutzen des Internet-Anschlusses die damit einhergehende Risiken aufwiegt [ISi-E]. Bei sehr hohem Schutzbedarf ist davon auszugehen, dass eine Online-Verbindung nicht gerechtfertigt ist.

In den meisten Fällen sollte von einer abgestuften Realisierung ausgegangen werden, bei der gezielt nur die Teile des lokalen Netzes in jeweils dem Maße Zugang zum Internet haben, wie es individuell sinnvoll und notwendig ist. IPv6 bietet durch seinen großen Adressraum hier viele zusätzliche Möglichkeiten, Netze besser zu strukturieren und optimaler an die lokalen Bedürfnisse anzupassen, ohne den Aufwand für das Filtern ins Extreme zu treiben.

4.1 Techniken zur Anbindung an das Internet

Es gibt unterschiedliche Techniken zur Anbindung eines LANs an ein Provider-Netz. Damit lassen sich unterschiedliche Bandbreiten und Übertragungsgüten (Bitfehlerraten) realisieren. Die wichtigsten Anschlussmöglichkeiten und ihre charakteristischen Merkmale sind:

- Leitungsgebunden (Kupfer): breite Verfügbarkeit, kostengünstige Anschlusstechnik, hohe Übertragungsraten, geringe Bitfehlerrate, geringe Betriebskosten
- Leitungsgebunden (Glasfaser): sehr hohe Übertragungsraten, sehr geringe Bitfehlerrate, sehr geringe Störanfälligkeit, aufwendigere Anschlusstechnik, Bereitstellung ortsabhängig, geringe Betriebskosten
- Drahtlos (terrestrisch): geringe Baumaßnahmen erforderlich, schnelle Bereitstellung, begrenzte Bandbreite, hohe Störanfälligkeit und Abhörgefährdung
- Drahtlos (Satellit): ortsunabhängige, schnelle Bereitstellung, geringe Bandbreite, große Übertragungslatenz aufgrund langer Signallaufzeiten, hohe Störanfälligkeit und Abhörgefährdung, hohe Betriebskosten

Eine vertiefende Analyse der verschiedenen Übertragungstechniken bietet [BSI Standl-Tech].

4.1.1 Permanente Verbindungen

Für die dauerhafte Einrichtung eines Zugangs zu einem Internet-Diensteanbieter kommen unterschiedlichste Übertragungsverfahren zum Einsatz (z. B. ATM, ISDN-S2M, Frame Relay, MPLS). Kundenseitig steht dem Benutzer typischerweise eine Ethernet-Schnittstelle zur Verfügung.

Der Provider-Zugang kann auf unterschiedlichen Protokollebenen hergestellt werden. Je niedriger die Protokollebene, desto größer ist in der Regel die Unabhängigkeit von den Sicherheitsvorkehrungen des Providers und die Entkopplung von anderen Provider-Kunden (d. h. die Exklusivität der Verbindung), desto höher aber auch der technisch-administrative Aufwand für den Betrieb. Die Abhängigkeit von einem Internet-Diensteanbieter erfordert eine präzise Dienstgütevereinbarung

(Service Level Agreement, SLA), eine klare Abgrenzung der administrativen Domänen von Provider und Kunde sowie die sorgfältige Auswahl eines vertrauenswürdigen Anbieters.

Es ist damit zu rechnen, dass einige der älteren erwähnten Techniken (zum Beispiel ATM oder Frame-Relay) nicht mehr als Trägertechnik für IPv6 am Markt angeboten werden. Für feste Verbindungen kann man bei IPv6-tauglichen Angeboten mit der Übergabe an einer Ethernet-Schnittstelle rechnen.

Lösungen unterhalb der Netzzugangsschicht

Bei Lösungen unterhalb der Netzzugangsschicht stellt der Anbieter entweder ein passives physisches Kommunikationsmedium zur Verfügung (z. B. Dark Fiber, Satelliten- oder Richtfunk-Verbindung), über das der Benutzer mit eigenem Netzabschlussgerät und einem Protokoll seiner Wahl kommuniziert. Alternativ dazu kann der Anbieter auch ein bittransparentes Übertragungsprotokoll bereitstellen, über das der Kunde eigene Netzzugangsprotokolle betreiben kann.

Leitungsgebundene „Leerverbindungen“ sind jedoch nur in Sonderfällen verfügbar. Drahtlose Verbindungen bieten hingegen nur beschränkte Verbindungsgüte, Bandbreite und Sicherheit zu oft hohen Betriebskosten. Sie eignen sich daher hauptsächlich als Notfall- oder Übergangslösung.

Lösungen auf der Netzzugangsschicht

Bei Lösungen auf der Netzzugangsschicht stellt der Anbieter dem Kunden ein Netz mit einer variablen Anzahl von Zugangspunkten bereit (z. B. in Form von Standard-Festverbindungen). Solche Netze werden auch als *Switched Links* bezeichnet, denn die Netzzugangsschicht bietet bereits eine Adressierung des Kommunikationspartners, was unter anderem Punkt-zu-Mehrpunkt-Verbindungen ermöglicht. Der Kunde muss allerdings darauf achten, dass der Anbieter ausreichende Sicherheitsvorkehrungen trifft, um eine exklusive Nutzung des Netzes zu gewährleisten. Wenn sich in einem Gebäudekomplex zum Beispiel mehrere Parteien ein gemeinsames Teilnehmeranschlussgerät teilen (z. B. einen Switch mit je einem VLAN pro Kunde), so ist der Netzzugangsbereich bereits als öffentliches, nicht vertrauenswürdiges Netz zu behandeln. In diesem Falle müssen die Verbindungen auf höheren Protokollschichten zusätzlich abgesichert werden.

Lösungen auf der Internet-Schicht

Bei Lösungen auf der Internet-Schicht stellt der Anbieter dem Kunden eine komplette virtuelle LAN-Infrastruktur (ein sogenanntes *Trusted VPN*, siehe Abschnitt 4.2.1) einschließlich Konfiguration, Management, Entstörung und Überwachung bereit. Aus Sicht des Kunden ist dies die komfortabelste Lösung. Allerdings hängt die Sicherheit und Güte der Verbindungen stark von der Kompetenz und dem Verhalten des Internet-Diensteanbieters ab. Für eine vertrauliche Übertragung ist ein Trusted VPN daher unzureichend. Sensible Informationen bedürfen zusätzlicher Maßnahmen zur Verschlüsselung und Authentisierung in höheren Protokollschichten.

4.1.2 Wählverbindungen

Eine preisgünstige Alternative zu einer aufwendigen, permanenten Internet-Anbindung ist eine temporäre, bedarfsweise Verbindung zu einem Einwahl-Knoten des Anbieters über eine ISDN- oder Analogverbindung. Angesichts des typischen Bandbreitenbedarfs heutiger Anwendungen eignen sich solche Verbindungen in der Regel nur zur Überbrückung akuter Notsituationen. Zudem werden dem Einwahl-Kunden dynamisch wechselnde IP-Adressen zugewiesen. Das Anbieten von Internet-Diensten über Wählverbindungen ist daher schwierig.

Ob und in welchem Umfang Wählverbindungen mit IPv6 am Markt angeboten werden, lässt sich zum Zeitpunkt der Erstellung des Leitfadens noch nicht abschätzen. Die zunehmende Verbreitung der DSL-Technik bietet inzwischen eine leistungsfähigere Anbindung zu vergleichbaren Kosten. Daher geht die Bedeutung von Wählverbindungen mit Hilfe von Modems oder ISDN-Anschlüssen stark zurück.

4.1.3 DSL

Eine Digital Subscriber Line (DSL) ermöglicht quasi-permanente Verbindungen über eine gewöhnliche Analog- oder ISDN-Teilnehmeranschlussleitung des vermittelnden Telefonnetzes, wahlweise mit asymmetrischer oder symmetrischer Uplink/Downlink-Bandbreite. DSL-Verbindungen werden im Allgemeinen in regelmäßigen Zeitintervallen vom Anbieter getrennt, bei Bedarf aber binnen Kurzem neu aufgebaut. Dies kann kurzzeitige Leitungsunterbrechungen, gegebenenfalls auch einen Wechsel der IP-Adresse des Kunden zur Folge haben.

Speziell für das Anbieten von Internet-Diensten gibt es eine symmetrische DSL-Variante (SDSL). Hier ist dem Kundenanschluss meist eine feste IP-Adresse zugeordnet. Für eine reine Dienstnutzung in begrenztem Umfang genügt jedoch die asymmetrische Variante (ADSL) mit dynamisch vergebener IP-Adresse.

4.2 Virtuelle Private Netze

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (meist des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen und die Kommunikationspartner sicher authentisieren, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Synonym für verschlüsselte Verbindungen verwendet. Zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls. Man unterscheidet zwei grundlegende VPN-Varianten: Trusted VPN und Secure VPN.

4.2.1 Trusted VPN

VPNs werden als *Trusted VPN* bezeichnet, wenn die vertrauliche Verbindung verschiedener Standorte durch externe VPN-Dienstleister gewährleistet wird. Dabei werden die Daten aus dem vertrauenswürdigen Netz in der Regel unverschlüsselt über einen dedizierten Kommunikationskanal zu einem Gateway-Router des Anbieters geleitet. Die Bildung des VPNs erfolgt dann durch logische Abschottung des VPN-Datenverkehrs vom übrigen Datenverkehr (z. B. mittels Multiprotocol Label Switching, MPLS [RFC 4364]). Für mobile Nutzer stellen Dienstleister zudem VPNs über Gateway-Router bereit, die nur über spezielle Einwahl-Knoten erreicht werden können. Diese Einwahlknoten müssen vor unberechtigtem Zugriff geschützt werden.

Für vertrauliche Daten sind Trusted VPNs ohne zusätzliche Verschlüsselung auf der Anwendungsschicht nicht geeignet, da die Sicherheit solcher Verbindungen ausschließlich in Händen des Internet-Diensteanbieters liegt. So bietet ein Trusted VPN zum Beispiel keinen Schutz gegen Innentäter des Anbieters. Für vertrauliche Datenkommunikation empfiehlt sich daher ein Secure VPN.

4.2.2 Secure VPN

Die Abhängigkeit von Dritten kann vermieden werden, wenn die Vertraulichkeit der Kommunikationsverbindung an den Endpunkten der Verbindung durch Verschlüsselung gewährleistet wird, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Man bezeichnet diese Lösung auch als *Secure VPN*.

Die am weitesten verbreiteten Technologien zur Erzeugung von Secure VPNs sind zurzeit IPSec und SSL-VPNs. Während IPSec eigens zur Realisierung von VPNs entworfen wurde, wird bei SSL-VPNs die SSL-Erweiterung des TCP/IP-Stacks zum Aufbau sicherer Transportverbindungen für alle Protokolle auf Anwendungsschicht verwendet.

Bei IPv6 kommt neu gegenüber IPv4 hinzu, dass nach den Spezifikationen und RFCs der IETF alle vollständigen Implementierungen von IPv6 als integralen Bestandteil IPsec enthalten müssen. IPsec sollte daher keine zusätzliche, extra zu implementierende Software sein, sondern ist nach dem Willen der IETF ein Bestandteil des Stacks, der lediglich noch konfiguriert werden muss. Allerdings klafft zwischen dem von der IETF angestrebten Zustand und der Umsetzung in den verfügbaren Implementierungen zum Teil noch eine große Lücke. IPsec ist oftmals nur rudimentär und nur sehr selten wirklich in vollem Umfang implementiert.

4.3 Komponenten eines Sicherheits-Gateways

Ein Sicherheits-Gateway gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Grundsätzlich besteht bei der Funktion eines Sicherheits-Gateways kein Unterschied zwischen IPv4 und IPv6, lediglich die Adressen sind entsprechend länger.

Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen *Paketfilter* und *Application-Level Gateway* (ALG) zu unterscheiden. Wie in Abbildung 4.1 dargestellt ist, baut sich ein Sicherheits-Gateway aus einem nach außen gerichteten Paketfilter (PF1), einem Application-Level-Gateway (ALG) und einem zum internen Netz hin zeigenden Paketfilter (PF2) auf.

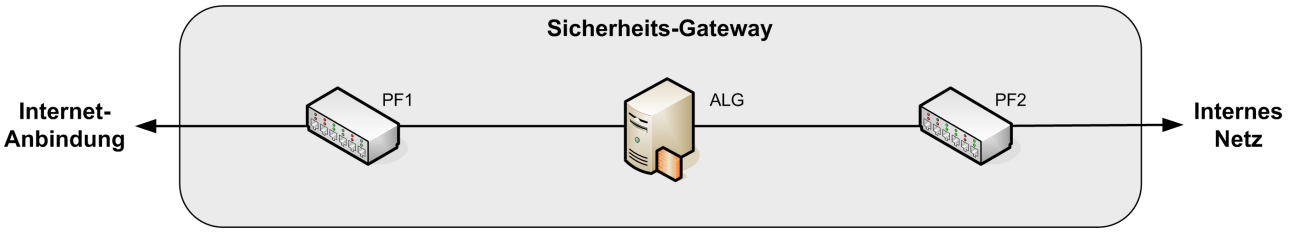

Abbildung 4.1: PAP-Struktur des Sicherheits-Gateways

Paketfilter verhindern Angriffe auf Internet- und Transportschicht und reglementieren den Zugriff auf ALGs. ALGs überwachen und kontrollieren die Kommunikation auf der Anwendungsschicht. Für IPv4 stellen Paketfilter bedarfsweise die Funktion Network Address Translation (NAT) zur Verfügung. Für IPv6 übernehmen diese Aufgabe implizit die ALGs.

Filter-Komponenten verfügen meist über kombinierte Funktionalität oder stellen diese Funktionen mit zwei Geräten in einem Gehäuse zur Verfügung. Bei modernen Geräten hat sich allgemein die

zustandsbehaftete Paketfilterung durchgesetzt. Paketfilter ohne Speicherung des Zustands und damit ohne Filterung abhängig vom Zustand der Verbindung genügen nur einfachsten Ansprüchen. Empfehlenswerte Geräte und Anwendungen bieten zusätzliche ALG-Funktionen sowie gegebenenfalls eine Auskoppelschnittstelle zur Integration weiterer, separat betriebener Sicherheits-Proxys an. Über die Schnittstelle sind modulare Erweiterungen des Sicherheits-Gateways möglich.

Für IPv6 sollte zusätzlich auf eine gute Bedienbarkeit bei der Eingabe und Verwaltung von IP-Adressen geachtet werden. Durch die längeren Adressen tritt der Wunsch von Eingabemöglichkeiten symbolischer Namen statt numerischer Adressen und Netzen deutlich weiter in den Vordergrund.

Ob man die Filterung von IPv4-Verkehr und IPv6-Verkehr im gleichen Gerät realisiert oder dafür getrennte Anwendungen oder Geräte einsetzt, unterliegt den gleichen Überlegungen wie die Kombination aus Paketfilter und ALG – ein Kombinieren spart Kosten und erleichtert die Bedienung, ein Trennen erfordert höheren Aufwand, bietet aber auch höhere Sicherheit bei der Kompromittierung einzelner Komponenten.

4.3.1 Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Vielfach bieten Paketfilter auch eine Möglichkeit zur Adressumsetzung (Network Address Translation, NAT), bei der eine IP-Adresse im IP-Paket-Header durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes gegenüber externen Kommunikationspartnern verborgen.

Paketfilter, die eine Filterentscheidung allein anhand der Header-Daten des Datenpakets treffen, werden *zustandslose Paketfilter* genannt. *Zustandsbehaftete Paketfilter* erweitern dagegen die zustandslose Filterung um die Möglichkeit zur Betrachtung des Kommunikationskontexts (sogenannte *Stateful Inspection*). Die Filterung erfolgt hierbei zum Beispiel abhängig davon, ob die Kommunikationsverbindung von innen nach außen oder von außen nach innen aufgebaut wurde, oder zeitabhängig in einem vorgegebenen Freigabeintervall. Darüber hinaus können zustandsbehaftete Filter oft auch einfache Anwendungsattribute oberhalb der Transportschicht in die Betrachtung einbeziehen.

Einfache Paketfilter lassen sich als Software-Lösung auf PC-Basis unter einem Standardbetriebssystem (z. B. Linux) realisieren. Reine Software-Realisierungen weisen jedoch eine Reihe gravierender Nachteile auf:

- Ihr Durchsatz ist gering, nicht zuletzt wegen der beschränkten Leistungsfähigkeit des Kommunikationsbusses gewöhnlicher PC-Architekturen.
- Aufgrund beweglicher Teile (Festplatte, Lüfter) haben PCs im Dauerbetrieb eine höhere Ausfallwahrscheinlichkeit als Hardware-Lösungen ohne solche mechanischen Komponenten.
- Der Bedienkomfort ist in der Regel geringer als bei spezialisierten Geräten.

Für höhere Ansprüche wird daher normalerweise der Einsatz von Paketfiltern mit maßgeschneiderter Hardware und angepasstem Betriebssystem empfohlen, zum Beispiel eine Appliance, ein Router oder ein kommerzielles „Firewall“-Produkt.

Bei IPv6 haben sich gegenüber IPv4 neben der neuen Adresslänge nur wenige weitere Änderungen ergeben:

- Der Paketfilter muss die Inspektion von Erweiterungsheadern erlauben.
- Der Paketfilter muss mit den veränderten Regeln für das Aufteilen von Paketen (Fragmentierung) zurechtkommen.

Bei der Implementierung zustandsbehafteter Paketfilter für IPv6 ist der erhöhte Speicherbedarf durch die größeren Adressen in Betracht zu ziehen. Dies sollte bei modernen Geräten mit entsprechendem Speicherausbau allerdings nicht mehr zu Problemen führen.

Bei der Auswahl eines Sicherheits-Gateway-Produktes ist darauf zu achten, dass IPv6 in Hardware und nicht in Software implementiert ist. Auch die Unterstützung von IPv6 an der Benutzerschnittstelle ist zu prüfen.

4.3.2 Application-Level Gateway (Sicherheits-Proxy)

Filterfunktionen oberhalb der Transportschicht werden von einem sogenannten Application-Level Gateway übernommen, auch Sicherheits-Proxy genannt. Ein Proxy ist eine Art Stellvertreter für Dienste in Netzen. Er nimmt Daten an seinem Eingang entgegen und leitet sie nach einer Prüfung an den eigentlichen Dienst weiter. Mittels eines Proxys lassen sich Datenströme auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten.

ALGs unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Implizit nehmen sie damit auch Funktionen auf den darunter liegenden Schichten des TCP/IP-Modells wahr. Bei einer Kommunikationsbeziehung zwischen Client und Server über das ALG hinweg nimmt das ALG die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt das ALG analog.

Diese Kommunikationsform ermöglicht es dem ALG beispielsweise, bestimmte Protokollbefehle auf der Anwendungsschicht zu filtern. Das ALG kann zudem die strikte Einhaltung von Anwendungsprotokollen erzwingen, unerwünschte Anwendungsdaten aus den Datenpaketen entfernen (bzw. austauschen) oder Verbindungen anwendungsspezifisch protokollieren.

Verglichen mit einem (meist vorgeschalteten) Paketfilter ermöglicht ein ALG in der Regel nur einen geringeren Durchsatz bei der Datenübermittlung. Um das ALG zu entlasten und seinen Durchsatz zu verbessern, können ALG-Proxy-Funktionen auf separate Proxy-Server ausgelagert werden, die parallel zum ALG betrieben werden (z. B. für das rechenintensive Auftrennen verschlüsselter Verbindungen). Dies verringert bei komplexen Anwendungsprotokollen (z. B. SOAP mit WSS-Erweiterungen) die Angriffsfläche des ALGs und beschleunigt die Übermittlung größerer Datenströme. Das Auskoppeln einzelner Protokolle und deren Umlenken auf einen unabhängigen Proxy-Server verursacht unter Umständen allerdings zusätzliche Paketlaufzeiten (Latenz) für die betroffenen Kommunikationsverbindungen, was sich vor allem bei interaktiven Kommunikationsmustern störend bemerkbar machen kann.

Sicherheits-Proxys können nur unverschlüsselte Daten filtern. Um auch bei verschlüsselter Kommunikation einen Sicherheitsgewinn zu erzielen, ist es daher erforderlich, die Verschlüsselung im Proxy aufzubrechen und gegebenenfalls die Daten für das interne Netz erneut zu verschlüsseln. Das Aufbrechen der Kommunikationsbeziehung zerstört jedoch die Ende-zu-Ende-Sicherheitsgarantien, was nicht in allen Anwendungen tolerierbar ist.

Mit IPv6 steigt die Bedeutung von ALGs durch die neuen Funktionen als Übergang zwischen IPv4 und IPv6 und als Ersatz von NAT deutlich an. Prinzipiell ist kein direkter Datenaustausch möglich zwischen Geräten, die nur IPv4 beherrschen, und solchen, die nur IPv6 implementieren. Um diese Lücke zu überbrücken, werden passende ALGs eingesetzt. ALGs können Adressen innerhalb des Datenstroms passend von IPv4 auf IPv6 umzusetzen.

TCP-Relays

Ein TCP-Relay (auch transparenter Proxy genannt) ist eine minimale Version eines ALGs. Wie bei einem gewöhnlichen, anwendungsspezifischen Sicherheits-Proxy verhindert das TCP-Relay direkte Verbindungen zwischen den Kommunikationspartnern. Statt dessen stellt es zwei getrennte Teilverbindungen zu den beiden Kommunikationsendpunkten her, sofern eine Kommunikation gemäß den konfigurierten Filterregeln zulässig ist. Ein TCP-Relay kann somit auch für die Umsetzung von IPv4 auf IPv6 genutzt werden.

Anders als ein gewöhnlicher Sicherheits-Proxy kontrolliert ein TCP-Relay allerdings nur den Verbindungsaufbau: Ist die Verbindung zulässig, so verbindet das Relay die beiden Kommunikationspartner, ohne den weiteren Datenaustausch zu prüfen oder durch Filterung einzuschränken. Für bestehende Verbindungen ist das Relay somit „transparent“.

Der Vorteil eines TCP-Relays besteht darin, dass es beliebige Anwendungsprotokolle oberhalb von TCP vermitteln kann. Daher werden TCP-Relays immer dann eingesetzt, wenn für ein benötigtes Anwendungsprotokoll kein protokollspezifischer Proxy verfügbar ist. Nachteilig ist jedoch, dass ein TCP-Relay bestenfalls eine Authentisierung der Kommunikationspartner erzwingen kann, nicht jedoch eine Kontrolle der übertragenen Daten. Daher sollten Relays nur als Notbehelf eingesetzt werden, und nur für Verbindungen zu vertrauenswürdigen Kommunikationspartnern.

Außerdem ist bei dieser Variante zu beachten, dass eine ganze Reihe von Anwendungen damit nicht funktionieren, da Adressen innerhalb des Datenstroms (nicht nur in den Headern) transportiert werden.

4.3.3 Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird und sowohl von innen als auch von außen erreichbar ist. Die DMZ ist weniger stark gesichert als das interne Netz, dafür aber besser vom äußeren Netz aus erreichbar. Sie dient der Schaffung eines zusätzlichen Sicherheitsbereichs für Dienste (z. B. E-Mail, Web) oder Proxys, die von externen Netzen aus nutzbar sein sollen, aber aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen.

Durch die Möglichkeit, bei IPv6 deutlich mehr Adressen und Subnetze verwenden zu können, als das bisher üblich war, ergeben sich bessere Möglichkeiten, die DMZ zu strukturieren und die benötigten Filter übersichtlicher aufzubauen und voneinander zu isolieren.

Auch wenn der prinzipielle Aufbau bei der Verwendung von IPv6 ähnlich bleibt, so sind doch zusätzliche Entscheidungen zu treffen:

- Welcher Dienst soll über welches Protokoll erreichbar sein?
- Soll innerhalb der DMZ eine Umsetzung IPv6-IPv4 erfolgen?
- Wie viel der Infrastruktur soll parallel für IPv6 und IPv4 zur Verfügung stehen?

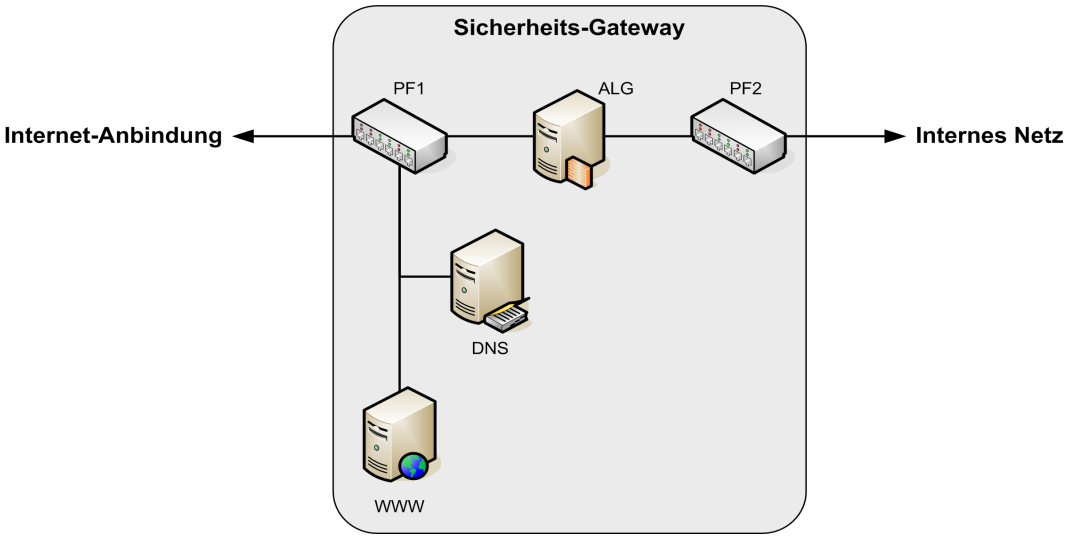

Abbildung 4.2: DMZ mit Server für WWW und DNS

4.3.4 Modulare Erweiterungen

Eine sichere Netzkopplung auf der Anwendungsschicht erfordert die individuelle Anpassung des Sicherheits-Gateways an spezifische Anwendungen im LAN. Daher sind Erweiterungen des Sicherheits-Gateways in der Regel unumgänglich. Dazu werden die betroffenen Anwendungsprotokolle im Gateway ausgekoppelt und gesonderten Erweiterungsmodulen zugeführt.

Grundlegende Empfehlungen zu modularen Erweiterungen eines Sicherheits-Gateways bietet [BSI SGW]. Die wichtigsten modularen Erweiterungen betreffen vor allem

- das Terminieren sicherer Fernzugänge,
- die Funktionsüberwachung der Internet-Anbindung sowie
- das Erkennen und Löschen schädlicher Daten.

Im Folgenden werden diese Erweiterungsmöglichkeiten kurz erörtert. Für alle Erweiterungen gilt bei der Einführung von IPv6 der grundsätzliche Hinweis:

Bei der Verwendung von automatisch generierten IPv6-Adressen (siehe Abschnitt 3.6.1) werden in einigen Fällen die unteren 64 Bit der Adresse (Interface ID) nach [RFC 2373] mit dem in EUI-64 definierten Format aus der MAC-Adresse des jeweiligen Gerätes abgeleitet. Es ist also relativ leicht, eine Zuordnung zwischen Geräten oder ihren Benutzern und Adressen zu erzeugen. Eine solche Adresse würde die Identifizierung von Personen anhand von Verkehrsdaten ermöglichen und hat somit Auswirkungen auf die Anforderungen des Schutzes von persönlichen Daten.

Terminieren von Fernzugriffen

Fernzugänge, die Mitarbeitern im Außendienst einen sicheren LAN-Zugriff über unsichere öffentliche Kommunikationsverbindungen (Client to Site) bieten (auch als *Fernzugriff* oder *Remote Access* bezeichnet) oder entfernte LAN-Segmente über das Internet sicher anbinden (Site to Site), können mit IPv4, IPv6 oder einem Mix aus beiden Protokollen betrieben werden.

Das Thema Fernzugriff wird innerhalb der ISi-Reihe in einem eigenen Modul mit detaillierten Empfehlungen [ISi-Fern] behandelt.

Monitoring

Um schnell auf Anzeichen für Fehlfunktionen oder mangelnde Verfügbarkeit reagieren zu können, ist die kontinuierliche Erfassung und Protokollierung von Parametern wie Kommunikationsaufkommen und Systemauslastung erforderlich.

Bei allen Monitoring-Maßnahmen sind allerdings die geltenden datenschutzrechtlichen Bestimmungen genau einzuhalten, da die erfassten Daten potenziell die Privatsphäre lokaler Netzteilnehmer oder externer Kooperationspartner berühren. Daher sind die Grundsätze des Datenschutzes − zum Beispiel das Wesentlichkeitsprinzip (Datensparsamkeit) und die Zweckbindung − schon bei der Planung und Durchführung von Monitoring-Maßnahmen umfassend zu berücksichtigen.

Beim Einsatz von IPv6 ist auf den notwendigen höheren Schutz der Privatsphäre zu achten, der aus den leichter zuzuordnenden Adressen resultiert. Dies gilt insbesondere für das Monitoring von Zugriffen in das Internet und die Protokollierung solcher Zugriffe.

Zentrales Erkennen und Löschen schädlicher Daten

Das Sicherheits-Gateway trägt entscheidend dazu bei, schädliche Daten (z. B. Computer-Viren, Spam, unerlaubte E-Mail-Dateianhänge) von den LAN-Anwendungen fernzuhalten. Virenschutzprogramme auf den Clients (siehe [ISi-Client]) sind eine weitere Verteidigungslinie, können jedoch eine zentrale Filterung nicht ersetzen.

Für das Ausfiltern schädlicher Daten auf der Anwendungsschicht werden Virenschutzprogramme eingesetzt, die als Sicherheits-Proxys im ALG betrieben werden. Weitergehende Informationen zum Einsatz von Anti-Spam-Maßnahmen finden sich in [ISi-Mail-Server].

4.4 Protokolle für Dienste und Anwendungen

Der Zugang zu öffentlichen E-Mail- und WWW-Funktionen ist ein wesentlicher Anreiz, ein LAN mit dem Internet zu verbinden. Die Vorkehrungen zur Realisierung von E-Mail und WWW sind deshalb in der Grundarchitektur für eine Internet-fähiges LAN zu berücksichtigen.

Am ALG sind daher Proxys für die jeweils relevanten Protokolle zu implementieren. Für E-Mail sind dies POP3, IMAP, SMTP nach [RFC 1939], [RFC 3501] und [RFC 2821] sowie die mit TLS abgesicherten Varianten POP3S, IMAPS und SMTPS nach [RFC 2595] und [RFC 3207]. Die relevanten Protokolle für WWW sind HTTP ([RFC 1945] und [RFC 2616]) sowie HTTPS [RFC 2818].

Eine vertiefende Darstellung der Dienste und ihrer spezifischen Sicherheitsaspekte bieten die ISi-Module [ISi-Mail-Client], [ISi-Mail-Server], [ISi-Web-Client] und [ISi-Web-Server].

Bei der Verwendung von IPv6 sind an den Übergängen noch entsprechende Proxys (siehe Abschnitt 5.1.4 und Abbildung 4.3) vorzusehen, damit die Dienste in der jeweils anderen Protokollwelt erreicht werden können.

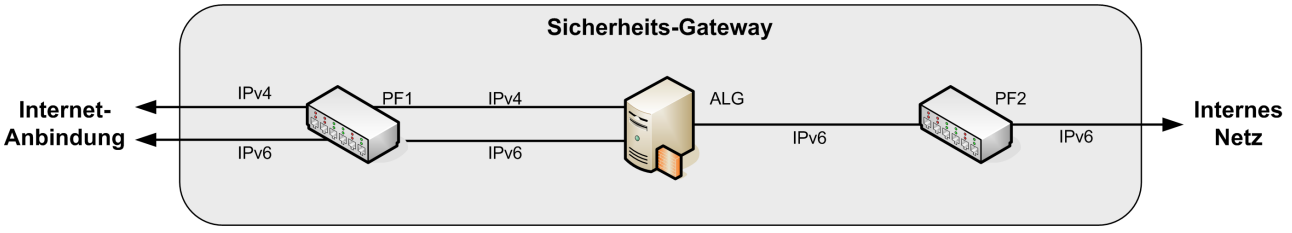

Abbildung 4.3: Sicherheits-Gateway mit ALG zum Übergang von IPv4 zu IPv6

5 Sichere Grundarchitektur für normalen Schutzbedarf

Die vorangegangenen Abschnitte haben die grundlegenden Protokolle, Dienste, Komponenten und Techniken zur Realisierung eines internetfähigen LANs eingeführt. Auf der Basis dieser Grundlagen beschreibt Abschnitt 5 eine Grundarchitektur für ein sicheres LAN mit Internet-Anbindung.

Die hier definierte Grundarchitektur bietet eine Reihe von Erweiterungen und schafft damit Spielräume für Realisierungsvarianten, aus denen unter den Gesichtspunkten Sicherheit und Wirtschaftlichkeit die jeweils geeignetste Lösung ausgewählt werden kann. Im Folgenden wird an passender Stelle auf mögliche Varianten hingewiesen. Eine ausführliche Darstellung aller Varianten, ihrer Vorzüge und Nachteile sowie der damit einhergehenden Restrisiken findet sich in Abschnitt 7. Jede Variante trägt eine eindeutige Identifikationsnummer, die dem Unterabschnitt entspricht, in dem eine ausführliche Darstellung der Variante nachzulesen ist.

Abbildung 5.1 zeigt die vorgeschlagene Grundarchitektur für normalen Schutzbedarf in der Übersicht. Die Architektur ist in drei Zonen untergliedert:

- Die erste Zone umfasst das interne Netz. Sie enthält alle Client-Systeme sowie alle Infrastruktur- und Anwendungs-Server, die für den autonomen, lokalen LAN-Betrieb benötigt werden.
- Die zweite Zone umfasst alle Bestandteile des Sicherheits-Gateways. Sie enthält die benötigten Paketfilter und ALGs zum Schutz des LANs vor Angriffen aus dem Internet sowie die erforderlichen Server zum Anbieten von Diensten im Internet.
- Die dritte Zone umfasst die Komponenten zur Internet-Anbindung. Sie enthält im einfachsten Fall einen einzelnen Router, der mit dem Netz eines Internet-Diensteanbieters verbunden ist.

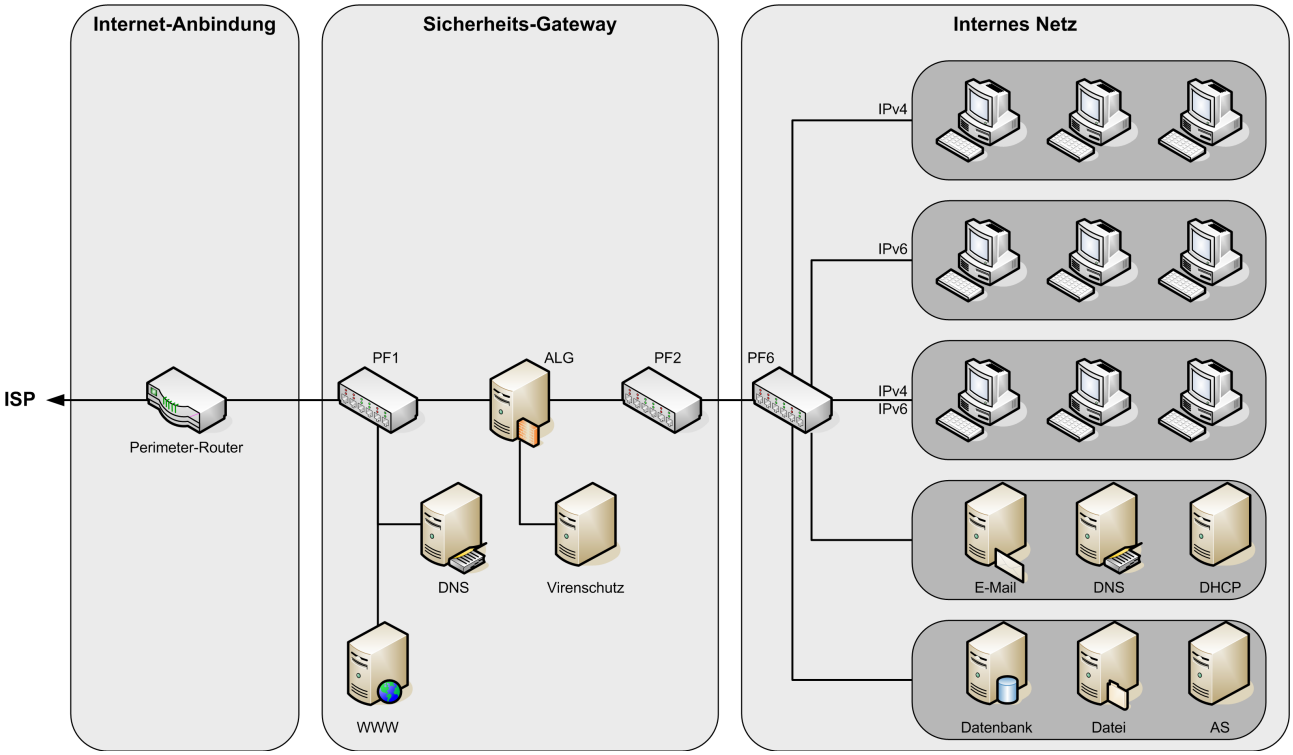

Abbildung 5.1: Grundarchitektur für den normalen Schutzbedarf

Die Wechselwirkungen zwischen den drei Zonen sind auf wenige, klar abgegrenzte Schnittstellen beschränkt. Hinzu kommen Management-Verbindungen zur Steuerung und Überwachung der Netzkomponenten, die erst in Abschnitt 5.4 erörtert werden.

Die Architektur ergibt sich aus der Anwendung der drei folgenden Grundprinzipien zur Netzwerksicherheit:

- Prinzip der gestaffelten Verteidigungslinien (engl. defence in depth): Es wird angestrebt, dass ein Angreifer möglichst mehrere unterschiedliche Sicherheitsfaktoren (d.h. Sicherheitsfunktionen, Sicherheitskomponenten oder Architekturelemente, die der Sicherheit des Netzes dienen), überwinden muss, um sein Ziel (d.h. die Rechner im internen Netz) zu erreichen.
- Prinzip der kleinen Netze: Es wird angestrebt, das Netz so aufzuteilen, dass sich nur solche Geräte in einem Netzsegment befinden, die ein sehr ähnliches (im Idealfall identisches) Anforderungsprofil und insbesondere den gleichen Schutzbedarf besitzen. Dies ermöglicht es, Sicherheitsmaßnahmen so genau wie möglich auf die Sicherheitsanforderungen der jeweiligen Geräte und Einsatzzwecke abzustimmen. Gleichzeitig hilft es, die Auswirkungen eines eventuellen erfolgreichen Angriffs zu begrenzen.
- Prinzip der lokalen Kommunikation: Kommunikationsbeziehungen, die ausschließlich zwischen Geräten im internen Netz bestehen, sollten so etabliert werden, dass die Kommunikation in keinem Fall das interne Netz verlässt.

5.1 Internes Netz

Das interne Netz (Abbildung 5.2) entspricht in seinen Grundzügen einem LAN ohne Internet-Anbindung. Die Grundarchitektur umfasst mindestens ein Client-Segment und mindestens ein Server-Segment mit den grundlegenden Diensten für den LAN-Betrieb.

Sinnvoll ist eine Aufteilung der Clients auf mehrere Teilnetze. Insbesondere IPv6 bietet gute Möglichkeiten zur Trennung und Strukturierung der Netze. Es lassen sich beispielsweise Teilnetze bilden, die nur IPv4, nur IPv6 oder beide Protokolle unterstützen. Der große Adressraum von IPv6 erlaubt es, im internen Netz nahezu beliebig viele Teilnetze aufzubauen und somit die Client-Systeme in leicht zu verwaltende Gruppen zusammenzufassen, etwa anhand ihrer Verwendung oder ihrer geographischen Lage. Daneben können weiterhin reine IPv4-Teilnetze und auch gemischte Netzbereiche eingerichtet werden.

Es wird folgendes Vorgehen empfohlen:

- Im ersten Schritt erfolgt eine Aufteilung nach geografischen und baulichen Gegebenheiten, wie in Anhang 10.2.1 ausgeführt.
- Im zweiten Schritt erfolgt dann die Aufteilung in einzelne Subnetze, eingeteilt nach Funktionsstufen (zum Beispiel Entwicklung, Vertrieb, Buchhaltung oder Ähnliches).

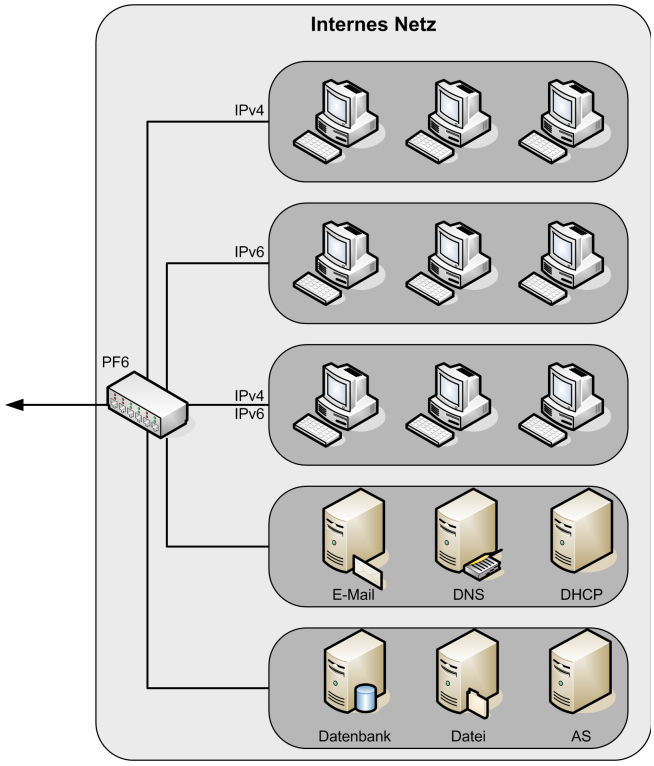

Abbildung 5.2: Internes Netz

Eine redundante Auslegung der Server und Kommunikationsverbindungen ist in der Grundarchitektur nicht vorgesehen, kann aber bei hohen Anforderungen an die Verfügbarkeit mit redundanten Komponenten realisiert werden (siehe Variante 7.1.4 D).

Die Schnittstelle zwischen den LAN-Segmenten und dem Sicherheits-Gateway bildet ein zustandsbehafteter Paketfilter (PF6), der in der Grundarchitektur zugleich für die physische Trennung der LAN-Segmente sorgt. PF6 schützt das Server-Segment gegen Innentäter und unterwanderte Client-Rechner und schützt im Falle mehrerer Subnetze für Clients die einzelnen Netze vor gegenseitigen Zugriffen.

Als zusätzliche Sicherungsmaßnahme dienen Schutzprogramme (z. B. ein Virenschutzprogramm) auf den Client-Systemen und gegebenenfalls auch auf relevanten Servern (siehe [ISi-Client] und [ISi-Server]). Dies bietet eine weitere Verteidigungslinie, ist allerdings kein Ersatz für ein vorgelagertes Sicherheits-Gateway.

5.1.1 Adressvergabe

Im gesamten internen Netz werden private IP-Adressen vergeben, die nicht im Internet geroutet werden. Für IPv4 sind private Adressen im [RFC 1918] definiert, für IPv6 werden Unique Local Adressen nach [RFC 4193] verwendet.

In IPv4-Netzen müssen nicht geroutete Adressen praktisch zwangsläufig verwendet werden, da nur in den allerwenigsten Fällen ausreichend viele global gültige IPv4-Adressen zur Verfügung stehen, um das gesamte interne Netz abzudecken.

In IPv6-Netzen besteht diese Beschränkung nicht. Welche Adressen im internen Netz eingesetzt werden, ist nach funktionalen Aspekten irrelevant, da ohnehin alle Verbindungen nach Außen am ALG terminiert werden. Im Sinne des Prinzips der lokalen Kommunikation sollten bei IPv6 Unique Local Adressen im internen Netz eingesetzt werden. Für den Einsatz von Unique Local Adressen spricht zudem, dass sie anhand ihres eindeutigen Präfixes gut zu erkennen sind, was die Einrichtung

von Filtern erleichtert. Des Weiteren bieten lokale Adressen einen Schutz im Falle von Fehlkonfigurationen des Sicherheits-Gateways, da diese Adressen nicht geroutet werden.

Um die Konfigurationseinstellungen zur Netztrennung (Zugriffslisten, Routen) zu vereinfachen, sollten die Adressen des internen Netzes möglichst systematisch zugewiesen werden, sodass jedem Teilsegment ein zusammenhängender privater Adressbereich entspricht.

Für Clients, bei denen der Bedarf für eine globale Adressierbarkeit besteht (beispielsweise, wenn Anwendungen oder Protokolle eingesetzt werden, die für die korrekte Funktion auf eine global eindeutige Adressierbarkeit der beteiligten Endgeräte angewiesen sind), können einzeln und gezielt global geroutete IPv6-Adressen (Global Unicast Adressen) vergeben werden. Für die entsprechenden Teilnetze kann dann der Zugang zum Internet in den entsprechenden Paketfiltern erlaubt werden. Es sollte jedoch beachtet werden, dass diese Variante nicht allen Schutzanforderungen der Grundarchitektur entspricht und daher getrennt in Variante 7.1.3 L beschrieben wird.

Die Adressvergabe erfolgt bei IPv4 über DHCP und bei IPv6 über stateful DHCPv6.

Bei sehr kleinen und statischen Konfigurationen kann auf eine dynamische Zuordnung von IP-Adressen und Konfigurationsdaten gegebenenfalls auch gänzlich verzichtet werden. Der DHCP-Server - und mit ihm die DHCP-Konfiguration des Paketfilters - entfallen dann (siehe Variante 7.5.7 A).

Bei IPv6 kann neben Stateful DHCPv6 auch SLAAC in Kombination mit Stateless DHCPv6 verwendet werden (siehe Variante 7.1.3 M). Diese Alternative sollte jedoch nicht für Global Unicast Adressen genutzt werden: diese sollten nach eingehender Prüfung nur gezielt für einzelne Client-Subnetze vergeben werden. Die grundsätzliche Betrachtung von DHCP zusammen mit Autokonfiguration findet sich in Abschnitt 3.6.6 und 3.7.1.

Subnetzpräfixe bei IPv6

Eine Site erhält von ihrem Internet-Provider einen zusammenhängenden Bereich global Adressen in Form eines Global Routing Prefix. Dieses Präfix wird typischerweise 48 bit lang sein (/48) womit noch 16 bit zur Strukturierung des Netzes verbleiben. Neben dem Global Routing Prefix wird in der Grundarchitektur noch ein Unique Local Prefix verwendet.

Um das Adresskonzept einfach zu halten, sollte beide Präfixe die gleiche Länge haben und alle Subnetze parallel aus beiden Präfixen vergeben werden (siehe auch [RFC 4193]). Das bedeutet, dass unabhängig vom Adresstypen der in einzelnen Teilnetzen eingesetzt wird, Subnetz-IDs immer einheitlich vergeben werden, egal welches Präfix ihnen vorangeht. Auf diese Weise können Subnetze immer anhand ihrer 16 bit Subnet ID identifiziert werden.

5.1.2 Segmentierung

Client-Rechner und Server sind in getrennten physischen Segmenten platziert, um die internen Server vor dem Einfluss fehlkonfigurierter oder potenziell böswilliger Clients zu schützen. Auch in dem Fall, dass ein Angreifer (beispielsweise durch Ausnutzen einer Schwachstelle in einem Anwendungsprogramm) einen Client-Rechner kompromittieren konnte, stellt die Trennung zwischen Clients und Servern eine weitere Verteidigungslinie dar, denn sie begrenzt die Möglichkeiten eines Angreifers, weitere Geräte zu übernehmen.

Darüber hinaus kann eine beliebige Anzahl weiterer LAN-Segmente eingerichtet werden, etwa um Anwendungs-Server nach ihrem jeweiligen Schutzbedarf von den übrigen LAN-Segmenten zu trennen oder um Benutzer je nach ihren Rollen in gesonderten Client-Bereichen anzusiedeln (z. B.

Gäste-Bereich und Mitarbeiter-Bereich). Die Segmente können parallel zu den bestehenden Segmenten eingerichtet werden − etwa an weiteren Ausgängen des mehrbeinigen Paketfilters PF6 (vgl. Abbildung 5.12) − oder hierarchisch als Untersegmente eines vorhandenen Segments. Eine hierarchische (baumartige) Segmentierung erfordert eine genaue Planung der Kommunikationsbeziehungen im Segmentierungsbaum. Hingegen benötigt sie weniger Schnittstellen pro Koppelelement und kann daher die Konfiguration der Paketfilter vereinfachen. Jedes physische Segment entspricht einer unabhängigen Sicherheitszone.

Prinzip der kleinen Netze

Bei IPv4 muss die Aufteilung des Netzes oft unter dem Gesichtspunkt der möglichst effizienten Ausnutzung des knappen Adressraums von IPv4 erfolgen. Infolgedessen finden sich in IPv4-Netzen häufig Subnetze mit Geräten, die deutlich unterschiedliche Anforderungsprofile und unterschiedlichen Schutzbedarf besitzen.

Mit dem großen Adressraum von IPv6 ergibt sich die Gelegenheit, die lokalen Netze in kleinere Teilnetze zu untergliedern, die der jeweiligen Aufgabenstellung und dem Schutzbedarf optimal angepasst sind. Man kann es sich auch durchaus leisten, jedem Typ von Anwendungs-Server (E-Mail-Server, Datei-Server, Datenbank-Server usw.) ein eigenes Subnetz zu geben und ist dann in der Lage, den Zugriff von den Client-Netzen aus sehr feingliedrig zu steuern, ohne auf einzelne IP-Adressen filtern zu müssen. Auch für Netzwerkdrucker oder ähnliche Geräte können in diesem Fall eigene Subnetze eingerichtet werden. Bei den Client-Netzen sollte die Aufteilung bei IPv6 so gewählt werden, dass in jedem Netz nur Clients angebunden sind, deren Anforderungsprofile hinreichend ähnlich sind und die insbesondere den selben Schutzbedarf besitzen. Durch die große Anzahl an verfügbaren Subnetzen können auch Reserve-Netze vorgesehen werden. Diese Reserve-Netze erlauben es in Verbindung mit entsprechend leistungsfähigen Netzkoppelelementen, flexibel auf kurzfristige vorübergehende veränderte Anforderungen einzelner Clients zu reagieren, indem die betreffenden Geräte vorübergehend in ein entsprechend konfiguriertes Reserve-Netz umgezogen werden.

Andererseits können bei der Einführung von IPv6 durchaus auch Teilnetze zusammengelegt werden, die unter IPv4 getrennt waren, weil für eine größere Anzahl von Geräten kein ausreichend großer zusammenhängender IPv4-Adressbreich zur Verfügung stand. Dies stellt keinen Widerspruch zum Prinzip der kleinen Netze dar, wenn die Geräte in den zusammengelegten Teilnetzen den oben genannten Anforderungen (gleicher Schutzbedarf, hinreichend ähnliche Anforderungsprofile) entsprechen.

Eine weitere schon aus den IPv4-Konzepten her bekannte Unterscheidung ist die Untergliederung in Gäste-Netze und Mitarbeiter-Netze. Auch dieser Ansatz kann mit IPv6 noch weiter verfeinert werden, so lässt sich zum Beispiel jeder Konferenzsaal mit einem eigenen Subnetz versorgen.

Durch diese Adressstruktur steigt die Anforderung an die Anzahl der verfügbaren Ports am Paketfilter. Dieser Engpass lässt sich gegebenenfalls durch die Verwendung mehrerer paralleler Paketfilter beseitigen. Gruppiert man dabei wieder Teilnetze gemäß ihrer Verwendung, lassen sich Filterregeln zusammenfassen und vereinfachen.

Sicherheitszonen

Das bestimmende Merkmal einer Sicherheitszone ist ihr homogener Schutzbedarf. Komponenten und Anwendungen mit unterschiedlichem Schutzbedarf sollten in getrennten Sicherheitszonen platziert werden. Andernfalls muss die gemeinsame Sicherheitszone bezüglich jedes Sicherheitsgrundwerts für die Schutzanforderungen des jeweils anspruchsvollsten Mitglieds ausgelegt sein, was aber meist die unwirtschaftlichere Lösungsvariante ist.

Mit IPv6 ist eine deutlich feinere Aufteilung und genauere Verwaltung der Sicherheitszonen möglich, als dies bei IPv4 der Fall ist.

Sicherheitszonen müssen durch ein Sicherheits-Gateway physisch voneinander getrennt werden. Bei normalem Schutzbedarf ist dies (im Inneren eines LANs) in der Regel ein Paketfilter (vgl. Abbildung 5.12). Je nach Schutzbedarf kann aber auch ein mehrstufiges Sicherheits-Gateway (Paketfilter−ALG−Paketfilter) erforderlich sein (siehe Variante 7.1.3 J).

Der Netzaufbau innerhalb einer Sicherheitszone erfolgt heute grundsätzlich mittels Switched Ethernet. Mit Hilfe von IEEE 802.1x lässt sich der Zugang von Clients zum Netz nach Authentisierung gezielt erlauben. Durch (MAC-)Adressfilter an den Ports und zusätzliche logische Segmentierung mittels VLANs kann der Durchsatz kontrolliert und die Robustheit des LANs gesteigert werden. Auch wird so innerhalb des Segments die Vertraulichkeit verbessert. VLANs sind jedoch kein ausreichend sicher bewertetes Mittel, um Sicherheitszonen voneinander zu trennen. Für eine sichere Zonen-übergreifende Abschottung ist eine physische Segmentierung unerlässlich.

WLAN

In der Grundarchitektur ist der Einsatz von WLAN nicht vorgesehen. Beim Einsatz von WLAN ist zu beachten, dass sich die Verfügbarkeit des Netzes und die zur Verfügung stehende Bandbreite nicht gewährleisten lassen. Funkverbindungen sind von vielen äußeren Einflüssen abhängig und lassen sich leicht stören.

Falls notwendig, können Netze mit normalem Schutzbedarf WLAN nutzen, sofern sie die grundlegenden Sicherheitsvorkehrungen beachten. Dazu zählen insbesondere:

- Sämtliche WLAN-Kommunikation muss durch sichere Verschlüsselung (z. B. WPA2, IPSec-VPN) gegen Ausspähen und Manipulation geschützt werden. Schwache Verschlüsselungsverfahren (z. B. WEP) sind zu vermeiden.
- Die Zugangsknoten des Funknetzes (WLAN Access Points) bilden eine eigene Sicherheitszone, die durch physische Segmentierung sicher vom kabelgebundenen LAN abgetrennt werden muss. Das heißt, alle WLAN-Zugriffe ins LAN müssen ein Sicherheits-Gateway passieren.

Detaillierte Sicherheitsempfehlungen für den Einsatz von WLANs bieten [TR-S-WLAN] sowie [ISi-WLAN]. Soweit erforderlich, kann das WLAN-Segment in der Grundarchitektur zum Beispiel an eine weitere Schnittstelle des Paketfilters PF6 (Abbildung 5.12) angeschlossen werden. Bei hohem Schutzbedarf kann statt eines einfachen Paketfilters eine höherwertige Filterkomponente (siehe Variante 7.1.3 I) oder ein dreistufiges Sicherheits-Gateway (siehe Variante 7.1.3 J) eingesetzt werden, um das LAN sicher gegen das WLAN-Segment abzuschotten.

Eine weitere Möglichkeit, WLAN-Segmente sicher in eine lokale Netzinfrastruktur zu integrieren ist, einen Zugriff aus dem WLAN-Segment auf das lokale Netz als Fernzugriff zu betrachten und die in [ISi-Fern] beschriebene Architektur umzusetzen.

5.1.3 Basisdienste

Unabhängig von dem Verwendungszweck eines LANs muss die Grundarchitektur verschiedene Basisdienste bereitstellen, um einen reibungslosen Betrieb zu gewährleisten. Zu diesen Diensten zählen bspw. DHCP, DNS und NTP. Da diese Basisdienste kritischen Gefährdungen ausgesetzt sind (siehe Abschnitt 7), sind sie in einer eigenen Sicherheitszone untergebracht, die durch den Paketfilter PF6 vom übrigen LAN getrennt ist (siehe Abbildung 5.12). Falls man auch intern höhere Sicherheit erreichen will, kann man die Server, die die Basisdienste erbringen, durch ein eigenes PAP-Gateway vom internen Netz abtrennen (siehe Variante 7.1.3 J).

DHCP

Der DHCP-Server vergibt die internen IP-Adressen im Client-Segment und versorgt die Clients dynamisch mit grundlegenden Netzattributen, wie zum Beispiel den Adressen des DNS-Servers und des Standard-Gateways. Anders als Clients erhalten Server feste IP-Adressen, werden also statisch konfiguriert und müssen nicht auf DHCP zurückgreifen.

Der Paketfilter PF6 (Abbildung 5.12) wandelt DHCP-Broadcast-Anfragen eines Clients, die normalerweise an der Segmentgrenze verworfen würden, mittels einer sogenannten DHCP Helper-Adresse in einen Unicast an den DHCP-Server. Dies ermöglicht Segment-übergreifende DHCP-Anfragen. Der DHCP-Server im Server-Segment kann so beliebige andere LAN-Segmente bedienen. Das Konfigurieren der Helper-Adresse öffnet den Paketfilter für DHCP-Pakete.

DNS

Der interne DNS-Server dient der Zuordnung alphanumerischer Bezeichnungen (Namen) zu den entsprechenden IP-Adressen im Inneren des LANs. Die interne Namensauflösung erfolgt direkt auf dem Server, zur Auflösung externer Namen stellt der Server rekursive DNS-Anfragen an den DNS-Proxy des Sicherheits-Gateways. Dazu müssen auf Paketfilter PF6 DNS-Anfragen aus den Client-Segmenten zum DNS-Server und vom DNS-Server zum Sicherheits-Gateway freigeschaltet sein (Port 53/UDP+TCP).

Durch die gegenüber IPv4 längeren IPv6-Adressen und die damit einhergehende aufwendigere Schreibweise gewinnt die Bedeutung von symbolischen Namen deutlich an Gewicht. Der Einsatz von Microsoft Windows als Server setzt, genau wie eine ganze Reihe von anderen modernen Systemen (E-Mail-Server, ENUM-Lookup, Telefonie mit SIP oder SSL als Beispiele), ein funktionierendes DNS im lokalen Netz voraus.

NTP

Der NTP-Server synchronisiert die Uhren aller Server- und Client-Rechner im LAN. Der NTP-Server selbst wird über ein separates Management-Netz (siehe Abschnitt 5.4) an eine hochgenaue Referenzzeitquelle angeschlossen.

NTP wird im LAN im Client-Server-Modus betrieben. Um NTP-Clients vor falschen NTP-Nachrichten zu schützen, werden dabei die Authentisierungs-Optionen des Protokolls genutzt. NTP-Anfragen aus dem Client-Segment zum NTP-Server Port 123/UDP müssen am Paketfilter PF6 freigeschaltet sein.

5.1.4 Interner E-Mail-Server

Der interne E-Mail-Server übernimmt für die Clients im LAN die kombinierte MSA/MTA/MDA-Funktion (siehe auch [ISi-Mail-Server]). Existieren sowohl Client-Segmente mit IPv4 als auch mit IPv6, muss er als Dual-Stack-Server ausgeführt werden. Damit Clients E-Mails senden, empfangen und verwalten können, müssen auf dem Paketfilter PF6 (Abbildung 5.12) zwischen den entsprechenden Client- und Server-Segmenten sowohl SMTP als auch POP3 (bzw. IMAP oder RPC bei Microsoft Exchange) freigeschaltet sein (vgl. Tabelle 16 auf Seite 159). Für den E-Mail-Abruf sollte auch im internen Netz eine verschlüsselte und authentisierte Variante der Protokolle verwendet werden. Die E-Mail-Kommunikation mit dem Internet erfordert zusätzlich eine Freischaltung von SMTP zwischen Server-Segment und E-Mail-Proxy (MRA) im Sicherheits-Gateway.

5.2 Sicherheits-Gateway – Internet-Dienste nutzen und anbieten

Das Sicherheits-Gateway sorgt für eine sichere Trennung zwischen LAN und Internet. Es ermöglicht, Dienste im Internet sicher zu nutzen und eigene Dienste sicher im Internet anzubieten.

PAP-Struktur

Abbildung 5.3 zeigt das grundlegende Architekturkonzept des Sicherheits-Gateways. Die Grundarchitektur für normalen Schutzbedarf sieht eine dreistufige Struktur des Gateways vor, bestehend aus einem äußeren und einen inneren Paketfilter (PF1 bzw. PF2), dazwischen ein ALG:

- Der äußere Paketfilter PF1 übernimmt eine Vorfilterung eingehender Datenpakete und schirmt damit das ALG gegen die gröbsten Gefährdungen aus dem Internet ab. Diese Filterstufe reduziert das Kommunikationsaufkommen und sorgt so für eine Entlastung des ALGs, das ressourcenintensivere Filteroperationen durchführen muss und daher leicht überlastet werden könnte. PF1 reduziert somit die Angriffsfläche des ALGs gegenüber Außentätern.
- Das ALG dient vornehmlich der Filterung des Datenverkehrs auf der Anwendungsschicht sowie der Auskopplung von Anwendungsprotokollen im Zuge modularer Erweiterungen des Sicherheits-Gateways. Daneben sind im ALG für alle die Anwendungen, bei denen ein Übergang zwischen IPv4 und IPv6 vorgesehen ist, entsprechende Proxys realisiert.
- Der innere Paketfilter PF2 nimmt die gleiche Funktion wie PF1 in Bezug auf den ausgehenden Datenverkehr wahr. Er reduziert die Angriffsfläche des ALGs gegenüber Innentätern oder Rechnern im LAN, die bereits unterwandert sind.

Um verbindungsorientierte Protokolle mit maximaler Effektivität zu filtern, werden die Paketfilter PF1 und PF2 im zustandsbehafteten Modus betrieben.

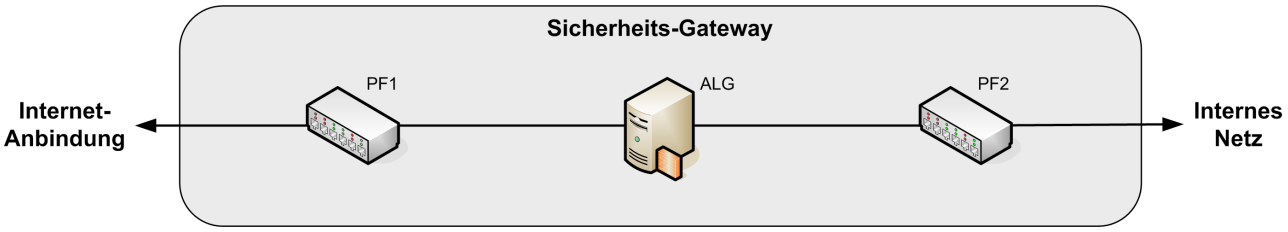

Abbildung 5.3: Aufbau des Sicherheits-Gateways

Die Schutzwirkung des Gateways gegen Hacking lässt sich steigern, indem für die drei Stufen Komponenten mit unterschiedlichen Technologien (z. B. mit unterschiedlichen Prozessoren und Betriebssystemen) eingesetzt werden (siehe Variante 7.1.3 F). Heterogene Gateway-Stufen erschweren jedoch die Konfiguration und den Betrieb des Gateways, darüber hinaus können sie dessen Verfügbarkeit beeinträchtigen: Kommt es vor allem auf eine hohe Verfügbarkeit des Sicherheits-Gateways an, so muss statt dessen eine Hochverfügbarkeits-Variante gewählt werden (siehe Varianten 7.1.4 B und 7.1.4 E).

Die Gateway-Architektur (Paketfilter–ALG–Paketfilter) wird auch als PAP-Gateway bezeichnet. Ein PAP-Aufbau ist die Standardlösung für ein Netz mit normalem Schutzbedarf. Nur bei kleinen, unkritischen Netzen kann aus Gründen der Wirtschaftlichkeit ein einfacher Paketfilter als Sicherheits-Gateway in Erwägung gezogen werden (siehe Variante 7.1.3 C). Die daraus resultierenden zusätzlichen Risiken müssen jedoch sorgfältig geprüft werden.

Abbildung 5.4 zeigt den Fall, dass das interne Netz zunächst IPv4-only bleibt und nur die externe Anbindung auf IPv4+IPv6 umgestellt wird. Dies wird zunächst der Standard sein, da die Außenanbindung umgestellt werden muss, die internen Netze jedoch nicht immer angepasst werden

müssen. Wichtig bei dieser Variante ist, dass das interne Netz tatsächlich IPv4 *only* ist, also IPv6 auf den Clients deaktiviert ist. Sonst sind die Clients auch über IPv6 angreifbar.

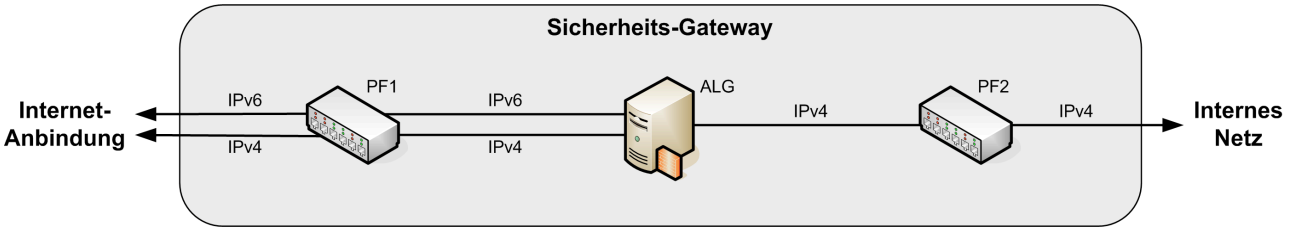

Abbildung 5.4: Sicherheits-Gateway für IPv4-only Netze mit IPv6-Anbindung

Abbildung 5.5 zeigt die Version des Sicherheits-Gateways, die verwendet werden kann, um ein internes IPv6-Netz mit Clients mit dem existierenden Internet ohne IPv6-Anschluss zu verbinden.

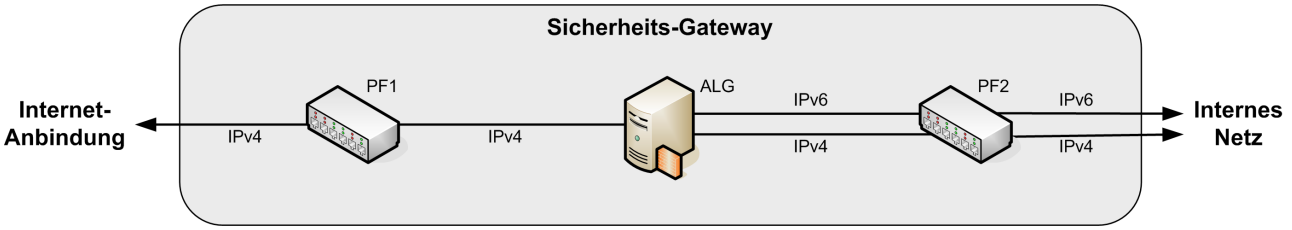

Abbildung 5.5: Sicherheits-Gateway mit IPv4-IPv6 Übergang

Abbildung 5.8 zeigt die Version des Sicherheits-Gateways, die sowohl über IPv4 als auch über IPv6 mit dem Internet verbunden ist.

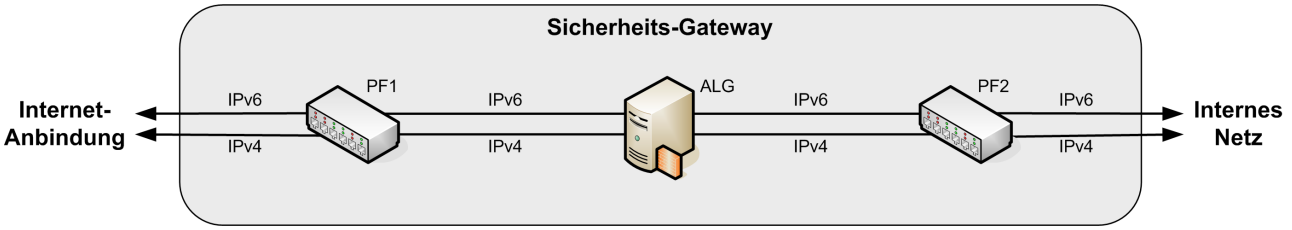

Abbildung 5.6: Sicherheits-Gateway mit IPv4 und IPv6

Sowohl die Variante in Abbildung 5.5 als auch die Version in Abbildung 5.8 stellen nur Übergangsszenarien zur langfristig erwarteten Variante in Abbildung 5.8 dar, bei der das interne Netz ausschließlich IPv6 verwendet. Ab welchem Zeitpunkt auch bei der Anbindung an das Internet komplett auf IPv4 verzichtet werden kann und damit wieder eine Struktur ähnlich wie in Abbildung 5.3, nur eben ausschließlich mit IPv6, erreicht werden kann, lässt sich derzeit noch nicht absehen.

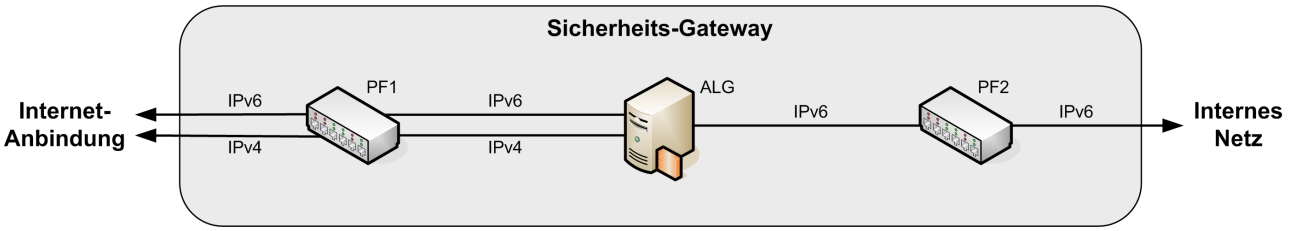

Abbildung 5.7: Sicherheits-Gateway für reine IPv6-Netze

Routing

Erweiterungen des Sicherheits-Gateways wie das Einrichten einer DMZ erfordern zusätzliche Komponenten und Verbindungspfade innerhalb der Gateway-Zone (siehe als Beispiel Abbildung 5.8). Die Datenströme werden dabei auf der IP-Ebene mit Hilfe von individuellen Routingein-

stellungen gezielt transportiert. Um die Robustheit des Sicherheits-Gateways und der umgebenden Komponenten gegenüber Angriffsversuchen zu erhöhen, werden innerhalb der Gateway-Zone alle Routen statisch festgelegt. Dynamische Routing-Protokolle sind abzuschalten, um Angreifern keine Angriffspotenziale zu eröffnen.

5.2.1 Internet-Dienste nutzen

Alle Zugriffe aus dem Inneren des LANs auf externe Dienste im Internet durchlaufen vollständig die PAP-Struktur des Sicherheits-Gateways. Dabei werden Protokolle auf der Anwendungsschicht durch protokollspezifische Sicherheits-Proxys gefiltert. Die Grundausstattung des ALGs umfasst Proxys für SMTP (d. h. einen MRA), DNS sowie HTTP und HTTPS. Um diese Dienste bei Servern, die nur IPv4 anbieten, aus einem reinen IPv6-Netz erreichen zu können, sind die ALGs auf der Seite zum internen Netz als Dual-Stack-Lösungen auszuführen (siehe Abbildung 5.5).

Beim Einsatz eines HTTPS-Proxys ist zu beachten, dass der Proxy verschlüsselte Verbindungen aufbrechen und umschlüsseln muss, um eine inhaltliche Datenkontrolle oder eine Datenprotokollierung zu ermöglichen. Dies hat den Verlust der Ende-zu-Ende-Sicherheit zur Folge. Beim Verbindungsaufbau muss das Zertifikat eines externen HTTPS-Servers im Internet zentral im Sicherheits-Gateway geprüft werden. Am Client wird daraufhin lediglich das Zertifikat des lokalen Proxys angezeigt. Dies hat den Vorteil, dass sich Sicherheitsvorgaben in Bezug auf externe Zertifikate zentral im ALG durchsetzen lassen. Ein weiterer Vorteil ist der Übergang von einem internen IPv6-Netz zu einem externen IPv4-HTTPS-Server. Nachteilig ist hingegen, dass der Server in umgekehrter Richtung auch nur den Proxy im Sicherheits-Gateway, nicht aber den eigentlichen Client im LAN authentisieren kann, was in einigen Anwendungen unzureichend ist.

Falls eine Ende-zu-Ende-Vertraulichkeit oder eine zertifikatsbasierte Client-Server-Authentisierung unterstützt werden muss, können verschlüsselte Verbindungen in Ausnahmefällen ungefiltert durch das ALG hindurch getunnelt werden, ohne sie zu entschlüsseln. Dieser Bruch der Grundregeln darf nur mit einer ausdrücklichen Zustimmung des Sicherheitsverantwortlichen erfolgen, die nur im Einklang mit der geltenden Sicherheitsrichtlinie und nur für ausgesuchte Kommunikationspartner gewährt werden darf (sogenanntes Whitelisting). Beim Einsatz von IPv6 ist zu beachten, dass das Durchleiten von HTTPS-Tunneln auch bedeutet, dass von IPv6-Clients im internen Netz nur IPv6-fähige Server im Internet erreicht werden können.

5.2.2 Internet-Dienste anbieten

Die hier vorgestellten Erweiterungen des Sicherheits-Gateways sind nur dann relevant, wenn eigene Dienste angeboten werden sollen, also beispielsweise Web-Angeboten selbst gehostet werden. Detaillierte Informationen zum Betrieb eines Web-Servers finden sich in [ISi-Web-Server].

Bei der Verwendung von IPv6 kommen noch folgende zusätzliche Überlegungen zum Tragen:

- Für wen werden diese Dienste angeboten?
- Ist zu erwarten, dass der Anwender aus dem Internet bereits über IPv6 verfügt?
- Müssen sowohl IPv4 als auch IPv6 angeboten werden?

In den meisten Fällen wird die Antwort so ausfallen, dass der Zugriff auf die von außen sichtbaren Dienste über beide Transportprotokolle unterstützt werden muss. Von dieser Annahme wird bei den folgenden Konfigurationen ausgegangen.

Das Sicherheits-Gateways wie in Abbildung 5.3 reicht aus, um Zugriffe von innen nach außen sicher zu ermöglichen. Das Anbieten von Diensten im Internet erfordert ein erweitertes Gateway-Konzept. Da externe Zugriffe auf lokale Internet-Server erhebliche Kommunikations-

lasten verursachen können und zugleich eine ernste Sicherheitsbedrohung darstellen, sollten sie nicht über das ALG geführt werden, sondern in einer vorgelagerten DMZ terminiert werden, die gegen das Internet durch einen zustandsbehafteten Paketfilter abgeschirmt wird (siehe Abbildung 5.8).

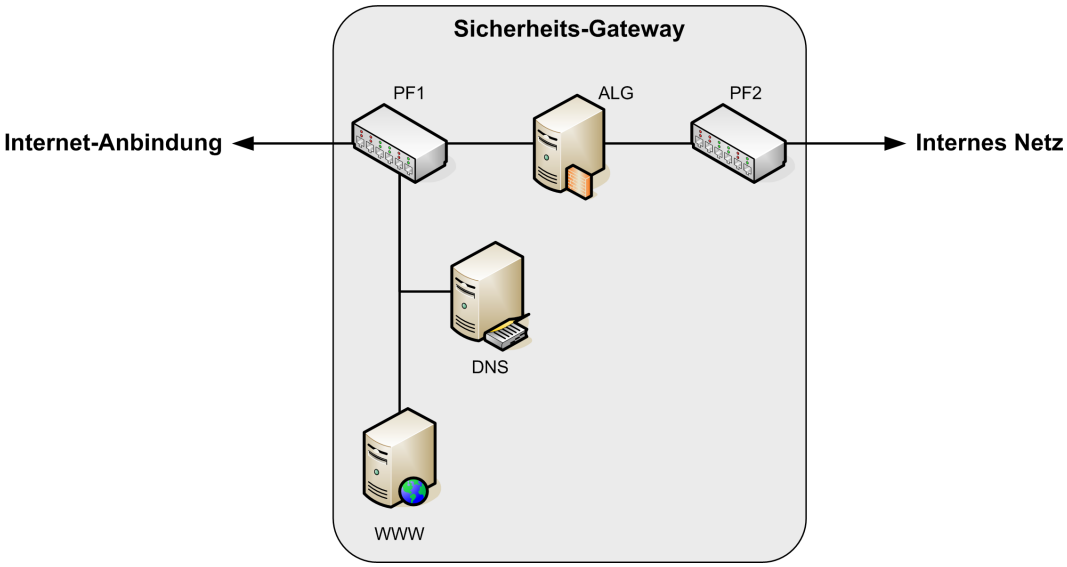

Abbildung 5.8: Sicherheits-Gateway mit DMZ für die Server WWW und DNS

Externer DNS-Server

Der externe DNS-Dienst wird auf einem eigenen Server betrieben, um den Web-Servers zu entlasten. Je nach der Größe des Namensraums und dem Dienstangebot des Web-Servers können beide Server erheblich belastet sein. Des Weiteren erleichtert die Trennung das Betreiben der beiden Server in einer Minimalkonfiguration, die nur eine geringe Angriffsfläche für Attacken aus dem Internet bietet. Schließlich müssen unabhängige Server auch unabhängig voneinander angegriffen werden: Eine etwaige Schwachstelle des DNS-Servers wäre aufgrund der Trennung nur von geringem Nutzen für Angriffe auf den Webserver − und umgekehrt.

Nur in kleinen, unkritischen Netzen mit geringer Kommunikationslast kann der DNS-Server aus Gründen der Wirtschaftlichkeit mit dem Web-Servers zusammengelegt werden, sofern der Anwender dazu bereit ist, die damit verbundenen Nachteile und Risiken in Kauf zu nehmen (siehe Variante 7.1.3 D).

Nach aktuellem Stand der Technik sollte der externe DNS-Server DNSSEC unterstützen und die zur Verfügung gestellten Daten sollten entsprechend signiert sein. Die Zuführung der DNS-Daten sollte getrennt vom normalen Netz über ein Management-Netz erfolgen.

Externer Web-Servers

Der externe Web-Servers ist zusammen mit dem externen DNS-Server in der DMZ hinter Paketfilter PF1 untergebracht. In der Regel sind für ein Web-Angebot weitere Server, wie beispielsweise ein Web-Anwendungs-Server und eine Datenbank notwendig. Detaillierte Informationen zum Bereitstellen von Web-Angeboten finden sich in [ISi-Web-Server].

In Zukunft ist darauf zu achten, dass externe Web-Angebote auch über IPv6 erreichbar sind. Bei dem derzeit noch recht unvollständigen Ausbau der IPv6-Konnektivität im Internet muss man genau planen, wie man seinen Web-Auftritt nach außen publiziert. Verwendet man den gleichen DNS-Namen für IPv4 und IPv6, so kann es leicht geschehen, dass ein Client im Internet lokal

bereits IPv6 eingeschaltet hat und dennoch keine Verbindung über das Internet mit IPv6 zum Server herstellen kann. Der Browser versucht dann zuerst, die Seite über IPv6 zu erreichen und wird erst nach einem Timeout den Versuch auf IPv4 wiederholen – was beim Anwender zu deutlich sichtbaren, unangenehmen Verzögerungen beim Seitenaufbau führt. Verwendet man getrennte Namen für den Web-Auftritt über IPv4 und IPv6 (zum Beispiel www.ip4.beispiel.de und www.ip6.beispiel.de), so funktioniert der Zugriff ohne Zeitverzögerung, man muss allerdings alle Links innerhalb seiner Seiten entsprechend anpassen (nur relative Links verwenden oder alle Links im Proxy umschreiben).

In der Praxis haben sich in vielen Fällen folgende Regelungen bewährt:

- Der Server erhält für IPv4 den Namen www.ip4.beispiel.de und für IPv6 www.ip6.beispiel.de.
- Für den Namen www.beispiel.de wird sowohl die IPv4- als auch die IPv6-Adresse im DNS eingetragen.
- Im Reverse Tree des DNS werden sowohl www.ip4.beispiel.de als auch www.ip6.beispiel.de eingetragen.

5.2.3 Adressumsetzung

Network Address Translation (NAT) ist der Sammelbegriff für Verfahren zum automatischen und transparenten Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und in Sicherheits-Gateways zum Einsatz, vor allem, um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen.

Die Adressumsetzung erfolgt am ALG. Die Adressen des internen Netzes werden dort auf öffentliche Adressen abgebildet. Bei IPv6 werden die im internen Netz eingesetzten Adressen ebenfalls am ALG auf global routbare Adressen umgesetzt.

Auf eine Umsetzung der nach außen sichtbaren Adressen der Server in der DMZ und des Sicherheits-Gateways wird verzichtet. Diese wenigen Kommunikationsendpunkte erhalten feste Adressen aus dem Bereich der öffentlichen Unicast-Adressen zugeordnet, die entsprechend im Paketfilter für das jeweilige Protokoll freigeschaltet werden.

5.2.4 Schutz vor Viren und E-Mail-Spam

Zum Schutz vor Viren und Spam werden potenziell gefährdete Datenverbindungen im ALG ausgekoppelt und einem Virenschutzprogramm oder einem Spam-Filter zugeführt. Entsprechende Proxys werden in der Grundarchitektur auf einem separaten Server platziert, der über ein drittes Bein des ALGs angeschlossen ist (Abbildung 5.9).

Da Viren- und Spam-Prüfung rechenintensive Operationen erfordern können, dient die Auskopplung der Entlastung des ALGs. Zudem vereinfacht sie die Software-Konfiguration des Gateways, was die Angriffsfläche des ALGs reduziert. Weitere Empfehlungen zum Schutz gegen Viren und Spam bieten [ISi-Client] beziehungsweise [ISi-Mail-Server].

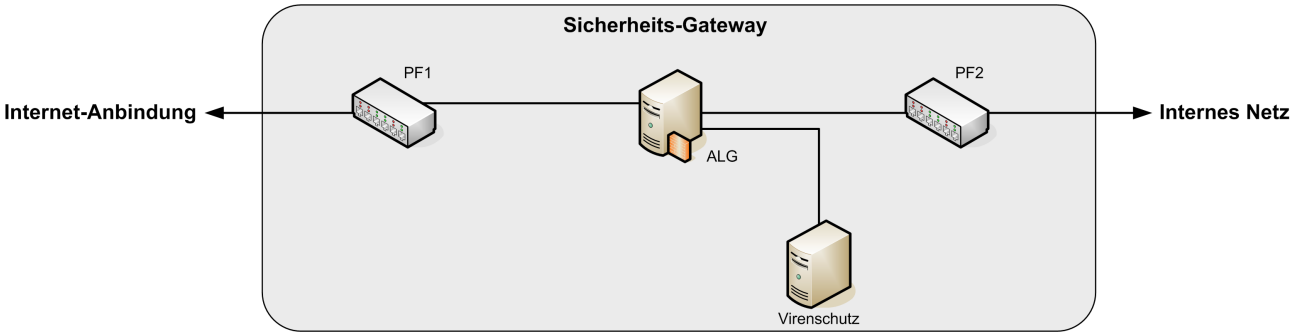

Abbildung 5.9: Sicherheits-Gateway mit Virenschutz-Erweiterung

5.2.5 VPN-Integration

Zur Realisierung einer LAN-LAN-Kopplung oder zur Anbindung kleiner Außenstellen kann ein secure VPN (vgl. Abschnitt 4.2.2) genutzt werden, um den Schutz von Integrität und Vertraulichkeit der Verbindungen zu gewährleisten. Auch wenn IPv6 IPsec als integralen Bestandteil mitbringt, sollte die Implementierung eines VPN-Gateways auf eine dedizierte Komponente auslagert werden.

Abbildung 5.10 zeigt die Integration einer VPN-Erweiterung in das Sicherheits-Gateway. Das VPN-Gateway wird dazu mit einer Schnittstelle am äußeren Paketfilter PF1 und mit der anderen Schnittstelle am ALG angeschlossen. Durch diese Platzierung wird die VPN-Box durch den äußeren Paketfilter gegen Angriffe aus dem Internet geschützt. Zugleich kann unverschlüsselter Internet-Verkehr am VPN-Abschluss vorbei geführt werden. Der Paketfilter PF1 beschränkt die Kommunikation mit der VPN-Box auf die VPN-spezifischen Protokolle.

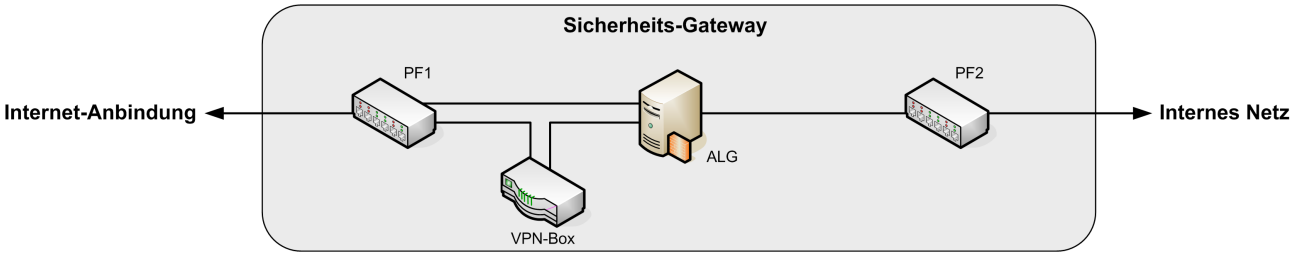

Abbildung 5.10: Sicherheits-Gateway mit VPN-Box

Vertiefende Informationen zur Realisierung von VPNs bieten die BSI-Studie [BSI SGW] sowie [ISi-VPN]. Der Fernzugriff auf das interne Netz wird in [ISi-Fern] beschrieben.

5.3 Internet-Anbindung

Die Bedeutung eines Anschlusses an das Internet hat in den letzten Jahren kontinuierlich zugenommen. Viele Prozesse in Wirtschaft und Verwaltung lassen sich ohne Zugriff auf das Internet nicht mehr abwickeln. Gleichzeitig nimmt aber auch die vom Internet ausgehende Bedrohung ständig zu.

Durch die noch relativ geringe Verbreitung von IPv6 sind Angriffe auf IPv6-Adressen bisher selten. Dies stellt jedoch keinen Gewinn an Sicherheit dar, sondern spiegelt lediglich die Ausrichtung der Angriffe auf lohnendere und verbreitetere Ziele dar. Sobald IPv6 eine höhere Verbreitung erreicht, werden auch Angriffe auf spezifische Eigenschaften von IPv6 aus dem Internet zunehmen.

Es wird daher empfohlen, Netze mit sehr hohem Schutzbedarf grundsätzlich nicht an das Internet anzuschließen. Wenn in solchen Umgebungen Zugriff zum Internet benötigt wird, sollte er durch eine physisch getrennte Sicherheitszone realisiert werden.

Bei normalem bis hohem Schutzbedarf ist eine Internet-Anbindung sinnvoll und auch bei Bewertung der Gefahren vertretbar, sofern dabei die empfohlenen Schutzmaßnahmen ergriffen werden.

Die Wahl eines geeigneten Internet-Diensteanbieters und einer passenden Anschlusstechnologie wird von vielen technischen und anwendungsabhängigen Faktoren beeinflusst, wie zum Beispiel

- der Verfügbarkeit der gewünschten Netztechnik (z. B. Verfügbarkeit von nativem IPv4 und IPv6),
- der zu realisierenden Verbindungstopologie zwischen entfernten Standorten,
- dem Bandbreiten-Bedarf und der benötigten Mindestverfügbarkeit,
- der erforderlichen Übertragungsgüte, Störanfälligkeit und Abhörsicherheit,
- dem Grad an gewünschter Verfügungsgewalt über die Anschlusskomponenten sowie
- der Vertrauenswürdigkeit des Providers.

Einige grundlegende Auswahlkriterien finden sich in Abschnitt 4.1.

Die Grundarchitektur für normalen Schutzbedarf umfasst eine einbeinige Internet-Anbindung über einen sogenannten Perimeter-Router, der die physische Grenze zwischen dem öffentlichen Netzbereich und der eigenen Netzinfrastruktur bildet (Abbildung 5.11).

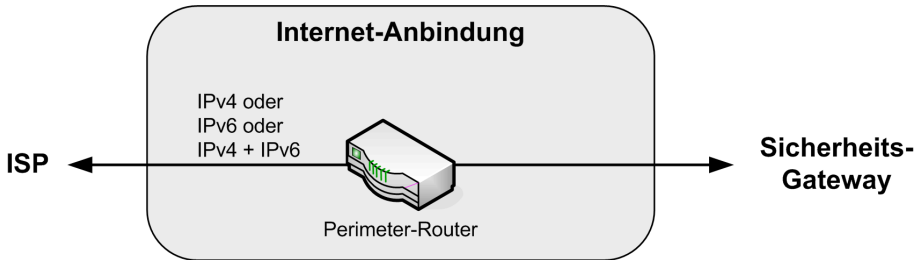

Abbildung 5.11: Internet-Anbindung über verschiedene Protokoll-Versionen

In der einfachen Ausführung bildet die Internet-Anbindung einen potenziellen Single Point of Failure, dessen Ausfall das lokale Netz vollständig vom Internet und allen darüber realisierten Verbindungen zu anderen Standorten abschneidet. Ein Ausfall kann vielfältige Ursachen haben:

- Versagen des Perimeter-Routers
- Störung im Zugangsnetz des Internet-Diensteanbieters
- Störung im Backbone des Diensteanbieters
- Störungen in der Authentifizierung des Anschlusses bei Wählverbindungen

Während sich lokale Störungen durch Reparaturmaßnahmen oder Ersatzgeräte oft schnell beheben lassen, erfordern Ausfälle im Zugangsnetz die Unterstützung des Diensteanbieters. Um ausreichende Verfügbarkeit der externen Kommunikationsverbindungen zu gewährleisten, ist eine sorgfältige Auswahl des Internet-Providers wichtig. Gerade beim Einsatz einer relativ neuen Technik wie IPv6 werden auch an die Technik des Anbieters und an die Qualität des Services und des Betriebspersonals beim Anbieter hohe Anforderungen gestellt. Service-Leistungen und Reaktionszeiten bei Entstörungsmaßnahmen müssen bei Bedarf in Dienstgütevereinbarungen (SLAs) vertraglich geregelt werden. Bei hohen Verfügbarkeitsansprüchen empfiehlt sich eine redundante

Auslegung der Internet-Anbindung und ein Anschluss über unabhängige Anbieter (siehe Variante 7.1.4 A).

Bei der Verwendung von IPv6 für eine redundante Anbindung an das Internet gibt es für die Realisierung derzeit noch keine weitverbreiteten und erprobten Lösungen. Einerseits kann man die schon bei IPv4 mögliche Lösung über BGP mit einem eigenen Provider-unabhängigen Adressraum nutzen oder man geht den von der IPv6-Normierung ursprünglich vorgesehenen Weg der mehrfachen globalen routbaren Adressen für jede Schnittstelle.

Die erste Lösung verwendet bekannte Techniken, hat aber als Nachteil den hohen Aufwand beim Endanwender für ein eigenes Routing (BGP), die Notwendigkeit einen Diensteanbieter zu wählen, der es dem Kunden erlaubt, BGP an seiner Netzschnittstelle zu verwenden, und den Aufwand, sich Provider-unabhängigen IPv6-Adressraum zu beschaffen. Die zweite Lösung lässt sich erheblich einfacher und ohne großen Aufwand realisieren, erfordert aber manuelle Eingriffe beim Umschalten und reagiert dadurch langsamer.

5.4 Netzmanagement

Unter Netzmanagement versteht man die Verwaltung, den Betrieb und die Überwachung von Kommunikationsnetzen. Das FCAPS Modell der International Organization for Standardization (ISO) definiert die Aufgabenbereiche des Netzmanagements wie folgt:

- *Fehlermanagement* (Fault Management*, F*): Erkennen, Protokollieren, Melden und Beheben von auftretenden Fehlerzuständen
- *Konfigurationsmanagement* (Configuration Management*, C*): Dies umfasst die Teilbereiche Organisation und Planung, Konfigurationsidentifizierung, Konfigurationsüberwachung und Konfigurationsaudit
- *Abrechnungsmanagement* (Accounting Management*, A*): Erfassen der Benutzung des Netzes, sodass Rechnungen gestellt werden können (im privaten LAN unüblich)
- *Leistungsmanagement* (Performance Management, *P*): Verkehrswerte/Leistungsdaten sammeln und Statistiken führen, Grenzwerte festlegen
- *Sicherheitsmanagement* (Security Management*, S*): Authentisierung von Benutzern, Autorisierung von Zugriff und Nutzung

Reale Netzmanagement-Systeme unterstützen in der Regel jedoch nur einen Teil dieser Aufgaben, dies ist allerdings unproblematisch, da für eine konkrete Anwendung nicht unbedingt alle Maßnahmen benötigt werden.

5.4.1 Umsetzung der Netzmanagement-Aufgaben

Das vorgestellte FCAPS-Modell einschließlich des Funktionsblocks Zeitsynchronisation umfasst verschiedene Maßnahmen, die in der Grundarchitektur wie folgt umgesetzt werden:

Fehlermanagement

Fehler in Komponenten werden durch SNMP-Abfragen und SNMP-Meldungen (engl. SNMP-Traps) und durch Protokollierung in Log-Dateien (syslog) erfasst. SNMP-Abfragen erfolgen von der zentralen Management-Station aus, SNMP-Traps werden an die zentrale Station gesendet und Log-Daten werden entweder kontinuierlich (syslog-Protokoll) oder als gesammelte Datei zur

zentralen Station gesendet, wo sie gesammelt, archiviert und weiterverarbeitet werden. Schwerwiegende Ereignisse protokolliert die Management-Station auf der Konsole des Systemadministrators. Bei Bedarf kann auch eine Benachrichtigung des IT-Personals durch E-Mail, SMS oder dergleichen erfolgen.

Der Transport von SNMP- und Syslog-Daten kann sowohl über IPv4 als auch über IPv6 erfolgen. Die Verfügbarkeit von SNMP- und Syslog-Transport über IPv6 ist zwar schon bei vielen Anbietern Stand der Technik, jedoch sollte beim Aufbau eines Netzes immer im Einzelfall geprüft werden, ob wirklich alle Komponenten durchgehend IPv6 für das Management unterstützen. Minimale Anforderung ist auf jedem Fall für alle Komponenten die Unterstützung und Protokollierung von IPv6-spezifischen Ereignissen und der IPv6-Adressen.

Bei der Festlegung der zu erfassenden Ereignisse und des Umfangs der Protokollierung muss der erforderliche Speicherplatzbedarf berücksichtigt werden, um zu verhindern, dass durch Speicherüberlauf wichtige Log-Informationen verloren gehen, ehe sie ausgewertet werden können. Der verfügbare Speicherplatz muss großzügig bemessen sein, um auch bei schwerwiegenden Zwischenfällen ausreichende Reserven zu bieten.

Bei allen Maßnahmen des Monitoring und Logging sind die datenschutzrechtlichen Bestimmungen einzuhalten. Dies beschränkt die Möglichkeiten der vorbeugenden Logdaten-Analyse.

Konfigurationsmanagement

Die Konfigurationsdaten aller wichtigen LAN-Komponenten sollten an zentraler Stelle sicher verfügbar vorgehalten werden, sowohl in elektronischer als auch in gedruckter Form. Das Konfigurationsmanagement erfordert eine Versionenverwaltung und eine verlässliche Datensicherung.

Um tatsächlich den aktuellen Konfigurationsstand einer Komponente zu erfassen, empfiehlt es sich, entweder die Konfiguration zentral zu erstellen und auf das Gerät hochzuladen, oder jede dezentrale Änderung der Gerätekonfiguration unverzüglich zur Management-Station zu übertragen und dort zu sichern: In beiden Fällen sollten dazu integritätsgesicherte und verschlüsselte Protokolle verwendet werden (z. B. SCP), soweit das Gerät dies unterstützt. Auch für die Fernadministration dürfen nur sichere Protokolle (z. B. SSH-2, HTTPS) verwendet werden. Jede Konfigurationsänderung ist zu dokumentieren.

Das Konfigurationsmanagement umfasst auch ein periodisches Sicherheits-Audit der relevanten Konfigurationseinstellungen. Dies bietet zum Beispiel Schutz gegen Innentäter und trägt dazu bei, Arbeitsfehler zu erkennen.

Abrechnungsmanagement

Die Grundarchitektur bietet keine konkreten Dienste, die verrechnet werden müssten. In typischen LAN-Umgebungen ist heutzutage eine Abrechnung der IT-Inanspruchnahme generell nicht mehr üblich.

Soweit einzelne LAN-Komponenten über Accounting-Funktionen verfügen, können diese zum Leistungsmanagement oder zur Anomalie-Erkennung herangezogen werden. Besteht kein Bedarf, so ist die überflüssige Funktionalität abzuschalten, um die Angriffsfläche der Komponenten zu minimieren.

Leistungsmanagement

Die grundlegenden Leistungsparameter werden typischerweise mittels SNMP zentral erfasst. Zu den wichtigsten Attributen, die überwacht werden sollten, zählen CPU-Auslastung, Speicherverbrauch, Festplatten-Kapazitätsreserve und Schnittstellenlast. Für diese Parameter sollten Schwellenwerte festgelegt und automatisch überwacht werden. Beim Überschreiten von Grenzwerten ist eine automatische Benachrichtigung sinnvoll. Zusätzlich empfiehlt sich eine Verfügbarkeitsüberwachung (z. B. mittels ICMP-Ping).

Für das zentrale Erfassen, Darstellen und Auswerten von Leistungsmerkmalen gibt es zahlreiche kommerzielle Lösungen, zum Teil aber auch Open-Source-Realisierungen, die skalierbare Monitoring-Lösungen ermöglichen. In jedem Fall sollten für die Datenerfassung sichere Protokolle verwendet werden, die eine Authentisierung und möglichst auch eine Verschlüsselung bieten.

Insbesondere aus dem Open-Source-Umfeld unterstützt eine große Auswahl an Monitoring-Software bereits IPv6.

Sicherheitsmanagement

Zur einheitlichen Authentisierung und Autorisierung von Netzmanagement-Zugriffen dient in der Grundarchitektur ein zentraler Authentisierungs-Server, zum Beispiel ein RADIUS-Server, auf dem alle Benutzer und Berechtigungen verwaltet werden. Ein verteiltes Sicherheitsmanagement der Netzkomponenten und Server mittels direktem lokalen Zugriff sollte nur bei kleinen Netzen ohne besonderen Schutzbedarf in Erwägung gezogen werden.

Zeit-Synchronisation

Die Uhren aller LAN-Komponenten, einschließlich der des Sicherheits-Gateways, müssen synchronisiert sein, damit verteilt erhobene Daten korreliert werden können. Die Synchronisation erfolgt innerhalb des lokalen Netzes von einem oder mehreren NTP-Servern. Diese Server erhalten ihre Referenzzeit entweder beispielsweise über ein DFC77- oder ein GPS-Empfangsmodul. Alternativ können auch Referenzserver aus dem Internet als Zeitquelle dienen.

5.4.2 Eingliederung der Management-Komponenten in die Grundarchitektur

Abbildung 5.12 zeigt die Integration des Management-Moduls in die Grundarchitektur. Die Grundarchitektur setzt dabei durchgängig auf Out-of-Band-Management über ein getrenntes Management-Netz. Ausschlaggebend für diese Empfehlung waren folgende Überlegungen:

- Eine gemeinsame Nutzung von Kommunikationsverbindungen sowohl für Nutz- als auch für Steuerkanäle bietet grundsätzlich leichtere Angriffsmöglichkeiten auf das Netzmanagement durch Abhören, Eindringen oder Denial-of-Service-Attacken.
- Bei Ausfall der Produktivverbindungen sind bei einem In-Band-Management auch keine Entstörungszugriffe mehr über das Netz möglich.
- Eine verschlüsselte Übertragung von Management-Protokollen, die bei In-Band-Management aus Sicherheitsgründen unverzichtbar ist, bereitet Probleme beim Überqueren des Sicherheits-Gateways: Einerseits sollen auch Management-Verbindungen nicht einfach das Gateway tunneln, andererseits ist ein Umschlüsseln solcher Verbindungen innerhalb des Gateways riskant, da entschlüsselte Daten potenziell unterwanderten Gateway-Komponenten preisgegeben wären.

Das Management-Netz ist in mehrere Sicherheitszonen gestaffelt, um ein Umgehen des Sicherheits-Gateways oder die vollständige Übernahme der Management-Zone zu verhindern. So kann zum Beispiel selbst nach der Kompromittierung des Paketfilters PF8 zunächst nur die unmittelbar betroffene Zone unterwandert werden und das ALG ist noch nicht ohne weitere Angriffserfolge zu umgehen. Ergänzend zur Staffelung der Management-Zone geltend folgende Schutzmaßnahmen:

- Die Kommunikation im Management-Netz ist auf wenige Management-Protokolle mit genau festgelegten Ursprüngen und Zielen beschränkt, die in den Paketfiltern PF9 und PF10 ausdrücklich freigegeben sind. Dabei ist für jeden Filtereintrag getrennt zu beachten, welche Dienste über IPv6 oder über IPv4 erreicht werden können. Alle übrigen, nicht explizit autorisierten Verbindungen werden unterbunden (Whitelist-Ansatz).
- Die verfügbaren Sicherheitsmechanismen der eingesetzten Management-Protokolle zur Authentisierung, Integritätssicherung und Verschlüsselung (vgl. Abschnitt 2.1.2) werden aktiviert.

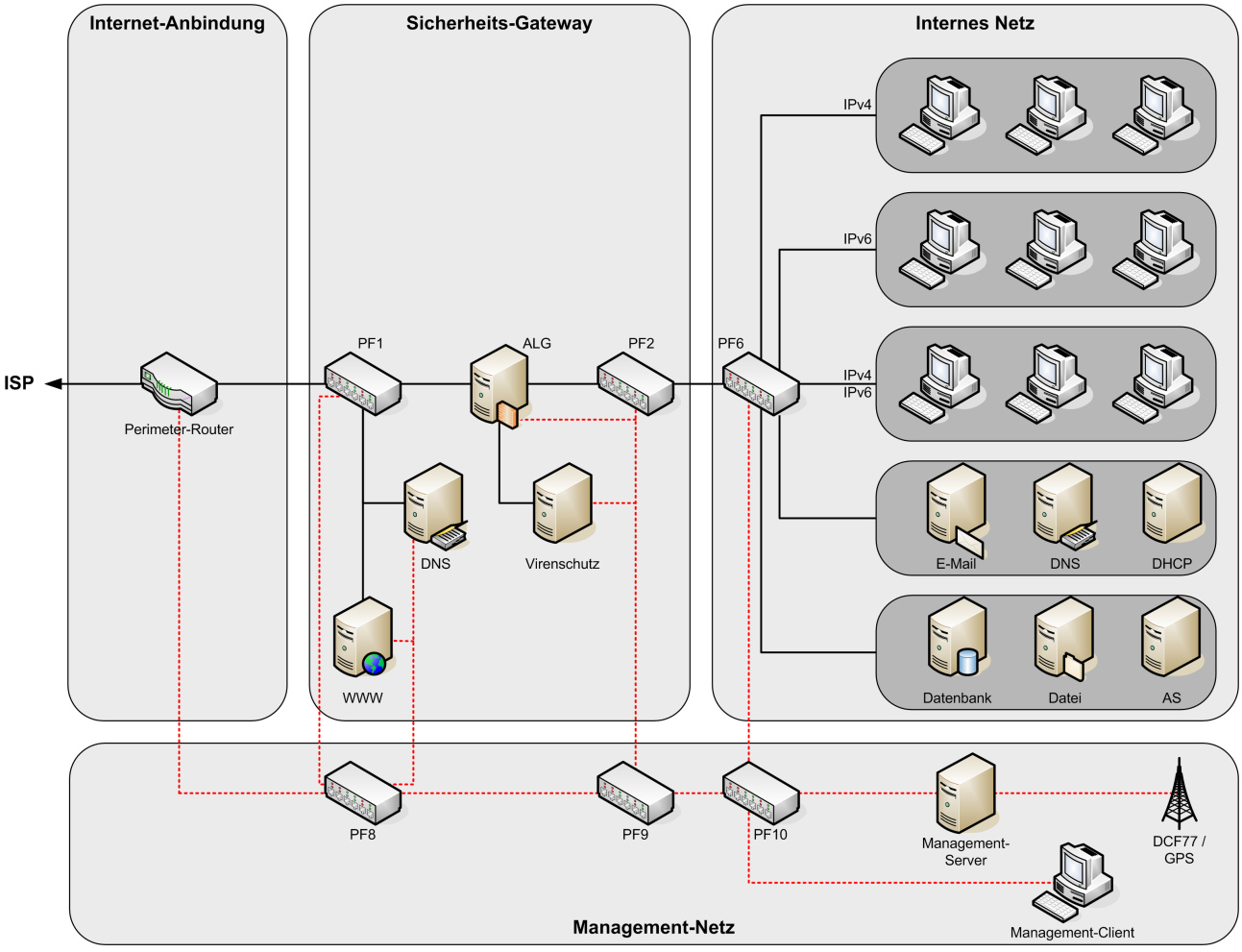

Abbildung 5.12: Grundarchitektur mit Management- und Überwachungsmodul

Eine Alternative zu einer gestaffelten Management-Zone sind getrennte Management-Zellen: Bei dieser Variante für hohen Schutzbedarf besteht keine physische Verbindung zwischen den einzelnen Segmenten des Management-Netzes (siehe Variante 7.1.3 G). Die Vor- und Nachteile einer solchen Lösung sind jedoch genau abzuwägen, denn die Trennung erschwert den Austausch von Überwachungsdaten und behindert zentrale Administrationszugriffe.

Eine wirtschaftliche Lösung für kleine, unkritische Netze mit normalem Schutzbedarf besteht darin, das interne Netz über den Paketfilter PF6 mittels In-Band-Management zu administrieren (siehe Variante 7.1.3 B). Sofern die damit verbundenen Risiken tragbar sind, vereinfacht diese Variante die Vernetzung der internen Server.

In der Management-Zone werden alle Management-Daten zentral gesammelt und verarbeitet. Hier ist auch der zentrale Zeitserver untergebracht, mit dem sämtliche Systemuhren im Netz synchronisiert werden. Anzahl und Ausstattung der Management-Systeme können, je nach Größe des Netzes, der zu sammelnden Datenmenge und der eingesetzten Management-Software, variieren. Das Netz sollte allerdings aus mindestens zwei Rechnern bestehen, einem Management-Server mit Synchronisation und einem Management-Client zum Abruf der Daten. Es besteht keine Notwendigkeit, IPv4- und IPv6-basierte Teile des Netzes mit getrennten Systemen zu administrieren.

6 Komponenten sicher auswählen, konfigurieren und betreiben

Die Grundarchitektur gemäß Abschnitt 5 liefert die Grundlage zur Konzeption eines sicheren LANs mit Internet-Anbindung, das ggf. auch IPv6 verwendet. Zur Realisierung dieses Konzepts müssen geeignete, ausreichend sichere Komponenten ausgewählt und in sicherer Konfiguration betrieben werden. Dieser Abschnitt fasst die grundlegenden Sicherheitsanforderungen an die Wahl geeigneter Komponenten sowie an deren Konfiguration und Betrieb zusammen. Er bietet dem Anwender Unterstützung in Phase 2 (Konzeption) des Ablaufplans gemäß [ISi-E].

6.1 Grundanforderungen an ein sicheres Produkt

Die Anforderungen an ein sicheres Produkt gliedern sich in generische, Produkt-unabhängige Eigenschaften sowie in solche, die nur Komponenten eines bestimmten Typs betreffen.

6.1.1 Grundlegende Anforderungen an alle Komponenten

Unabhängig vom Typ einer Komponente gibt es allgemeine Mindestanforderungen an die Ausstattung der eingesetzten Geräte und an die Leistungsfähigkeit des Lieferanten.

Funktionalität und Leistungsfähigkeit der Komponenten

- Die Leistungsfähigkeit (z. B. Rechenleistung, Speicherkapazität, Netzwerk- und I/O-Durchsatz) der Komponenten muss den konkreten Anforderungen gerecht werden.
- Grundlegende Schnittstellen der Komponenten müssen standardkonforme Protokolle unterstützen, um eine möglichst gute Herstellerunabhängigkeit zu erreichen.
- Alle Komponenten müssen über Mechanismen zur Deaktivierung ungenutzter Schnittstellen, Module und Funktionen verfügen.
- Verschlüsselungsfunktionen müssen auf der Basis standardkonformer, kryptografisch starker Algorithmen mit ausreichender Schlüssellänge realisiert sein.
- Die Komponente muss Zugangspasswörter verschlüsselt speichern.
- Alle Komponenten müssen IPv6 bei allen Schnittstellen und relevanten Services unterstützen.
- Implementierungen sollten grundsätzlich die Standards und alle relevanten aktuellen RFCs vollständig umfassen. Lösungen, die nicht den in den Standards genannten Minimalanforderungen entsprechen, sind zu vermeiden. Zusammenstellungen relevanter RFCs finden sich beispielsweise in [RIPE-501], dessen Nachfolger [RIPE-554] und dem Leitfaden des BVA [BVA-IPv6].

  Für Sicherheitskomponenten, wie Paketfilter oder ALGs, kann es in bestimmten Fällen erforderlich sein, sich nicht strikt an RFCs zu halten. Beispielsweise müssen Paketfilter ggf. fragmentierte Pakete zusammensetzen (und neu fragmentieren), um ihre Funktion erfüllen zu können. Eine Abweichung von den Vorgaben der RFCs kann bei diesen Komponenten notwendig sein.
- Die Implementierung soll soweit erforderlich mit Hardwareunterstützung erfolgen, insbesondere sind Lösungen für IPv6 in Software abzulehnen, wenn IPv4 in Hardware implementiert ist.

Hinweis für IPsec: Bei der Auswahl von Komponenten muss in jedem Einzelfall geprüft werden, ob die jeweilige Implementierung den lokalen Anforderungen entspricht. Insbesondere ist festzustellen, ob die benötigten Verschlüsselungs- und Authentisierungsverfahren zum Lieferumfang gehören. Auch bei der Konfiguration und Parametrierung von IPsec weisen die am Markt erhältlichen Produkte oft deutliche Unterschiede auf und vielfach ist die Implementierung so reduziert, dass eine sinnvolle Interoperabilität kaum mehr möglich ist.

Administration, Management und Protokollierung

- Die Unterstützung von personenbezogenen Benutzer-Kennungen und Zugriffsrechten wird vorausgesetzt.
- Alle Komponenten müssen ein Out-of-Band-Management unterstützen. Zudem muss eine gegebenenfalls vorhandene In-Band-Konfigurierbarkeit deaktivierbar sein.
- Die Management-Schnittstellen der Komponenten müssen sichere Management-Protokolle unterstützen (z. B. SNMPv3). Zugriffsrechte sollten, wo sinnvoll und vom jeweiligen Protokoll unterstützt, auf reinen Lesezugriff (read-only) einschränkbar sein.
- Eine Fernadministration über sichere Protokolle (z. B. SSH-2, HTTPS) muss unterstützt werden. Gleichzeitig müssen gegebenenfalls vorhandene unverschlüsselte Zugänge (z. B. Telnet, FTP) deaktivierbar sein.
- Alle Administrations- und Management-Zugänge müssen auf einzelne Quelladressen (Rechner) einschränkbar sein (z. B. mittels Zugriffslisten).
- Zur sicheren Synchronisation muss NTP im Client-Server-Mode mit Authentisierungsoption unterstützt werden.
- Eine Export-Schnittstelle zur Sicherung von Konfigurationseinstellungen muss vorhanden sein. Grundsätzlich ist dabei eine Textdarstellung (ASCII, XML) der Einstellungen gegenüber proprietären Binär-Formaten zu bevorzugen.
- Die Komponenten müssen eine Event-Benachrichtigung über standardisierte Protokolle (SNMP-Trap, syslog bzw. syslog-ng) unterstützen.
- Die automatische Protokollierung von Konfigurationsänderungen muss möglich sein.
- IPv6 muss in der Protokollierung und bei der Darstellung von Adressen unterstützt werden.
- Die Management-Schnittstellen sollten über IPv6 adressierbar sein. Dies ist leider bei vielen Produkten noch unzureichend umgesetzt.
- IPv6 muss sich analog zu IPv4 konfigurieren lassen. Auch hier haben viele Produkte noch Nachholbedarf.

Anbieter

- Bei der Auswahl der Komponenten sollte auf eine ausreichende MTBF (Mean Time Between Failure) und MTTR (Mean Time to Repair) geachtet werden.
- Der Anbieter muss einen Kundendienst bieten. Für die Grundarchitektur sollte dazu bei normalem Schutzbedarf eine Erreichbarkeit an Werktagen innerhalb der Arbeitszeit ausreichen.
- Der Anbieter muss eine sichere Versorgung mit Ersatzgeräten gewährleisten. Auch hier genügt für die Grundarchitektur bei normalem Schutzbedarf eine Erreichbarkeit innerhalb der regulären Arbeitszeit.

- Der Hersteller muss eine dauerhafte Versionspflege gewährleisten und unverzüglich auf bekannt gewordene Sicherheitsschwachstellen seiner Produkte reagieren, indem er nach vorherigen Tests unverzüglich Updates und Patches zur Verfügung stellt.

In den meisten Fällen wird eine explizite Prüfung des Umfangs und der Vollständigkeit der IPv6-Implementierung notwendig sein, da sich der Markt noch sehr im Fluss befindet und an vielen Stellen IPv6 erst relativ neu zum Standardlieferumfang gehört.

Bei der Auswahl des Internetserviceproviders sollte darauf geachtet werden, dass sowohl IPv4 als auch IPv6 nativ bereitgestellt werden. Die Bereitstellung von IPv4 über ein Carrier-Grade-NAT (CGN), Dual-Stack-Lite [RFC 6333] oder vergleichbare Mechanismen sollte ebenso vermieden werden wie die Bereitstellung von IPv6 über Tunnelmechanismen (siehe Abschnitt 3.12).

6.1.2 Anforderungen an Switches

Alle Verbindungen in der Grundarchitektur-Skizze (Abbildung 5.2), bei denen mehr als zwei Geräte direkt miteinander verbunden sind, werden durch Switch-Komponenten realisiert. Diese sind aus Gründen der Übersichtlichkeit in den Netzplänen nicht eingezeichnet.

Für einen Switch gelten folgende Anforderungen:

- Die Unterstützung von Protokollen zum Vermeiden redundanter Netzpfade (STP, RSTP, MSTP) wird vorausgesetzt. Gleichzeit muss eine Option zum Deaktivieren von BPDU-Paketen (ein- und ausgehend) an Endgeräte-Ports unterstützt werden.
- Sofern VLAN-Funktionalität nach dem Standard IEEE 802.1q integriert ist, muss sich diese Funktionalität pro Port einstellen lassen, um eine klare Trennung zwischen Zugriffs- und Trunk Ports zu gewährleisten.
- Die Anzahl der MAC-Adressen pro Port muss konfigurierbar sein.
- Es muss möglich sein, Ports so zu konfigurieren, dass an ihnen nur bestimmte MAC-Adressen zulässig ist.
- Bei Verletzung einer MAC-Filterregel muss es möglich sein, den Port für eine bestimmte Zeit zu sperren.

An Switches, die ausschließlich auf Layer 2 arbeiten, stellt IPv6 keine neuen Anforderungen. Switches, die auf Layer 3 arbeiten, müssen IPv6 vollständig unterstützen.

- Ein Switch für IPv6 muss in der Lage sein, Routeradvertisements zu filtern,
- Ein Switch für IPv6 muss Neighbor Discovery und Duplicate Address Detection verstehen und auswerten können
- Wenn in einem IPv6-Netz Multicast eine wesentliche Rolle spielt, sollten die verwendeten Switches MLD-aware sein, um Multicasts möglichst effizient verarbeiten zu können.

6.1.3 Anforderungen an Paketfilter

Im Folgenden werden Anforderungen für zustandsbehaftete Paketfilter (engl. stateful paket filter) definiert. Zustandslose Paketfilter entsprechen heute kaum mehr dem Stand der Technik und können allgemein durch zustandsbehaftete Paketfilter ersetzt werden:

- Das Weiterleiten oder Verwerfen von Paketen muss anhand folgender Kriterien möglich sein:

- Quell- und Zielport
- Quell- und Zieladresse einzelner Rechner oder Netze (für IPv6 in geeigneter Präfixdarstellung)
- ICMP-Typ und ICMP-Code
- ungültige TCP-Flag-Kombinationen
- Typ und Inhalt von IPv6-Erweiterungsheadern

Zusätzlich sind folgende Eigenschaften zu fordern:

- Filterregeln müssen getrennt für jede Schnittstelle konfigurierbar sein.
- Eine unabhängige Filterung kommender und gehender Pakete muss realisierbar sein.
- Für die Entscheidung, ob ein Datenpaket durchgelassen oder abgelehnt wird, muss klar sein, in welcher Reihenfolge die Filterregeln vom Paketfilter abgearbeitet werden und ob die erste zutreffende Regel (first match) oder die letzte zutreffende Regel (last match) über den Zugriff entscheidet.
- Der Paketfilter muss sogenanntes Whitelisting unterstützen: Wenn auf ein Datenpaket keine der vorgegebenen Filterregeln zutrifft, muss das Paket automatisch verworfen werden.
- Die Protokollierung von Regelverletzungen muss mindestens die folgenden Informationen umfassen:
  - IP-Adressen (Quelle und Ziel) des beanstandeten Pakets
  - betroffener Dienst (Quell- und Ziel-Port)
  - Datum und Uhrzeit der Regelverletzung
- Die Paketfilter müssen über Mechanismen zur Abwehr von Fragmentierungsangriffen (siehe Abschnitt 7.3.6) verfügen, wie zum Beispiel das Setzen der minimalen Fragmentgröße und die Begrenzung auf eine maximale Anzahl von Fragmenten pro Frame.
- Neben den Standardprotokollen TCP und UDP muss auch ICMP zustandsbehaftet filterbar sein.
- Es müssen Funktionen zum Verwerfen ungültiger TCP-Flag-Kombinationen integriert sein.
- Obergrenzen für offene und halboffene TCP-Verbindungen müssen konfigurierbar sein, ebenso Rate Limits für UDP-Verbindungen.
- Der Paketfilter sollte es bei IPv4 ermöglichen, das ID-Feld im IP-Header mit Zufallswerten zu belegen.
- Falls der Paketfilter als IPv4-NAT arbeitet, muss es die TCP-Implementierung ermöglichen, zufällig gewählte, nicht erratbare TCP-Sequenznummern zu vergeben.
- Der Paketfilter sollte bei IPv6 Mechanismen gegen Angriffe mit Router-Advertisements implementieren, wie beispielsweise den Router-Advertisement Guard [RFC 6105], [RFC 7113].

6.1.4 Anforderungen an den Perimeterrouter

In der Grundarchitektur wird nur ein expliziter Router eingesetzt − der Perimeterrouter in der Internet-Zone (Abbildung 5.11). Dieser wird in der Praxis oft vom Internet-Service-Provider gestellt und liegt damit außerhalb der Administrationshoheit des Netzverwalters.

Generell muss der Perimeterrouter die Anforderungen für Paketfilter erfüllen. Darüber hinaus gelten folgende Zusatzanforderungen:

- Statisches und dynamisches Routing müssen zum Standardfunktionsumfang gehören und sich gegebenenfalls abschalten lassen. Für das dynamische Routing sollten sichere Protokolle mit Authentisierung und Integritätssicherung nutzbar sein.
- Die folgenden Pakete sollten filterbar sein:
  - ICMP-IPv6-Pakete laut Tabellen in Abschnitt 6.2.4
  - ICMP-IPv4-Redirect und -Mask-Reply
  - alle Pakete mit einer Unique Local Address
- Die folgenden Funktionen sollten entweder nicht vorhanden oder deaktivierbar sein:
  - Proxy ARP
  - ICMP Router Discovery Protocol (IRDP)
  - Directed Broadcast (siehe [RFC 2644])
  - Source Routing

6.1.5 Anforderungen an das Application-Level Gateway

Das ALG muss alle für die Internet-Kommunikation benötigten Protokolle unterstützen, mindestens also DNS, SMTP, HTTP sowie HTTPS mit Zertifikatsprüfung. Für modulare Erweiterungen muss es außerdem Ein- bzw. Auskoppelschnittstellen bereitstellen, etwa zur Integration einer VPN-Box und oder eines Virenschutzprogramms.

Das ALGs muss so konfiguriert werden, dass es nur solche Protokolle und Dienste zulässt, die gemäß der geltenden Sicherheitsrichtlinie erwünscht sind und für die sie über entsprechende Sicherheits-Proxys verfügen. Kommunikationsbeziehungen, die nicht explizit erlaubt sind, müssen verworfen werden, ebenso alle Verbindungsversuche, die das ALG mit seiner Proxy-Ausstattung nicht angemessen kontrollieren kann. Insbesondere dürfen Pakete niemals ungeprüft weitergeleitet werden (forwarding).

In einer gemischten Umgebung mit einem internen IPv6-Netz und eines zumindest noch zu großen Teilen nur über IPv4 erreichbaren Internets müssen die ALGs auch in der Lage sein, als Proxy zwischen den beiden Protokollfamilien zu agieren. Optimal für diesen Zweck sind ALGs, die zum Internet hin als Dual-Stack-Lösung ausgeführt sind. Dies gilt auch für den umgekehrten Fall eines internen IPv4-Netzes und Diensten, die im Internet nur oder besser über IPv6 erreichbar sind.

Der bei IPv4 strikt geltende Grundsatz, dass Verbindungen über das ALG hinweg nur von innen nach außen, nicht aber aus dem Internet ins interne Netz aufgebaut werden dürfen, muss bei IPv6 dann aufgegeben werden, wenn ein ALG als IPv4-IPv6-Übergang vor einem Server in der DMZ betrieben wird (siehe 7.1.3 N). In diesem Sonderfall sind die daraus einstehenden zusätzlichen Gefährdungspotenziale genau zu bewerten und beim Aufbau zu berücksichtigen.

Die ALG-Komponente und die darauf eingesetzten Proxys der Grundarchitektur müssen folgenden dienstspezifischen Anforderungen genügen:

Anforderungen bezüglich HTTP

Für die sichere Nutzung von Informations- und Diensteangeboten des WWW muss das ALG folgende Filtermöglichkeiten bieten:

- Die Browserkennung sollte bei ausgehenden Web-Anfragen der LAN-Clients austauschbar sein.

- Informationen aus dem Request- und Response-Header müssen filterbar sein.
- Einzelne Webseiten müssen anhand ihrer Internet-Adresse bzw. URL, beigefügten Cookies (dediziert oder komplett), Aktiven Inhalten (z. B. ActiveX, Java) und Mime-Typen gesperrt werden können.

Zusätzliche Anforderungen bezüglich HTTPS

Für die sichere Nutzung verschlüsselter Verbindungen, etwa zur Übermittlung vertraulicher Informationen bei der WWW-Nutzung, muss das ALG darüber hinaus folgende Filterfunktionen anbieten.

- Eine Überprüfungsfunktion von Zertifikaten zur Kontrolle der Vertrauenswürdigkeit muss unterstützt werden. Bei Beanstandung des Zertifikats muss es möglich sein, die Verbindung abzuweisen. Konkret sind folgende Eigenschaften eines Zertifikats zu prüfen:
  - Überprüfung des Root-Zertifikats
  - Abgleich von aufgerufener URL mit der im Zertifikat enthaltenen URL (Common Name)
  - Überprüfung des Ablaufdatums
  - Überprüfung, ob das Zertifikat zurückgezogen wurde, beispielsweise mittels OCSP (Online Certificate Status Protocol)
- Veraltete Verschlüsselungsoptionen (z. B. SSLv2) und kryptografische Algorithmen (z. B. DES, MD5) sollten nicht unterstützt werden oder müssen deaktivierbar sein.
- Eigene Zertifikate müssen nachrüstbar sein, um auch „interne“ Root-Zertifikate konfigurieren und prüfen zu können.
- Vorkonfigurierter Zertifikate müssen entfernt werden können.

Anforderungen bezüglich SMTP

Für die sichere Nutzung von E-Mail sind folgende Filterfunktionen erforderlich:

- Der SMTP-Proxy (MRA) muss es ermöglichen, SMTP-Nachrichten anhand ihrer IP-Adresse, E-Mail-Adresse oder anhand des Domain-Namens zu filtern.
- Die Filterung von Dateianhängen bestimmter, konfigurierbarer Typen muss möglich sein.
- Der MRA sollte sogenanntes *Greylisting* unterstützen: E-Mails von bisher unbekannten Sendern werden zunächst temporär abgelehnt. Ein regulärer E-Mail-Server versucht die Zustellung ein zweites Mal, und diesmal wird die Nachricht akzeptiert; die meisten Spam-Quellen verzichten derzeit hingegen auf wiederholte Zustellversuche und sind daher nicht in der Lage, das Greylisting zu überwinden.
- Der MRA sollte in der Lage sein, interne IP-Adressen, insbesondere lokale IPv6-Adressen mit MAC-Adresse in den unteren 64 Bit, aus den E-Mail-Headern zu entfernen

Darüber hinaus muss es möglich sein, E-Mails über eine Auskoppelschnittstelle zu einem Virenschutzprogramm weiterzuleiten.

Anforderungen bezüglich DNS

Für die sichere Nutzung von DNS sind folgende Anforderungen zu erfüllen:

- Rekursive DNS-Anfragen müssen auf einzelne Netze oder IP-Adressen einschränkbar sein.

- Der DNS-Proxy sollte in der Lage sein, die DNS-Versionsnummer zu unterdrücken.
- Der Proxy muss eine Option zum Abweisen von Anfragen mit nicht gesetztem „Recursion-Bit“ anbieten.

6.1.6 Anforderungen an Server

Ergänzend zu den in Abschnitt 6.1.1 geforderten grundlegenden Eigenschaften gelten die folgenden Anforderungen für die Basisdienste DNS, DHCP und NTP in der Grundarchitektur. Ergänzende Anforderungen an E-Mail- und Web-Server werden in den ISi-Modulen [ISi-Mail-Server] und [ISi-Web-Server] dargestellt. Auf konkrete Auswahlkriterien für Management-Server wurde an dieser Stelle verzichtet, da die entsprechenden Anforderungen stark von der eingesetzten Management-Software abhängen.

Anforderungen an DNS-Server

Für die sichere Nutzung der DNS-Server sind folgende Anforderungen zu erfüllen:

- Rekursive DNS-Anfragen müssen auf einzelne Netze oder IP-Adressen einschränkbar sein.
- DNS-Server sollten in der Lage sein, die DNS-Versionsnummer zu unterdrücken.
- Die List-Domain-Funktion (AXFR und IXFR) muss deaktivierbar sein.
- Die dynamische Aktualisierung von DNS-Daten muss deaktivierbar sein.
- Es muss eine Option zum Abweisen von Anfragen mit nicht gesetztem „Recursion-Bit“ vorhanden sein.
- Zonentransfers müssen auf einzelne berechtigte Server einschränkbar sein.
- IPv6 muss für Anfragen (eingehend und ausgehend) unterstützt werden.
- IPv6-Records vom Typ AAAA müssen unterstützt werden.
- Unabhängig von IPv6 und IPv4 sollte DNSSEC unterstützt werden.

Anforderungen an DHCP-Server

Für die sichere Nutzung des DHCP-Servers im Stateful-Modus muss dieser über eine Funktion verfügen, um IP-Adressen nur an DHCP-Clients mit registrierter MAC-Adresse zu vergeben.

Für den Betrieb mit IPv6 sind zusätzlich zu fordern:

- Unterstützung von DHCPv6
- Verfügbarkeit von stateless DHCPv6

Anforderungen an NTP-Server

Für die sichere Nutzung der NTP-Servers sind folgende Anforderungen zu erfüllen:

- Der Server muss authentisierte Synchronisation im Client-Server-Modus anbieten.
- Der Broadcast-Modus muss deaktivierbar sein.
- Der Server muss seine Zeit über einen DCF77- oder GPS-Empfänger beziehen können.

6.2 Sichere Grundkonfiguration der Komponenten

Die sichere Grundkonfiguration der in Abschnitt 5 verwendeten Komponenten umfasst eine Reihe von Einstellungen, die unabhängig vom Komponententyp vorzunehmen sind. Darüber hinaus gibt es spezifische Empfehlungen, die nur bestimmte Komponententypen betreffen.

Unabhängig von konkreten Konfigurationsempfehlungen gilt der Grundsatz, dass alle, insbesondere die IPv6 betreffenden Konfigurationsmaßnahmen ausgiebig getestet werden müssen, ehe die betroffenen Komponenten im Online-Betrieb eingesetzt werden dürfen.

6.2.1 Grundlegende Konfigurationsvorgaben für alle Komponenten

Folgende Konfigurationsempfehlungen gelten allgemein, unabhängig vom Typ einer Komponente.

Funktion und Leistungsfähigkeit

- Alle Schnittstellen sollten auf standardkonforme, nicht-proprietäre Protokolle eingestellt werden. Zusätzlich müssen die Authentisierungs- und Verschlüsselungs-Optionen der eingesetzten Protokolle aktiviert werden, soweit eine Verschlüsselung sinnvoll ist und von der Umgebung oder Anwendung erforderlich ist.
- Bei der Wahl von Verschlüsselungsmechanismen müssen standardkonforme, starke Algorithmen mit ausreichender Schlüssellänge eingestellt werden[3]. Schwächere Verfahren, die oft aus Gründen der Interoperabilität als Alternative angeboten werden, sind ausdrücklich zu sperren.
- Die Konfiguration aller Komponenten ist möglichst einfach zu halten und auf das Notwendige zu beschränken (Minimalitätsprinzip). Konkret bedeutet dies:
  - Getrennte Funktionen sind auf getrennten Komponenten einzurichten (Ein Dienst pro Server!). Wenn man bei IPv6 von dieser Regel abweicht, sollte zumindest eine eigene Adresse für jeden Service verwendet werden.
  - Alles, was nicht ausdrücklich benötigt wird, sollte aus der Konfiguration entfernt oder zumindest deaktiviert werden.
  - Die Betriebssystem-Konfiguration muss auf einen möglichst geringen Funktionsumfang reduziert werden. Bei besonders sicherheitskritischen Komponenten empfiehlt sich der Einsatz speziell gehärteter Varianten.
  - Alles, was nicht explizit erlaubt ist, muss die Grundkonfiguration abweisen (Whitelist-Ansatz).
  - Innerhalb des Sicherheits-Gateways ist dynamisches Routing nicht erforderlich und muss deaktiviert werden.
- Informationen über den internen Konfigurations- und Betriebszustand der Komponenten sind nach außen bestmöglich zu verbergen (Need-to-Know-Prinzip). Unnötige „Auskunft-Dienste“ (z. B. rwho, rup) müssen stillgelegt werden.
- Vor Inbetriebnahme müssen die Komponenten mit einem aktuellen Betriebssystem einschließlich der neuesten Updates und Patches ausgestattet werden.

3 Die Bundesnetzagentur (www.bundesnetzagentur.de) veröffentlicht regelmäßig auf Basis der Angaben des BSI im Bundesanzeiger eine Übersicht über Kryptoalgorithmen, die zur Erzeugung von Signaturschlüsseln, zum Hashen von Daten und zur Prüfung und Erzeugung von digitalen Signaturen als geeignet angesehen werden.

- Wann immer möglich, sollte ein Gerät nur mit einem IP-Stack betrieben werden (entweder IPv4 *oder* IPv6). Dual-Stack sollte nur dort eingeschaltet werden, wo es für die Funktion notwendig ist.

Wenn IPsec verwendet wird, so sollte die jeweilige Implementierung auf Leistungsumfang und Vollständigkeit geprüft werden. Insbesondere ist darauf zu achten, dass ausreichend sichere Kryptoalgorithmen vorhanden sind und schwache Algorithmen abschaltbar sind.

Administration, Management und Protokollierung

- Allen Benutzern und Administratoren müssen personenbezogene Kennungen mit individuellen Zugriffsrechten zugewiesen werden, die durch kennungsspezifische Passwörter, Zertifikate oder dergleichen geschützt sind. Es müssen sichere Passwörter verwendet werden.
- Für Benutzerschnittstellen sollten Zeitbeschränkungen (Session Timeouts) vorgegeben werden.
- Alle Komponenten müssen über die Out-of-Band-Schnittstelle mit dem Management-Netz verbunden werden. Zudem muss die In-Band-Konfigurierbarkeit deaktiviert werden.
- Zum Administrieren der Komponenten muss ein sicheres Management-Protokoll (z. B. SNMPv3) konfiguriert werden. Die Zugriffsrechte sind so weit wie möglich einzuschränken (z. B. auf reinen Lesezugriff).
- Für die Fernadministration sind sichere Protokolle (z. B. SSH-2, HTTPS mit Zertifikatsprüfung) einzurichten, wobei diese auf die Verwendung starker Kryptografie einzuschränken sind. Unverschlüsselte Zugänge wie zum Beispiel Telnet müssen deaktiviert werden.
- Der Zugriff auf die Administrations- und Management-Zugänge muss auf autorisierte Quelladressen eingeschränkt werden (z. B. auf den Management-Server).
- Zur Synchronisation muss NTP im Client-Server-Mode mit Authentisierung aktiviert werden.
- Sicherungskopien der Konfigurationen müssen angelegt werden. Diese sollten grundsätzlich (auch) in einer Textdarstellung (ASCII, XML) abgespeichert und dokumentiert werden. Ein Zugriff muss auch bei einem Ausfall des Management-Systems jederzeit möglich sein; notfalls sind Papierkopien vorzuhalten.
- Eine unverzügliche Event-Benachrichtigung muss über standardisierte Protokolle umgesetzt werden (z. B. SNMP-Traps, syslog). Bei der Konfiguration des Logdaten- und Monitoring-Umfangs ist allerdings sorgfältig auf die Einhaltung der gesetzlichen Bestimmungen zu achten. Die Auswahl der zu protokollierenden Ereignisse ist im Konfigurationskonzept festzuschreiben.

6.2.2 Konfigurationsvorgaben für Switche

Die Grundarchitektur sieht eine Realisierung auf Basis von Switched Ethernet vor. Die Switch-Komponenten sind wie folgt zu konfigurieren:

- Alle ungenutzte Switch-Ports sind zu sperren.
- Protokolle zum Vermeiden redundanter Netzpfade (z. B. STP) sollten nur bei Bedarf − individuell für jeden Port − aktiviert werden. BPDU-Paketen (ein- und ausgehend) müssen an Endgeräte-Ports verworfen werden.
- VLAN-Funktionalität nach dem Standard [IEEE 802.1q] sollte nur bei Bedarf aktiviert werden. Bei der konsequenten Umsetzung des Prinzips „viele kleine Netze“ mit IPv6 gewinnt die Verwendung entsprechend vieler VLANs höhere Bedeutung. Der Einsatz von VLANs ist dann

sinnvoll, wenn die einzelnen kleinen Teilnetze nicht auf physikalisch getrennten Leitungen ausgeführt werden können.

- Endgeräte-Ports müssen statisch einem festen VLAN zugeordnet werden.
- Zum Schutz vor Angriffen sollte die maximale Anzahl von MAC-Adressen pro Port auf eine einzelne eingeschränkt werden. Noch sicherer ist es, pro Port eine feste statische MAC-Adresse zu konfigurieren (siehe Variante 7.2.3 A) oder die Endgeräte im Switch anhand ihrer MAC-Adresse zu authentisieren (siehe Variante 7.2.3 B). Bei normalem Schutzbedarf ist eine Überprüfung der Geräteadresse in der Regel ausreichend. Anwender mit hohem Schutzbedarf sollten statt dessen eine Geräteauthentisierung nach dem Standard [IEEE 802.1X] konfigurieren (siehe Variante 7.2.3 C).
- Switch-Ports sollten die Annahme von IPv6-Router-Advertisements auf allen Client-Ports sperren und sie lediglich an Ports zulassen, an denen Router angeschlossen sind.
- Falls vorhanden (bei IPv6 nur, falls stateful DHCP verwendet wird), sollten darüber hinaus die gerätespezifischen Mechanismen gegen DHCP-Manipulationen aktiviert werden (siehe Abschnitt 7.5.7). Gegebenenfalls kann auf den Einsatz von DHCP ganz verzichtet werden (siehe Variante 7.5.7 A). Auch in reinen IPv6-Teilnetzen, in denen Autokonfiguration und stateless DHCP eingesetzt werden, können die speziellen DHCP-Sperren entfallen.

6.2.3 Konfigurationsvorgaben für Paketfilter

Bei Teilnetzen mit reinem IPv6-Betrieb können die Einstellungen für NAT entfallen.

Für Paketfilter gelten folgende Konfigurationsempfehlungen:

- Alle Filterregelsätze sind nach einem Whitelist-Ansatz zu konzipieren: „Alles, was nicht explizit erlaubt ist, wird verworfen“. Man erreicht dies zum Beispiel, indem man grundsätzlich die zulässigen Paketformate auflistet (Permit-Regeln) und jede Regelliste mit einer universellen Verbotsregel (deny any) abschließt.
- ICMP-Nachrichten am Übergang zwischen einem vertrauenswürdigen und einem nicht-vertrauenswürdigem Netz sind für IPv4 grundsätzlich zu sperren. Nur bei Bedarf dürfen diese (ausschließlich für Administrationszwecke) dediziert freigeschaltet werden. Da die Administration in der Grundarchitektur über ein getrenntes Management-Netz erfolgt, kann ICMP an allen Nutzdaten-Schnittstellen der Paketfilter grundsätzlich gesperrt werden. Nur im Management-Netz sind in der Regel einige ICMP-Nachrichten zu transportieren (siehe Tabelle 9).
- ICMP-v6-Nachrichten sind nach den in Tabelle 4 definierten Regeln für Netze mit IPv6-Verkehr und nach den Regeln in Tabelle 5 für den Verkehr von IPv6 in Management-Netzen zu filtern. Alle in der Tabelle nicht erwähnten ICMP-Typen (insbesondere für Mobile IPv6 und alle privaten und experimentellen Erweiterungen) sollten grundsätzlich gesperrt werden. Zusätzlich sollte die Zahl der ICMP-Nachrichten mit einem rate-limit beschränkt werden.
- Das Verschicken von Router-Advertisements darf nur von berechtigten Adressen erfolgen.
- Im IPv4-NAT-Betrieb muss für TCP die zufällige Generierung von Initial Sequence Numbers (ISNs) aktiviert werden.
- Die verfügbaren Mechanismen gegen Fragmentierungsangriffe müssen aktiviert werden.
- Auch für die verbindungslosen Protokolle UDP und ICMP sollten zustandsbehaftete Filterregeln konfiguriert werden.

- Die Funktionen zum Verwerfen ungültiger TCP-Flag-Kombinationen müssen aktiviert werden. Typische ungültige Kombinationen sind zum Beispiel: Kein Bit gesetzt, `SYN-FIN`, `SYN-RST`, `FIN-SYN-RST-PSH-ACK-URG` oder `RST-FIN`.
- Limits für offene und halboffene TCP-Verbindungen und Rate Limits für UDP-Verbindungen sollten definiert werden.
- Die Option zum Überschreiben des ID-Felds im IP-Header mit einem Zufallswert sollte aktiviert werden.
- Die Integritätsprüfung der Datenpakete (z. B. das Auswerten von Prüfsummen im Paket-Header) sollte aktiviert sein.

IPv4-ICMP Nachricht	*Von der Management-Station*	*Zur Management-Station*	*Bemerkung*
Echo-Request (8)	Erlauben	Sperren	Diagnose Ping
Echo-Antwort (0)	Sperren	Erlauben	Diagnose Ping
DestinationUnreachable (Typ 3)	Sperren	Erlauben	Diagnose
Time Exceeded (Typ 11)	Sperren	Erlauben	Diagnose von Routingproblemen
Andere	Sperren	Sperren	

Tabelle 8: IPv4-ICMP Sperren

IPv6-ICMP Nachricht	*Von der Management-Station*	*Zur Management-Station*	*Bemerkung*
Echo-Request (128)	Erlauben	Sperren	Diagnose
Echo-Antwort (129)	Sperren	Erlauben	Diagnose
ICMP-Information-Request (139) Reverse-Neighbor-Reques (141)	Erlauben	Sperren	Diagnose
ICMP-Information-Answer (140) Reverse-Neighbor-Answer (142)	Sperren	Erlauben	Diagnose

Tabelle 9: Sperren von ICMP-Paketen zur Management Station

Für das Blockieren von ICMP-Nachrichten gelten bei IPv6 andere Regeln, als bei IPv4. da für einen reibungslosen Betrieb von IPv6 einige der ICMP-Nachrichten zwingend benötigt werden.

Tabelle 9 fasst Sonderfälle im Zusammenhang mit der Management-Station zusammen. In Tabelle 10 werden die wesentlichen bei IPv6 verwendeten ICMP-Typen aufgelistet und ihre Behandlung festgelegt.

IPv6-ICMP Nachricht	*Zwischen den internen Netzen*	*Vom externen Internet*	*Zum externen Internet*	*Bemerkung*
Destination	Zulassen	Zulassen	Zulassen	Fehlererkennung

IPv6-ICMP Nachricht	*Zwischen den internen Netzen*	*Vom externen Internet*	*Zum externen Internet*	*Bemerkung*
unreachable (1)				
Packet too big (2)	Zulassen	Zulassen	Zulassen	Notwendig für korrekte Fragmentierung
Time exceeded (3)	Zulassen	Zulassen	Zulassen	Fehlererkennung
Parameter Problem (4)	Zulassen	Zulassen	Zulassen	Fehlererkennung
Echo-Request (128)	Siehe Tabelle 9	Sperren	Nur von der Management Station	Diagnose
Echo-Antwort (129)	Siehe Tabelle 9	Nur zur Management Station (rate-limited)	Sperren	Diagnose
Multicast (130, 131, 132, 143, 151, 152, 153)	Zulassen (ohne Forwarding)	Zulassen (ohne Forwarding)	Zulassen (ohne Forwarding)	Multicast-Verwaltung
Router (133, 134)	Zulassen (ohne Forwarding)	Sperren	Sperren	Autoconfiguration
Neighbor (135,136)	Zulassen (ohne Forwarding)	Zulassen (ohne Forwarding)	Zulassen (ohne Forwarding)	Neighbor Discovery
Redirect (137)	Zulassen (ohne Forwarding, nur ausgehend vom Router)	Sperren	Sperren	Umleitung
ICMP-Information (139,140) Reverse-Neighbor (141,142)	Siehe Tabelle 9 zusätzlich[4]	Sperren	Sperren	Diagnose

Tabelle 10: Sperren von IPv6-ICMP-Paketen im Netz

6.2.4 Konfigurationsvorgaben für den Perimeterrouter

In der Grundarchitektur wird nur ein Router eingesetzt: der Perimeterrouter. Dessen genaue Konfigurationseinstellungen sind von der verwendeten Anschlusstechnologie abhängig. Allgemein gelten jedoch folgende Konfigurationsempfehlungen:

- Dynamisches Routing sollte nur bei Bedarf aktiviert werden. Soweit erforderlich, sollten sichere Routing-Protokolle mit Authentisierung und Integritätssicherung konfiguriert werden. Derzeit ist

4 Bei der Verwendung von Windows-Server-Systemen und Clients mit Active Directory müssen Echo-Request und Echo-Answer auch innerhalb des Netzes zwischen Clients und Servern erlaubt werden. Man kann dies unter Umständen auf Echo-Request vom Client zu Server und Echo-Answer vom Server zum Client einschränken.

allerdings bei IPv6 kein derartiges Protokoll verfügbar. Es sind daher entsprechende Einschränkungen bei der Sicherheit in Kauf zu nehmen. Anwender mit hohem Schutzbedarf bezüglich Vertraulichkeit können darüber hinaus erwägen, ein verschlüsseltes Routing-Protokoll einzusetzen (siehe Variante 7.3.13 A).

- Die folgenden Pakete müssen gesperrt werden:
  - ICMP gemäß der Tabellen 8 (IPv4) und 9 (IPv6)
  - insbesondere ICMP Redirect
  - und ICMP Mask-Reply
- Die folgenden Funktionen müssen gesperrt werden (sofern vorhanden):
  - Proxy ARP für IPv4 und Proxy Neigbour Detection (ND) für IPv6
  - ICMP Router Discovery Protocol (IRDP) (siehe [RFC 1256])
  - IP Directed Broadcast (siehe [RFC 2644])
  - IP Source Routing
- Am Perimeter-Router muss Anti-Spoofing nach [RFC 2827], [RFC 3704], [RFC 1918] und [RFC 5735] konfiguriert werden:
  - Eingehende Filterung (ingress) ist für IPv4 nach Tabelle 11 und für IPv6 nach Tabelle 12 einzurichten: Pakete mit den genannten Quelladressen sind zu verwerfen, der restliche Datenverkehr bleibt von der Anti-Spoofing-Filterung unberührt.
  - In ausgehender Richtung (egress) sind für IPv4 als Quelladresse nur eigene Netzadressen zugelassen, der restliche Datenverkehr ist zu sperren. Bei IPv6 sind nur Pakte aus den eigenen Adressbereichen mit Global-Unicast-Adressen zulässig, alle anderen, insbesondere mit Unique-Local-Adressen, sind zu verwerfen.

Adressbereich	*Name*	*Anmerkung*
a.b.c.d/e	Eigener Adressbereich	Offiziell zugeteilter öffentlicher Adressraum
0.0.0.0/8	Das eigene Netz („This“ Network)	[RFC 5735]
10.0.0.0/8	Private Adressen (Private-Use Network)	[RFC 1918]
127.0.0.0/8	Loopback (u. a. eigener Rechner (localhost))	[RFC 5735]
169.254.0.0/16	Verbindungslokale Adressen (Link Local addresses)	[RFC 5735]
172.16.0.0/12	Private Adressen (Private-Use Network)	[RFC 1918]
192.0.0.0/24	Reserviert (Reserved but subject to allocation)	[RFC 5735]
192.0.2.0/24	Test-Netz	
192.88.99.0/24	Tunnelmechanismen, um IPv6-Pakete über IPv4 transportieren zu können. (6to4 Relay Anycast)	[RFC 3068]
192.168.0.0/16	Private Adressen (Private-Use Network)	[RFC 1918]
198.18.0.0/15	Network Interconnect Device Benchmark Testing	[RFC 2544]
224.0.0.0/4	Multicast	[RFC 3171]
240.0.0.0/4	Reserviert (Reserved for Future Use)	[RFC 5735]

Tabelle 11: IPv4-Adressbereiche

Die IP-Adressbereiche 14.x.x.x, 24.x.x.x, 39.x.x.x, 128.x.x.x, 191.255.x.x und 223.255.255.x, die früher nach [RFC 1700], [RFC 1797], [RFC 1918] und [RFC 3330] reserviert waren, sind mit [RFC 5735] für die allgemeine Nutzung freigegeben worden und werden in nächster Zeit als normale Adressen verteilt und benutzt werden. Von einer generellen Sperrung dieser Bereiche, wie sie ursprünglich in der ersten Version von ISi-LANA empfohlen wurde, ist daher abzusehen.

Adressbereich	*Name*	*Anmerkung*
xx::/p	Eigener Adressbereich	Offiziell zugeteilter öffentlicher Adressraum
::/128	Undefinierte Adresse	[RFC 5156]
::1/128	Eigener Rechner	[RFC 5156]
::ffff:0:0/96	IPv4-Adressen im IPv6-Format (mapped addresses)	[RFC 5156]
::<IPv4-address>/96	IPv4-kompatible Adressen	[RFC 4291] - Sollten eigentlich nicht vorkommen, sind nicht mehr zulässig
fe80::/10	Link-Local-Adressen (außer den von der Gegenstelle benutzten)	[RFC 5156]
fec0::/10	Ehemals Site-Local-Adressen	Sollten eigentlich nicht vorkommen, sind nicht mehr zulässig
fc00::/8	Unique-Local-Adressen mit zentraler Registrierung	[RFC 5156] und [RFC 4193] - „private“ Adressen für das lokale Netz
fd00::/8	Unique-Local-Adressen lokal zufällig erzeugt	[RFC 5156] Und [RFC 4193] - „private“ Adressen für das lokale Netz
(ff00::/8)	Multicast-Adressen, soweit nicht benutzt	Die Mulitcast-Bereiche für ND müssen zugelassen werden, kein Forwarding erlaubt.
2001:db8::/32	Adressen zur Verwendung in Dokumentationen und Handbüchern	[RFC 5156]
2001::/32	Teredo – Relay-Adressen	[RFC 4380]
2002::/16	6to4-Tunnel	[RFC 3056]
0000::/3, 4000::/2, 8000::/2, c000::/3. e000::/4, f000::/5, f800::/6, fe00::/9, fec0::/10	Nicht zugewiesene Adressbereiche (siehe [IANA IPv6])	Aus diesen Bereichen können jederzeit von IANA oder der IETF Bereiche für neue Anwendungsfelder definiert werden.

Tabelle 12: IPv6-Adressbereiche (Stand Ende 2010)

6.2.5 Konfigurationsvorgaben für das Application-Level Gateway

Grundsätzlich ist das ALG so zu konfigurieren, dass es nur solche Protokolle und Dienste zulässt, die gemäß der geltenden Sicherheitsleitlinie erwünscht sind und für die es über Sicherheits-Proxys verfügt. Kommunikationsbeziehungen, die nicht explizit erlaubt sind, müssen verworfen werden, ebenso alle Verbindungsversuche, die das ALG mit seiner Proxy-Ausstattung nicht angemessen kontrollieren kann. Soweit Anwendungsprotokolle über Mechanismen zur Integritätskontrolle verfügen, sollten die entsprechenden Integritätsstests des zuständigen Proxys aktiviert werden.

Insbesondere dürfen Pakete, im Gegensatz zu einem transparenten Proxy, niemals ohne Prüfung des Inhalts weitergeleitet werden (forwarding). Darüber hinaus gilt der Grundsatz, dass Verbindungen über das ALG hinweg nur von innen nach außen, nicht aber aus dem Internet ins interne Netz aufgebaut werden dürfen. Im einzelnen gelten folgende Vorgaben:

Konfigurationsvorgaben für HTTP

- Es muss eine Sperrung von bedenklichen URLs, aktiven Inhalten und Cookies gemäß der geltenden Sicherheitsleitlinie umgesetzt werden.
- Ein Filtern bzw. Ersetzen der Browser-Kennung ist zu empfehlen.
- Eine Filterung von unerwünschten Informationen aus dem Request- und Response-Header sollte umgesetzt werden. Hierbei sollte auch auf eine Filterung und Umsetzung von IPv6-Adressen geachtet werden.
- Nur die erforderlichen und erwünschten MIME-Typen dürfen freigeschaltet werden.

Konfigurationsvorgaben für HTTPS

Ein HTTPS-Proxy ist die zentrale Entscheidungsinstanz für die Akzeptanz von Zertifikaten. Der Proxy übernimmt statt des Benutzers am Arbeitsplatz die Kontrolle über die Zertifikate. Aus diesem Grund sind die Einstellungen des HTTPS-Proxys bzgl. der Zertifikatsprüfung von besonderer Wichtigkeit. Folgende Einstellung sollten zusätzlich zu den HTTP-Vorgaben umgesetzt werden:

- Nur solche Zertifikate dürfen akzeptiert werden, die allgemein anerkannt sind (z. B. in gängigen Browsern vorkonfigurierte Wurzelzertifikate renommierter Zertifizierungsstellen) oder die gemäß der lokalen Sicherheitsleitlinie ausdrücklich als vertrauenswürdig eingestuft werden. Einzelne, vom Hersteller des ALGs vorkonfigurierte Zertifikate sind zu entfernen, wenn sie mit der lokalen Sicherheitsleitlinie unvereinbar sind.
- Es sollte eine Prüfung der URL gegen den im Zertifikat enthaltenen Common Name durchgeführt werden. Stimmen die beiden nicht überein, so könnte dies auf eine Manipulation oder eine fehlerhafte Konfiguration hindeuten. Die Verbindung sollte dann abgewiesen werden.
- Zertifikate mit abgelaufenem Datum sowie zurückgezogene Zertifikate dürfen grundsätzlich nicht akzeptiert werden.

Es dürfen nur hinreichend sichere Verschlüsselungsverfahren mit ausreichender Schlüssellänge unterstützt werden. Dazu ist zum Beispiel die Deaktivierung veralteter SSL-Versionen (SSLv2) und alter Krypto-Algorithmen erforderlich.

Konfigurationsvorgaben für SMTP

Für die sichere Nutzung von SMTP sind folgende Konfigurationsvorgaben umzusetzen:

- Es sollte kontrolliert werden, ob Server des vertrauenswürdigen Netzes als Mail Relay missbraucht werden. Dazu ist bei eingehenden E-Mails zu überprüfen, ob der Domain-Name des Empfängers zum vertrauenswürdigen Netz gehört. Bei ausgehenden E-Mails muss die Absender-Domain zum vertrauenswürdigen Netz gehören.
- Auffällige E-Mail-Adressen bzw. Domains sollten über eine Sperrliste (Blacklist) gesperrt werden.
- Eingehende E-Mails sollten vor ihrer Auslieferung über die Auskoppelschnittstelle des ALG an ein Virenschutzprogramm weitergeleitet werden.
- Nicht zugelassene Dateianhänge sollten ausgefiltert werden. Hierzu können beispielsweise bat, vbx, chm, com, hta, inf, js, jse, lnk, mdb, wsh, vbs, vbe, pif, scr, rm oder reg zählen. Für höhere Sicherheitsansprüche empfiehlt sich auch hier ein Whitellist-Ansatz, bei dem nur Dateianhänge mit bestimmten vorher definierten Typen zugelassen werden und alle anderen Anhänge verworfen werden.

Konfigurationsvorgaben für DNS

Für die sichere Nutzung von DNS sind folgende Konfigurationsvorgaben umzusetzen:

- Rekursive DNS-Anfragen dürfen nur von internen DNS-Clients angenommen werden. Rekursive Anfragen aus dem Internet muss das ALG zurückweisen.
- Die Versionsnummern-Anzeige des Proxys muss unterdrückt werden.
- Anfragen mit nicht gesetztem „Recursion-Bit“ sind abzuweisen.

In allen Anwendungsfällen kommt die Forderung hinzu, dass IPv6-Adressen in den umgesetzten Paketen und auch im Datenstrom (zum Beispiel in E-Mail-Adressen oder in URLs/URIs) korrekt erkannt und umgesetzt werden müssen.

6.2.6 Konfigurationsvorgaben für Server

Ergänzend zu den in Abschnitt 6.2.1 geforderten grundlegenden Konfigurationsvorgaben gelten die folgenden Einstellungen für die Basisdienste DNS, DHCP und NTP in der Grundarchitektur. Ergänzende Anforderungen an E-Mail- und Web-Server werden in den Modulen [ISi-Mail-Server] und [ISi-Web-Server] der ISi-Reihe dargestellt.

Auf konkrete Konfigurationsempfehlungen für Management-Server wurde an dieser Stelle verzichtet, da die entsprechenden Vorgaben stark von der eingesetzten Management-Software abhängig sind.

Ein wichtiges Grundprinzip bei der Konfiguration der Server ist die Vorgabe, für eine Datentrennung zwischen internen und externen Benutzern der Server zu sorgen. Ein Zugriff aus dem Internet sollte − soweit überhaupt zulässig − grundsätzlich eine andere Sicht auf die bereitgestellten Informationen eines Dienstes liefern als ein Zugriff aus dem LAN. Bei grundlegenden Diensten ist es deshalb erforderlich, mehrere Ausprägungen des Servers zu betreiben (einen „inneren“ und einen „äußeren“ Server), die nur über ein Sicherheits-Proxy untereinander Daten austauschen.

DNS-Server

Die Grundarchitektur unterscheidet zwischen einem inneren und einem äußeren DNS, die durch zwei getrennte Server realisiert werden. Für beide DNS-Server gelten folgende Anforderungen:

- Rekursive DNS-Anfragen dürfen nur aus vertrauenswürdige Netzen akzeptiert werden, um einem Missbrauch der Rekursion vorzubeugen (siehe Abschnitt 7.5.3). Dies bedeutet für den äußeren DNS-Server eine Einschränkung auf rekursive Anfragen durch Rechner aus dem internen Netz und für den inneren DNS-Server − laut Grundarchitektur − keine Einschränkung, da dieser ohnehin nur von vertrauenswürdigen Rechnern im Inneren des LANs erreichbar ist. (Umfasst ein Netz mehrere interne Sicherheitszonen mit eigenen DNS-Servern, so ist der Kreis vertrauenswürdiger Clients pro DNS-Server entsprechend einzuschränken.)
- Die Versionsnummer-Unterdrückung muss aktiviert werden.
- Um ein Ausspähen zu vermeiden, muss die List-Domain-Funktion (AXFR und IXFR) deaktiviert werden.
- Dynamische Aktualisierungen von NS-Daten sollten gesperrt sein.
- Anfragen mit nicht gesetztem *Recursion-Bit* müssen zum Schutz gegen Außen- und Innentäter verworfen werden. Durch gezielte nicht-rekursive Anfragen kann sonst der DNS-Cache ausgespäht werden (siehe Abschnitt 7.5.4).
- Zonentransfers müssen auf einzelne berechtigte Server eingeschränkt werden.
- Dynamische Aktualisierungen von DNS-Daten sollten gesperrt sein. Ausgenommen hiervon können rein interne DNS-Zonen bleiben, bei denen die Aktualisierung nur von autorisierten Geräten vorgenommen werden kann (zum Beispiel Windows Active-Directory-Umfeld).
- Da in vielen Fällen der Umgang mit den deutlich längeren IPv6-Adressen beim manuellen Pflegen der Einträge im DNS, insbesondere der Reverse-Einträge, doch sehr aufwendig ist, kann man in Umgebungen mit normalen Sicherheitsanforderungen für die internen DNS-Zonen dynamische Updates freischalten (z. B. bei Windows 2008 als Server und Windows 7 als Client), allerdings nur unter der Bedingung, dass eine ausreichende Authentisierung der Clients erfolgt.

Weiterhin sollte nach heutigem Stand der Technik unabhängig von IPv6 die DNS-Resolver-Konfiguration mit DNSSEC betrieben werden, so dass mit signierten Daten gearbeitet werden kann. Auf jeden Fall sollten die eigenen Zonendaten signiert werden und sobald Registry und Registrar der Zone dies anbieten, auch die entsprechenden Trust Anchors publiziert werden.

Wenn E-Mail- oder Web-Server betrieben werden, dann sollten die zugehörigen Zertifikate mittels DANE im DNS hinterlegt und per DNSSEC signiert werden.

DHCP-Server

- Zur sicheren Nutzung von DHCP dürfen nur IP-Adressen für registrierte MAC-Adressen vergeben werden. Die MAC-Adressen aller autorisierten DHCP-Clients sollten zentral verwaltet werden.
- Die Konfiguration des DHCP-Servers kann sich bei Verwendung von Autoconfiguration in reinen IPv6-Teilnetzen auf die feste Konfiguration der per stateless DHCP zu verteilenden Dienste-Informationen beschränken. Bei stateless DHCP erübrigt sich eine Einschränkung auf bestimmte MAC-Adressen und damit die Verwaltung der MAC-Adressen.

NTP-Server

Für die sichere Nutzung der NTP-Server sind folgende Vorgaben zu erfüllen:

- Die Zeit kann von einem DCF77- oder GPS-Modul bezogen werden. Alternativ kann die Zeit auch von vertrauenswürdigen Servern bezogen werden.
- Der Server sollte im Client-Server-Modus betrieben werden. Die NTP-Kommunikation muss authentisiert sein.
- Die Zeitverteilung per Broadcast-Modus sollte deaktiviert werden.

6.3 Grundvorgaben für einen sicheren Betrieb

Nachdem ein Konzept für die Beschaffung geeigneter IT-Komponenten erstellt ist und sichere Konfigurationsvorgaben festgelegt sind, ist gemäß dem in [ISi-E] empfohlenen Ablaufplan ein Konzept für den sicheren Betrieb der Systemkomponenten zu entwickeln. Dieser Abschnitt gibt dazu grundlegende Empfehlungen.

Generelle Vorgaben

Die Vorgaben für den sicheren Betrieb der Grundarchitektur sind überwiegend allgemein und nicht auf spezielle Komponenten bezogen. Sie gelten generell für vernetzte IT-Systeme. Soweit es komponentenspezifische Empfehlungen gibt, sind diese in der Regel schon durch die Grundarchitektur selbst und durch die Konfigurationsvorgaben abgedeckt.

Typische allgemeine Vorgaben an den Betrieb betreffen zum Beispiel die regelmäßige Datensicherung und die sporadische Überprüfung der Wiederherstellbarkeit von Sicherungskopien, die kontinuierliche Überwachung der Logdaten und Fehlermeldungen mit Anpassung der Schwellenwerte für Alarmierungen, das Verfolgen aktueller Sicherheitswarnungen und das unverzügliche Einspielen sicherheitsrelevanter Updates und Patches nach vorherigem Test, die periodische Überprüfung und Erprobung der Notfallpläne sowie die Aktualisierung der Systemdokumentation nach jeder Konfigurationsänderung. Insbesondere bei der relativ jungen Software im Umfeld von IPv6 ist noch mit ständigen Updates und Verbesserungen zu rechnen, wenn im Laufe der Zeit die Betriebserfahrung zunimmt. Zu diesen Maßnahmen bieten die IT-Grundschutz-Kataloge des BSI [ITGSK] umfassende Informationen und genaue Vorgaben, auf die an dieser Stelle verwiesen sei.

Vorgaben für die Komponenten der Grundarchitektur

Für die Komponenten der Grundarchitektur sind folgende Vorgaben für den sicheren Betrieb von besonderer Bedeutung:

- Die tatsächlich verwendeten Konfigurationseinstellungen aller Komponenten müssen zentral gesichert und dokumentiert werden. Zur Änderungsverfolgung empfiehlt sich bei der Konfigurationsverwaltung der Einsatz eines Versionierungswerkzeugs sowie die genaue Protokollierung aller Wartungseingriffe.
- Es ist darauf zu achten, dass die im Betrieb verwendeten Konfigurationseinstellungen (Running Configuration) mit der in den Geräten gesicherten Konfiguration (Startup Configuration) für den Neustart übereinstimmt, um den automatischen Wiederanlauf in einem sicheren Betriebsmodus zu gewährleisten.
- Es ist zu prüfen, ob alle sicherheitsrelevanten Komponenten − insbesondere die Paketfilter und Sicherheits-Proxys − nach einem Systemfehler in einen sicheren Betriebsmodus wechseln (Fail Secure). So darf beispielsweise ein Paketfilter beim Auftreten von Fehlern seine Filterregeln nicht lockern, sondern höchstens verschärfen.

- Die sicherheitsrelevanten Konfigurationseinstellungen sind periodisch auf innere Konsistenz und auf Übereinstimmung mit den geltenden Sicherheitsleitlinien zu prüfen. Dies dient der kontinuierlichen Verbesserung sowie der Vermeidung von Fehlkonfigurationen und Altlasten (wie z. B. Filterregeln für Komponenten und Dienste, die inzwischen außer Betrieb gesetzt wurden).
- Bei einer schrittweisen Umstellung der Teilnetze von IPv4 auf IPv4+IPv6 und schließlich auf reines IPv6 sind die Konfigurationseinstellungen bei jedem Schritt auf innere Konsistenz und auf Übereinstimmung mit den geltenden Sicherheitsleitlinien zu prüfen.

Diese Empfehlungen gelten insbesondere für die Komponenten des Sicherheits-Gateways, das für das gesamte LAN eine wichtige Schutzfunktion übernimmt.

Darüber hinaus erfordert die Anbindung an das Internet eine genaue Abstimmung mit dem Internet-Diensteanbieter sowie den Registriervergabestellen, die für eine Zuteilung von IP-Adressen und Domain-Namen verantwortlich sind. Daher ist bei allen lokalen Konfigurationsänderungen darauf zu achten, dass diese Änderungen mit den extern getroffenen Absprachen verträglich sind.

7 Gefährdungen und Empfehlungen mit Varianten für normalen und hohen Schutzbedarf

Dieser Abschnitt analysiert die Gefährdungen, denen die Grundarchitektur ausgesetzt ist. Er stellt dar, wie die Architektur- und Konfigurationsvorgaben der Abschnitte 5 und 6 diese Sicherheitsgefahren bei normalem Schutzbedarf abwehren. Darüber hinaus werden Varianten der Grundarchitektur vorgeschlagen, die mit höherem Aufwand höheren Schutzbedarf abdecken oder die bei geringerem technischen Realisierungsaufwand ein höheres, in speziellen Szenarien jedoch noch akzeptables Restrisiko mit sich bringen.

Lösungen, die sich mit geringerem Hardware-Aufwand realisieren lassen, sind in der Beschaffung kostengünstiger. Mit der Vereinfachung steigen jedoch die Sicherheitsrisiken, zudem erhöht sich unter Umständen der Aufwand für die Konfiguration und den Betrieb der Komponenten. Der Anwender muss daher von Fall zu Fall entscheiden, ob die mit technischen Vereinfachungen einhergehenden Nachteile und Risiken auf Dauer nicht doch unwirtschaftlicher sind als die Grundarchitektur in der Grundkonfiguration. Maßnahmen zur Vereinfachung eignen sich nur für geringen oder normalen Schutzbedarf und müssen im Einzelfall genau abgewogen werden.

Die Abdeckung höherer Sicherheitsansprüche ist in der Regel mit größerem Aufwand und Mehrkosten verbunden, entweder aufgrund der Beschaffungskosten für zusätzliche Sicherheitskomponenten oder infolge eines erhöhten Aufwands für die Einrichtung und den Betrieb einer anspruchsvolleren Netzkonfiguration. Teilweise führen die Maßnahmen für erhöhte Sicherheit auch zu deutlichen Einschränkungen des Benutzungskomforts, in extremen Fällen wird die Verwendung bestimmter Anwendungen und Prozesse völlig ausgeschlossen.

Empfehlungen für Schutzmaßnahmen über die Grundarchitektur hinaus richten sich daher an Anwender mit überdurchschnittlichem Schutzbedarf und an Betreiber lokaler Netze, die ein besonders attraktives Angriffsziel bieten.

Es liegen bisher noch wenig Erfahrungen mit Angriffen auf Netze vor, die IPv6 einsetzen. In den nächsten Jahren, sobald IPv6 weit genug verbreitet ist, um ein lohnendes Angriffsziel abzugeben, ist mit vielen neuen und heute noch unerwarteten Angriffsszenarien zu rechnen. Die Liste der hier behandelten Angriffe ist daher nicht als vollständig anzusehen; wer IPv6 einsetzt, muss die aktuellen Entwicklungen unbedingt im Auge behalten und sich auf laufende Aktualisierungen einstellen. In jedem Falle muss man mit vielfachen Änderungen und Anpassungen rechnen und sollte die dazu notwendige Flexibilität beim Netzentwurf berücksichtigen.

7.1 Grundlegende Bedrohungen und empfohlene Gegenmaßnahmen

Unabhängig von spezifischen Schwachstellen einzelner Komponenten und Dienste der Grundarchitektur gibt es generelle Bedrohungen, die allgemein mit dem Betrieb von IT-Systemen einhergehen. Dieser erste Abschnitt erörtert, wie die Grundarchitektur und die empfohlenen Konfigurationsmaßnahmen dazu beitragen, solchen allgemeinen Bedrohungen zu begegnen. Darüber hinaus werden Empfehlungen für alternative oder ergänzende Maßnahmen ausgesprochen, um den technischen Realisierungsaufwand und die Schutzwirkung individuellen Bedürfnissen anzupassen. Die nachfolgenden Abschnitte 7.2 bis 7.5 sind dann konkreten Gefährdungen gewidmet, die durch spezifische Schwachstellen auf den verschiedenen Protokoll-Schichten des TCP/IP-Stacks verursacht werden.

7.1.1 Sniffing (Bedrohung der Vertraulichkeit)

Sniffing (schnüffeln) bezeichnet Techniken, um den Datenverkehr eines Computer-Netzes unautorisiert auszuspähen und sich unrechtmäßig Zugriff auf vertrauliche Informationen zu verschaffen. Sniffing bedroht die Vertraulichkeit der Informationsverarbeitung, gegebenenfalls auch Urheberrechte des Informationseigentümers. Indirekt kann Sniffing auch zur Informationsbeschaffung für weitergehende Angriffe dienen, etwa zum Ausspähen von Passwörtern.

Neben einer bestmöglichen physischen Abschottung der Netzkomponenten besteht die grundlegende Maßnahme gegen Sniffing-Angriffe in einer Verschlüsselung aller sicherheitsrelevanten Protokolle und Anwendungsdaten.

Folgende Aspekte der Grundarchitektur tragen zur Abwehr von Sniffing bei:

- die Segmentierung der LAN-Zone, um die Gelegenheit zum Sniffing einzuschränken,
- ein Out-of-Band-Management mittels separatem Management-Netz sowie
- eine modulare VPN-Erweiterungsmöglichkeit des Sicherheits-Gateways für verschlüsselte Kommunikation mit Außenstellen und externen Partnern.

Folgende Grundvorgaben in Abschnitt 6 tragen zur Abwehr von Sniffing bei:

- die Verwendung verschlüsselter Protokolle für das Netzmanagement (z. B. SSH, SNMPv3) sowie
- die Deaktivierung „geschwätziger“ Dienste, die unnötig viele Informationen über das System preisgeben.

Folgende Eigenschaften von IPv6 könnten zu Änderungen führen:

- IPv6-Implementierungen bringen i.d.R. IPsec mit sich und erleichtern so eine durchgehende Verschlüsselung des Datentransports (siehe auch Abschnitt 3.10.1).
- IPv6 erleichtert die Unterteilung des Client-Netzes in viele kleine Subnetze. Da zwischen diesen Subnetzen Daten nur per explizites Routing übertragen werden, können auch manipulatorische Eingriffe auf Layer 2 kein Abhören anderer Teilnetze mehr möglich machen.

Restrisiko: Mit den gängigen LAN-Technologien und -Protokollen allein ist ein vollständiger Schutz gegen Ausspähen in der Grundarchitektur vor allem in Bezug auf Innentäter kaum erzielbar. Unbedingte Vertraulichkeit kann nur mit einer Ende-zu-Ende-Verschlüsselung auf der Anwendungsschicht erzielt werden. Dazu müssen die spezifischen Anwendungen und Dienste eines Netzes in das Sicherheitskonzept mit einbezogen werden.

Über die grundlegenden Empfehlungen hinaus können Anwender die folgende zusätzliche Maßnahme ergreifen, wenn sie hohe Vertraulichkeitsanforderungen haben.

Variante 7.1.1 A für hohen Schutzbedarf: Verschlüsselung im internen Netz

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Vertraulichkeit
Phase im Ablaufplan: Konzeption

Zum Schutz vertraulicher Daten gegen Angriffe von Innentätern oder unterwanderten lokalen Rechnern können interne Kommunikationskanäle nach Bedarf verschlüsselt werden. Sind die Kommunikationsendpunkte im Voraus bekannt, so kann eine anwendungsunabhängige, lokale VPN-Verbindung eingerichtet werden (z. B. mittels IPSec-fähigen VPN-Geräten, z.B. eine SINA-VW). Bei komplexeren

Kommunikationsbeziehungen zwischen vielen potenziellen Kommunikationspartnern empfiehlt sich eher eine Software-basierte Lösung auf der Anwendungsschicht (z. B. mittels SSL).

Restrisiko: Durch diese Maßnahme wird der Gefährdung durch Innenangriffe auch bei hohem Schutzbedarf ausreichend begegnet. Eine verschlüsselte Kommunikation über mehrere Sicherheitszonen hinweg ist unter Umständen inkompatibel zur Filterfunktion der Sicherheits-Gateways, die eine sichere Trennung der Zonen gewährleisten sollen.

Umsetzungsaufwand: hoher Beschaffungs- und Realisierungsaufwand bei Verwendung von Hardware-basierten VPN-Lösungen; deutlich kostengünstiger bei IPsec-Software-Lösung zusammen mit IPv6; unter Umständen aufwendiges Schlüsselmanagement auch bei Software-Lösungen

Variante 7.1.1 B für hohen Schutzbedarf: Verschlüsselung mittels SINA-Box bei Anbindung von Außenstellen

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Vertraulichkeit
Phase im Ablaufplan: Konzeption

Um verschiedene Standorte mit schutzwürdigen Netzen in Bezug auf Vertraulichkeit und Integrität sicher über potenziell unsichere Netze zu verbinden, kann die Sicherheit der Grundarchitektur durch den Einsatz eines VPN auf Basis einer Verschlüsselungs-Hardware gesteigert werden. Speziell im Behördenumfeld empfiehlt sich dafür die SINA-Plattform [SINA]. Eine SINA-Box ist funktional vergleichbar mit einem herkömmlichen IPSec-basierten VPN-Gateway. Als Hochsicherheitslösung ausgelegt, sind die VPN-Funktionalitäten hierbei aber in ein speziell gehärtetes Linux-Betriebssystem eingebettet und um besondere sicherheitsrelevante Zusatzfunktionen ergänzt.

Zur Integration in die Grundarchitektur wird die SINA-Komponente anstelle der VPN-Box (vgl. Abbildung 5.10) im Sicherheits-Gateway platziert. Zum Datenaustausch benötigt die Gegenstelle eine entsprechende SINA-Ausstattung, da es sich um eine proprietäre VPN-Lösung handelt. Der Sicherheitsgewinn einer SINA-Lösung erfordert daher zusätzliche Hardware bei allen Kommunikationspartnern.

Restrisiko: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.

Umsetzungsaufwand: hoher Realisierungsaufwand, um alle VPN-Teilnehmer mit entsprechender Hardware auszustatten

7.1.2 Spoofing (Bedrohung der Authentizität)

Spoofing (englisch für manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

Die grundlegende Maßnahme gegen Spoofing-Angriffe besteht in der Verwendung integritätsgesicherter Protokolle und in der Authentisierung von Benutzern, Diensten und Hardware-Komponenten.

Die bei IPv6 neu hinzugekommenen Möglichkeiten des Spoofings von Angaben bei Autokonfiguration werden in Abschnitt 7.5.7 behandelt.

Folgende Grundvorgaben in Abschnitt 6 tragen zur Abwehr von Spoofing bei:

- Nutzung von Authentisierungs- und Integritätssicherungsoptionen für E-Mail und WWW (z. B. IMAP, HTTPS),
- Netzmanagement (z. B. NTP, SSH, SNMPv3, RADIUS),
- Routing (z. B. OSPF, BGP) sowie für die
- Redundanz-Steuerung (z. B. VRRP).

Restrisiko: Die Grundarchitektur sichert nur die grundlegenden Netzprotokolle und Basisdienste gegen Spoofing-Bedrohungen, nicht aber konkrete Anwendungen. Die Dienstlogik vieler Internet-Dienste ist für Spoofing-Angriffe auf Anwendungsschicht empfänglich, die auf den unteren Protokollschichten des TCP/IP-Stacks kaum zu bekämpfen sind. In vielen Fällen (z. B. bei der Zustellung von E-Mails aus dem Internet) kann die wahre Identität des Senders und die Integrität der Nachricht nur Ende-zu-Ende − etwa durch eine digitale Signatur des Inhalts − garantiert werden. Die Wahl einer geeigneten Schutzmaßnahme hängt von der Dienstlogik ab.

7.1.3 Hacking (Bedrohung durch Eindringen)

Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offen zu legen und es gegebenenfalls zu übernehmen. Hacking bedroht die Systemhoheit des LAN-Betreibers.

Neben einer bestmöglichen physischen Abschottung der Netzkomponenten besteht die grundlegende Maßnahme gegen Hacking in der physischen Segmentierung der Netze und dem systematischen Einsatz von Zugriffskontrolle.

Neuerungen durch IPv6 sind:

- die möglichst feingliedrige Aufteilung der einzelnen Client-Zonen, die durch den großen Adressraum von IPv6 ermöglicht wird und eine feingestufte Sicherheitsleitlinie auf Teilnetzen ermöglicht,
- der dünn besiedelte Adressraum von IPv6, der es Angreifern erschwert, potenzielle Ziele zu finden; den Adressraum einfach durch Probieren auf lohnende Ziele zu untersuchen („durch-zu-pingen“) ist mit praktikablem Aufwand nicht mehr möglich. Dennoch ist eine Suche nicht ausgeschlossen, da es diverse Möglichkeiten gibt, den Suchraum einzuschränken.

Folgende Aspekte der Grundarchitektur tragen zur Abwehr von Hacking bei:

- die Einschränkung der Datenflüsse in LAN und Management-Netz auf die benötigten Protokolle und Kommunikationspartner mittels Paketfiltern,
- die strikte Trennung von LAN und Internet durch ein dreistufiges Sicherheits-Gateway, das jeglichen Datenaustausch zwischen LAN und Internet bis hoch zur Anwendungsschicht kontrolliert, zugleich aber seine Angriffsfläche gegenüber Innen- und Außentätern durch eine PAP-Struktur minimiert,

- die physische Segmentierung der LAN-Zone, um die Zugriffsmöglichkeiten eines potenziellen Angreifers im LAN räumlich zu begrenzen und Sicherheitszonen mit unterschiedlichem Schutzbedarf voneinander zu trennen,
- ein Out-of-Band-Management mittels separatem Management-Netz, das dem Zugriff gewöhnlicher LAN-Teilnehmer entzogen und vom Internet aus nicht erreichbar ist sowie
- die funktionale Trennung aller Netz-Komponenten nach dem Prinzip „Nur ein Dienst pro Server".

Folgende Grundvorgaben in Abschnitt 6 tragen zur Abwehr von Hacking bei:

- die Verringerung der Angriffsfläche durch Minimalkonfiguration aller Komponenten und eine Beschränkung auf die ausdrücklich zulässige Funktionalität (Whitelist-Ansatz) sowie
- die Einrichtung maximaler Zugriffsbeschränkungen für Management-Schnittstellen.

Restrisiko: Ein wirksamer Schutz gegen Hacking erfordert immer auch eine physische Abschottung der IT-Infrastruktur. Während logische Filterung und Segmentierung guten Schutz gegen Hacking-Angriffe aus dem Internet bieten, sind Innentäter weit schwieriger zu stoppen: Mitarbeiter, die Zugang zu den LAN-Komponenten haben, können auf Dauer nur schwer daran gehindert werden, ein IT-System zu unterwandern. Da die autorisierten Benutzer zumindest einen angemessenen Zugang zu den Client-Segmenten erhalten müssen, können technische Sicherungsmaßnahmen für sich allein Innentäter kaum abwehren, sondern nur den erforderlichen Angriffsaufwand erhöhen und die Auswirkungen eines erfolgreichen Angriffs begrenzen. Einen höheren Schutz gegen Innentäter bieten erst ergänzende organisatorische Maßnahmen (z. B. sorgfältige Auswahl des Personals, 4-Augen-Prinzip).

Die nachfolgend dargestellten Varianten ermöglichen es dem Leser, die Schutzwirkung der Grundarchitektur und den erforderlichen Realisierungsaufwand seinem individuellen Bedarf anzupassen.

Variante 7.1.3 A für normalen Schutzbedarf: Zusammenlegen von Paketfiltern

Anwendungsbereich: Normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

Die Grundarchitektur (Abbildung 5.12) sieht gestaffelte Verteidigungslinien vor und meidet dabei die Doppelbelegung von Paketfiltern mit mehreren Schutzfunktionen. In kleinen, wenig exponierten IT-Netzen mit normalem Schutzbedarf lässt sich durch das Zusammenlegen von Filter-Komponenten Hardware einsparen. Die daraus resultierenden zusätzlichen Gefährdungspotenziale können in unkritischen Anwendungsszenarien oft akzeptiert werden.

Folgende „Rückverschmelzungen" von Paketfiltern kommen unter Einsparungsgesichtspunkten in Betracht (vgl. Abbildung 5.12):

Paketfilter 2 und 6 → PF2/6: Bei der Kopplung des Sicherheits-Gateway-Moduls mit dem LAN-Modul folgen die Paketfilter PF2 und PF6 unmittelbar aufeinander. Diese können zu PF2/6 verschmolzen werden (siehe Abbildung 7.1). Dadurch bleibt das PAP-Prinzip des Sicherheits-Gateways gewahrt. Nachteilig ist jedoch die größere

Angriffsfläche, die das Sicherheits-Gateway dadurch für Angriffe aus dem LAN-Inneren bietet.

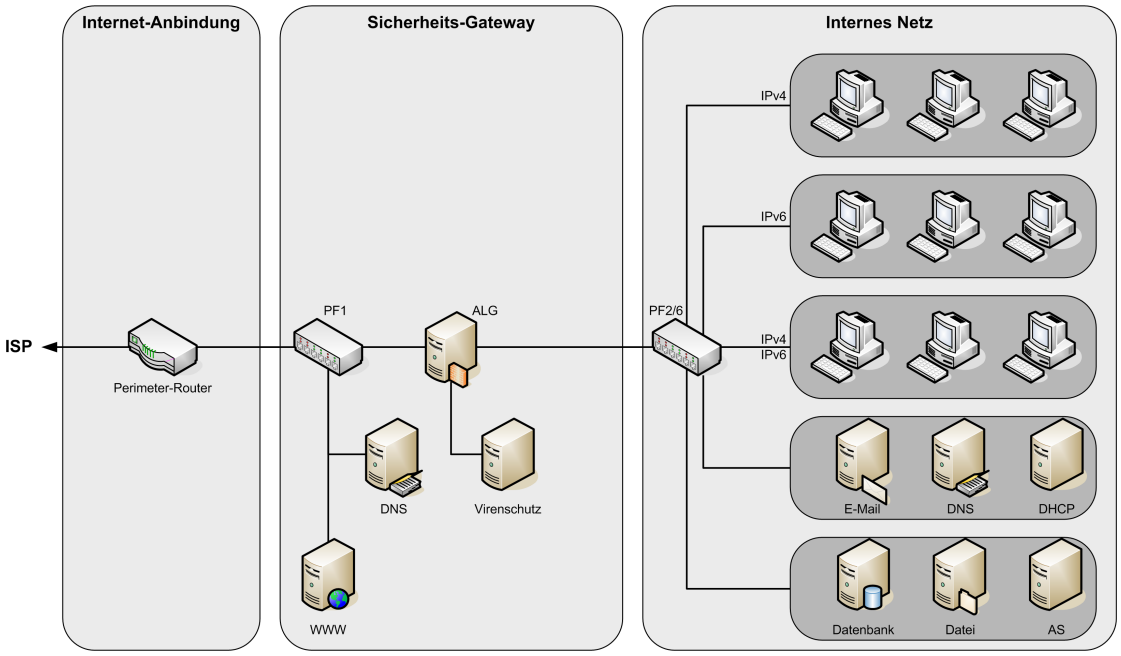

Abbildung 7.1: Zusammenlegung von Paketfiltern

Von einer noch weitergehenden Zusammenlegung (z. B. PF8 und PF9 zu PF8/9) ist abzuraten, weil sonst das Management-Netz in zu große Nähe zum Internet gerät. Grundsätzlich steht bei diesen Maßnahmen der Hardware-Vereinfachung ein erhöhtes Restrisiko entgegen. Daher ist eine Zusammenlegung von Paketfiltern von Fall zu Fall genau abzuwägen.

Neben der direkten Zusammenlegung von Paketfiltern kann auch der Paketfilter PF1 direkt im Perimeterrouter integriert werden. Dies ist aber nur dann möglich, wenn Paketfilter und Router von den gleichen Personen administriert werden und der Router nicht vom ISP gestellt und verwaltet wird.

Restrisiko: Das Zusammenlegen von Paketfiltern erfordert komplexere Filterregeln, insbesondere wenn sowohl IPv4- als auch IPv6-Verkehr gefiltert werden muss, was die Gefahr von Konfigurationsfehlern erhöht. Außerdem vergrößert sich durch eine Lockerung der Vorgabe „Nur eine Funktion pro Komponente“ die Angriffsfläche der Paketfilter, was vor allem Hacking oder Angriffe auf die Verfügbarkeit potenziell begünstigt. Insbesondere die Integration von PF1 in den Perimeterrouter verletzt diese Regel, so dass sie nur bei sehr kleinen Netzen in Betracht gezogen werden sollte. Wenn das Management-Netz zu wenig segmentiert ist, besteht eine erhöhte Gefahr, dass durch Fehlkonfigurationen eine Umgehung des Sicherheits-Gateways möglich wird.

Umsetzungsaufwand: geringerer Beschaffungsaufwand als für die Grundarchitektur; höherer Aufwand für Konfiguration und Betrieb aufgrund komplexerer Filterregeln

Variante 7.1.3 B für normalen Schutzbedarf: In-Band-Management für das interne Netz

Anwendungsbereich: Normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

> Durch die Verwendung von In-Band-Management im internen Netz kann bei allen Rechnern im internen Server-Segment die zweite Schnittstelle eingespart und somit die LAN-Verkabelung vereinfacht werden. Zusätzlich benötigt der Paketfilter PF10 weniger Schnittstellen zum Anschluss der internen Server. Der Management-Datenverkehr wird bei dieser Variante ab Paketfilter PF6 über das Produktivnetz zum Server-Segment geleitet.
>
> Da bei dieser Lösung Nutzdaten- und Management-Kanäle im LAN nur durch Zugriffslisten voneinander getrennt sind, sollten ausschließlich Management-Protokolle verwendet werden, die eine sichere Authentisierung und Verschlüsselung der übertragenen Daten ermöglichen.
>
> Durch die verfügbare Zahl von Adressen bei IPv6 kann man für alle Management-Aufgaben statt eigener Interfaces zumindest eigene IP-Adressen aus einem getrennten Netz, das für Management reserviert ist, verwenden. Diese Trennung macht die Erstellung der Zugriffslisten einfacher und ermöglicht so eine höhere Sicherheit gegenüber ungewollten Zugriffen von Clients auf die Managementanschlüsse der Server.

Restrisiko: Durch den In-Band-Management-Verkehr können im LAN-Bereich höhere Netzlasten auftreten. Zudem schwächt die physische Verbindung zwischen Management- und Produktivnetz den Schutz vor Angriffen durch Innentäter. Da die Management-Kommunikation im Produktivnetz abhör- und manipulationsgefährdet ist, erfordert In-Band-Management unbedingt integritätsgesicherte und verschlüsselte Management-Protokolle. Bei einem Ausfall des Produktivnetzes können die Server nicht mehr vom Management-Netz erreicht werden. Die Systemadministration muss dann lokal am jeweiligen Server erfolgen, was eine schnelle Reaktion in Krisensituationen erschwert.

Umsetzungsaufwand: geringerer Beschaffungs- und Realisierungsaufwand als in der Grundarchitektur

Variante 7.1.3 C für normalen Schutzbedarf: Einstufiges Sicherheits-Gateway

Anwendungsbereich: Normaler Schutzbedarf (kleine Netze)

Phase im Ablaufplan: Konzeption

> Bei kleinen, wenig exponierten Netzen mit normalem Schutzbedarf lässt sich das dreistufige PAP-Sicherheits-Gateway im Ausnahmefall durch ein einstufiges Sicherheits-Gateway ersetzen, um Hardware einzusparen. Dies schwächt die Schutzwirkung gegen Hacking jedoch erheblich, daher darf eine solche Maßnahme nicht leichtfertig ergriffen werden. Diese Variante ist für Behörden ungeeignet.
>
> Ein einfacher Paketfilter ist möglich, wenn sich die Internet-Kommunikation nur auf sehr grundlegende Protokolle beschränkt, die schon auf der Transportschicht ausreichend filterbar sind. Andernfalls empfiehlt sich für PF1 (vgl. Abbildung 7.2) der Einsatz eines Kombi-Geräts, das auch auf der Anwendungsschicht Proxy-Funktionen bietet. Falls auch ein Übergang zwischen IPv4 und IPv6 notwendig ist, muss dieser dann auch innerhalb des PF1 mit entsprechenden Proxys realisiert werden.

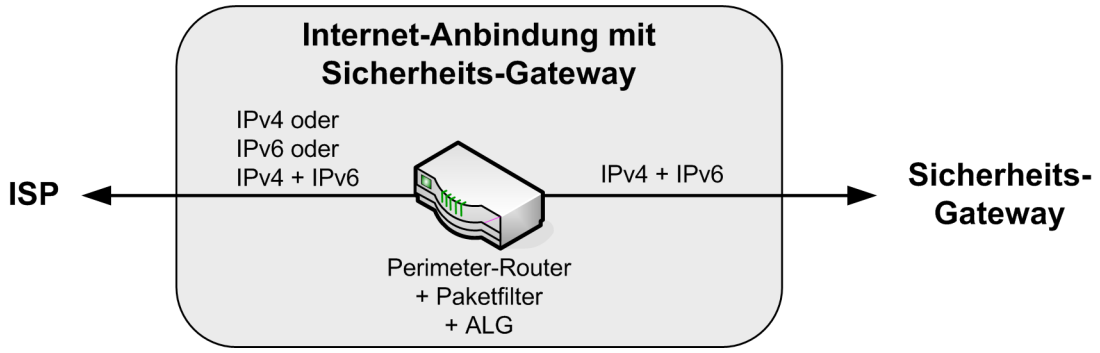

Abbildung 7.2: Einstufiges Sicherheits-Gateway

Restrisiko: Ein einstufiges Gateway setzt Hacking-Angriffen erheblich weniger Widerstand entgegen als eine PAP-Sicherheitsarchitektur. Des Weiteren steht durch den Wegfall des ALG und des Virenschutzes keine zentrale Prüfung des Verkehrs mehr zur Verfügung.

Umsetzungsaufwand: deutlich geringerer Realisierungs- und Betriebsaufwand als bei der Grundarchitektur

Variante 7.1.3 D für normalen Schutzbedarf: Zusammenlegung des Web- und DNS-Servers

Anwendungsbereich: Normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

In kleineren IT-Infrastrukturen ohne besonderen Schutzbedarf lassen sich Hardware-Einsparungen auch durch das Zusammenlegen von Servern in der DMZ realisieren.

Ein nur gering belasteter Web-Servers kann mit dem DNS-Server zusammengelegt werden (Abbildung 7.3). Dabei ist allerdings zu bedenken, dass Web-Servers zu den am meisten bedrohten Rechnern eines Netzes zählen. Somit steigt das Risiko, dass nach Übernahme des Web-Servers auch der DNS-Dienst für weitergehende Angriffe manipuliert wird.

Durch Vergabe von getrennten IPv6-Adressen für die unterschiedlichen Dienste am Server (WWW und DNS) lassen sich etwas bessere und einfachere Filter aufbauen.

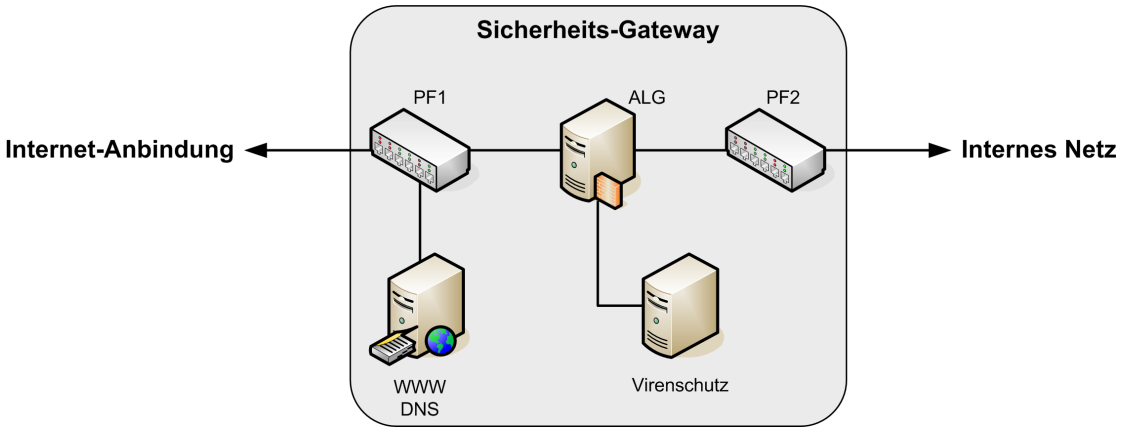

Abbildung 7.3: Zusammenlegung des Web- und des DNS-Servers

Restrisiko: Diese Empfehlung stellt eine Abkehr von der Maxime „Ein Dienst pro Server“ dar. Ein Zusammenlegen der Dienste vergrößert die Angriffsfläche des Servers, erleichtert das Unterwandern und erhöht die Last der Hardware-Plattform.

Umsetzungsaufwand: Geringerer Realisierungsaufwand als in der Grundarchitektur, höherer Betriebsaufwand wegen komplexerer Administration, da die Zusammenlegung der Dienste eventuell eine explizite Ressourcenzuteilung und zusätzliche Einstellungen verlangt, um gegenseitige Störungen auszuschließen.

Variante 7.1.3 E für normalen Schutzbedarf: Zusammenlegung des Virenschutz-Servers und des ALG

Anwendungsbereich: Normaler Schutzbedarf
Phase im Ablaufplan: Konzeption

Analog zur Variante 7.1.3 D lassen sich Hardware-Einsparungen auch dadurch erzielen, dass für das Virenschutzprogramm kein eigener Server eingesetzt wird, sondern dieses mit auf dem ALG installiert wird. Dabei ist allerdings zu bedenken, dass das ALG die dafür notwendigen Leistungsreserven bieten muss, damit es nicht zu Performance-Engpässen bei der Internet-Nutzung kommt. Zudem ist das Virenschutzprogramm eine besonders bedrohte Komponente des Sicherheits-Gateways, da es ja gerade potenziell gefährliche Inhalte analysieren muss. Dies erhöht das Risiko einer Kompromittierung des ALG.

Restrisiko: Diese Empfehlung stellt eine Abkehr von der Maxime „Ein Dienst pro Server“ dar. Ein Zusammenlegen der Dienste vergrößert die Angriffsfläche des Servers, erleichtert das Unterwandern und erhöht die Last der Hardware-Plattform.

Umsetzungsaufwand: Geringerer Realisierungsaufwand als in der Grundarchitektur; höherer Betriebsaufwand wegen komplexerer Administration, da die Zusammenlegung der Dienste eventuell eine explizite Ressourcenzuteilung und zusätzliche Einstellungen verlangt, um gegenseitige Störungen auszuschließen und höhere Auslastung des Servers durch ALG und Virenschutzprogramm.

Variante 7.1.3 F für hohen Schutzbedarf: Einsatz gestaffelter Komponenten verschiedener Hersteller

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Integrität oder der Vertraulichkeit
Phase im Ablaufplan: Konzeption

Grundsätzlich besteht immer die Gefahr, dass eine Sicherheitskomponente ihre Schutzwirkung aufgrund eines technischen Versagens verfehlt. Um sich dagegen ab-zusichern, können Anwender hintereinander liegende Koppelelemente, Paketfilter und ALGs verschiedener Hersteller mit unterschiedlichen Technologien (z. B. Betriebssystemen) einsetzen. Selbst wenn ein Angreifer eine Sicherheitsschwachstelle findet, mit der er eine Sicherheitskomponente eines Herstellers überwinden kann, ist es unwahrscheinlich, dass nachgeordnete Komponenten anderer Hersteller die gleiche Schwachstelle aufweisen: Sie müssen auf anderem Wege überwunden werden. Dies liefert mehrere, gestaffelte Verteidigungslinien zum Schutz der IT-Infrastruktur (Defense in Depth).

Anders verhält es sich bei parallel angeordneten Komponenten (z. B. zum Zwecke der Lastverteilung): Hier sollten immer Komponenten des gleichen Typs verwendet

werden, da sich sonst die Schwachstellen-Wahrscheinlichkeiten der einzelnen Systeme addieren, was die verfügbare Angriffsfläche für Eindringlinge vergrößert.

Die Wahl unterschiedlicher Hersteller empfiehlt sich bei entsprechendem Schutzbedarf vor allem für die drei Stufen des PAP-Sicherheits-Gateways. Der Nachteil heterogener Komponenten besteht vor allem in dem höheren Schulungsbedarf des Bedien- und Wartungspersonals sowie in der Gefahr von Inkompatibilitäten, deren Beseitigung zusätzlichen Konfigurationsaufwand verursachen kann.

Restrisiko: Das Staffeln heterogener Komponenten verringert die Gesamtwahrscheinlichkeit eines erfolgreichen Hacking-Angriffs, erhöht jedoch die Gefahr mangelnder Verfügbarkeit, da der Betrieb unterschiedlicher Gerätetypen fehleranfälliger ist als die Nutzung einer homogenen Systemausstattung.

Umsetzungsaufwand: Erhöhter Aufwand für die Schulung des Betriebspersonals und für die Wartung heterogener Gerätekonfigurationen

Variante 7.1.3 G für hohen Schutzbedarf: Untergliederung des Management-Netzes in physisch getrennte Sicherheitszonen

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts

Phase im Ablaufplan: Konzeption

Sollte es einem Angreifer gelingen, in das Management-Netz einzudringen, so besteht die Gefahr, dass er sämtliche Management-Schnittstellen unterwandert. Um die Auswirkungen einzelner Schwachstellen im Management-Netz zu begrenzen, kann dieses in getrennte Management-Zonen für LAN, Sicherheits-Gateway und

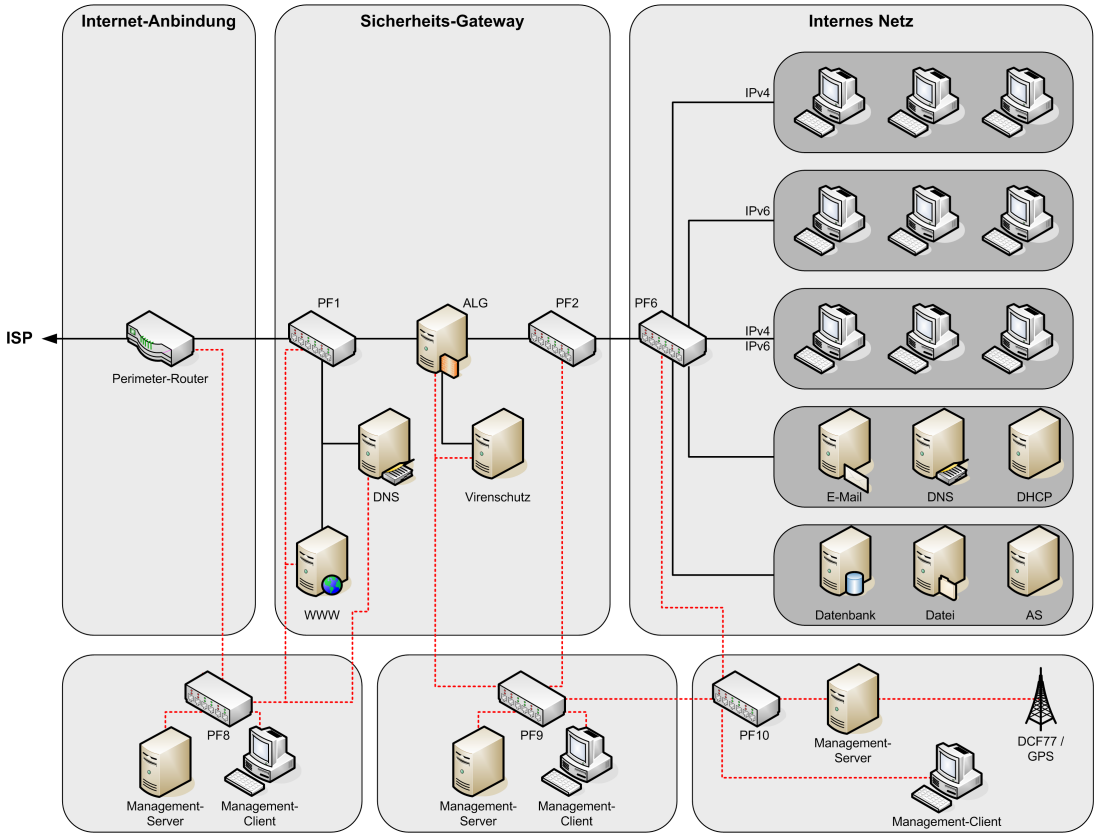

Abbildung 7.4: Grundarchitektur mit getrennten Management-Zellen

Internet-Anbindung zerlegt werden (Abbildung 7.4). Gegenüber der Grundarchitektur bietet dies einen verbesserten Schutz gegen Angriffe, die auf die Unterwanderung des Out-of-Band-Managements oder auf die Umgehung des Sicherheits-Gateways über das Management-Netz zielen.

Da bei Umsetzung der Maßnahme zwischen den einzelnen Management-Zonen in Abbildung 7.4 keine physische Kommunikationsverbindung mehr besteht, können die Zonen nur unabhängig voneinander angegriffen werden. Nachteilig ist hingegen der höhere Hardware-Aufwand dieser Lösung. Zudem erschwert die Trennung auch autorisiertem Personal, die erhobenen Management-Informationen (Log-, Monitoring- und IDS-Daten) zonenübergreifend zu korrelieren, um sich einen genaueren Überblick über den Zustand der IT-Infrastruktur zu verschaffen. Unter Umständen verzögert dies das Erkennen drohender Gefahren und das Initiieren koordinierter Abwehrmaßnahmen. Zudem führen fehlende Korrelationsmöglichkeiten beim Einsatz von IDS zu einer höheren Rate von Fehlalarmen. Daher sind die Vor- und Nachteile dieser Architekturvariante auch bei hohem Schutzbedarf genau abzuwägen.

Restrisiko: Die Maßnahme schützt wirkungsvoll gegen Hacking-Angriffe auf die Management-Zone. Sie erschwert aber das Erkennen drohender Gefahrensituationen und behindert eine unverzügliche, koordinierte Reaktion im Krisenfall.

Umsetzungsaufwand: Deutlich erhöhter Realisierungsaufwand aufgrund zusätzlicher Hardware-Komponenten gegenüber der Grundarchitektur, hoher Aufwand im Betrieb aufgrund des dezentralen Netzmanagements

Variante 7.1.3 H für normalen Schutzbedarf: Zusammenlegen der Client-Netze

Anwendungsbereich: Normaler Schutzbedarf
Phase im Ablaufplan: Konzeption

In der Grundarchitektur sind alle Clients in physisch getrennten, kleinen Subnetzen untergebracht. Ist man aus baulichen Gründen dazu gezwungen, mehrere Teilnetze auf der Leitungsebene zusammenzufassen, so kann man bei IPv6 die verwendeten Adressbereiche getrennt halten und damit ein Mindestmaß an Sicherheit gewährleisten. Gleichzeitig wird eine leichtere Administration sichergestellt.

Restrisiko: Durch die fehlende physische Trennung der Teilnetze ergibt sich ein erhöhtes Angriffspotential.

Umsetzungsaufwand: Durch Wegfall von Leitungen und Interfaces am Paketfilter PF6 ergeben sich Einsparungen.

Variante 7.1.3 I für hohen Schutzbedarf: Einsatz höherwertiger Paketfilter

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts
Phase im Ablaufplan: Konzeption

Der Schutz gegen Eindringlinge lässt sich gegenüber der Grundarchitektur auch durch den Austausch der vorgesehenen Paketfilter durch höherwertige (Kombi-)Geräte steigern. Einfache Paketfilter betrachten den Netzverkehr nur bis zur Transportschicht, daher entziehen sich die Anwendungsprotokolle ihrer Kontrolle.

Für eine tiefer gehende Filterung können Paketfilter grundsätzlich durch höherwertige Geräte ersetzt werden, wie etwa Appliances oder Sicherheits-Gateways, die den Datenverkehr − für ausgewählte Protokolle − auch auf der Anwendungsschicht analysieren. Dies bietet einen besseren Schutz gegen Hacking und Spoofing. Allerdings sind höherwertige Komponenten in der Regel teurer in der Anschaffung, bieten aufgrund ihrer höheren Komplexität eine potenziell größere Angriffsfläche als einfache Filter und sind außerdem meist aufwendiger zu administrieren.

Diese Maßnahme bezieht sich ausdrücklich nur auf den Austausch der Paketfilter. Sie dient nicht dazu, getrennte Geräte (z. B. die drei Stufen des PAP-Sicherheits-Gateways) zusammenzufassen.

Restrisiko: Höherwertige Paketfilter bieten mehr Angriffsfläche und bedrohen daher unter Umständen die Verfügbarkeit.

Umsetzungsaufwand: Erhöhter Realisierungsaufwand (Beschaffung, Konfiguration) gegenüber der Grundarchitektur aufgrund höherwertiger und komplexerer Geräteausstattung.

Variante 7.1.3 J für hohen Schutzbedarf: Segmentierung des internen Netzes mittels PAP-Sicherheits-Gateways

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts in den abgetrennten Netzsegmenten

Phase im Ablaufplan: Konzeption

Ein Angreifer, der erst einmal im Inneren des LANs Fuß gefasst hat, kann die innere Zone Schritt für Schritt weiter unterwandern. Dies fällt umso leichter, je enger die Vertrauensbeziehungen zwischen den LAN-Komponenten sind. Um die Schadensausbreitung bei solchen Angriffen zu begrenzen, empfiehlt sich eine Segmentierung im Inneren des LANs mittels PAP-Sicherheits-Gateways an Stelle einfacher Paketfilter (vgl. Abschnitt 5.1.2) − insbesondere im Hinblick auf mögliche Innentäter.

Gegenüber der Grundvorgabe bietet dies eine noch striktere physische Abschottung der verschiedenen Sicherheitszonen im LAN. Abbildung 7.5 zeigt das Prinzip am Beispiel eines Sicherheits-Gateways, das einen besonders schutzbedürftigen Verwaltungsserver von den sonstigen Server- und Client-Segmenten des LANs trennt.

Eine Fortentwicklung dieses Konzepts ist die weitere Unterteilung in mehrere Schutzzonen analog zur Aufteilung des Managementnetzes. Dieses Konzept kann bei IPv6 wieder mit einer Zuordnung eines oder mehrerer Subnetze zu jeder der Sicherheitszonen einhergehen.

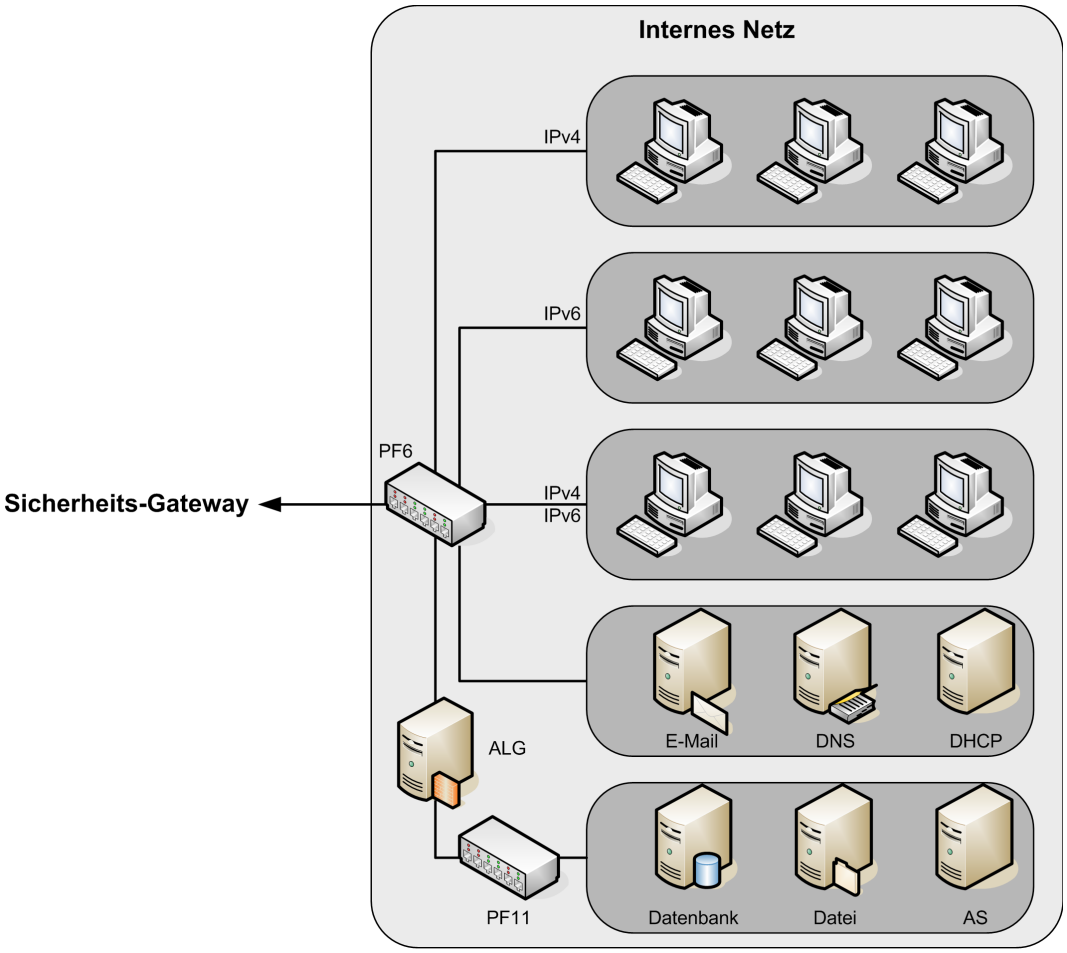

Abbildung 7.5: Schutz eines internen Netzsegmentes mittels PAP-Sicherheits-Gateway

Restrisiko: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.

Umsetzungsaufwand: Hoher Realisierungsaufwand aufgrund zusätzlicher Hardware-Komponenten; erhöhter Aufwand im Betrieb, um kontrollierte Kommunikationsbeziehungen im LAN über das PAP-Gateway hinweg zu ermöglichen.

Variante 7.1.3 K für hohen Schutzbedarf: Getrennte äußere Paketfilter für das Nutzen und Anbieten von Internet-Diensten

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts
Phase im Ablaufplan: Konzeption

In der Grundkonfiguration ist der äußere Paketfilter PF1 sowohl für ausgehenden als auch für eingehenden Internet-Verkehr zuständig. Die konfigurierten Filterregeln müssen daher beide Kommunikationsrichtungen berücksichtigen. Ein Konfigurationsfehler könnte das ALG der Gefährdung durch direkte Anfragen aus dem Internet aussetzen, die eigentlich nur die DMZ erreichen dürfen.

Um die Konfiguration des äußeren Paketfilters zu vereinfachen und das ALG vor fehlgeleiteten eingehenden Verbindungen bestmöglich zu schützen, kann der Paketfilter PF1 in der Grundarchitektur (vgl. Abbildung 5.1) durch zwei getrennte Paketfilter, PF1a und PF1b, ersetzt werden. In dieser Konfiguration fungiert PF1a als äußerer Paketfilter des PAP-Sicherheits-Gateways, während PF1b zum Anschluss

der DMZ sowie − an einem getrennten Interface des Filters − des äußeren DNS-Servers dient (s. Abbildung 7.6). Somit bedient PF1a ausschließlich Anfragen aus dem LAN, während PF1b für Anfragen aus dem Internet zuständig ist.

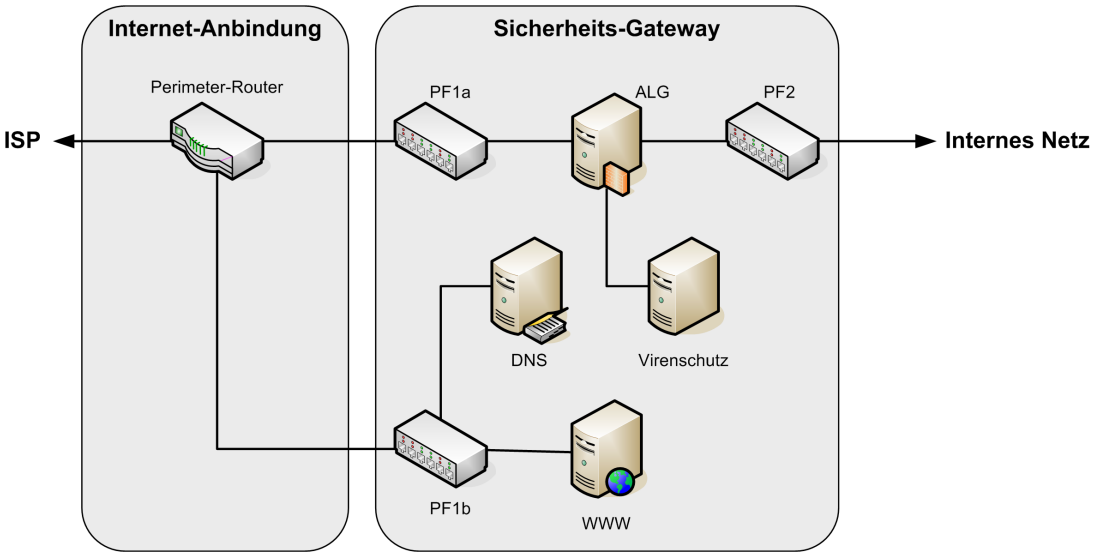

Abbildung 7.6: Getrennte Paketfilter für das Anbieten und Nutzen von Diensten im Internet

Restrisiko: Diese Maßnahme minimiert die Gefahr einer Fehlkonfiguration, Störung oder Unterwanderung des äußeren Paketfilters bei hohem Schutzbedarf.
Umsetzungsaufwand: Erhöhter Realisierungsaufwand für die Beschaffung eines zusätzlichen Paketfilters.

Variante 7.1.3 L für normalen Schutzbedarf: Verwendung von global gerouteten Adressen im internen Netz

Anwendungsbereich: Normaler Schutzbedarf
Phase im Ablaufplan: Konzeption

Wenn für einen Teil des inneren Netzes die direkte Ende-zu-Ende-Kommunikation im Vordergrund steht und der Schutz gegen Angreifer von außen weniger Bedeutung hat, können für die Clients in diesem Bereich direkt global eindeutige routbare IPv6-Adressen vergeben werden.

Der Verkehr zwischen diesen Netzen und dem Internet ist jedoch unbedingt über ein geeignetes Sicherheits-Gateway zu führen und dort entsprechend den geltenden Sicherheitsrichtlinien zu filtern.

Restrisiko: Durch diese Maßnahme wird die Gefährdung von außen dann erhöht, wenn die sonstigen Schutzmaßnahmen wie ALG und Paketfilter versagen. Da die Endgeräte in dieser Variante über im Internet routbare Adressen verfügen, könnten sie bei Fehlfunktion oder fehlerhafter Konfiguration der schützenden Einrichtungen direkt und unkontrolliert mit der Außenwelt kommunizieren.
Umsetzungsaufwand: Gering, Einsparungen sind durch Wegfall oder Verringerung der Applikation-Gateways möglich.

Variante 7.1.3 M für normalen Schutzbedarf: Verwendung von SLAAC in Verbindung mit Stateless DHCP in den internen Client-Netzen

Anwendungsbereich: Normaler Schutzbedarf

Phase im Ablaufplan: Konzeption

> Für Client-Netze, bei denen keine besonders enge Kontrolle darüber erforderlich ist, welche Geräte Zugang zu den betreffenden Netzen erhalten, kann die Adresskonfiguration per SLAAC und Stateless DHCP erfolgen.

Restrisiko: Durch diese Maßnahme wird die Gefährdung durch Angriffe auf dem lokalen Link erhöht, sofern nicht zusätzliche Maßnahmen auf der Netzzugangsschicht ergriffen werden, um zu verhindern, dass nicht autorisierte Geräte an das Netz angeschlossen werden.

Umsetzungsaufwand: Gering, Einsparungen sind durch einfachere Konfiguration und verringerte Anforderungen an die Leistungsfähigkeit der DHCP-Infrastruktur möglich. Allerdings muss vorher geprüft werden, wie die Clientsysteme mit DHCP und SLAAC umgehen (siehe hierzu auch [DHCP/SLAAC]).

Variante 7.1.3 N für normalen Schutzbedarf: IPv6-Proxy für Server

Anwendungsbereich: Normaler Schutzbedarf
Phase im Ablaufplan: Konzeption

> Wenn für einzelne Dienste, die nach außen hin über IPv6 angeboten werden sollen, nur Implementierungen mit IPv4 zur Verfügung stehen oder die betreffende Hardware

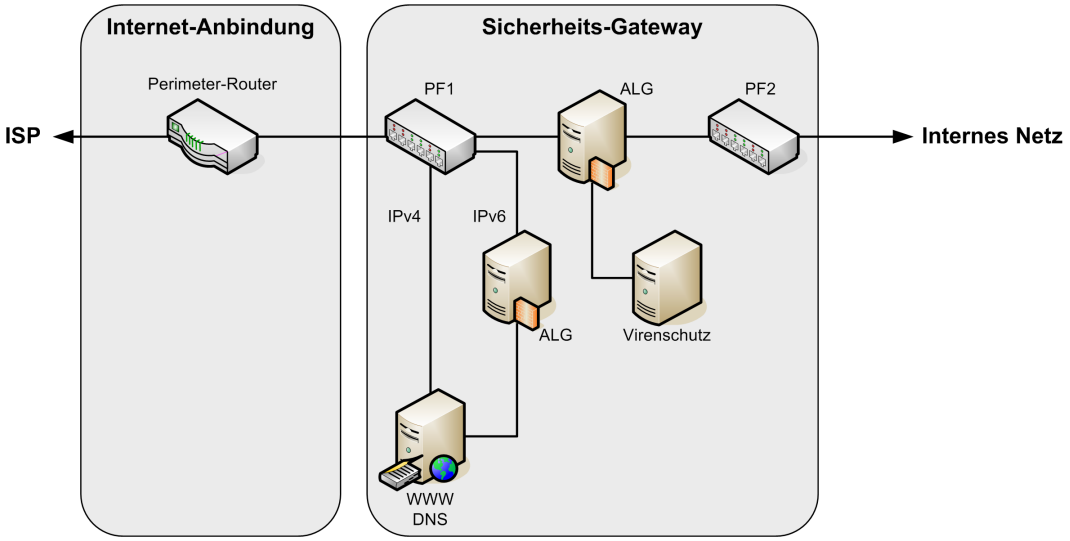

Abbildung 7.7: Web-Server mit vorgeschaltetem ALG inklusive IPv6-Proxy

> nur IPv4 unterstützt, so kann ein Proxy in der DMZ vor den Server geschaltet werden, um einen Zugriff vom Internet mit IPv6 zu ermöglichen.
>
> In diesem Fall muss der Proxy Verbindungen, die von außen kommen zulassen und unter Beachtung der geltenden Sicherheitsrichtlinien an den Server weiterleiten.

Restrisiko: Durch diese Maßnahme wird der Gefährdung von außen durch die zusätzlichen Komponenten geringfügig erhöht.

Umsetzungsaufwand: Zusätzlicher Proxy ist notwendig.

7.1.4 Denial of Service (Bedrohung der Verfügbarkeit)

Denial of Service (DoS) bezeichnet einen Zustand, in dem ein System den Dienst verweigert, also nicht mehr verfügbar ist. DoS-Angriff ist der Sammelbegriff für Angriffe, die darauf abzielen, die Verfügbarkeit von Systemen bewusst zu schädigen. Dies kann erreicht werden, indem Software- oder Hardware-Schwächen genutzt werden, um den Rechner zum Absturz zu bringen. Eine andere Angriffsvariante besteht darin, das System durch mutwillig erzeugte Rechen-, Speicher- oder Kommunikationslasten an die Grenzen seines Leistungsvermögens zu bringen, um es in die Knie zu zwingen. Um entsprechende Lasten zu generieren, basieren solche Angriffe meist auf einem ferngesteuerten, koordinierten Angriff auf den Zielrechner, ausgehend von einer sehr großen Zahl von Angriffsrechnern; man spricht in diesem Falle von verteilten DoS-Angriffen (Distributed DoS, DDoS).

Ein Schutz gegen DoS-Angriffe ist nur bedingt möglich. Die grundlegende Maßnahme gegen mutwillige Systemabstürze besteht darin, das System in einer Minimalkonfiguration mit möglichst geringer Angriffsfläche zu betreiben und die aktuellen Korrekturen (Patches) der Systemhersteller unverzüglich einzuspielen, um bekannt gewordene Schwachstellen zu eliminieren.

Ein kontinuierliches Überwachen der Systemlast kann Schutz gegen Überlastungsversuche bieten, da bei Bedarf (D)DoS-Ursprünge durch gezielte Filterung bereits an der Netzgrenze abgewiesen und so zumindest eine Beeinträchtigung interner Netzkomponenten verhindert werden kann. Im Übrigen hilft es nur, ausreichende Leistungsreserven − bis hin zu redundanten Ausweichsystemen − vorzuhalten, um den IT-Betrieb zumindest so lange aufrecht zu erhalten, bis eine Abwehrreaktion gegen den DoS-Angriff greift. Es sollte ein Notfallvorsorgekonzept erstellt werden, um die Vorgehensweise für den Ernstfall zu dokumentieren.

Die Grundarchitektur trägt in folgender Weise zur Abwehr von DoS bei:

- Die Entkopplung von LAN und Internet durch ein Sicherheits-Gateway hilft, Beeinträchtigungen auf externe Kommunikationsverbindungen zu begrenzen und zumindest die Verfügbarkeit des internen Netzes zu erhalten.

Folgende Grundvorgaben in Abschnitt 6 tragen zur Abwehr von DoS bei:

- Das Prinzip der Minimalkonfiguration aller Komponenten reduziert die Angriffsfläche des Systems.
- Das unverzügliche Einspielen von Updates und Patches minimiert die Angriffsfläche der Systemkomponenten.

Restrisiko: Die empfohlenen Maßnahmen können die DoS-Risiken nur mildern, aber nicht wirklich beseitigen. Vor allem eine sichere Abwehr von Überlast ist kaum möglich, sofern der Angreifer über genügend Ressourcen verfügt, die gesamte verfügbare Bandbreite aller vorhandenen Schnittstellen zu belegen. Leider bieten die vielen unsicheren Systeme im Internet einem entschlossenen Angreifer die Möglichkeit, durch gezielte DDoS-Attacken schon mit geringen eigenen Mitteln selbst leistungsfähige Netze mit Last zu überhäufen.

Variante 7.1.4 A für hohen Schutzbedarf: Mehrbeinige Anbindung an das Internet

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Verfügbarkeit der Anbindung an das Internet

Phase im Ablaufplan: Konzeption

Die Verfügbarkeit des Internet-Zugangs ist durch den Ausfall der Anschlussleitung zum Internet-Diensteanbieter gefährdet. Bei hohen Verfügbarkeitsansprüchen bezüglich der Internet-Kommunikation muss die Internet-Anbindung daher redundant, also mehrbeinig ausgeführt sein. Dies verringert nicht nur die Ausfallwahrscheinlichkeit der Anbindung, sondern kann auch genutzt werden, um im Normalbetrieb den Durchsatz der Anbindung durch Lastverteilung zu steigern. Dazu dient ein Lastverteiler (Load Balancer) als Koppelelement.

Lastverteiler verteilen eingehende Pakete nach vorgegebener Strategie auf mehrere Ausgänge. Im einfachsten Fall wird − soweit verfügbar − immer der gleiche Ausgang gewählt, nur bei Ausfall der Verbindung erfolgt die Umschaltung auf eine Ausweich-Schnittstelle. Die Last kann aber auch gleichmäßig auf gleichwertige Ausgänge verteilt werden.

Für eine mehrbeinige Internet-Anbindung wird ein Lastverteiler (oder mehrere, redundante Lastverteiler) im Internet-Segment platziert (Abbildung 7.8). Der Lastverteiler ist über mehrere unabhängige physische Anschlussleitungen mit dem Internet verbunden, bevorzugt mit verschiedenen Internet-Diensteanbietern, um die Abhängigkeit vom Netz eines einzelnen Providers zu verringern. Der LAN-Betreiber muss dabei sorgfältig auf die Trassenführung der Anschlussleitungen achten, um die Unabhängigkeit von Leitungsausfällen zu gewährleisten. Beispielsweise sollten die Anschlussleitungen das Gebäude an verschiedenen Stellen verlassen.

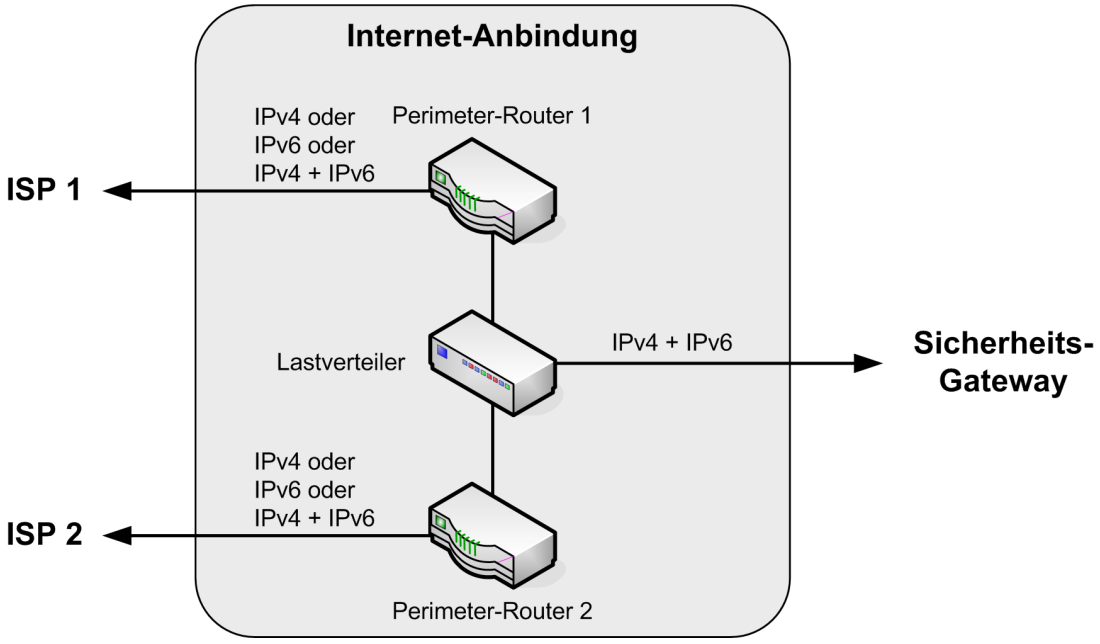

Abbildung 7.8: Redundante Anbindung an das Internet mittels Lastverteiler

Statt einer symmetrischen Anbindung über mehrere gleichwertige Kommunikationsverbindungen kann alternativ auch eine asymmetrische Anbindung gewählt werden, sofern dem nicht ein hoher Bandbreitenbedarf entgegensteht. Bei dieser Lösung umfasst der Anschluss eine Primäranbindung und eine zusätzliche Notfall-Anbindung mit nur geringer Bandbreite (z. B. ISDN S_0, DSL).

Restrisiko: Selbst die mehrbeinige Internet-Anbindung über unterschiedliche Trassen beseitigt das Restrisiko eines Verbindungsausfalls nur bedingt: Ein Ausfall des Lastverteilers unterbricht die Internet-Kommunikation. Um dies zu um-

gehen, ist zusätzlich eine hochverfügbare, also redundante Auslegung des Moduls „Internet-Anbindung“ erforderlich.

Umsetzungsaufwand: Erhöhter technischer, organisatorischer und finanzieller Aufwand für Konzeption, Realisierung und Betrieb der redundant ausgelegten Internet-Anbindung verglichen mit der Grundarchitektur.

Variante 7.1.4 B für hohen Schutzbedarf: Einsatz eines hochverfügbaren Sicherheits-Gateways

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Verfügbarkeit der Internet-Anbindung
Phase im Ablaufplan: Konzeption

Bei einem Ausfall oder einer Überlastung im Bereich des Sicherheits-Gateways droht der vollständige Verlust der Internet-Anbindung. Das Sicherheits-Gateway ist besonders externen Angriffen ausgesetzt. Es bildet in der Grundarchitektur eine mögliche Bruchstelle für die gesamte externe Kommunikation einer Organisation.

In einer Hochverfügbarkeitsvariante des Sicherheits-Gateways müssen die wichtigsten Elemente redundant ausgelegt werden. Dies sind vor allem diejenigen Komponenten, die zum Abruf oder zum Versand von Informationen unbedingt durchlaufen werden müssen. In diese Kategorie fallen in der Regel Paketfilter, ALG und gegebenenfalls VPN-Komponenten. Bei anderen Gateway-Elementen (z. B. dem Virenschutzprogramm oder einem Intrusion-Detection-System) muss die Bedeutung für die Sicherheit des zu schützenden Netzes im Einzelfall betrachtet werden; eventuell kann hier auf Redundanz verzichtet werden.

Es gibt verschiedene Möglichkeiten, die Verfügbarkeit von Komponenten eines Sicherheits-Gateways zu steigern. Bei einem *Cold-Standby-Ansatz* ist ein Ersatz für ausgefallene Komponenten zwar vorbereitet, aber nicht unmittelbar betriebsbereit. Gegebenenfalls ist es erforderlich, vor Inbetriebnahme des Ausweichsystems zunächst Komponenten zu tauschen, Konfigurationen zu aktualisieren oder neue Kommunikationsverbindungen einzurichten. Dadurch entsteht eine Versorgungslücke, während der kein Betrieb des Sicherheits-Gateways möglich ist. Bei dieser Lösung liegt der Vorteil vor allem im geringen Hardware-Aufwand, da nur besonders bedrohte Komponenten in Reserve vorzuhalten sind.

Bei der *Hot-Standby-Variante* sind alle notwendigen Ersatzschaltungen bereits vorbereitet und es ist dafür gesorgt, dass die Konfiguration des Standby-Systems (im Wesentlichen) der Konfiguration des Primärsystems entspricht, sodass der Ausweichbetrieb ohne größeren zeitlichen Verzug aufgenommen werden kann. Das stetige Synchronisieren der Systemkonfigurationen erfordert in der Regel den Einsatz von Redundanzprotokollen (z. B. VRRP).

Ein *Parallelbetrieb* ermöglicht eine verzugslose Übernahme von Systemlast, da Primär- und Ersatz-System lastteilig betrieben werden. Beide Systeme sind aktiv, und ihre Konfiguration ist jederzeit und ohne gesonderte Synchronisationsmaßnahme betriebsbereit. Ein weiterer Vorteil des Parallelbetriebs ist vor allem die wirtschaftliche Auslastung der redundanten Komponenten, die im Normalbetrieb sinnvolle Verwendung finden, um den Durchsatz des Sicherheits-Gateways zu steigern.

Als Maßnahme gegen DoS-Angriffe eignet sich Cold Standby wegen der langen Reaktionszeiten eher nicht. Auch Hot Standby und Parallelbetrieb bieten nur dann nennenswerten Schutz gegen DoS, wenn Primärsystem und Standby-System unabhängige Ressourcen nutzen, die physisch (z. B. bezüglich Rechnern, Koppelelementen, Verbindungspfaden) und logisch (z. B. bezüglich IP-Adressen, Portnummern) möglichst entkoppelt sind, da sonst beide Systeme dem gleichen Angriff ausgesetzt sind und der gleichen Schwachstelle zum Opfer fallen.

Restrisiko: Die Restrisiken hängen in hohem Maße von dem gewählten Lösungsansatz und vom konkreten Anwendungsszenario ab. Generell gilt, dass Redundanz die Gefahr von DoS-Angriffen mindert, aufgrund höherer Komplexität die Angriffsfläche für Hacking-Attacken jedoch vergrößert. Ein hochverfügbares Sicherheits-Gateway entfaltet nur dann seine volle Wirkung, wenn zugleich eine mehrbeinige Internet-Anbindung vorhanden ist.

Umsetzungsaufwand: Hoher technischer, organisatorischer und finanzieller Aufwand für Konzeption, Realisierung und Betrieb der redundant ausgelegten Gateway-Komponenten verglichen mit der Grundarchitektur (je nach gewähltem Ansatz und Anwendungsszenario stark variierender Mehraufwand).

Variante 7.1.4 C für hohen Schutzbedarf: Bandbreitenmanagement

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Verfügbarkeit kritischer Anwendungen und Dienste

Phase im Ablaufplan: Konzeption

Um zu verhindern, dass ein Angreifer die verfügbare Übertragungsbandbreite im Netz mit böswillig erzeugtem Datenverkehr belegt und damit anderen Protokollen die notwendigen Ressourcen entzieht, kann die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und Protokollen aufgeteilt werden. Man bezeichnet dies als Bandbreitenmanagement.

Bandbreitenmanagement-Systeme werden an Netzübergängen platziert. Sie analysieren die Datenströme und weisen ihnen die Bandbreite zu, die ihnen nach vorgegebenen Priorisierungsregeln jeweils zustehen. Die Klassifizierung der Datenströme kann anhand der IP-Quell- oder Zieladressen, des Transportprotokolls, der Quell- oder Ziel-Ports, des Type-of-Service-Felds (TOS) im IP-Header oder sogar anhand von Attributen der Anwendungsschicht-Protokolle erfolgen. Für jede Verkehrsklasse können statisch reservierte Mindest-Bandbreiten oder gegebenenfalls relative Vorrangstufen für den Netzzugriff zugewiesen werden. Dies ermöglicht es, für besonders kritische Dienste (z. B. Voice-over-IP, E-Mail) stets ein Minimum an Übertragungskapazität zu garantieren.

Um Bandbreitenmanagement in der Grundarchitektur einzuführen, können die Paketfilter an Netzübergängen und am Übergang zwischen verschiedenen Sicherheitszonen (z. B. PF1 und PF6 in Abbildung 5.1) gegen entsprechende Komponenten mit Bandbreitenmanagement-Funktion ausgetauscht werden.

Restrisiko: Im lokalen Verantwortungsbereich lässt sich ein durchgängiges Bandbreitenmanagement realisieren, bei der Nutzung öffentlicher Netze ist dazu im Allgemeinen jedoch die Kooperation des Internet-Diensteanbieters erforderlich (SLAs). Dienste, die während des Betriebs unterschiedliche, womöglich dynamisch vergebene Ports benutzen, erfordern eine aufwendige Datenstromanalyse auf der Anwendungsschicht; solche Analysen können ein

Bandbreitenmanagement-System überfordern oder seine Angriffsfläche vergrößern.

Umsetzungsaufwand: Je nach Ausmaß und Wirkungsbereich des Bandbreitenmanagements mittlerer bis hoher technischer, organisatorischer und finanzieller Aufwand für Konzeption, Realisierung und Betrieb des Bandbreitenmanagement-Systems.

Variante 7.1.4 D für hohen Schutzbedarf: Redundante Auslegung des internen Netzes

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Verfügbarkeit im LAN
Phase im Ablaufplan: Konzeption

Um Komponentenausfälle jederzeit zu kompensieren, können Koppelelemente, Paketfilter und Server im LAN redundant ausgelegt werden. Welche Komponenten Redundanz benötigen, hängt von den spezifischen Verfügbarkeitsansprüchen einzelner Dienste, Anwendungen und Kommunikationsverbindungen ab. Eine verbindliche Redundanzarchitektur kann daher hier nicht angegeben werden, sondern muss anwendungsspezifisch konzipiert werden.

Auch die Entscheidung, ob alle Teile oder nur die Netzanteile für IPv4 oder IPv6 redundant sein sollen, muss anwendungsspezifisch entschieden werden.

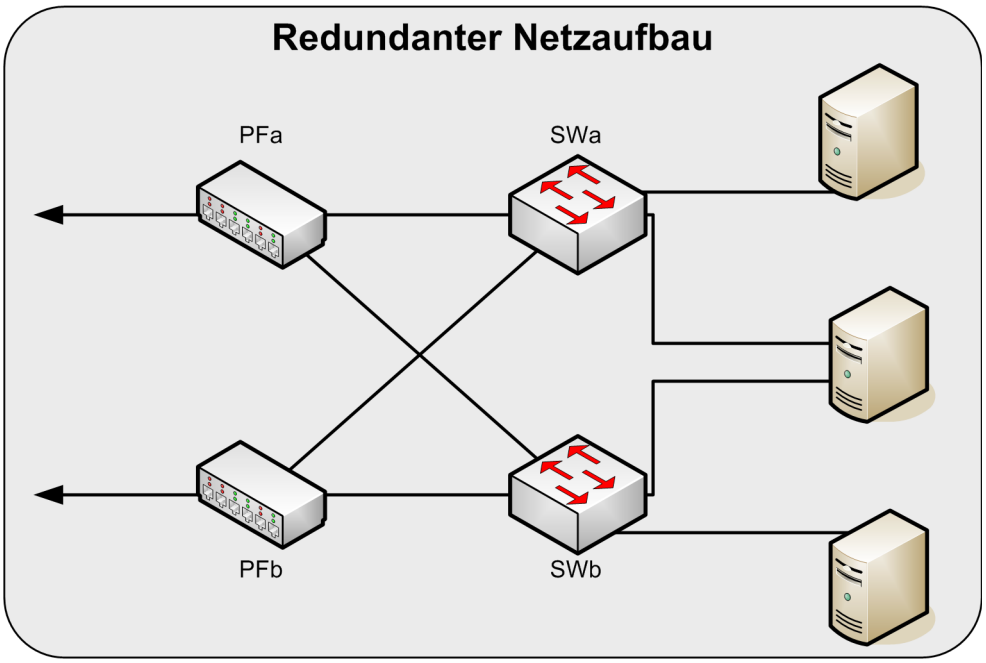

Abbildung 7.9: Redundante Auslegung des Netzes

Abbildung 7.9 zeigt die Kombination mehrerer Redundanzvarianten für das interne Netz, die das generelle Vorgehen illustrieren. Der mittlere Server ist in diesem Beispiel über zwei Netzwerkkarten an unterschiedliche Switches angeschlossen.

Die Paketfilter PFa und PFb demonstrieren eine Komponenten-Redundanz auf der Internet-Schicht. Zusammen realisieren die beiden Paketfilter ein gedoppeltes Standard-Gateway. Das aktuell zuständige Standard-Gateway wird zwischen PFa und PFb dynamisch mittels VRRP oder HSRP ausgehandelt.

Eine redundante Auslegung des internen Netzes erfordert erheblichen technischen Mehraufwand bezüglich Komponentenzahl und Vernetzung.

Restrisiko: Redundanz verbessert die Verfügbarkeit des Netzes, macht es aufgrund der komplexeren Netzkonfiguration jedoch anfälliger für Hacking-Angriffe.

Umsetzungsaufwand: Hoher technischer, organisatorischer und finanzieller Aufwand für Konzeption, Realisierung und Betrieb der redundant ausgelegten Komponenten verglichen mit der Grundarchitektur (je nach gewähltem Ansatz und Anwendungsszenario stark variierender Mehraufwand).

Variante 7.1.4 E für hohen Schutzbedarf: Einsatz redundanter Komponenten verschiedener Hersteller

Anwendungsbereich: Hoher Schutzbedarf bezüglich der Verfügbarkeit
Phase im Ablaufplan: Konzeption

Bei hohen Verfügbarkeitsansprüchen kann die Robustheit der IT-Infrastruktur durch den Einsatz von Komponenten verschiedener Hersteller verbessert werden. Da sich die Schwachstellen bei unterschiedlichen Fabrikaten eines Komponententyps unterschiedlich verteilen, lassen sich durch heterogene IT-Komponenten eher unabhängige Fehlerwahrscheinlichkeiten erzielen. In Kombination mit einer redundant ausgelegten Systemarchitektur steigt so die Wahrscheinlichkeit, dass zumindest eines der Replikate funktionstüchtig ist, auch wenn andere Replikate aufgrund einer herstellerspezifischen Schwachstelle ausgefallen sind.

Der Einsatz heterogener Komponenten als Maßnahme gegen DoS-Angriffe wirkt nur bei Parallelschaltung. Dadurch vergrößert sich jedoch die Angriffsfläche des Systems bezüglich Eindringversuchen (vgl. Abschnitt 7.1.3).

Als weiterer Nachteil steht dem prinzipiellen Vorteil unabhängiger Versagenswahrscheinlichkeiten ein erhöhter Administrations- und Schulungsaufwand für die Betreiberkräfte entgegen. Die Heterogenität der Komponenten und die damit verbundenen Inkompatibilitäten bedingen komplexere Konfigurationsvorgaben, die sich − bedingt durch Konfigurationsfehler − ihrerseits leicht als Sicherheitsschwachstelle erweisen können. Daher ist diese Maßnahme sorgfältig abzuwägen.

Restrisiko: Der Betrieb heterogener IT-Komponenten erhöht das Risiko von sicherheitskritischen Fehlkonfigurationen oder Bedienungsfehlern. Während der Parallelbetrieb unterschiedlicher Geräte das DoS-Risiko reduziert, vergrößert er zugleich die Angriffsfläche für Hacking-Attacken.

Umsetzungsaufwand: Erheblicher Mehraufwand bei Konzeption, Realisierung und Betrieb, da Maßnahme mit einer redundanten Netzauslegung kombiniert werden muss.

7.2 Gefährdungen auf der Netzzugangsschicht und empfohlene Gegenmaßnahmen

In diesem Abschnitt werden die maßgeblichen Gefährdungen auf der Netzzugangsschicht und geeignete Gegenmaßnahmen vorgestellt. Anders als im Abschnitt 7.1 handelt es sich im Folgenden um sehr konkrete Gefährdungen, die auf spezifische Schwachstellen der Netzzugangsschicht zielen. Entsprechend spezifisch sind die empfohlenen Gegenmaßnahmen.

7.2.1 ARP Spoofing / ARP Poisoning / Gratuitous ARP bei IPv4

Bedrohung: Vortäuschen einer falschen IP-Adresse
Schwachstelle: Fehlende Möglichkeiten, die Korrektheit von ARP-Informationen zu verifizieren

Die Zuordnung von IP-Adresse zur MAC-Adresse wird in einem sogenannten ARP Cache in jedem Endsystem gespeichert und kann durch falsche ARP-Informationen (ARP Spoofing) gezielt verändert werden (ARP Poisoning). Durch gezielt eingesetzte ARP-Mitteilungen (Gratuitous ARP) kann der Netzverkehr zum Angreifer umgeleitet werden. Das angegriffene Endsystem verwendet die MAC-Adresse des Angreifers fälschlicherweise als die des Routers, und der Router verwendet sie als die MAC-Adresse des Rechners. So kann ein Angreifer sämtlichen Verkehr mitlesen und gegebenenfalls verändern. Wird hingegen der Eintrag des Standard-Gateways im ARP Cache des Opfers mit einer nicht existierenden MAC-Adresse manipuliert, so führt dies zu einem Denial of Service. Sämtliche Kommunikationsbeziehungen innerhalb einer Broadcast-Domäne können mit dieser Art von Angriffen kompromittiert werden.

Gegenmaßnahme in der Grundkonfiguration:

- Switched Ethernet mit maximal einer MAC-Adresse pro Switch-Port für die Dauer der Port-Aktivierung oder zumindest für ein ausreichend bemessenes Zeitintervall konfigurieren (genaue Konfigurationsmöglichkeiten gerätespezifisch)

Restrisiko: Einzelne ARP-Einträge sind zwar trotz der empfohlenen Maßnahme angreifbar, allerdings kann von einem Port aus immer nur mit der aktuellen MAC-Adresse angegriffen werden. Die Switch-Konfiguration beschränkt somit die Rate, mit der ein Angreifer sein Angriffsziel wechseln kann.

Variante 7.2.1 A für hohen Schutzbedarf: Statisch konfigurierte ARP-Einträge bei IPv4

Anwendungsbereich: Optional für hohen Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts
Phase im Ablaufplan: Realisierung (Konfiguration)

Um das Einbringen falscher ARP-Informationen in die ARP-Tabellen sicher zu verhindern, kann auf eine dynamische Aktualisierung der ARP-Tabellen ganz verzichtet werden. Statt dessen werden die benötigten Informationen in der Konfiguration fest vorgegeben.

Der erforderliche Konfigurations- und Wartungsaufwand ist jedoch beträchtlich. Das Netz ist bei statischem ARP-Modus auch nicht mehr in der Lage, selbstständig auf Änderungen zu reagieren, die sich durch das Anschließen neuer Geräte oder den Austausch von IP-Adressen ergeben.

Restrisiko: Durch diese Maßnahme wird der Gefährdung ausreichend begegnet.
Umsetzungsaufwand: Hoher Konfigurationsaufwand; hoher Wartungsbedarf im Betrieb.

7.2.2 Missbrauch von Proxy ARP bei IPv4

Bedrohung: Unentdecktes ARP Spoofing
Schwachstelle: Legitimes Proxy ARP und ARP Spoofing sind schwer unterscheidbar

Mit Hilfe von Proxy ARP [RFC 1027] können Rechner über einen Koppel-Router hinweg direkt miteinander kommunizieren. Der Router ist dabei auf IP-Schicht transparent, braucht also nicht angesprochen zu werden, sondern dient mit seiner MAC-Adresse als Proxy für Rechner in anderen Teilnetzen. Der Koppel-Router antwortet dann stellvertretend auf ARP-Anfragen für diese Rechner. Somit ist anhand der ARP-Tabelle (mehrere Einträge mit gleicher MAC-Adresse) nicht erkennbar, ob es sich um einen Spoofing-Angriff handelt oder um legitimes Proxy-ARP-Verhalten.

Gegenmaßnahme in der Grundkonfiguration:

- Proxy ARP deaktivieren

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet. ARP Spoofing wird zwar nicht verhindert, ist jedoch ohne Proxy-ARP-Funktion leichter erkennbar.

7.2.3 MAC Spoofing

Bedrohung: Vortäuschen einer falschen Identität
Schwachstelle: Fehlende Möglichkeit, im Switch die Korrektheit verwendeter MAC-Adressen zu verifizieren

Sendet ein Angreifer Pakete unter der MAC-Adresse eines Opfersystems an einen Switch, so ordnet dieser den Port, an dem der Angreifer angeschlossen ist, der MAC-Adresse des Opfers zu und sendet in der Folge alle Ethernet-Pakete, die für das Opfer bestimmt sind, an den Angreifer. Der ursprüngliche Eintrag in der MAC-Tabelle ist überschrieben, und das angegriffene System erhält so lange keine Datenübermittlung vom Switch, bis es selbst ein Paket aussendet und der Switch den falschen Eintrag in der Tabelle wieder überschreibt. Sendet der Angreifer ständig Pakete mit gefälschter MAC-Adresse aus, so schneidet er sein Opfer von eintreffenden Datenpaketen ab. Sendet der Angreifer die umgeleiteten Daten nach dem Empfang zudem an das ursprüngliche Ziel weiter, so kann er unbemerkt in den Kommunikationskanal zwischen Sender und rechtmäßigem Empfänger eindringen (Man-in-the-Middle-Angriff).

Gegenmaßnahme in der Grundkonfiguration:

- Switched Ethernet mit maximal einer MAC-Adresse pro Switch-Port für die Dauer der Port-Aktivierung oder zumindest für ein ausreichend bemessenes Zeitintervall konfigurieren (genaue Konfigurationsmöglichkeiten gerätespezifisch)

Restrisiko: Der Angreifer kann den Port zwar nur mit einer MAC-Adresse verwenden. Durch Umkonfigurieren seiner Netzwerkkarte kann er allerdings unter einer fremden MAC-Adresse auftreten.

Variante 7.2.3 A für normalen Schutzbedarf: Statische MAC-Einträge für Switch-Ports konfigurieren

Anwendungsbereich: Normaler Schutzbedarf
Phase im Ablaufplan: Realisierung

Angreifer mit Zugriff auf die LAN-Verkabelung können leicht eigene Client-Rechner anschließen, um sie für weitere Angriffe zu nutzen. Die Schutzwirkung der Grundkonfiguration gegen Eindringlinge kann gesteigert werden, indem an jedem

Switch-Port die zulässigen MAC-Adressen vorkonfiguriert werden, die von dem Port bedient werden. Netzwerkkarten mit der falschen MAC-Adresse können die Port-Verbindung dann nicht nutzen (Whitelist-Ansatz). Eine manuelle Freischaltung ist allerdings sehr konfigurations- und wartungsaufwendig und kann somit bei größeren Installationen nicht eingesetzt werden.

Restrisiko: Die MAC-Adresse vieler Netzwerkkarten ist umkonfigurierbar und bietet daher wenig Schutz gegen Angreifer, die eine gültige MAC-Adresse für einen zugreifbaren Port kennen.

Umsetzungsaufwand: Mittel bis hoch bei Realisierung (Erstkonfiguration) und Betrieb (Pflege der Zuordnungen), je nach Anzahl der Switch Ports, Anzahl der zulässigen MAC-Adressen und Dynamik der Adresszuordnung zu den Ports.

Variante 7.2.3 B für normalen Schutzbedarf: Geräteauthentisierung am Switch anhand der MAC-Adressen

Anwendungsbereich: Normaler Schutzbedarf

Phase im Ablaufplan: Realisierung

Um Clients mit unzulässiger MAC-Adresse von den Switch-Ports im gesamten LAN fernzuhalten, können die MAC-Adressen aller autorisierten Rechner zentral registriert werden. Vor Aktivierung eines Ports fragt jeder Switch bei dem zentralen Registrierungs-Server an, ob die MAC-Adresse des angeschlossenen Endgeräts eine LAN-Autorisierung hat. Auf dem Server können neben den gültigen MAC-Adressen auch zusätzliche Attribute wie etwa die VLAN-Zuordnung hinterlegt werden.

Leider wird diese Technik nicht von allen Herstellern unterstützt. Das Verfahren erfordert keine zusätzliche Software auf den Netz-Clients und keine dezentralen Wartungseingriffe, ist also mit vergleichsweise moderatem Zusatzaufwand umsetzbar.

Restrisiko: Die Authentisierung kann mit manipulierten MAC-Adressen umgangen werden und bietet daher nur begrenzten Schutz vor Angreifern, die eine im LAN gültige MAC-Adresse kennen.

Umsetzungsaufwand: Mittlerer Konfigurationsaufwand.

Variante 7.2.3 C für hohen Schutzbedarf: Geräteauthentisierung am Switch gemäß IEEE 802.1x

Anwendungsbereich: Hoher Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts

Phase im Ablaufplan: Realisierung

Gegenüber einer einfachen MAC-Authentisierung von Endgeräten bietet Port Security auf der Basis des IEEE-Standards 802.1x einen verbesserten Schutz gegen den Anschluss von Fremdgeräten im LAN. Die Authentisierung der Client-Rechner erfolgt unter IEEE 802.1x per Benutzername und Kennwort oder mittels Zertifikat.

Dazu ist eine spezielle Software auf den Netz-Clients zu installieren, was mit höherem Aufwand für Konfiguration und Betrieb des Netzes verbunden ist. Allerdings ist das Verfahren wesentlich sicherer als eine MAC-Authentisierung.

Restrisiko: Gegenüber Angreifern von außen genügt die Maßnahme selbst hohem Schutzbedarf. Allerdings können Innentäter nach erfolgreicher Authentisierung nach wie vor fremde MAC-Adressen vortäuschen. Sie sind dabei jedoch eindeutig anhand ihrer Zugangskennung identifizierbar.

Umsetzungsaufwand: Erhöhter Konfigurationsaufwand für neue Client-Rechner; hoher Aufwand im Betrieb für die Schlüsselverwaltung.

7.2.4 MAC Flooding

Bedrohung: Vorsätzlich herbeigeführter Überlauf der MAC-Tabelle
Schwachstelle: Switch schaltet bei Überlauf der MAC-Tabelle in den Hub-Modus um

Beim MAC Flooding werden massenhaft Datenpakete versendet, die alle eine andere MAC-Quelladresse enthalten. Der Switch speichert nun jede einzelne MAC-Adresse, bis seine interne MAC-Tabelle überläuft. In diesem Fall schaltet der Switch in den sogenannten Fail-open Modus. In diesem Betriebsmodus werden nun alle Pakete, ob Unicast oder Broadcast, an alle angeschlossenen Netzteilnehmer gesendet (Funktionsprinzip eines Hubs). Dies bietet dem Angreifer die Möglichkeit, den Netzverkehr an seinem Port mitzulesen oder das Netz zu überlasten (DoS).

Gegenmaßnahme in der Grundkonfiguration:

- Switched Ethernet mit maximal einer MAC-Adresse pro Switch-Port für die Dauer der Port-Aktivierung oder zumindest für ein ausreichend bemessenes Zeitintervall konfigurieren (genaue Konfigurationsmöglichkeiten gerätespezifisch)

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet, da die für erfolgreiche Angriffe benötigten Flooding-Raten nicht mehr erzielbar sind.

7.2.5 STP-Angriffe

Bedrohung: Manipulation der logischen Verbindungstopologie auf der Netzzugangsschicht
Schwachstelle: Datenpakete des STP sind fälschbar, und das Umkonfigurieren des Spannbaums stört den Nutzdatenaustausch

Das Versenden falscher STP-Informationen (BPDUs) kann eine erneute Berechnung des Spannbaums in angegriffenen Switches provozieren und diese dadurch einige Sekunden von der aktiven Teilnahme an der Kommunikation ausschließen. Die Folge hiervon können Unterbrechungen der Kommunikationsverbindungen sein.

Ein weiterer STP-basierender Angriffstyp beruht auf der Anbindung eines Angreifers an zwei Switches. Ein Angreifer, der beispielsweise zwei Netzwerkkarten in seinem System im Bridge-Modus betreibt und am STP teilnimmt, kann erreichen, dass sämtlicher Verkehr über seinen Rechner läuft. Das ermöglicht ihm, den Datenverkehr mitzulesen oder zu manipulieren.

Gegenmaßnahme in der Grundkonfiguration:

- keine BPDU-Pakete an Zugriffs-Ports zulassen, sondern STP auf Trunk Ports beschränken

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.2.6 VLAN-Angriffe

Bedrohung: Eindringen in fremde VLANs

Schwachstelle: Offene Trunk Ports, fehlender Schutz gegen gefälschte oder manipulierte VLAN-Markierungen

Eine Kommunikation zwischen verschiedenen logischen Netzen eines VLANs ist regulär nur über Router, also auf der Internet-Schicht möglich. Werden logische Netze über mehrere Switches aufgebaut, so werden die Pakete zwischen den Switches über den sogenannten Trunk Port ausgetauscht. Auf Trunk-Verbindungen sind die Pakete dabei durch VLAN-Markierungen (sogenannte VLAN Tags) getrennten VLANs zugeordnet. Baut der Angreifer eine Trunk-Verbindung zu einem Switch auf, so kann er Zugriff auf alle logischen Netze erhalten.

Ein weiterer Angriffspunkt ist das sogenannte VLAN Hopping, bei dem der Angreifer ein Paket gleich zweifach markiert und dadurch Ethernet-Pakete von einem Switch zu einem anderen Switch in ein anderes VLAN leiten kann. Die erste Markierung entspricht dem Native VLAN und die zweite Markierung dem des anzugreifenden VLANs. Der Switch entfernt beim Empfang die erste Markierung und leitet das Paket über einen Trunk Port zum nächsten Switch. Die zweite Markierung wird dort entfernt und das Ethernet-Paket an das vom Angreifer bestimmte VLAN weitergeleitet. Somit ergibt sich die Gefahr des Einspeisens von Paketen in fremde VLANs.

Gegenmaßnahme in der Grundarchitektur:

- VLANs nicht zur Trennung verschiedener Sicherheitszonen verwenden (stattdessen physische Trennung mittels Sicherheits-Gateway)

Gegenmaßnahme in der Grundkonfiguration:

- kein Trunking an Zugriffs-Ports zulassen

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.2.7 ND-Spoofing (Man in the middle)

Bei IPv6 wird ARP durch Neighbor Discovery ersetzt.

Prinzipiell lassen sich auch bei ND ähnliche Szenarien des Spoofings vorstellen wie bei IPv4.

Bedrohung: Vortäuschen einer falschen IP-Adresse
Schwachstelle: Fehlende Möglichkeiten, die Korrektheit von ND-Informationen zu verifizieren

Die Zuordnung von IPv6-Adresse zu MAC-Adresse wird in einem sogenannten ND-Cache in jedem Endsystem gespeichert und kann durch falsche ND-Informationen (ND Spoofing) gezielt verändert werden (ND Poisoning). Durch gezielt eingesetzte ND-Mitteilungen (ND-Antworten) kann der Netzverkehr zum Angreifer umgeleitet werden. Das angegriffene Endsystem verwendet die MAC-Adresse des Angreifers fälschlicherweise anstatt der des Routers, und der Router verwendet sie anstatt der MAC-Adresse des Rechners. So kann ein Angreifer sämtlichen Verkehr mitlesen und gegebenenfalls verändern.

Gegenmaßnahme in der Grundkonfiguration:

- viele kleine Subnetze
- Verwendung von DHCP

- Switched Ethernet mit maximal einer MAC-Adresse pro Switch-Port für die Dauer der Port-Aktivierung oder zumindest für ein ausreichend bemessenes Zeitintervall konfigurieren (genaue Konfigurationsmöglichkeiten gerätespezifisch)

Restrisiko: Einzelne ND-Einträge sind zwar trotz der empfohlenen Maßnahme angreifbar, allerdings kann von einem Port aus immer nur mit der aktuellen MAC-Adresse angegriffen werden. Ein Angriff ist bei IPv6 auf einen physischen Link beschränkt. Die Switch-Konfiguration beschränkt somit die Rate, mit der ein Angreifer sein Angriffsziel wechseln kann.

Variante 7.2.7 A für hohen Schutzbedarf: Statisch konfigurierte ND-Einträge bei IPv6

Anwendungsbereich: Optional für hohen Schutzbedarf bezüglich mindestens eines Sicherheits-Grundwerts
Phase im Ablaufplan: Realisierung (Konfiguration)

Um das Einbringen falscher ND-Informationen in die ND-Tabellen sicher zu verhindern, kann auf eine dynamische Aktualisierung des ND-Caches ganz verzichtet werden. Stattdessen werden die benötigten Informationen in der Konfiguration fest vorgegeben. Der erforderliche Konfigurations- und Wartungsaufwand ist jedoch beträchtlich.

Man sollte sehr genau abwägen, ob sich der hohe Aufwand und die verlorene Flexibilität durch das bei IPv6 deutlich verringerte Angriffsrisiko rechtfertigen lassen.

Das Netz ist bei statischem ND-Modus auch nicht mehr in der Lage, selbstständig auf Änderungen zu reagieren, die sich durch das Anschließen neuer Geräte oder den Austausch von IP-Adressen ergeben.

Restrisiko: Durch diese Maßnahme wird der Gefährdung ausreichend begegnet.
Umsetzungsaufwand: Hoher Konfigurationsaufwand; hoher Wartungsbedarf im Betrieb

Variante 7.2.7 B für hohen Schutzbedarf: SEcure Neighbor Discovery (SEND)

Anwendungsbereich: Hoher Schutzbedarf bezüglich Verfügbarkeit
Phase im Ablaufplan: Realisierung

Die SEcure Neighbor Diescovery (SEND) nach [RFC 3971] ist eine Erweiterung mit der sich die inhärent unsichere Neighbor Discovery absichern lässt. Mittels kryptografisch generierter Adressen (CGA) wird eine IPv6-Adresse an ein asymmetrisches Schlüsselpaar gebunden. Mit SEND lassen sich Angriffe über ND- und RA-Nachrichten erkennen und mitigieren.

Restrisiko: Durch diese Maßnahme wird der Gefährdung ausreichend begegnet.
Umsetzungsaufwand: Sehr hoch, da eine Zertifikatsinfrastruktur vorausgesetzt wird und zudem noch nicht für alle Betriebssysteme Implementierungen verfügbar sind.

7.2.8 ND-Spoofing (Denial of Service)

Bedrohung: Speicherüberlauf des Neighbor-Caches, Verweigerung des Netzzugangs
Schwachstelle: Fehlende Möglichkeiten, die Korrektheit von ND-Informationen zu verifizieren

Die Zuordnung von IPv6-Adresse zu MAC-Adresse wird in einem sogenannten ND-Cache in jedem Endsystem gespeichert. Der ND-Cache kann durch das Flooding mit falschen

ND-Informationen zum Überlauf gebracht werden. Relevante Zuordnungen können verloren gehen. Im Extremfall kann es durch den Überlauf zu einem Systemabsturz kommen.

Wird der Eintrag des Standard-Gateways im ND Cache des Opfers mit einer nicht existierenden MAC-Adresse manipuliert, so führt dies zu einem Denial of Service. Sämtliche Kommunikationsbeziehungen in einem Subnetz können mit dieser Art von Angriffen kompromittiert werden.

Durch die Ausnutzung der Duplicate Address Detection ist ein weiterer Denial of Service Angriff möglich. Nodes, die sich selbst eine Adresse generieren, fragen zuerst im Netz nach, ob diese Adresse noch frei ist. Wenn ein Angreifer auf alle Anfragen dieser Art mit „nein“ antwortet, wird dem Opfersystem der Zugang zum Netz verweigert.

Gegenmaßnahme in der Grundkonfiguration:

- viele kleine Subnetze
- Verwendung von DHCP
- Switched Ethernet mit maximal einer MAC-Adresse pro Switch-Port für die Dauer der Port-Aktivierung oder zumindest für ein ausreichend bemessenes Zeitintervall konfigurieren (genaue Konfigurationsmöglichkeiten gerätespezifisch)

Restrisiko: Einzelne ND-Einträge sind zwar trotz der empfohlenen Maßnahme angreifbar, allerdings kann von einem Port aus immer nur mit der aktuellen MAC-Adresse angegriffen werden. Ein Angriff ist bei IPv6 auf einen physischen Link beschränkt. Die Switch-Konfiguration beschränkt somit die Rate, mit der ein Angreifer sein Angriffsziel wechseln kann.

7.3 Gefährdungen auf der Internet-Schicht und empfohlene Gegenmaßnahmen

Im Folgenden werden die maßgeblichen Gefährdungen auf der Internet-Schicht sowie geeignete Gegenmaßnahmen vorgestellt.

7.3.1 IP Source Routing bei IPv4

Bedrohung: Umlenken von IP-Verkehr
Schwachstelle: Verfügbare IP-Mechanismen zum Festlegen der Wegewahl

Beim IP Source Routing legt der sendende Rechner − also potenziell ein Angreifer − die Route eines IP-Pakets über das Internet fest. Der Zielrechner benutzt für die Antwortpakete dieselbe Route. Ein Angreifer kann damit Anfragen eines autorisierten Clients vortäuschen und die vertraulichen Antworten des Servers auf einen beliebigen Rechner umleiten, um sie dort auszulesen oder zu manipulieren.

IP Source Routing wurde bei IPv6 im Zuge einer Überarbeitung aus den Standards entfernt. Es sollte daher bei aktuellen Implementierungen nicht mehr unterstützt werden und ist damit auch nicht mehr zu Angriffen nutzbar. Der ehemals dafür reservierte Header kann aber zu-

sätzlich im Filter blockiert werden. Zusätzlich kann der zu Mobile IPv6 gehörende Routing Header vom Typ 2 mit vergleichbarer Funktion blockiert werden.

Gegenmaßnahme in der Grundkonfiguration:

- IP Source Routing deaktivieren

Restrisiko: Diese Maßnahme beseitigt die Gefährdung.

7.3.2 Land Attack

Bedrohung: Denial of Service durch Absturz älterer TCP/IP-Implementierungen
Schwachstelle: Unzureichende Konsistenzprüfungen bei der Verarbeitung der IP- bzw. TCP-Datenpakete

Bei einem Land Attack werden falsch formatierte IP-Pakete (Quell- und Zieladresse sind gleich) an das Opfersystem versendet. Dies führt bei einigen TCP/IP-Implementierungen zum Absturz des gesamten Systems. Bei einer erweiterten Variante gegen Windows-Rechner werden TCP-Pakete zusätzlich noch mit gleichem Quell- und Zielport (z. B. Port 139/TCP) versendet. Dies führt genauso wie bei der Standardvariante unter Umständen zu einem Systemausfall.

Derartige Angriffsvektoren sind bei IPv6-Implementierungen bisher nicht bekannt und sollten auch bei heutigen neueren Implementierungen von IP allgemein nicht mehr vorkommen.

Gegenmaßnahme in der Grundkonfiguration und beim Betrieb:

- aktuelle Updates einspielen

Restrisiko: Dieser Angriff ist seit Langem bekannt. Moderne TCP/IP-Implementierungen enthalten entsprechende Abwehrmaßnahmen. Durch den Einsatz aktueller Protokoll-Implementierungen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.3.3 Ping of Death

Bedrohung: Ausfall des Rechners
Schwachstelle: Unzureichende Prüfung der Längenbeschränkung bei fragmentierten ICMP-Paketen

Der Angreifer sendet ein ICMP-Paket mit mindestens 65.510 Byte Nutzdaten. Dieses wird in kleinere Pakete fragmentiert, zum Opfersystem übermittelt und dort wieder zusammengesetzt. Nutzdaten zuzüglich Paket-Header ergeben dann nach dem Zusammenfügen ein Paket, das größer ist als die maximal zulässige Größe von 65.536 Byte. Bei einigen Betriebssystemen führt dies zu einem Pufferüberlauf, der einen Systemabsturz zur Folge haben kann.

Diese Art des Angriffs, der durch eine unzureichende Längenprüfung bei der Rekombination von Fragmenten möglich wird, sollte bei neueren IP-Implementierungen nicht mehr auftreten. Dennoch gab es 2013 eine Neuauflage des Ping-of-Death – diesmal jedoch nicht für IPv4, sondern im IPv6-Stack. Dementsprechend kann leider nicht davon ausgegangen werden, dass altbekannte Fehler in neuen Versionen nicht mehr auftauchen.

Gegenmaßnahme in der Grundkonfiguration:

- In Paketfiltern die Übertragung von ICMP-Nachrichten zwischen Nutzdaten-Schnittstellen möglichst sperren, insbesondere an Netzübergängen zwischen verschiedenen Sicherheitszonen (z. B. im äußeren Paketfilter PF1)

Restrisiko: Diese Maßnahme beseitigt die Gefährdung für normalen und hohen Schutzbedarf.

7.3.4 IRDP Angriffe bei IPv4

Bedrohung: Umlenken von IP-Verkehr
Schwachstelle: Fehlende Authentisierungsmöglichkeit für IRDP-Pakete

Das ICMP Router Discovery Protokoll (IRDP) wird von Routern verwendet, um angeschlossene Systeme dynamisch über das aktuelle Standard-Gateway zu informieren. Dies geschieht mit einer ICMP-Nachricht (Typ 9, Router Advertisement) an die Broadcast-Adresse des Netzes oder als Multicast an die IP-Adresse 224.0.0.1. Unter Sicherheitsaspekten ist das Protokoll jedoch sehr anfällig, da keine Authentisierung verwendet wird. Potenzielle Angreifer können durch das Senden von gefälschten Advertisement-Nachrichten Verbindungen zum Standard-Gateway umleiten und so einen Man-in-the-Middle- oder Denial-of-Service-Angriff durchführen.

IRDP wird bei IPv6 nicht benutzt und bietet somit keinen Angriffsweg. Die bei IPv6 eingesetzten Router-Advertisements und die damit möglichen Angriffe werden in Abschnitt 7.3.14 behandelt.

Gegenmaßnahme in der Grundkonfiguration:

- IRDP deaktivieren

Restrisiko: Diese Maßnahme beseitigt die Gefährdung.

7.3.5 IP Spoofing

Bedrohung: Vortäuschen einer falschen Identität
Schwachstelle: Fehlende Authentisierung der Quelladresse von IP-Paketen

Wird eine IP-Adresse mit dem Ziel verwendet, einen anderen Ursprung vorzutäuschen, so spricht man von IP Spoofing. Je nach Angriff kann diese Adresse aus unterschiedlichen Adressbereichen stammen. Zum Überwinden von Paketfiltern wird beispielsweise die Adresse eines vertrauenswürdigen Systems genutzt. Für Denial-of-Service-Angriffe werden mitunter auch nicht vergebene oder im Internet nicht geroutete Adressen verwendet.

Gegenmaßnahmen in der Grundkonfiguration:

- Einrichten von Anti-Spoofing-Filtern mittels Zugriffslisten (siehe Tabellen 11 und 12 in Abschnitt 6.2.4)
- Systematische Zuordnung von IP-Adressräumen zu den verschiedenen Netzsegmenten
- Bei IPv6: Aufteilung des Netzes auf viele Subnetze

Restrisiko: Durch diese Maßnahmen können nur unplausible Spoofing-Versuche entlarvt werden, nicht jedoch vorgetäuschte, prinzipiell aber mögliche IP-Adressen.

Je systematischer in einem Netz die IP-Adressen vergeben werden und je feiner das Netz partitioniert ist, desto besser gelingt es, gefälschte IP-Adressen aufgrund mangelnder Plausibilität zu entlarven – dies ist durch den großen Adressraum bei IPv6 deutlich besser möglich.

7.3.6 Fragmentierungsangriffe

Bedrohung: Eindringen durch Umgehen der Paketfilterung
Schwachstelle: Paketfilterung auf der Basis von unzusammenhängenden Paket-Fragmenten

Fragmentierungsangriffe zielen darauf ab, unzulässige Pakete durch Fragmentierung unkenntlich zu machen. Geschickt gestückelte Datenpakete können von den Filterregeln eines Paketfilters nicht erfasst werden und können daher − Fragment für Fragment − den Filter passieren.

Beim Tiny Fragment Attack [RFC 1858] zerlegt der Angreifer seine Nutzdaten in sehr kleine Fragmente. Dabei wird zum Beispiel ein TCP-Header auf mehrere Fragmente aufgeteilt und kann daher von zustandslosen Paketfiltern nicht analysiert werden. Eine Filterung aufgrund von Regeln, die den TCP-Header betreffen, ist dann nicht mehr möglich.

Ein zweiter Angriff, der die IP-Fragmentierung ausnutzt, ist der sogenannte Overlapping Fragment Attack [RFC 1858]. Die Internet-Protokoll-Spezifikation [RFC 791] beschreibt ein Verfahren zum Wiederzusammensetzen fragmentierter IP-Pakete, bei dem jedes neue Fragment jeden überlappenden Teil der zuvor erhaltenen Fragmente überschreibt. Wird ein solcher Algorithmus angewendet, so könnte ein Angreifer eine Folge von Paketen konstruieren, deren erstes Fragment harmlose Daten beinhaltet und folglich den Paketfilter passieren darf. Ein beliebiges nachfolgendes Fragment mit einem Offset, der größer als Null ist, könnte TCP-Header-Informationen (z. B. den Ziel-Port) überlappen. Beim Zusammensetzen der Fragmente wird der Überlappungsbereich des ersten Fragments überschrieben, wobei sich potenziell ein unzulässiges Paket ergibt, das ein zustandsloser Paketfilter aber nicht erkennt und daher nicht zurückweist.

Auch bei IPv6 sind Fragmentierungsangriffe möglich. Einige IDS-Versionen überprüfen Pakete nur bis zu einer begrenzten Anzahl an Fragmenten. Wird diese Anzahl überschritten, so wird das Paket bei der Prüfung ignoriert. Problematisch ist auch, dass verschiedene Betriebssysteme überlappende Fragmente unterschiedlich zusammenbauen. Ein für eine Firewall auf Linuxbasis harmlos erscheinendes, fragmentiertes Paket könnte auf einem Windows PC Schaden anrichten. Beispiele für Sicherheitsaspekte von Fragmentierung unter IPv6 und den Umgang mit Fragmenten finden sich in [RFC 6946] und [RFC 6980].

Gegenmaßnahmen in der Grundkonfiguration:

- Bei IPv6 ist eine Fragmentierung auf dem Transportweg nicht mehr erlaubt. Zu große Pakete müssen vom Absender fragmentiert werden. Da gleichzeitig für IPv6 die minimal zu transportierenden Paketlängen gegenüber IPv4 deutlich erhöht wurden, sind kleine Fragmente am Anfang eines IPv6-Datenpakets nicht mehr möglich und können bedenkenlos gefiltert werden. Dies macht schon in der einfachsten Version einen Paketfilter für IPv6 deutlich robuster gegen derartige Angriffe.
- Am Übergang zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netz zustandsbehaftete Paketfilterung einsetzen

– Geeignete Schwellenwerte für Fragment-Größe und maximale Fragment-Anzahl im Paketfilter vorgeben

Restrisiko: Generell ist das Restrisiko abhängig vom Gerätetyp des Paketfilters. Auch zustandsbehaftete Filter sind nicht völlig gefeit gegen Fragmentierungsangriffe. Eine zustandsbehaftete Filterung fragmentierter Pakete bindet unter Umständen Ressourcen des Paketfilters, was für Angriffe auf die Verfügbarkeit genutzt werden könnte.

7.3.7 VRRP-Angriffe

Bedrohung: Umlenken des Datenverkehrs
Schwachstelle: Fehlende Authentisierung der VRRP-Teilnehmer

Um sich als Master Router (Standard-Gateway) in das lokale Subnetz einzubinden, muss der Angreifer VRRP-Pakete (Advertisements) mit einer Priorität von 255 und einer höheren IP-Adresse als die der Mitbewerber senden. Dadurch kann die Master-Funktion übernommen werden. In der Rolle des Masters ist ein Mitlesen, Manipulieren oder Unterbinden des Datenverkehrs möglich.

Bei einigen Implementierung kann statt der Multicast-Adresse auch die Unicast-Adresse des Masters verwendet werden. Das heißt, VRRP ermöglicht unter Umständen sogar Angriffe von Systemen, die nicht im lokalen Netz liegen.

Bei IPv6 ergibt sich durch Verwendung von Neighbor Unreachability Detection (NUD) und Adress-Autokonfiguration eine Alternative zu VRRP, so dass auf eine Verwendung von VRRP entweder verzichtet werden kann oder die Anwendung auf einen sehr kleinen und strikt kontrollierten Netzabschnitt eingeschränkt werden kann.

Gegenmaßnahme in der Grundkonfiguration:

– VRRP (in Grundarchitektur mangels Redundanz nicht benötigt) deaktivieren

Restrisiko: Diese Maßnahme beseitigt die Gefährdung.

Variante 7.3.7 A für normalen Schutzbedarf: Teilnehmer am VRRP durch Zugriffslisten einschränken

Anwendungsbereich: Normaler Schutzbedarf bezüglich Integrität
Phase im Ablaufplan: Realisierung

Wird VRRP benötigt, um redundant ausgelegte Systemkomponenten zu koordinieren, so muss das Protokoll auf die betroffenen Ursprünge und Ziele − also die Mitglieder der jeweiligen Redundanzgruppe − eingeschränkt werden, um das Eindringen unbeteiligter Netzkomponenten in das Protokoll zu erschweren. Durch geeignete Zugriffsbeschränkungen ist eine logische Trennung zwischen Nutzdaten- und VRRP-Ports möglich.

Restrisiko: Zugriffslisten lassen sich unter Umständen durch IP Spoofing überwinden.
Umsetzungsaufwand: Geringer Konfigurationsaufwand

Variante 7.3.7 B für hohen Schutzbedarf: VRRP-Authentisierung verwenden

Anwendungsbereich: Hoher Schutzbedarf bezüglich Verfügbarkeit

Phase im Ablaufplan: Realisierung

Verglichen mit einfachen Zugriffslisten bietet eine kryptografische Authentisierung der VRRP-Teilnehmer einen wesentlich besseren Schutz gegen VRRP-Attacken. Allerdings erfordert die Maßnahme Mechanismen und Prozesse zur Schlüsselverwaltung, was erheblichen administrativen Aufwand verursachen kann. Da die neue VRRP-Version nach [RFC 3768] ausdrücklich keine ins Protokoll integrierten Authentisierungsmechanismen mehr vorsieht, muss unter Umständen sogar ein separater Mechanismus mit entsprechendem Realisierungsaufwand eingesetzt werden.

Restrisiko: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.

Umsetzungsaufwand: Mittel bis hoch, je nach VRRP-Version, Größe und Redundanzgrad des Netzes sowie vorhandener Schlüssel-Infrastruktur

7.3.8 Smurf Attack / Fraggle Attack

Bedrohung: Überlastung durch ICMP-Pakete

Schwachstelle: Quelladresse eines IP-Pakets leicht fälschbar, Broadcast von außerhalb des Netzes möglich

Bei einem Smurf Attack sendet der Angreifer ICMP-Echo-Nachrichten (Ping) mit der gefälschten Quelladresse eines Opfers an die Broadcast-Adresse eines Netzes. Alle Rechner im Netz antworten dem angegebenen Rechner mit einem ICMP Echo Reply. Das Opfer bricht unter der Last der Antworten zusammen.

Ein Fraggle Attack verwendet anstatt des ICMP-Anregungspakets ein UDP-Paket, als Antwort wird in den meisten Fällen ein ICMP Destination Unreachable gesendet. Auch die Fraggle-Attacke zielt auf eine Überlastung des Opfers durch ICMP-Antworten.

Angriffe auf Basis von Netzwerk-Broadcasts sind bei IPv6 grundsätzlich nicht mehr möglich, da es diese Funktionalität nicht mehr gibt. Vergleichbare Angriffe auf Basis von Multicast sind bei IPv6 nicht Erfolg versprechend, da die Anzahl der jeweils angesprochenen Stationen um Größenordnungen geringer ist. Die mit einem Broadcast am ehesten vergleichbaren Multicasts, wie zum Beispiel an die Adresse FF02::1 für ND, sind immer nur auf einen Link beschränkt, da sie nicht geroutet werden und somit auch nicht zu größeren Angriffen geeignet sind.

Gegenmaßnahme in der Grundkonfiguration:

- Broadcasts mit einem Ursprung außerhalb des lokalen Teilnetzes (Directed Broadcasts) deaktivieren (z. B. unter Cisco IOS mittels: `no ip directed-broadcast`)

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet. Innerhalb eines Netzsegments ist ein entsprechender Angriff prinzipiell weiterhin möglich, durch die Beschränkung auf das Subnetz in seiner Stärke jedoch begrenzt und nur für Innentäter unmittelbar durchführbar.

7.3.9 ICMP Sweep / ICMP Inverse Mapping

Bedrohung: Ausspähen der Netztopologie

Schwachstelle: Fehlende Beschränkungen für ICMP-Echo- und ICMP-Echo-Reply-Nachrichten

Ein ICMP Sweep ist quasi eine Erweiterung des Ping-Kommandos, die dazu dient, gleich mehrere Rechner (z. B. ein komplettes Netz) auf Erreichbarkeit zu untersuchen. Ein Angreifer kann damit die Netztopologie ausspähen, um weitergehende Angriffe vorzubereiten.

ICMP Inverse Mapping dient dazu, den internen Aufbau eines Netzes zu bestimmen, das durch einen Paketfilter geschützt wird. Dazu sendet der Angreifer ICMP-Echo-Pakete an das zu erkundende Netz. Bei den ICMP-Antworten `Host Unreachable` oder `Time Exceeded` ist davon auszugehen, dass der Rechner nicht existiert. Bekommt der Angreifer keine Antwort, so deutet dies darauf hin, dass die entsprechende Zieladresse im Netz existiert.

Die unsystematische Ausforschung eines Netzes per ICMP Sweep wird bei IPv6 durch den großen Adressraum unpraktikabel. Jedoch kann es für einen entsprechend motivierten Angreifer durchaus Erfolg versprechend sein, gezielt bestimmte Teile des Adressbereiches abzusuchen: per DHCP vergebene Adressen werden beispielsweise oft in aufsteigender Reihenfolge aus einem bestimmten Bereich vergeben, Server erhalten meist vorhersagbare Adressen, gelegentlich auch in Verbindung mit Wörtern wie *beef, food, cafe, babe* oder ähnlichen, die sich in die hexadezimale Schreibweise der IPv6-Adressen einbauen lassen. Bei Adressen, die per SLAAC generiert werden, wird die MAC-Adresse der Netzwerkkarte zur Bildung der Interface ID herangezogen, so dass auch in diesem Fall der effektiv abzusuchende Adressbereich deutlich kleiner ist, als es die theoretische Größe von 2^{64} vermuten lassen würde.

Für Angreifer, die sich direkt in einem bestimmten Netzsegment befinden, stellt in IPv6-Netzen die Verwendung des ND Multicasts an die Adresse FF02::1 eine weitere Möglichkeit zur Ausforschung des Netzes dar. Hiermit lassen sich allerdings nur die Stationen an einem Link erreichen und abfragen.

Gegenmaßnahme in der Grundkonfiguration:

- Am Übergang zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netz eintreffende ICMP-Echo- und ICMP-Echo-Reply-Nachrichten verwerfen

Restrisiko: Diese Maßnahme beseitigt die Gefährdung für normalen und hohen Schutzbedarf.

7.3.10 ICMP Redirect Attack

Bedrohung: Umlenken von IP-Verkehr
Schwachstelle: Fehlende Authentisierungsmöglichkeit für ICMP-Redirect-Empfehlungen

Eine ICMP-Redirect-Nachricht wird von einem Router an ein anderes System versendet, um dieses über eine bessere Route zu informieren. Bei einem Angriff versendet ein Angreifer eine ICMP-Redirect-Nachricht mit einem fingierten Gateway an das anzugreifende System, um so entweder die Pakete auf von ihm selbst kontrollierte Zwischenknoten umzuleiten (Man in the Middle) oder auf nicht erreichbare Ziele zu lenken (DoS).

Gegenmaßnahme in der Grundkonfiguration:

- Am Übergang zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netz werden eintreffende ICMP-Redirect-Nachrichten verworfen.

- ICMP-Redirects werden bei IPv6 nicht geroutet und sind damit in ihrer Auswirkung auf das jeweilige Subnetz beschränkt. Durch die Unterteilung in viele Subnetze wird die Wirksamkeit des Angriffs stark vermindert.

Restrisiko: Diese Maßnahme beseitigt die Gefährdung für normalen und hohen Schutzbedarf.

7.3.11 ICMP Echo Flood Attack

Bedrohung: Überlastung der Netzverbindung
Schwachstelle: Begrenzte Verarbeitungskapazität für ICMP-Echo-Nachrichten

Bei diesem Angriff sendet der Angreifer in schneller Folge ICMP-Echo-Nachrichten an das Opfersystem, um die Netzverbindung des Ziels zu überlasten. Dazu muss der Angreifer allerdings über mehr Bandbreite als das Opfer verfügen.

Gegenmaßnahme in der Grundkonfiguration:

- Am Übergang zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netz eintreffende ICMP-Echo-Nachrichten bei IPv4 verwerfen und bei IPv6 mit Hilfe eines rate-limits auf eine geringe Anzahl pro Minute beschränken.

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet. Ein Schutz gegen Überlastung ist prinzipiell jedoch nur eingeschränkt möglich, da selbst das Filtern unerwünschter Datenpakete Bandbreite und Ressourcen bindet und zumindest die jeweilige Zubringerverbindung und betroffene Router oder Filter weiterhin überlastet werden können.

7.3.12 Router-Advertisement Flooding

Bedrohung: Überlastung lokaler Ressourcen
Schwachstelle: Begrenzte Verarbeitungskapazität für ICMPv6-Nachrichten

Unter IPv6 sind mehrere Flooding Angriffe mit Router-Advertisements (RA) möglich. Allen ist gemein, dass sie Ressourcen beim Zielsystem verbrauchen und so zu einem Denial-of-Service führen.
Die bekannteste Variante ist das Versenden vieler neuer Präfixe. Dies führt dazu, dass Geräte im gleichen Subnetz sich für jedes neue Präfix auch neue Adressen generieren. Mit diesem Angriff lässt sich die Performance der Arbeitsplatz-Clients im Netz stark beeinträchtigen. Im Extremfall stürzen PCs sogar ab.
Andere RA-Flooding Angriffe verwenden Default-Routen oder spezifischen Routen. Es sind viele weitere Szenarien denkbar.

Gegenmaßnahme in der Grundkonfiguration:

- Durch das „Prinzip der kleinen Netze“ sind die Angriffe auf eine geringe Zahl an Geräten beschränkt.
- Beschränkung der Paketzahl durch rate-limits
- Verwendung von Router-Advertisement-Guard

Restrisiko: Diese Gefährdung ist Protokoll-inhärent und lässt sich nicht vollständig vermeiden. Alle Angriffe wirken nur innerhalb eines Subnetzes und sind somit in ihrer Auswirkung beschränkt. Features wie der Router-Advertisement-Guard helfen nur gegen „versehentliches“ RA-Flooding, jedoch nicht gegen Angriffe.
Varianten: 7.2.7 A für hohen Schutzbedarf: Statisch konfigurierte ND-Einträge bei IPv6
7.2.7 B für hohen Schutzbedarf: SEcure Neighbor Discovery (SEND)

7.3.13 Manipulation des Routings

Bedrohung: Umlenken von IP-Verkehr, Ausspähen der Netztopologie
Schwachstelle: Fehlende Authentisierung, Integritätssicherung oder Verschlüsselung von Routing-Protokollen

In komplexeren Netzen werden oftmals dynamische Routing-Protokolle eingesetzt, die unter Umständen das Einschleusen falscher Routen ermöglichen und so eine Umleitung von IP-Paketen ermöglichen. Routing-Protokolle ohne sichere Authentisierung und Integritätssicherung sind durch Spoofing- und DoS-Angriffe bedroht.

Ein anderer Angriff besteht darin, Datenpakete beim Austausch von Routing-Informationen mitzulesen, um so Kenntnisse über die interne Netzstruktur zu erlangen.

Gegenmaßnahme in der Grundarchitektur:

- Trennung von internem und externem Routing durch das Sicherheits-Gateway

Gegenmaßnahmen in der Grundkonfiguration:

- Statisches Routing im Sicherheits-Gateway und angeschlossenen DMZn
- Nutzung privater IP-Adressen im Netz-Inneren, die aus dem Internet nicht adressierbar sind
- Ausschließliche Verwendung von Routing-Protokollen mit Möglichkeit zur Authentisierung und Integritätssicherung

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen Schutzbedarf ausreichend begegnet.

Variante 7.3.13 A für hohen Schutzbedarf: OSPF mit IPSec-Verschlüsselung einsetzen

Anwendungsbereich: Hoher Schutzbedarf bezüglich Vertraulichkeit
Phase im Ablaufplan: Realisierung

Um Routing nicht nur gegen Manipulation zu sichern, sondern es zusätzlich auch gegen ein Ausspähen zu schützen, können die verfügbaren Verschlüsselungsoptionen genutzt werden. OSPF bietet hierzu die IPSec-Mechanismen.

Der Einsatz von Verschlüsselung erfordert eine entsprechende Infrastruktur für die Schlüsselverwaltung. Je nach Größe des Netzes und Komplexität der Routing-Topologie entsteht dadurch beträchtlicher Zusatzaufwand, sofern eine Schlüsselverwaltung nicht aus anderen Gründen ohnehin bereits verfügbar ist.

Restrisiko: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.

Umsetzungsaufwand: Mittel bis hoch aufgrund des Aufwands zur Schlüsselverwaltung

7.3.14 Rogue Router Advertisements

Bedrohung: Angreifer versendet IPv6 Router-Ankündigung und lenkt Verkehr um
Schwachstelle: Keine Authentisierung von Router-Advertisements

Bei diesem Angriff sendet der Angreifer eine falsche Router-Ankündigung. Das darin genannte Präfix überdeckt entweder nur bestimmte Zielbereiche im Adressraum oder kann den gesamten Adressraum übernehmen. Der Angreifer ernennt sich dadurch zum Default-Router für diesen Adressbereich. Durch diese Einstellung kann er Verkehr falsch lenken, um dort mitzulesen (Angriff auf die Vertraulichkeit) oder den Verkehr dort ins Leere laufen zu lassen (Angriff auf die Verfügbarkeit).

Diese Gefährdung ist insbesondere in reinen IPv4-Netzen relevant. Hier kann ein Angreifer durch das Integrieren eines eigenen IPv6-Routers in das Netzwerk Verkehr zu sich ziehen, da die Betriebssysteme der Clients in der Regel IPv6 gegenüber IPv4 bevorzugen.

Als unterstützende Maßnahme kann der Angreifer neben dem Bereitstellen eines Routers auch versuchen vorhandene Router außer Betrieb zu setzen, indem er beispielsweise durch gefälschte Router-Advertisements die Lifetime oder die Priorität eines „echten“ Routers herabsetzt.

Gegenmaßnahme in der Grundkonfiguration:

- Router-Advertisements von Endgeräten kommend werden bei den Switches gefiltert und damit unschädlich gemacht.
- Router-Advertisements sind nur innerhalb eines Subnetzes wirksam. Durch die Aufteilung in viele kleine Subnetze bleibt die Wirksamkeit des Angriffs stark eingeschränkt.
- Will man größere WLAN-Netze mit IPv6 bedienen (zum Beispiel für Konferenzen), so stehen von einigen Herstellern bereits speziell für das Aufspüren von Rogue Router Advertisements ausgerüstete zentrale WLAN-Controller zur Verfügung. Mit diesen Informationen ist es dann möglich, gezielt diese Störer zu ermitteln und aus dem Netz zu entfernen.

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet. Innerhalb gemeinsam genutzter Subnetze (zum Beispiel WLAN-Bereiche) ist ein Schutz prinzipiell nur eingeschränkt möglich. Weiterentwicklungen des Router-Advertisements bieten Möglichkeiten der Authentisierung, allerdings sind diese Varianten am Markt noch nicht weit verfügbar.
Varianten: 7.2.7 B für hohen Schutzbedarf: SEcure Neighbor Discovery (SEND)

7.3.15 Overflow von Blacklists

Bedrohung: Der große Adressraum bei IPv6 kann von einem Angreifer durch das Versenden einer großen Zahl gefälschter Absenderadressen dazu missbraucht werden, die Kapazität von Blacklists zu erschöpfen.
Schwachstelle: Begrenzte Speicherkapazität der Blacklist führt zum Overflow.

Bei diesem Angriff sendet der Angreifer Daten mit einer großen Zahl gefälschter Absenderadressen, die dann in die jeweilige Blacklist (z. B. für die Sperrung des Zugangs zum E-Mail-Server oder SSH-Server) bis zur Erschöpfung füllen und nach einem Overflow die

eigentlich zu sperrenden Adressen überschreiben. Die Wirkung der Sperrliste wird damit zumindest teilweise aufgehoben.

Gegenmaßnahme in der Grundkonfiguration:

- Für einen erfolgreichen Angriff muss der Angreifer über eine große Bandbreite verfügen.
- Blacklisten entsprechend groß dimensionieren und gegen Overflow härten

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen Schutzbedarf ausreichend begegnet.

7.4 Gefährdungen auf der Transportschicht und empfohlene Gegenmaßnahmen

Im Folgenden werden die maßgeblichen Gefährdungen auf der Transportschicht und geeignete Gegenmaßnahmen vorgestellt.

7.4.1 TCP-SYN-Flooding

Bedrohung: Ausfall der Kommunikationsverbindung
Schwachstelle: Begrenzte Ressourcen für unvollständig aufgebaute (halboffene) TCP-Verbindungen

TCP-SYN-Flooding wird typischerweise für Denial-of-Service-Angriffe verwendet. Der Angreifer sendet dazu ein Verbindungsaufbau-Paket (SYN) und das Opfer antwortet mit einer Bestätigung (SYN−ACK). Normalerweise würde der Client jetzt ein Paket mit gesetztem ACK-Bit erwidern und die Verbindung wäre aufgebaut. Antwortet ein böswilliger Client aber nicht wie erwartet, so bleibt die Verbindung halboffen, und der Server gibt die Ressourcen erst wieder nach einer festgelegten Zeitspanne frei. Ab einer gewissen Anzahl halboffener Verbindungen sind die Ressourcen des Opfers erschöpft, sodass keine neuen Verbindungen mehr möglich sind.

Gegenmaßnahme in der Grundkonfiguration:

- Limit für halboffene und offene Verbindungen am Paketfilter setzen

Restrisiko: Ein Limit für die Zahl der bestehenden TCP-Verbindungen beeinträchtigt immer auch die zweckgebundene Kommunikation. Sobald der Schwellenwert ausgeschöpft ist, können keine weiteren TCP-Verbindungen mehr aufgebaut werden. Dies kann ebenfalls für DoS-Angriffe genutzt werden.

7.4.2 Sequence Number Guessing

Bedrohung: Eindringen in TCP-Verbindungen
Schwachstelle: Leichte Vorhersagbarkeit der Initial Sequence Number, fehlende Authentisierung oberhalb der Transportschicht

Gelingt es einem Angreifer, die beim TCP-Verbindungsaufbau verwendete initiale Sequenznummer (Initial Sequence Number, ISN) zu erraten, so kann er unbemerkt TCP-Pakete in eine bestehende Verbindung einstreuen und so die Identität eines fremden Senders vortäuschen.

Gegenmaßnahme in der Grundkonfiguration:

- Am Übergang zwischen verschiedenen Sicherheitszonen ISN per Zufall bilden (bei modernen Koppelelementen ist diese Option standardmäßig aktiviert).

Restrisiko: Durch diese Maßnahme wird der Gefährdung durch eingestreute, zusätzliche TCP-Pakete für normalen und hohen Schutzbedarf ausreichend begegnet. Allerdings bietet eine sichere Sequenznummer alleine keinen ausreichenden Schutz gegen TCP-Manipulationen: Für sensible Daten ist darüber hinaus immer auch eine sichere Authentisierung und Integritätssicherung erforderlich, um die Verfälschung gesendeter Datenpakete wirksam zu unterbinden.

7.4.3 Desynchronized State

Bedrohung: Eindringen in TCP-Verbindungen
Schwachstelle: Verwundbarkeit von TCP-Verbindungen in der Resynchronisations-Phase

Ein Angreifer kann TCP-Pakete erstellen, die sowohl vom Server als auch vom Client einer zuvor unterbrochenen TCP-Verbindung akzeptiert werden. Der Angriff basiert darauf, zunächst einen asynchronen Zustand auf beiden Seiten einer bestehenden TCP-Verbindung zu erzwingen, der dann nur unter Mithilfe beider Seiten − in diesem Falle eines Angreifers als Man-in-the-Middle in Kooperation mit den ursprünglichen Kommunikationspartnern − wieder synchronisiert werden kann. Der Angreifer nutzt die unübersichtliche Situation, um in die Verbindung einzudringen.

Gegenmaßnahme in der Grundkonfiguration:

- Schutzbedürftige Daten verschlüsseln und authentisieren.

Restrisiko: Diese Maßnahme beseitigt die Gefährdung für normalen und hohen Schutzbedarf.

7.4.4 Firewalking

Bedrohung: Ausspionieren von Paketfiltern
Schwachstelle: Allzu auskunftsfreudige Netze

Firewalking wird verwendet, um die Konfiguration eines Paketfilters zu analysieren. Dazu werden IP-Pakete (UDP oder TCP) mit einer Time to live (TTL) gesendet, die genau um eins größer ist als die Anzahl der Router, die zum Erreichen des Paketfilters zu durchlaufen sind. Lässt der Paketfilter diese Pakete passieren, so antwortet der nächste Rechner bzw. Router hinter dem Paketfilter mit einer ICMP-Time-Exceeded-Nachricht. Falls der Angreifer diese Nachricht erhält, kann er daraus schließen, dass die Konfiguration des Paketfilters die Weiterleitung des gesendeten IP-Pakets zulässt.

Gegenmaßnahme in der Grundkonfiguration:

- Am Übergang zwischen einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netz eintreffende ICMP-Time-Exceeded-Nachrichten verwerfen

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.4.5 UDP Packet Storm

Bedrohung: Überlastung von UDP-Schnittstellen
Schwachstelle: Fehlende Flusskontrolle des UDP

Der Angreifer sendet eine große Zahl von UDP-Paketen an das Angriffsziel. Dies kann zu einer erheblichen Leistungsminderung oder sogar zu einem kompletten Ausfall des Opfers führen.

Gegenmaßnahmen in der Grundkonfiguration:

- Nur unverzichtbare UDP-Dienste anbieten
- An Netzübergängen sogenannte Rate Limits für UDP-Datenströme definieren

Restrisiko: Rate Limits beeinträchtigt immer auch die zweckgebundene Kommunikation, was im Extremfall zu einem indirekten Denial-of-Service führen kann, den es ohne diese Schutzvorrichtung nicht gegeben hätte.

7.5 Gefährdungen auf der Anwendungsschicht und empfohlene Gegenmaßnahmen

Im Folgenden werden die maßgeblichen Gefährdungen auf der Anwendungsschicht und geeignete Gegenmaßnahmen vorgestellt. Dabei werden allerdings nur die Basisdienste und -protokolle betrachtet, die zur Grundarchitektur gehören: DNS, NTP, DHCP und SNMP.

Für Hinweise zu Gefährdungen auf der Anwendungsschicht von E-Mail und WWW sei auf die entsprechenden Module der ISi-Reihe [ISi-Mail-Client], [ISi-Mail-Server], [ISi-Web-Client] und [ISi-Web-Server] verwiesen.

7.5.1 DNS Spoofing / DNS (Cache) Poisoning

Bedrohung: Vortäuschen einer falschen Identität
Schwachstelle: Fehlende Authentisierung des DNS-Protokolls

DNS Spoofing zielt darauf, die Zuordnung zwischen einem Rechnernamen und der zugehörigen IP-Adresse zu fälschen, sodass der Name in eine falsche IP-Adresse aufgelöst wird oder umgekehrt der IP-Adresse ein falscher Name zugeschrieben wird. Der Angreifer gaukelt seinem Opfer so eine falsche Identität vor, was zum Beispiel zur Vorbereitung von Denial-of-Service- und Man-in-the-Middle-Angriffen dienen kann.

DNS Cache Poisoning ist ein spezielle Variante des DNS Spoofing, bei der einem anfragenden DNS-Server − zusätzlich zu der regulären Antwort der vorgesehenen Gegenstelle − von dritter Seite gefälschte Informationen untergeschoben werden. Dies ist so ohne Weiteres allerdings nur bei älteren DNS-Servern möglich, die weder eine Manipulationserkennung noch einen Zufallszahlengenerator zur Erzeugung von Abfragenummern (Query IDs) verwenden.

Gegenmaßnahme in der Grundarchitektur:

- Trennung der internen und externen DNS-Funktion zur Minimierung der Angriffsfläche

Gegenmaßnahme in der Grundkonfiguration:

- Aktuelle DNS-Software verwenden
- DNS-Server vor Modifikationen schützen, zum Beispiel kein dynamisches DNS einsetzen

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet. Bei der Internet-Nutzung sind Anwender jedoch auf fremde DNS-Server angewiesen, auf deren Integrität sie keinen Einfluss nehmen können. Namen oder IP-Adressen liefern daher keine sicheren Merkmale zur Identifizierung; sie ersetzen nicht eine förmliche Authentisierung auf der Anwendungsschicht.

7.5.2 DNS Sniffing

Bedrohung: Ausspähen von Namen, Adressen oder Verbindungstopologien
Schwachstelle: Zu große Auskunftsfreudigkeit des DNS-Servers

Anhand von DNS-Daten kann ein potenzieller Angreifer existierende und besonders wichtige Server identifizieren und Rückschlüsse auf die Netzstruktur ziehen. Solche Informationen sind die Basis für weitergehende Angriffe.

Gegenmaßnahme in der Grundarchitektur:

- Trennung der internen und externen DNS-Funktion zur Minimierung der Angriffsfläche

Gegenmaßnahmen in der Grundkonfiguration:

- Zonen-Transfers nur für ausgewählte Server zulassen
- List-Funktion des DNS deaktivieren

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.3 DNS Amplification Attack

Bedrohung: Überlastung des DNS
Schwachstelle: Lawinen-Effekt rekursiver DNS-Anfragen

DNS-Server, die rekursive Anfragen weltweit beantworten, können als Plattform für Angriffe auf fremde DNS-Server verwendet werden. Aufgrund des Verstärkungseffekts der Rekursion können sich solche Angriffe auch gegen die Verfügbarkeit des eigenen LANs richten.

Gegenmaßnahme in der Grundkonfiguration:

- rekursive Anfragen nur autorisierten, vertrauenswürdigen Rechnern ermöglichen, für fremde DNS-Clients jedoch sperren

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.4 DNS (Cache) Snooping

Bedrohung: Ausspähen des Kommunikationsverhaltens der Nutzer

Schwachstelle: Zugreifbare Rest-Informationen über frühere DNS-Anfragen im Cache

Auf iterative Anfragen (Recursion-Bit nicht gesetzt) antworten DNS-Server weltweit mit den Informationen aus den eigenen Zonendateien (falls vorhanden) und mit dem Inhalt ihres Zwischenspeichers (Cache). Somit lassen sich die vom DNS-Server bereits aufgelösten Anfragen im Cache ermitteln, was ein Ausspionieren des Kommunikationsverhaltens der Internet-Nutzer ermöglicht.

Gegenmaßnahme in der Grundkonfiguration:

- Anfragen mit nicht gesetztem Recursion-Bit verwerfen

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.5 NTP Manipulation

Bedrohung: Falsch synchronisierte Systemuhren
Schwachstelle: Fehlende Authentisierung von NTP-Nachrichten, vor allem bei NTP-Broadcasts

NTP bietet mehrere Betriebsarten, um eine Synchronisation durchzuführen. Zeitinformationen können beispielsweise per Broadcast an alle Rechner im Netz versendet werden, und nicht alle NTP-Implementierungen unterstützen eine Authentisierung der NTP-Nachrichten. Wenn dem Zielsystem eine falsche Uhrzeit vorgetäuscht wird, können dadurch eine Reihe von Problemen entstehen, etwa bei der Analyse von Logdaten oder beim Erkennen abgelaufener Kerberos-Tickets.

Gegenmaßnahmen in der Grundarchitektur:

- NTP-Server im Management-Netz unterbringen und NTP out-of-band betreiben
- Zeit über eine hochgenaue, sichere Quelle (DCF) unabhängig vom Internet beziehen

Gegenmaßnahmen in der Grundkonfiguration:

- Client-/Server-Mode des NTP mit Authentisierung verwenden

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.6 NTP Amplification Attack

Bedrohung: Beteiligung an DDoS-Angriffen
Schwachstelle: Offene NTP-Server

Ähnlich wie DNS (siehe Abschnitt 7.5.3) lässt sich auch NTP für Amplification Angriffe ausnutzen. Das Prinzip der Angriffe ist es mit kleinen Anfragen an Server große Antworten zu provozieren. Werden diese Anfragen mit einer gefälschten IP-Adresse gestellt, so erhält nicht der Angreifer die Antwort, sondern derjenige, dessen Adresse gefälscht wurde. Auf diese Weise lässt sich die Internetanbindung des Zielsystems blockieren.

Gegenmaßnahme in der Grundkonfiguration:

- NTP nicht von außen erreichbar

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.7 DHCP Starvation / DHCP Rogue Server / DHCP Spoofing

Bedrohung: Unterwandern oder Stören von Kommunikationsverbindungen
Schwachstelle: Fehlende Authentisierung von DHCP-Clients und -Servern, begrenzter verfügbarer IP-Adressraum des DHCP-Servers

Beim DHCP-Starvation-Angriff täuscht der Angreifer eine Serie gültiger Client-Anfragen vor, um alle verfügbaren IP-Adressen des DHCP-Servers zu belegen. Dadurch kann der Server anderen Clients keine neuen IP-Adressen mehr zuweisen (Denial of Service).

Ein DHCP Rogue Server (Angreifer) liefert einem DHCP-Client gefälschte DHCP-Optionen, indem er Anfragen des Clients schneller beantwortet als der eigentlich zuständige DHCP-Server. Der Angreifer kann dem Client so falsche Konfigurationsvorgaben unterschieben (z. B. für die Adressen von Standard-Gateway oder DNS-Server). Dies ermöglicht einen Denial-of-Service- oder Man-in-the-Middle-Angriff.

Beim DHCP Spoofing werden zwei Angriffe kombiniert, zum einen DHCP Starvation, um den vorgesehenen Server an der Vergabe von IP-Adressen zu hindern, zum anderen wird zusätzlich ein DHCP Rogue Server eingesetzt, um falsche Informationen an die Clients zu übergeben. Auf diese Weise können Denial-of-Service- und Man-in-the-Middle-Angriffe durchgeführt werden.

Gegenmaßnahmen in der Grundkonfiguration:

- Bei IPv6: bei der Verwendung von stateless DHCP und Autokonfiguration entfällt das Angriffszenario *DHCP Starvation*
- Feste Zuordnung von IP- und MAC-Adresse auf dem DHCP-Server
- Vorkonfektionierte Gegenmaßnahmen auf den Switches aktivieren (geräteabhängig: z. B. bei Cisco-Geräten die *DHCP Snooping*-Optionen, die es dem Switch ermöglicht, nicht vertrauenswürdige DHCP-Pakete zu erkennen und zu verwerfen)

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen Schutzbedarf ausreichend begegnet. Die verfügbaren Abwehrmechanismen sind allerdings gerätespezifisch; daher sollten moderne, leistungsfähige Koppelelemente eingesetzt werden, die über wirksame Schutzoptionen verfügen.

Variante 7.5.7 A für hohen Schutzbedarf: Verzicht auf DHCP

Anwendungsbereich: Hoher Schutzbedarf bezüglich Integrität, Vertraulichkeit oder Verfügbarkeit
Phase im Ablaufplan: Konzeption

Anstatt den Clients ihre IP-Adresse oder sonstige Konfigurationsparameter dynamisch zuzuweisen, können die entsprechenden Konfigurationseinstellungen auch statisch vorgenommen werden. Dadurch wird der Betrieb eines DHCP-Servers entbehrlich und die entsprechenden Risiken entfallen.

Restrisiko: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.
Umsetzungsaufwand: Mittel bis hoch, je nach der Fluktuationsrate der Client-Population im lokalen Netz

7.5.8 SNMP Abhören

Bedrohung: Ausspähen oder Manipulieren von Konfigurationsdaten
Schwachstelle: Unsichere SNMP-Standardkonfiguration, Nutzung unsicherer SNMP-Versionen

Ein größeres Netz lässt sich nicht ohne zentrales Management betreiben. In den meisten Fällen wird SNMP eingesetzt. Leider werden Netzkomponenten oft mit aktiviertem SNMP-Agent ausgeliefert. Da die voreingestellten Zugangsdaten in der Dokumentation vermerkt sind oder übliche Standardwerte verwendet werden, können Angreifer die SNMP-Informationen leicht auslesen. Zudem wird auch bei neueren Geräten SNMPv3 mit integrierten Verschlüsselungsalgorithmen oft noch nicht unterstützt.

Gegenmaßnahme in der Grundarchitektur:

- SNMP-Kommunikation über separates Management-Netz (Out-of-Band-Management)

Gegenmaßnahmen in der Grundkonfiguration:

- SNMP nur bei Bedarf aktivieren und nur minimal erforderliche Zugriffsrechte einräumen
- SNMP Version 3 mit Authentisierung und Verschlüsselung verwenden
- SNMP-Zugriffsberechtigungen auf die Management-Station einschränken
- keine Standard-Passwörter (Community Strings) verwenden

Restrisiko: Durch diese Maßnahmen wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

7.5.9 IPv4-only VPN

Bedrohung: Umgehen des VPN
Schwachstelle: Unzureichende Berücksichtigung von IPv6

Insbesondere wenn auf eine explizite IPv6-Konfiguration verzichtet wurde, besteht die Gefahr, dass Geräte, die für ein reines IPv4-Netz ausgelegt sind, unvorbereitet in eine IPv6-Umgebung gelangen.

Dies tritt beispielsweise dann auf, wenn ein mobiles Gerät in einem fremden Netz verwendet wird. Gemäß [ISi-Fern] sollte das Gerät einen VPN-Tunnel ins Netz der eigenen Institution aufbauen, um dann über die Infrastruktur – insbesondere das Sicherheits-Gateway – der eigenen Institution ins Internet zu gelangen.

Ist das VPN dabei nur für IPv4 konfiguriert und bietet das fremde Netz auch IPv6 an, so kann es sein, Verbindungen am VPN und damit an der eigenen Sicherheitsinfrastruktur vorbei laufen. Es müssen entweder Produkte eingesetzt werden, die beide Protokolle unterstützen, oder der IP-Stack des nicht unterstützen Protokolls muss deaktiviert werden.

Gegenmaßnahme in der Grundkonfiguration:

- Konfiguration oder Deaktivierung von IPv6
- Verwendung von Produkten, die IPv4 und IPv6 unterstützen

Restrisiko: Durch diese Maßnahme wird der Gefährdung für normalen und hohen Schutzbedarf ausreichend begegnet.

8 Fazit

Sollen in einem lokalen Netz (LAN) Web oder E-Mail nicht nur intern genutzt werden, so muss dieses Netz an das Internet angeschlossen werden. Mit diesem Schritt setzt der Betreiber eines LANs sein bislang geschlossenes Netz jedoch erheblichen zusätzlichen Gefährdungen aus. Angreifer aus dem Internet können Schwachstellen der grundlegenden Internet-Protokolle, -Dienste und -Komponenten ausnutzen und so in das interne Netz eindringen (Hacking), Datenverkehr abhören (Sniffing) oder Systeme mit gefälschten Absenderangaben zu unerwünschtem Verhalten bringen (Spoofing).

Die vorliegende Studie gibt Empfehlungen, wie diesen Gefahren sowohl bei normalem als auch bei hohem Schutzbedarf durch eine robuste Grundarchitektur, eine geeignete Geräteauswahl, sichere Konfigurationseinstellungen und einen kontrollierten Betrieb zu begegnen ist. Dadurch wird es möglich, das Restrisiko auf ein tragbares Maß zu reduzieren. Es gibt jedoch Risiken, vor denen man sich trotz der empfohlenen Maßnahmen nur bedingt schützen kann. Hierzu gehören insbesondere Denial-of-Service-Angriffe (DoS) sowie Spoofing-Angriffe im Zusammenhang mit Protokollen, die keine sichere Authentisierung vorsehen. Solche Restrisiken lassen sich reduzieren, indem unsichere Protokolle, wie DNS, durch sicherere Protokoll-Varianten oder -Erweiterungen wie zum Beispiel DNSSEC abgelöst werden.

Ein Umstellen des eigenen Netzes auf IPv6 erfordert zunächst einiges Umdenken, macht das Netz jedoch insgesamt einfacher und damit prinzipiell zuverlässiger als bei IPv4. Selbst der radikal anmutende Schritt, auf NAT zu verzichten, entpuppt sich in Verbindung mit mehrstufigen Sicherheits-Gateways, wie sie heute Stand der Technik sind, genauso als Erleichterung wie die vielen kleinen Detailänderungen, mit denen Altlasten des IPv4-Designs beseitigt wurden.

Der größte Unterschied zu IPv4 ist, dass IPv6 eine sicherheitszentrische Netztopologie der *vielen kleinen Subnetze* notwendig macht. Einerseits bedeutet das, dass eine IPv6-Migration nicht darin bestehen kann, in existierenden Topologien einfach nur zusätzlich überall IPv6 zur Verfügung zu stellen. Andererseits ist es aber positiv, dass damit unzeitgemäße und inhärent unsichere Topologien aus der NetBIOS-Ära endgültig überdacht werden müssen.

Um den Betriebsaufwand und die möglichen Fehlerquellen zu minimieren, ist es sinnvoll, möglichst wenige Geräte und Subnetze dual-stacked zu betreiben. Intern lässt sich das erreichen, indem man Client-Rechner nur mit IPv4 oder IPv6 anbindet und nur die Server, die sowohl von IPv4- als auch von IPv6-Clients genutzt werden, sowohl mit IPv4 als auch IPv6 konfiguriert. Den Zugriff auf externe Server, der im Rahmen der Grundarchitektur bereits über Application Level Gateways (Sicherheits-Proxys) innerhalb des Sicherheits-Gateways erfolgt, stellt man sicher, indem man die vorhandenen Application Level Gateways als IPv4/IPv6-Proxys benutzt. Dienste, die man selbst nach außen zur Verfügung stellt, bietet man parallel mit IPv4 und IPv6 an.

Insgesamt ist die Einführung von IPv6 zwar mit initialem Aufwand verbunden, schon mittelfristig ist aber abzusehen, dass sich IPv6-orientierte Umgebungen einfacher, zuverlässiger und sicherer betreiben lassen als heutige IPv4-Netze. Voraussetzung dafür ist eine gute und umfassende IPv6-Unterstützung aller Produkte und Netzkomponenten. Während diverse Betriebssysteme an dieser Stelle bereits sehr weit sind – wenn auch in der Umsetzung stark voneinander abweichen – so haben Router- und Firewall-Hersteller noch an einigen Stellen aufzuholen. Dies wird jedoch erst bei entsprechend großer Nachfrage und Kundendruck erfolgen. Unter anderem aus diesem Grund sollte IPv6 frühzeitig bei Beschaffungen eingeplant werden.

9 Literaturverzeichnis

[BSI-CS-058] Bundesamt für Sicherheit in der Informationstechnik, Effekte von IPv6 auf reine IPv4 Netze, 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-058.html

[BSI SGW] Bundesamt für Sicherheit in der Informationstechnik (BSI), Modulare Erweiterungen von Sicherheits-Gateways, 2007, https://www.bsi.bund.de/cln_136/DE/Publikationen/imBundesanzeigerVerlag/imbundesanzeigerverlag_node.html

[BSI Standl-Tech] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherheitseigenschaften von Standleitungstechnologien, 2007, https://www.bsi.bund.de/cae/servlet/contentblob/471610/publicationFile/31043/sicherheit_standleitungen_pdf.pdf

[BVA-IPv6] Bundesverwaltungsamt, IPv6-Best Practice für die öffentliche Verwaltung, 2013, http://www.bva.bund.de/DE/Organisation/Abteilungen/Abteilung_BIT/Leistungen/IT_Beratungsleistungen/IPv6/best_practice/bestpractice_node.html

[DHCP/SLAAC] B. Liu, R. Bonica et al, DHCPv6/SLAAC Address Configuration Interaction Problem Statement, 2013, http://tools.ietf.org/html/draft-liu-bonica-v6ops-dhcpv6-slaac-problem

[DRAHT-KOM] Bundesamt für Sicherheit in der Informationstechnik (BSI), Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte, 2007, https://www.bsi.bund.de/cln_164/ContentBSI/Publikationen/Broschueren/drahtkom/index_htm.html

IANA IPv6: IANA, , 2010, http://www.iana.org/assignments/ipv6-address-space/

[IEEE 802.11] Institute of Electrical and Electronics Engineers, Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications, 2007, http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[IEEE 802.11i] Institute of Electrical and Electronics Engineers, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004, http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[IEEE 802.15.1] Internet Engineering Task Force (IETF), SMTP Service Extension for Authentication, 2005, http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf

[IEEE 802.15.4] Institute of Electrical and Electronics Engineers, , 2005, http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

[IEEE 802.16] Institute of Electrical and Electronics Engineers, , 2004, http://standards.ieee.org/getieee802/download/802.16-2004.pdf

[IEEE 802.16e] Institute of Electrical and Electronics Engineers, , 2006, http://standards.ieee.org/getieee802/download/802.16e-2005.pdf

[IEEE 802.1q] Institute of Electrical and Electronics Engineers (IEEE), 802.1Q-2005, 2005, http://standards.ieee.org

[IEEE 802.1X] Institute of Electrical and Electronics Engineers (IEEE), IEEE 802.1X-2004 Port-Based Network Access Control, 2004, http://standards.ieee.org

[ISi-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Anti-Viren-Programme und Personal Firewalls am Client, in Bearbeitung, http://www.isi-reihe.de/

[ISi-E] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, in Bearbeitung, http://www.isi-reihe.de/

[ISi-Fern] Bundesamt für Sicherheit in der Informationstechnik, Sicherer Fernzugriff auf das interne Netz, 2010, https://www.bsi.bund.de/DE/Themen/InternetSicherheit/RemoteServices/remoteservices_node.html

[ISi-Mail-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Nutzung von E-Mail, 2009, http://www.isi-reihe.de/

[ISi-Mail-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicherer Betrieb von E-Mail-Servern, 2009, http://www.isi-reihe.de/

[ISi-VPN] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Virtual Private Network, 2009, http://www.isi-reihe.de/

[ISi-Web-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Nutzung von Web-Angeboten, 2008, http://www.isi-reihe.de/

[ISi-Web-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicheres Bereitstellen von Web-Angeboten, 2008, http://www.isi-reihe.de/

[ISi-WLAN] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: WLAN, 2009, http://www.isi-reihe.de/

[ITGSK] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT Grundschutzkataloge, Stand 2006, http://www.bsi.bund.de/gshb/

[RFC 768] Internet Engineering Task Force (IETF), User Datagram Protocol, 1980, http://www.ietf.org/rfc/rfc768.txt

[RFC 791] Internet Engineering Task Force (IETF), Internet Protocol, 1981, http://www.ietf.org/rfc/rfc791.txt

[RFC 792] Internet Engineering Task Force (IETF), Internet Control Message Protocol, 1981, http://www.ietf.org/rfc/rfc792.txt

[RFC 793] Internet Engineering Task Force (IETF), Transmission Control Protocol, 1981, http://www.ietf.org/rfc/rfc793.txt

[RFC 826] Internet Engineering Task Force (IETF), An Ethernet Address Resolution Protocol, 1982, http://www.ietf.org/rfc/rfc826.txt

[RFC 854] Internet Engineering Task Force (IETF), Telnet Protocol Specification, 1983, http://www.ietf.org/rfc/rfc854.txt

[RFC 959] Internet Engineering Task Force (IETF), File Transfer Protocol, 1985, http://www.ietf.org/rfc/rfc959.txt

[RFC 1027] Internet Engineering Task Force (IETF), Using ARP to implement transparent subnet gateways, 1987, http://www.ietf.org/rfc/rfc1027.txt

[RFC 1034] Internet Engineering Task Force (IETF), Domain Names - Concepts and Facilities, 1987, http://www.ietf.org/rfc/rfc1034.txt

[RFC 1058] Internet Engineering Task Force (IETF), Routing Information Protocol, 1988, http://www.ietf.org/rfc/rfc1058.txt

[RFC 1142] Internet Engineering Task Force (IETF), OSI IS-IS Intra-domain Routing Protocol, 1990, http://www.ietf.org/rfc/rfc1142.txt

[RFC 1157] Internet Engineering Task Force (IETF), A Simple Network Management Protocol (SNMP), 1990, http://www.ietf.org/rfc/rfc1157.txt

[RFC 1256] Internet Engineering Task Force (IETF), ICMP Router Discovery Messages , 1991

[RFC 1350] Internet Engineering Task Force (IETF), The TFTP Protocol (Revision 2), 1992, http://www.ietf.org/rfc/rfc1350.txt

[RFC 1700] Internet Engineering Task Force (IETF), Assigned Numbers, 1994

[RFC 1797] Internet Engineering Task Force (IETF), Class A Subnet Experiment, 1995

[RFC 1858] Internet Engineering Task Force (IETF), Security Considerations for IP Fragment Filtering, 1995, http://www.ietf.org/rfc/rfc1858.txt

[RFC 1886] Internet Engineering Task Force (IETF), DNS Extensions to support IP version 6, 1995

[RFC 1918] Internet Engineering Task Force (IETF), Address Allocation for Private Internets, 1996, http://www.ietf.org/rfc/rfc1918.txt

[RFC 1918] Internet Engineering Task Force (IETF), Address Allocation for Private Internets, 1996

[RFC 1939] Internet Engineering Task Force (IETF), Post Office Protocol - Version 3, 1996, http://www.ietf.org/rfc/rfc1939.txt

[RFC 1945] Internet Engineering Task Force (IETF), Hypertext Transfer Protocol -- HTTP/1.0, 1996, http://www.ietf.org/rfc/rfc1945.txt

[RFC 2080] Internet Engineering Task Force (IETF), RIPng for IPv6, 1997

[RFC 2131] Internet Engineering Task Force (IETF), Dynamic Host Configuration Protocol, 1997, http://www.ietf.org/rfc/rfc2131.txt

[RFC 2281] Internet Engineering Task Force (IETF), Cisco Hot Standby Router Protocol (HSRP), 1998, http://www.ietf.org/rfc/rfc2281.txt

[RFC 2328] Internet Engineering Task Force (IETF), OSPF Version 2, 1998, http://www.ietf.org/rfc/rfc2328.txt

[RFC 2338] Internet Engineering Task Force (IETF), Virtual Router Redundancy Protocol, 1998, http://www.ietf.org/rfc/rfc2338.txt

[RFC 2362] Internet Engineering Task Force (IETF), Protocol Independent Multicast-Sparse Mode (PIM-SM), 1998

[RFC 2453] Internet Engineering Task Force (IETF), RIP Version 2, 1998, http://www.ietf.org/rfc/rfc2453.txt

[RFC 2460] Internet Engineering Task Force (IETF), Internet Protocol, Version 6 (IPv6) Specification, 1998

[RFC 2460] Internet Engineering Task Force (IETF), Internet Protocol, Version 6 (IPv6) Specification, 1998, http://www.ietf.org/rfc/rfc2460.txt

[RFC 2526] Internet Engineering Task Force (IETF), Reserved IPv6 Subnet Anycast Addresses, 1999

[RFC 2529] Internet Engineering Task Force (IETF), Transmission of IPv6 over IPv4 Domains without Explicit Tunnels, 1999

[RFC 2544] Internet Engineering Task Force (IETF), Benchmarking Methodology for Network Interconnect Devices, 1999

[RFC 2595] Internet Engineering Task Force (IETF), Using TLS with IMAP, POP3 and ACAP, 1999, http://www.ietf.org/rfc/rfc2595.txt

[RFC 2616] Internet Engineering Task Force (IETF), Hypertext Transfer Protocol -- HTTP/1.1, 1999, http://www.ietf.org/rfc/rfc2616.txt

[RFC 2644] Internet Engineering Task Force (IETF), Changing the Default for Directed Broadcasts in Routers, 1999

[RFC 2644] Internet Engineering Task Force (IETF), Changing the Default for Directed Broadcasts in Routers, 1999, http://www.ietf.org/rfc/rfc2644.txt

[RFC 2675] Internet Engineering Task Force (IETF), IPv6 Jumbograms, 1999

[RFC 2710] Internet Engineering Task Force (IETF), Multicast Listener Discovery (MLD) for IPv6, 1999

[RFC 2711] Internet Engineering Task Force (IETF), IPv6 Router Alert Option, 1999

[RFC 2784] Internet Engineering Task Force (IETF), Generic Routing Encapsulation (GRE), 2000

[RFC 2818] Internet Engineering Task Force (IETF), HTTP Over TLS, 2000, http://www.ietf.org/rfc/rfc2818.txt

[RFC 2827] Internet Engineering Task Force (IETF), Network Ingress Filtering, Defeating Denial of Service Attacks which employ IP Source Address Spoofing, 2000

[RFC 2865] Internet Engineering Task Force (IETF), Remote Authentication Dial In User Service (RADIUS), 2000, http://www.ietf.org/rfc/rfc2865.txt

[RFC 3056] Internet Engineering Task Force (IETF), Connection of IPv6 Domains via IPv4 Clouds, 2001

[RFC 3068] Internet Engineering Task Force (IETF), An Anycast Prefix for 6to4 Relay Routers, 2001

[RFC 3207] Internet Engineering Task Force (IETF), SMTP Service Extension for Secure SMTP over Transport Layer Security, 2002, http://www.ietf.org/rfc/rfc3207.txt

[RFC 3315] Internet Engineering Task Force (IETF), Dynamic Host Configuration Protocol for IPv6 (DHCPv6), 2003

[RFC 3315] Internet Engineering Task Force (IETF), Dynamic Host Configuration Protocol for IPv6 (DHCPv6), 2003, http://www.ietf.org/rfc/rfc3315.txt

[RFC 3410] Internet Engineering Task Force (IETF), Introduction and Applicability Statements for Internet Standard Management Framework, 2002, http://www.ietf.org/rfc/rfc3410.txt

[RFC 3446] Internet Engineering Task Force (IETF), Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP), 2003

[RFC 3501] Internet Engineering Task Force (IETF), Internet Message Access Protocol - Version 4rev1, 2003, http://www.ietf.org/rfc/rfc3501.txt

[RFC 3569] Internet Engineering Task Force (IETF), An Overview of Source-Specific Multicast (SSM), 2003

[RFC 3596] Internet Engineering Task Force (IETF), DNS Extensions to Support IP Version 6, 2003

[RFC 3692] Internet Engineering Task Force (IETF), Assigning Experimental and Testing Numbers Considered Useful, 2004, http://tools.ietf.org/html/rfc3692

[RFC 3704] Internet Engineering Task Force (IETF), Ingress Filtering for Multihomed Networks , 2004

[RFC 3736] Internet Engineering Task Force (IETF), Stateless Dynamic Host Configuration Protocol (DHCP), 2004

[RFC 3810] Internet Engineering Task Force (IETF), Multicast Listener Discovery Version 2 (MLDv2) for IPv6, 2004

[RFC 3956] Internet Engineering Task Force (IETF), Embedding the Rendezvous Point (RP) Address in an IPv, 2004

[RFC 3973] Internet Engineering Task Force (IETF), Protocol Independent Multicast - Dense Mode (PIM-DM), 2005

[RFC 4033] Internet Engineering Task Force (IETF), DNS Security Introduction and Requirments, 2005, http://www.ietf.org/rfc/rfc4033.txt

[RFC 4191] Internet Engineering Task Force (IETF), Default Router Preferences and More-Specific Routes, 2005

[RFC 4193] Internet Engineering Task Force (IETF), Unique Local IPv6 Unicast Addresses, 2005

[RFC 4213] Internet Engineering Task Force (IETF), Basic Transition Mechanisms for IPv6 Hosts and Routers, 2005

[RFC 4250] Internet Engineering Task Force (IETF), The Secure Shell (SSH) Protocol Assigned Numbers, 2006, http://www.ietf.org/rfc/rfc4250.txt

[RFC 4271] Internet Engineering Task Force (IETF), A Border Gateway Protocol 4 (BGP-4), 2006, http://www.ietf.org/rfc/rfc4271.txt

[RFC 4272] Internet Engineering Task Force (IETF), BGP Security Vulnerabilities Analysis, 2006, http://www.ietf.org/rfc/rfc4272.txt

[RFC 4291] Internet Engineering Task Force (IETF), IP Version 6 Addressing Architecture, 2006

[RFC 4301] Internet Engineering Task Force (IETF), Security Architecture for the Internet Protocol, 2005, http://www.ietf.org/rfc/rfc2460.txt

[RFC 4302] Internet Engineering Task Force (IETF), IP Authentication Header, 2005, http://tools.ietf.org/html/rfc4302

[RFC 4303] Internet Engineering Task Force (IETF), IP Encapsulating Security Payload (ESP), 2005, http://tools.ietf.org/html/rfc4303

[RFC 4305] Internet Engineering Task Force (IETF), Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2005

[RFC 4364] Internet Engineering Task Force (IETF), BGP/MPLS IP Virtual Private Networks (VPNs), 2006, http://www.ietf.org/rfc/rfc4364.txt

[RFC 4380] Internet Engineering Task Force (IETF), Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs), 2006

[RFC 4443] Internet Engineering Task Force (IETF), Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, 2006

[RFC 4487] Internet Engineering Task Force (IETF), Mobile IPv6 and Firewalls: Problem Statement, 2006

[RFC 4727] Internet Engineering Task Force (IETF), Experimental Values in IPv4, IPv6, ICMPv4, ICMPv6, UDP, and TCP Headers, 2004, http://tools.ietf.org/html/rfc4727

[RFC 4760] Internet Engineering Task Force (IETF), Multiprotocol Extensions for BGP-4, 2007

[RFC 4861] Internet Engineering Task Force (IETF), Neighbor Discovery for IP version 6 (IPv6), 2007

[RFC 4862] Internet Engineering Task Force (IETF), IPv6 Stateless Address Autoconfiguration, 2007

[RFC 4941] Internet Engineering Task Force (IETF), Privacy Extensions for Stateless Address Autoconfiguration in IPv6, 2007

[RFC 4966] Internet Engineering Task Force (IETF), Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status, 2007

[RFC 5095] Internet Engineering Task Force (IETF), Deprecation of Type 0 Routing Headers in IPv6, 2007, http://tools.ietf.org/html/rfc5095

[RFC 5201] Internet Engineering Task Force (IETF), Host Identity Protocol, 2008, http://tools.ietf.org/html/rfc5201

[RFC 5214] Internet Engineering Task Force (IETF), Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), 2008, http://tools.ietf.org/html/rfc5214

[RFC 5246] Internet Engineering Task Force (IETF), The Transport Layer Security (TLS) Protocol Version 1.2, 2008, http://tools.ietf.org/html/rfc5246

[RFC 5321] Internet Engineering Task Force (IETF), Simple Mail Transfer Protocol, 2008, http://tools.ietf.org/html/rfc5321

[RFC 5340] Internet Engineering Task Force (IETF), OSPF for IPv6, 2008

[RFC 5424] Internet Engineering Task Force (IETF), The Syslog Protocol, 2009, http://tools.ietf.org/html/rfc5424

[RFC 5533] Internet Engineering Task Force (IETF), Shim6: Level 3 Multihoming Shim Protocol for IPv6, 2009, http://tools.ietf.org/html/rfc5533

[RFC 5569] Internet Engineering Task Force (IETF), IPv6 Rapid Deployment on IPv4 Infrastructures (6rd), 2010

[RFC 5771] Internet Engineering Task Force (IETF), IANA Guidelines for IPv4 Multicast Address Assignments, 2010, http://tools.ietf.org/html/rfc5771

[RFC 5798] Internet Engineering Task Force, Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, 2010,

[RFC 5905] Internet Engineering Task Force, Network Time Protocol Version 4: Protocol and Algorithms Specification, 2010, http://tools.ietf.org/html/rfc5905

[RFC 6105] Internet Engineering Task Force (IETF), IPv6 Router Advertisement Guard, 2011, http://tools.ietf.org/html/rfc6105

[RFC 6145] Internet Engineering Task Force (IETF), IP/ICMP Translation Algorithm, 2011, http://tools.ietf.org/html/rfc6145

[RFC 6146] Internet Engineering Task Force (IETF), Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, 2011, http://tools.ietf.org/html/rfc6146

[RFC 6147] Internet Engineering Task Force (IETF), DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, 2011, http://tools.ietf.org/html/rfc6147

[RFC 6169] Internet Engineering Task Force (IETF), Security Concerns with IP Tunneling, 2011, http://tools.ietf.org/html/rfc6169

[RFC 6275] Internet Engineering Task Force (IETF), Mobility Support in IPv6, 2011, http://tools.ietf.org/html/rfc6275

[RFC 6564] Internet Engineering Task Force (IETF), A Uniform Format for IPv6 Extension Headers, 2012, http://tools.ietf.org/html/rfc6564

[RFC 6751] Internet Engineering Task Force (IETF), Native IPv6 behind IPv4-to-IPv4 NAT Customer Premises Equipment, 2012, http://tools.ietf.org/html/rfc6751

[RFC 6830] Internet Engineering Task Force (IETF), The Locator/ID Separation Protocol (LISP), 2013, http://tools.ietf.org/html/rfc6830

[RFC 6890] Internet Engineering Task Force (IETF), Special-Purpose IP Address Registries, 2013, http://tools.ietf.org/html/rfc6890

[RFC 6946] Internet Engineering Task Force (IETF), Processing of IPv6 "Atomic" Fragments, 2013, http://tools.ietf.org/html/rfc6946

[RFC 6980] Internet Engineering Task Force (IETF), Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery, 2013, http://tools.ietf.org/html/rfc6980

[RFC 7045] Internet Engineering Task Force (IETF), Transmission and Processing of IPv6 Extension Headers, 2013, http://tools.ietf.org/html/rfc7045

[RFC 7059] Internet Engineering Task Force (IETF), A Comparison of IPv6-over-IPv4 Tunnel Mechanisms, 2013, http://www.ietf.org/rfc/rfc7059.txt

[RFC 7112] Internet Engineering Task Force (IETF), Implications of Oversized IPv6 Header Chains, 2014, http://tools.ietf.org/html/rfc7112

[RFC 7113] Internet Engineering Task Force (IETF), Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard), 2014, http://tools.ietf.org/html/rfc7113

[RFC 7217] Internet Engineering Task Force (IETF), A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), 2014, http://www.ietf.org/rfc/rfc7217.txt

[RIPE-501] Jan Žorž, Sander Steffann, Requirements For IPv6 in ICT Equipment, 2010, http://www.ripe.net/ripe/docs/ripe-501

[RIPE-554] Merike Käo, Jan Žorž, Sander Steffann, Requirements For IPv6 in ICT Equipment, 2012, http://www.ripe.net/ripe/docs/ripe-554

[SINA] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sichere Inter-Netzwerk Architektur (SINA), 2003, https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sina/sina.html

[Syslog] Institute of Electrical and Electronics Engineers, Security Issues in Network Event Logging (syslog), 2007, http://www.ietf.org/html.charters/syslog-charter.html

[TR-S-WLAN] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie Sicheres WLAN, 2005, https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/TechnischeRichtlinien/trwlan/index_htm.html

[TR-TLS] Bundesamt für Sicherheit in der Informationstechnik (BSI), Kryptographische Verfahren und Schlüssellängen Teil 2: Verwendung von Transport Layer Security, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.html

10 Anhang

10.1 Varianten der Grundarchitektur

In Abschnitt 5 wurde eine sichere Grundarchitektur für eine große Organisation mit normalem Schutzbedarf vorgestellt. Darüber hinaus werden in Abschnitt 7 ausgehend von der Grundarchitektur verschiedene Architektur- und Konfigurationsvarianten beschrieben. Dort findet man Möglichkeiten, wie sich einerseits kleine, unkritische IT-Infrastrukturen mit moderatem Aufwand realisieren lassen, andererseits kann aber auch einem großen Unternehmen mit hohem Schutzbedarf durch ergänzende Maßnahmen oder modulare Erweiterungen entsprochen werden.

Eine Abweichung von der Grundarchitektur hat jedoch Auswirkungen auf die Gefährdungen, denen das Unternehmen ausgesetzt ist. Hier muss der Nutzer abwägen, ob das unter Umständen erhöhte Restrisiko zu tragen ist oder nicht.

Im folgenden Anhang werden einige Beispiele vorgestellt, wie die Architektur an eine veränderte Unternehmensgröße oder einen veränderten Schutzbedarf angepasst werden kann und welche Konsequenzen dies auf die Gefährdungslage hat.

Für jedes vorgestellte Szenario werden Annahmen getroffen, die beispielhaft eine kleine, mittelgroße bzw. große Organisation kennzeichnen. Aufbauend auf diesen Annahmen werden Änderungsmöglichkeiten aufgegriffen, die bereits als Varianten in Abschnitt 7 vorgestellt worden sind. Die Änderung der Gefährdungslage des Unternehmens durch die Abweichung von der Grundarchitektur wird jeweils in einer Tabelle dargestellt.

In der Tabelle bedeutet „↑↑“ deutlich erhöhte Gefährdung, „↑“ erhöhte Gefährdung, „↔“ Gefähr-dung, wie bei Verwendung der Grundarchitektur, „↑↓“ teils erhöhte, teils erniedrigte Gefährdung, „↓“ verringerte Gefährdung und „↓↓“ deutlich verringerte Gefährdung.

10.1.1 Kleines Unternehmen

Annahmen

Für ein kleines Unternehmen werden folgende Annahmen getroffen:

- Keine Behörde
- Kein Anbieten von Webinhalten in der eigenen IT-Infrastruktur
- Wenige (< 50) Clients im internen Netz
- Wenige (< 3) interne Server mit nur wenig kritischen Inhalten
- Kein hoher Datenverkehr über das Internet
- Keine besonderen Anforderungen an die Ausfallsicherheit
- Geringe Wahrscheinlichkeit von Angriffen

10.1.1.1 Änderungen der Grundarchitektur für den normalen Schutzbedarf

Für den normalen Schutzbedarf können folgende Varianten verwendet werden:

- Da keine Webinhalte angeboten werden, entfallen Web-, DNS-Server und die Paketfilter (PF3, PF4, PF5).
- Einsatz eines einstufigen Sicherheits-Gateways (Variante 7.1.3 C)
- In-Band-Management für das interne Netz (Variante 7.1.3 B)
- Verwendung von global gültigen Adressen im internen Netz für Clients (Variante 7.1.3 L).

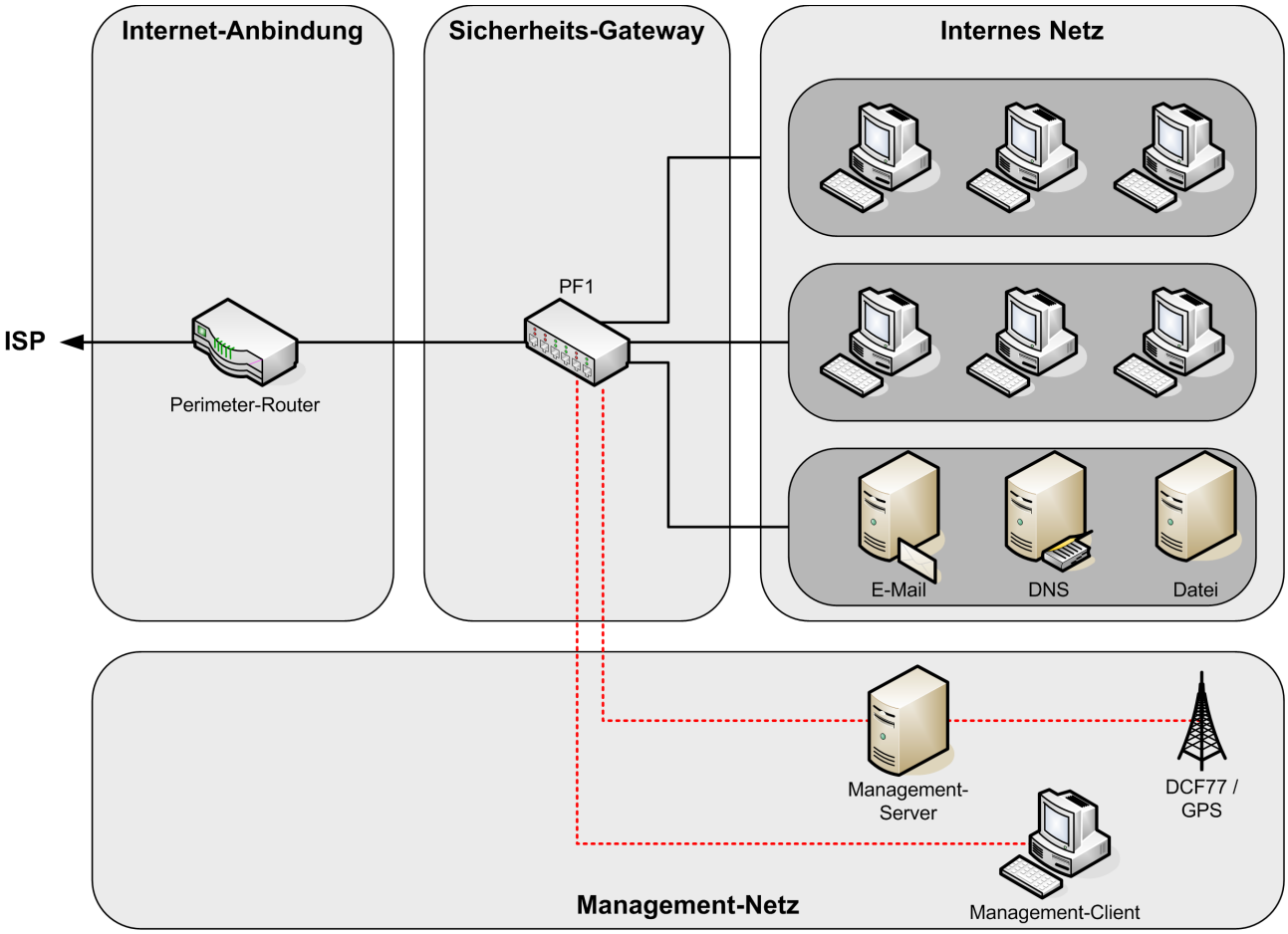

Abbildung 10.1: Beispiel für ein kleines Unternehmen mit normalem Schutzbedarf

Konsequenzen für die Gefährdung eines kleinen Unternehmens mit normalem Schutzbedarf

Bedrohung	*Gefährdung*	*Bemerkung*
Grundlegend (Sniffing, Spoofing, Hacking)	↑↑	Leicht auszuspähen, da keine PAP-Struktur, internes Netz kann bei DoS-Angriff ausfallen, kein Schutz gegen versehentliche Datenlecks
Netzzugangsschicht	↑	Geschützt nur durch einen Paketfilter
Internetschicht	↔	Kein erhöhtes Risiko
Transportschicht	↔	Kein erhöhtes Risiko
Anwendungsschicht	↑↓	Erhöhtes Risiko wegen In-Band-Management; verringertes Risiko, da keine externen Dienste angeboten werden

Tabelle 13: Gefährdungskonsequenzen - Kleines Unternehmen - normaler Schutzbedarf

10.1.1.2 Änderungen der Grundarchitektur für den hohen Schutzbedarf

Für den hohen Schutzbedarf können folgende Varianten verwendet werden:

- Da keine Webinhalte angeboten werden entfallen die entsprechenden Server (DNS, WWW).
- Zusammenlegung der Paketfilter PF2 und PF6 (Variante 7.1.3 A).
- Zusammenlegung der Paketfilter PF8/PF9 (Variante 7.1.3 A)

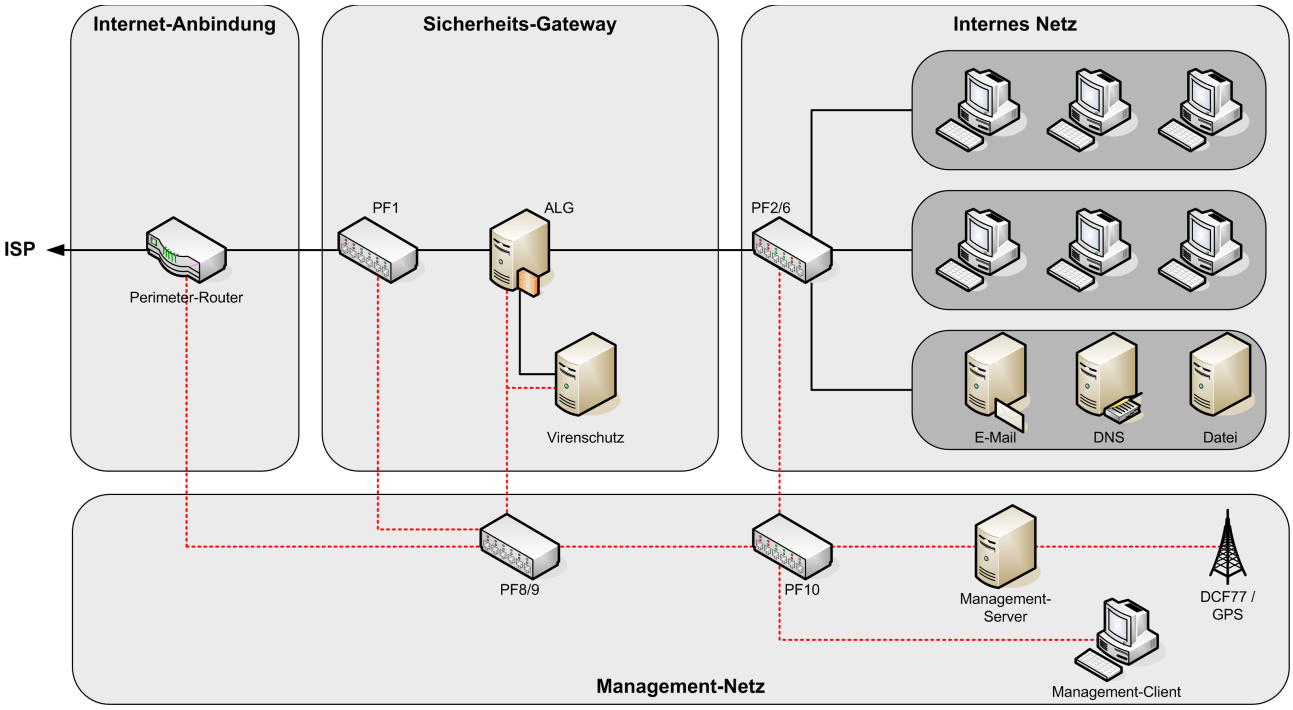

Abbildung 10.2: Beispiel für ein kleines Unternehmen mit hohem Schutzbedarf

Konsequenzen für die Gefährdung (kleines Unternehmen mit hohem Schutzbedarf)

Bedrohung	*Gefährdung*	*Bemerkung*
Grundlegend (Sniffing, Spoofing, Hacking)	↑	Leicht verringerter Schutz für das interne Netz, da ein Paket-filter weniger
Netzzugangsschicht	↑	Geschützt nur durch ein Paketfilter
Internetschicht	↔	Kein erhöhtes Risiko
Transportschicht	↔	Kein erhöhtes Risiko
Anwendungsschicht	↑↓	Erhöhtes Risiko wegen In-Band-Management; verringertes Risiko, da keine externen Dienste angeboten werden

Tabelle 14: Gefährdungskonsequenzen - Kleines Unternehmen - hoher Schutzbedarf

10.1.2 Mittelgroßes Unternehmen

Annahmen

Für ein mittelgroßes Unternehmen werden folgende Annahmen getroffen:

- Anbieten von Webinhalten
- Mittlere Anzahl (100 - 500) von Clients
- Normale Ausfallsicherheit
- Potenzielles Ziel von Angriffen

10.1.2.1 Änderungen für den normalen Schutzbedarf

Für den normalen Schutzbedarf können folgende Varianten verwendet werden:

- Paketfilter PF2 und PF6 werden zusammengelegt (Variante 7.1.3 A). Diese Variante ist in mittelgroßen Unternehmen nur für den normalen Schutzbedarf zu empfehlen, da sie die Angriffsfläche für Innentäter vergrößert.
- Zusammenlegen der Paketfilter PF3/PF5 (Variante 7.1.3 A)
- Zusammenlegung der Paketfilter PF8/PF9 (Variante 7.1.3 A)
- Zusammenlegung der Server WWW und DNS (Variante 7.1.3 D)
- In-Band-Management für das interne Netz (Variante 7.1.3 B)

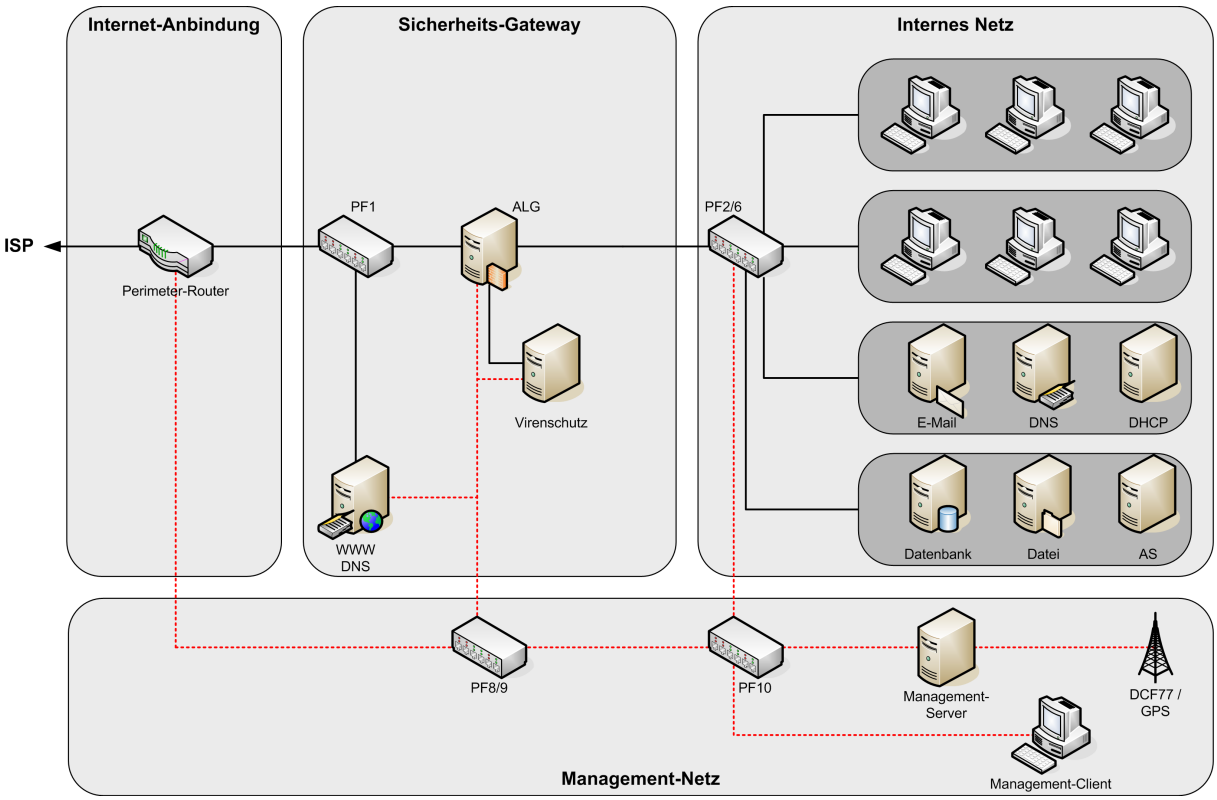

Abbildung 10.3: Beispiel für ein mittleres Unternehmen mit normalem Schutzbedarf

Konsequenzen für die Gefährdung (mittleres Unternehmen mit normalem Schutzbedarf)

Bedrohung	*Gefährdung*	*Bemerkung*
Grundlegend (Sniffing, Spoofing, Hacking)	↑	Leicht verringerter Schutz für das interne Netz, da ein Paketfilter weniger.
Netzzugangsschicht	↔	Kein erhöhtes Risiko
Internetschicht	↔	Kein erhöhtes Risiko
Transportschicht	↔	Kein erhöhtes Risiko
Anwendungsschicht	↑↓	Erhöhtes Risiko wegen In-Band-Management; erhöhtes Risiko gegen DoS-Angriffe wegen Zusammenlegung der extern sichtbaren Server

Tabelle 15: Gefährdungskonsequenzen - Mittleres Unternehmen - normaler Schutzbedarf

10.1.2.2 Änderungen für den hohen Schutzbedarf

Für den hohen Schutzbedarf können folgende Varianten verwendet werden:

- Mehrbeinige Anbindung an das Internet zur Erhöhung der Ausfallsicherheit (Variante 7.1.4 A)

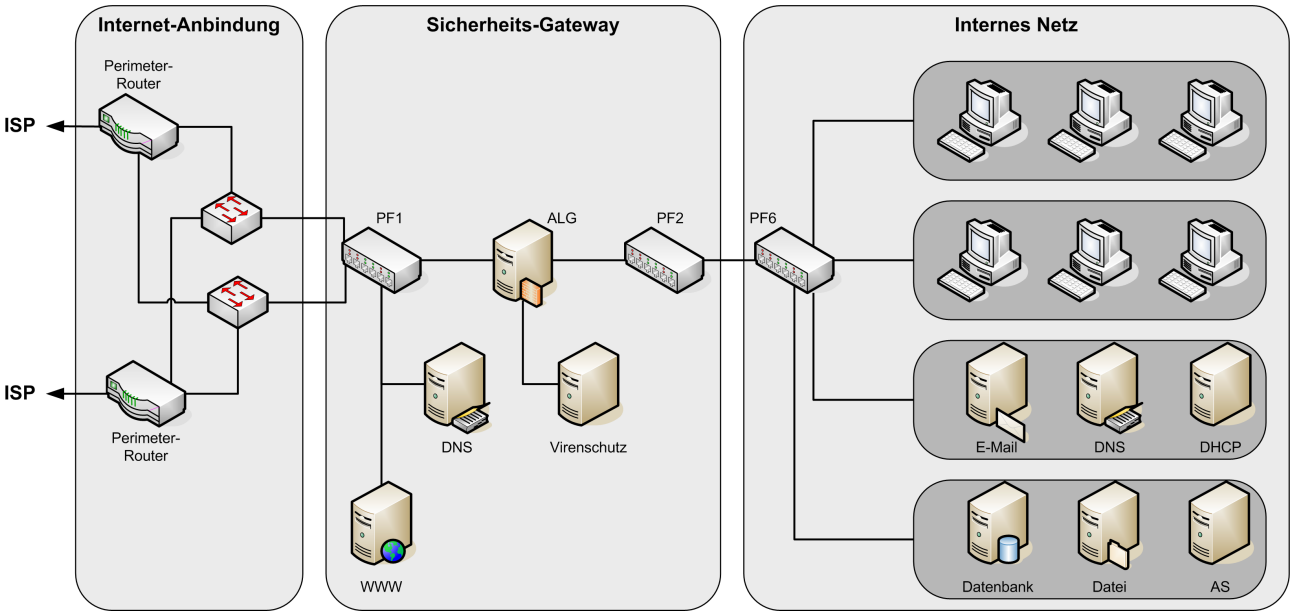

Abbildung 10.4: Beispiel für ein mittleres Unternehmen mit hohem Schutzbedarf

Konsequenzen für die Gefährdung (mittleres Unternehmen mit hohem Schutzbedarf)

Bedrohung	*Gefährdung*	*Bemerkung*
Grundlegend (Sniffing, Spoofing, Hacking)	↓	Verringerte Ausfallwahrscheinlichkeit durch redundante Internetanbindung.
Netzzugangsschicht	↔	Kein erhöhtes Risiko
Internetschicht	↔	Kein erhöhtes Risiko
Transportschicht	↔	Kein erhöhtes Risiko
Anwendungsschicht	↔	Kein erhöhtes Risiko

Tabelle 16: Gefährdungskonsequenzen - Mittleres Unternehmen - hoher Schutzbedarf

10.1.3 Großes Unternehmen

Für ein großes Unternehmen werden folgende Annahmen getroffen:

- Anbieten von komplexen Webinhalten, die auch von internen Anwendern verwendet werden
- große Anzahl (1000+) von Clients im internen Netz
- hoher Datenverkehr über das Internet
- erhöhte Ausfallsicherheit
- Ziel von Angriffen

10.1.3.1 Änderungen für den normalen Schutzbedarf

Für den normalen Schutzbedarf gilt die Grundarchitektur (siehe Abschnitt 5).

10.1.3.2 Änderungen für den hohen Schutzbedarf

Für den hohen Schutzbedarf können folgende Varianten verwendet werden:

- mehrbeinige Anbindung an das Internet und redundante Auslegung kritischer Teilbereiche zur Erhöhung der Ausfallsicherheit (Variante 7.1.4 A)
- getrennte äußere Paketfilter für das Nutzen und Anbieten von Internet-Diensten (Variante 7.1.3 K)
- Segmentierung einzelner, besonders kritischer interner Netze durch Sicherheits-Gateways (Variante 7.1.3 J
- Untergliederung des Management-Netzes in physisch getrennte Sicherheitszonen (Variante 7.1.3 G)

Konsequenzen für die Gefährdung des Unternehmens

Bedrohung	*Gefährdung*	*Bemerkung*
Grundlegend (Sniffing, Spoofing, Hacking)	↓↓	Verringerte Ausfallwahrscheinlichkeit durch redundante Auslegung kritischer Teilbereiche und mehrfache Internetanbindung
Netzzugangsschicht	↓	Höherer Schutz durch internes ALG
Internetschicht	↔	Kein erhöhtes Risiko
Transportschicht	↔	Kein erhöhtes Risiko
Anwendungsschicht	↔	Kein erhöhtes Risiko

Tabelle 17: Gefährdungskonsequenzen - Großes Unternehmen - hoher Schutzbedarf

Auf eine Darstellung des Netzdiagramms wurde verzichtet, da die redundante Auslegung von Komponenten und der (bei einem großen Unternehmen sinnvolle) Aufbau eines internen Backbones den Umfang einer hier darstellbaren Zeichnung übersteigt.

10.2 Empfehlungen zum Erstellen eines Adresskonzepts für IPv6

Für Umgebungen, die nicht als Service Provider (ISP) fungieren, kann sich – in Abhängigkeit von den spezifischen Randbedingungen – das Vorgehen beim Erstellen eines Adressplans an den folgenden Punkten orientieren.

10.2.1 Zielsetzung und Entscheidungskriterien

Während sich Adresskonzepte für IPv4 oft im Wesentlichen daran orientieren, die verfügbaren Adressen möglichst effizient zu nutzen, fällt diese Anforderung mit IPv6 weg. Stattdessen werden andere Kriterien relevant.

Der große Adressraum, der mit IPv6 innerhalb einer Site zur Verfügung steht, stellt intern so viele Subnetze zur Verfügung, dass ohne eine sorgfältige Netzwerkplanung die Gefahr besteht, dass die Routing-Tabellen der verwendeten Router diese nicht mehr effizient handhaben können. Das Prinzip der *vielen kleinen Subnetze* verschärft dieses potenzielle Problem noch zusätzlich. Ein Adresskonzept muss deshalb so angelegt sein, dass sich Routen effizient zu kürzeren Präfixen aggregieren lassen. Solange man von Anfang an beim Erstellen des Adresskonzeptes darauf achtet, lässt sich dieses potenzielle Problem gut beherrschen; eine nachträgliche Korrektur ist allerdings mit einigem Aufwand verbunden.

Darüber hinaus ist das primäre Ziel bei der Erstellung eines Adresskonzepts, die verfügbaren Adressen so zu nutzen, dass das Adresskonzept möglichst einfach wird. Schon die per Spezifikation auf /64 festgelegte Länge von Subnetz-Präfixen trägt deutlich zur Vereinfachung bei.

10.2.2 Global Routing Prefix und Unique-Local-Prefix

Einer Site werden mit IPv6 typischerweise Adressen in Form eines Global Routing Prefix mit einer Präfixlänge von /48 zugeteilt. Diesem Prefix wird in der Grundarchitektur ein weiteres /48-Präfix aus dem Adressbereich der Unique-Local-Adressen zur Seite gestellt, dass gemäß [RFC 4193] zufällig gewürfelt wird.

Um das Adresskonzept einfach zu halten, sollten grundsätzlich Subnetz-Präfixe parallel aus beiden /48-Präfixen zugeteilt werden, auch wenn nicht in allen Subnetzen global geroutete Adressen verwendet werden. Der Vorteil dieses Ansatzes ist, dass Subnetze immer anhand der 16 Bit Subnet ID identifiziert werden können, was die Handhabung in vielen Bereichen vereinfacht.

Sollen in einem Subnetz global geroutete Adressen zur Verfügung stehen, so werden auf den unmittelbar daran angeschlossenen Routern und Paketfiltern entsprechende Routen und Filterregeln aktiviert. Für Netze, die keine direkte Verbindung nach außen benötigen, werden nur Unique-Local Präfixe konfiguriert.

10.2.3 Aggregierte Routen

An diesem Punkt stehen 16 Bit für die Subnet ID jedes Subnetzes zur Verfügung. In kleinen Umgebungen, in denen sämtliche Subnetze über einen zentralen Router miteinander verbunden sind, können nun einfach den Subnetzen Subnet IDs zugeordnet werden, wie im folgenden Abschnitt beschrieben. In Umgebungen mit mehreren Routern, die untereinander über einen Backbone verbunden sind, muss der Adressraum so aufgeteilt werden, dass unnötig große Routing-Tabellen vermieden werden.

Der naheliegende Ansatz, einfach den gesamten verfügbaren Adressbereich „gleichmäßig aufzuteilen“, ist *nicht* empfehlenswert, weil er die weitere Entwicklung der Netztopologie in eine zu

diesem Zeitpunkt noch nicht erkennbare Richtung erschwert. Eine Verteilung in aufsteigender Reihenfolge nach Bedarf verhindert andererseits ein erfolgreiches Aggregieren. Grundsätzlich sollten bei der Planung Reserven für spätere Erweiterungen wie Neubauten und Ähnliches mit eingeplant werden.

Ein sinnvoller Kompromiss ist deshalb, aggregierte Routing-Prefixe so lang zu wählen, dass selbst bei vollständiger Nutzung des gegebenen Adressbereichs die Größe der Routing-Tabelle handhabbar bleibt. Abhängig von der verwendeten Router-Hardware wird dazu als Erstes festgelegt, wie viele Routen maximal auf den jeweiligen Routern eingerichtet werden sollen. Dann wird der verfügbare Adressraum in aggregierte Routing-Prefixe (mit einer Länge zwischen /49 und /63 Bits) so aufgeteilt, dass die Gesamtzahl der Routing-Prefixe die maximale Anzahl dieser Routen nicht überschreitet.

In der Praxis hat sich eine Präfix-Länge von /56 als Standardwert für die meisten am Markt erhältlichen Router bewährt; insbesondere bei sehr kleinen Routern sollte dieser Wert als Obergrenze angesehen werden.

In mehrstufigen Backbones wird das Verfahren für jede Ebene wiederholt. Bei nicht sauber hierarchisch strukturierten Backbone-Topologien muss im Einzelfall entschieden werden, wobei aber der beschriebene Ansatz zur Orientierung herangezogen werden kann.

10.2.4 Subnet IDs

Für die einzelnen Subnetze können Subnet IDs aus dem agreggierten Routing-Prefix fortlaufend vergeben werden.

In Umgebungen, in denen VLANs nach IEEE 802.1Q (Tagged VLANs) eingesetzt werden, kann darüber hinaus angestrebt werden, Subnet IDs und VLAN IDs gleich zu halten. In existierenden Installationen ist das oft nachträglich nicht möglich, aber gerade dann, wenn IPv6-Umgebungen „neben“ einer existierenden IPv4-Umgebung neu aufgebaut werden, kann dieses Vorgehen zur Vereinfachung des Netzaufbaus beitragen.

Einige Subnetze sollten für spezielle Zwecke reserviert werden:

Das Subnetz mit der Subnet ID 0 wird in manchen Fällen für die externe Anbindung benutzt, deshalb sollte es nicht für andere Zwecke verwendet werden.

Das Subnetz mit der Subnet ID 1 sollte für den primären DNS-Server verwendet werden. Diese Konvention ist nicht zwingend, erleichtert es aber neuen Kollegen und temporären externen Helfern, sich im Netz zu orientieren.

Ein Plan zur Vergabe von Subnet IDs sieht unter Berücksichtigung dieser Konventionen beispielsweise folgendermaßen aus:

Subnet ID	*VLAN ID*	*Autoconf?*	*Global geroutet?*	*Beschreibung*
0	---	Nein	Ja	Reserviert für externe Anbindung
1	1	Nein	Nein	Primärer DNS-Server
...	...	...	...	...

Tabelle 18: Adressplan

10.2.5 Router-Adressen

Router werden auf allen Netzwerkschnittstellen mit Adressen aus dem jeweiligen Subnetz konfiguriert. Dazu sollten zunächst alle vorhandenen Router durchnummeriert werden; wenn OSPF als dynamisches Routing-Protokoll eingesetzt wird, sollten Router-Nummer und OSPF Router ID gleichgesetzt werden. Soweit die Netzwerkschnittstellen der Router sequenziell durchnummeriert sind, sollte für die Netzwerkschnittstelle *I* des Routers *R* die Interface ID `0:feed:`*<R>*`:`*<I>* verwendet werden.

An dem konstanten Wert `feed` sind sie als Router erkennbar und sowohl der Router als solcher als auch seine Netzwerkschnittstelle lassen sich an der Adresse bereits erkennen.

In Fällen, in denen sich die Netzwerkschnittstellen des Routers nicht einfach durchnummerieren lassen, etwa weil unterschiedliche Schnittstellentypen verbaut sind, die von der jeweiligen Implementierung getrennt durchnummeriert werden, muss diese Konvention so erweitert werden, dass sie den jeweiligen Gegebenheiten gerecht wird.

Bei den Routern mancher Hersteller ist es unabhängig von IPv4 oder IPv6 eine etablierte Vorgehensweise, auf Routern eine zusätzliche Loopback-Schnittstelle mit einer gerouteten Adresse einzurichten. In diesem Fall sollten Empfehlungen des jeweiligen Herstellers umgesetzt werden.

Zwei Punkte sind dabei zu berücksichtigen, um eventuelle negative Auswirkungen auf die Router-Performance zu vermeiden:

- Jedem Router sollte eine eigene Subnet ID zugeordnet werden, weil Host-Routen bei IPv6 je nach verwendeten Routern erhebliche Performance-Einbußen nach sich ziehen können.
- Diese Subnet ID sollte außerdem aus einem aggregierten Routing-Prefix stammen, das insgesamt zu diesem Router geroutet wird, um unnötige Einträge in den Routing-Tabellen der anderen Router zu vermeiden.

10.2.6 Server- und Service-Adressen

Server sollten nicht per Autoconfiguration, sondern mit statischen Adressen konfiguriert werden. Ähnlich wie bei den Routern sollte eine einheitliche Konvention definiert werden.

Interface IDs sollten fortlaufend, mit `0:0:0:1` beginnend, vergeben werden. Dabei sollte jedem Server eine Interface ID für den Server als solchen und außerdem jedem Service eine weitere Interface ID zugewiesen werden. Dieses Vorgehen erleichtert ein späteres Verschieben einzelner Services zwischen verschiedenen Servern.

Für einen virtualisierten Server sollte für jeden virtuellen Server (Guest, domU) analog vorgegangen werden. Außerdem sollte dem physikalischen Server (Host) oder der privilegierten Domain (dom0) eine eigene Interface ID zugeteilt werden.

Analog zur in Abschnitt 10.2.4 beschriebenen Konvention zur Verwendung der Subnet ID `1` für den primären DNS-Server sollte dem primären DNS-Server die Interface ID `0:0:0:1` zugeteilt werden.

Anders als bei IPv4, wo vergebene und später wieder freigegebene Adressen oft erneut verwendet werden mussten, sollte bei IPv6-Adressen bzw. Interface IDs darauf verzichtet werden. Dies erleichtert die Verwaltung der vergebenen Interface IDs erheblich: Benutzte Adressen werden im DNS eingetragen und es muss lediglich an geeigneter Stelle – durchaus auch innerhalb des DNS – die nächste unbenutzte Interface ID verwaltet werden.

10.2.7 Beispiele mit Adressplänen

Im Folgenden sind die Beispiele für kleine Unternehmen aus Abschnitt 10.1.1 mit beispielhaften Adressen ausgestattet.

Kleines Unternehmen mit normalem Schutzbedarf

Für das kleine Unternehmen mit normalem Schutzbedarf aus Abbildung 10.1 muss für die Beispieladressen Folgendes beachtet werden:

- Der Präfix `2001:DB8::` ist durch den vom Provider zugewiesenen globalen Präfix zu ersetzen.
- Die Subnetze wurden nach folgender Tabelle definiert:

Subnetz	*Verwendung*
0	Zugang zum Internet
1	DNS-Dienste
2	Mail-Dienste
3	File-Dienste
1001	Client-Netz 1
1002	Client-Netz 2
FFF0	Management-Netz

Tabelle 19: Kleines Unternehmen – normaler Schutzbedarf - Subnetze

- Die Server werden gemäß den Empfehlungen in Abschnitt 10.2.6 nummeriert und die Router und Filter gemäß Abschnitt 10.2.5 nach Interfaces und Anschlüssen nummeriert.
- Insbesondere bei der Verwendung von Global-Unicast Adressen ist auf eine konsequente Filterung des eingehenden Verkehrs (hier an PF1) zu achten.

Abbildung 10.5 zeigt einen möglichen Adressplan.

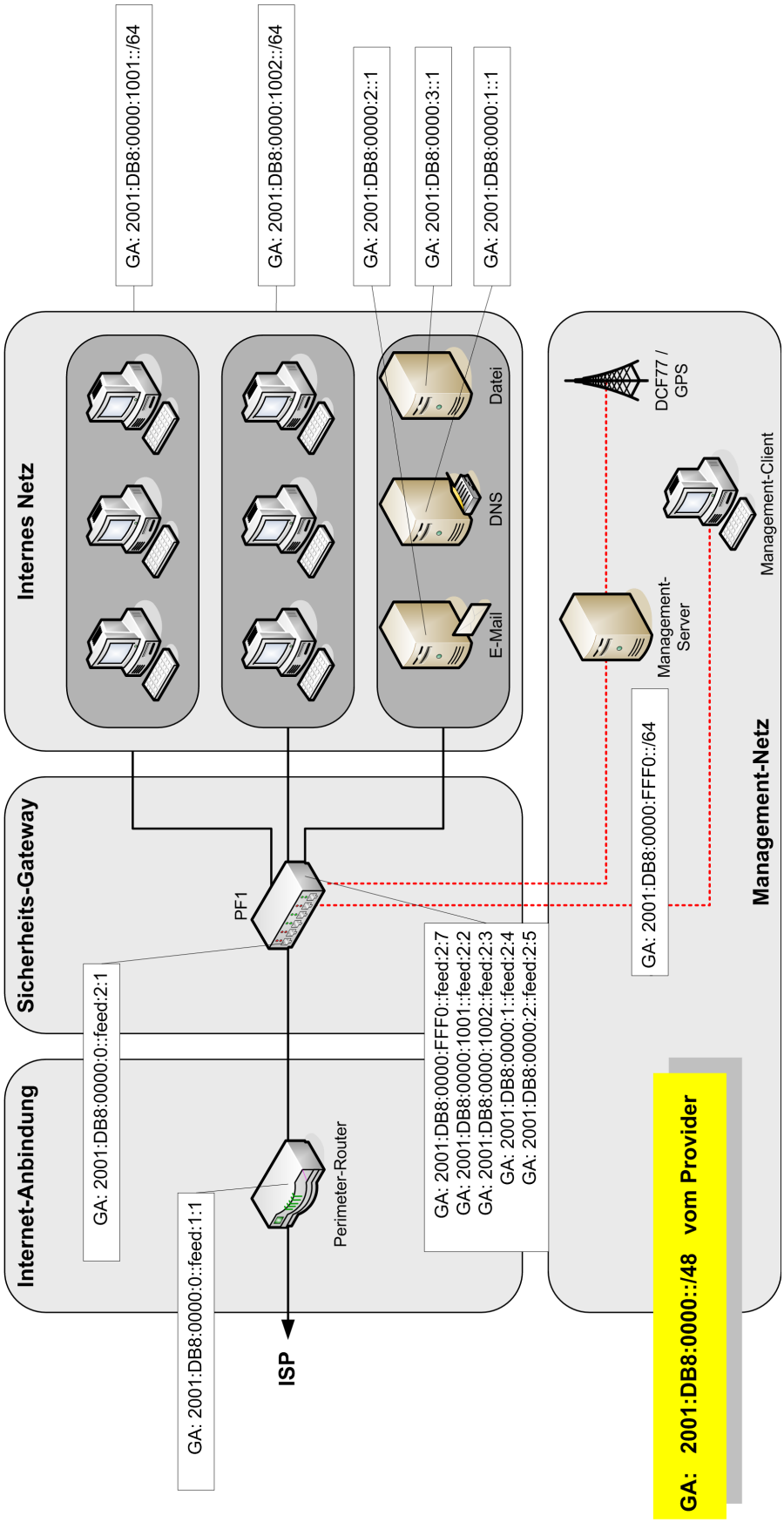

Abbildung 10.5: Beispielhafter Adressplan für das Beispiel aus 10.1.1.1

Kleines Unternehmen mit hohem Schutzbedarf

Für das kleine Unternehmen mit hohem Schutzbedarf aus Abbildung 10.2 muss für die Beispieladressen Folgendes beachtet werden:

- der Präfix `FD00:0000:0000::` ist durch den zu Beginn der Realisierung einmalig zufällig ausgewählten Wert (siehe Abschnitt 10.2.2) zu ersetzen.
- Der Präfix `2001:DB8::` ist durch den vom Provider zugewiesenen globalen Präfix zu ersetzen.
- Die Subnetze wurden nach folgender Tabelle definiert:

Subnetz	*Verwendung*
0	Zugang zum Internet
1	DNS-Dienste
2	Mail-Dienste
3	File-Dienste
10	Externe Seite ALG
11	Interne Seite ALG
12	Intern DMZ
1001	Client-Netz 1
1002	Client-Netz 2
FFF0	Management-Netz Server
FFF1 … FFF6	Management Teilnetze

Tabelle 20: Kleines Unternehmen – hoher Schutzbedarf - Subnetze

Die Server werden gemäß den Empfehlungen in Abschnitt 10.2.6 nummeriert und die Router und Filter gemäß Abschnitt 10.2.5 nach Interfaces und Anschlüssen nummeriert.

Abbildung 10.6 zeigt einen möglichen Adressplan.

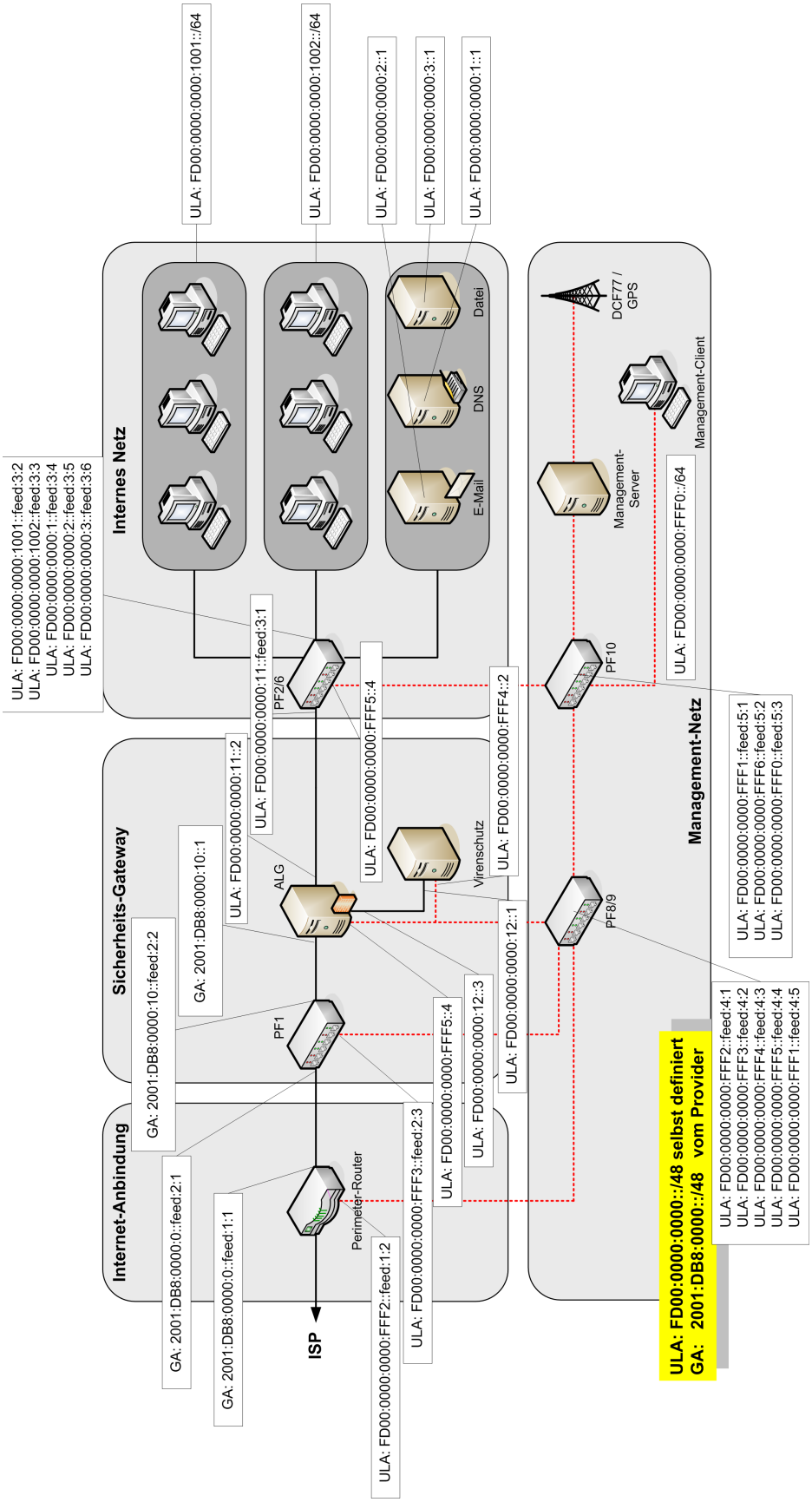

Abbildung 10.6: Bsp-Adressplan für ein kleines Unternehmen mit hohem Schutzbedarf