

Organisatorische Maßnahmen:

1. Zugangskontrolle zu Server- und Verteilerräumen und gesondert den hierin befindlichen Schränken
2. Einweisung der Benutzer, z.B. in Passwortrichtlinien
3. Gewährung eines Benutzerkontos nur nach Quittierung einer Benutzerordnung
4. Gewährung des Netzzugangs nur nach vorheriger, passwortgesicherter Anmeldung

Technische Maßnahmen:

1. Einschränkung der technischen Möglichkeiten bei den Clients (z.B. unkontrolliertes Booten vom USB-Speicher)
2. Verteilung aller Netzdienste auf möglichst viele Servermaschinen, insbesondere eigene Nameserver
3. Abschalten nicht gebrauchter Serverprozesse auf jeder Servermaschine
4. Verzicht auf unsichere Dienste. Beispiel: Bei Telnet wird das Passwort im Klartext übertragen und kann insbesondere bei Verwendung von Hubs leicht ausgespäht werden ⇒ Ersatz von Telnet durch SSH (Secure Shell, Telnetersatz mit guter Verschlüsselung) und ggf. Ersatz von Hubs durch Switches
5. Einsatz spezieller Überwachungssoftware mit dem Ziel, unautorisierte (erfolgte) Eingriffe aufzuspüren (Intrusion Detection System)
6. Einsatz von Firewalls
7. Installation von Verschlüsselungssoftware auf Systemebene (VPN) und Anwendungsebene
8. Zentralisierte Authentifizierung

Ausführlichere und breiter angelegte Handlungsempfehlungen können wiederum dem BSI-Maßnahmenkatalog entnommen werden. Den Punkten 6 und 7 sind die nachfolgenden Unterkapitel gewidmet.

1.7.2.3 Technische Mittel der IT-Sicherheit

Firewall

Ausführlicher wird nun ein Baustein betrachtet, der in jeder Sicherheitskonzeption unerlässlich ist: die **Firewall** (engl. für Brandschutzmauer) – der Katalog spricht im Baustein B 3.301 allerdings von einem **Sicherheitsgateway**, um anzudeuten, dass die Schutzfunktion oft nicht mehr von nur einem Gerät, sondern von einer Reihe von IT-Systemen ausgeübt wird.¹

Die Firewall soll eine Hürde zwischen zwei Netzen darstellen, die für Unberechtigte möglichst unüberwindlich ist. Sie ist meistens auf dem Router zwischen lokalem Netz und öffentlichem Weitverkehrsnetz angesiedelt (Bild 1.185). Für die Konstruktion einer Firewall stehen grundsätzlich zwei Elemente zur Verfügung: Proxies und Paketfilter.

¹ IT-Grundschutz-Kataloge, 2011, S. 190 ff.

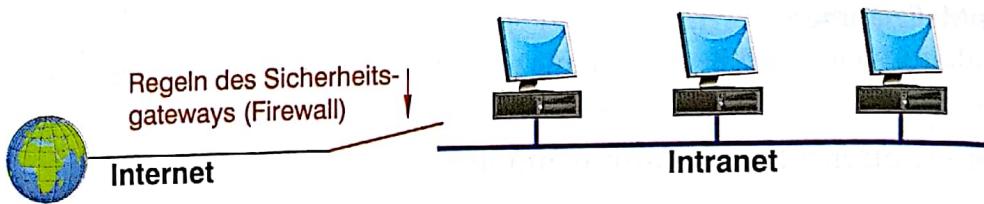


Bild 1.185: Brandschutzmauer zwischen Netzen unterschiedlicher Vertrauenswürdigkeit

Proxies wurden bereits kurz in Kap. 1.4.4.3 behandelt. Sie werden auch „Application Level Gateways“ (BSI), abgekürzt ALG, oder „Application Firewall“ genannt, weil sie auf der OSI-Schicht 7 („Application Layer“) arbeiten. Man muss entweder für jedes Anwendungsprotokoll einen gesonderten Proxy betreiben oder der Universal-Proxy wird kompliziert. Eventuell muss Anwendungssoftware angepasst werden. Als Vorteile sind jedoch in der BSI-Maßnahmen-Empfehlung M 2.75 genannt:

- „Oft geringere Anzahl von Programmierfehlern als in den vom Proxy geschützten Client- bzw. Serverdienstprogrammen
- Filterung einzelner Protokollbefehle (z. B. bei HTTP der Befehl POST) in Abhängigkeit von der Parametrisierung der Befehle, der Zeit und des Benutzers möglich
- Entfernung unerwünschter Inhalte in den übertragenen Daten
- Abwehr von Angriffen, die auf fehlerhaften Header-Daten beruhen
- Ersetzung der Absender-Adresse eines weitergeleiteten IP-Pakets durch die IP-Adresse der Netzschwittersstelle, über die das Paket den Proxy verlässt. Dadurch werden IP-Adressen des vertrauenswürdigen Netzes verheimlicht. Im DNS braucht zudem nur eine IP-Adresse eingetragen werden.
- Erzwingen einer starken Authentisierung möglich
- Umfangreiche Protokollierungsmöglichkeiten. Für jede Verbindung auf der Anwendungsebene kann protokolliert werden:
 - Benutzeridentifikation
 - IP-Adresse des Quell- und Zielrechners
 - Portnummern
 - Zeit und Datum
- In Abhängigkeit vom Dienst können weitergehende Informationen protokolliert werden (z. B. URL bei HTTP).“

Paketfilter („Paketfilter Firewalls“) sind Router, die ihre Weginformation (*Routing*) überhaupt nur dann zum Einsatz bringen, wenn vorgegebene Richtlinien (*Policy of Forwarding*) dies zulassen. Paketfilter inspizieren die einzelnen Felder in den TCP/UDP und den IP-Headern und vergleichen sie mit ihrem Regelwerk. So kann ein Paketfilter beispielsweise dazu konfiguriert werden, sowohl

- UDP-Pakete an Port 53 nur dann durchzulassen, wenn sie von einem Host mit vorgegebener IP-Adresse stammen (der standardmäßige NS des Providers etwa), als auch
- TCP-Verbindungen von außen nach innen generell nicht zuzulassen (Inspektion des SYN-Flags), es sei denn, sie stammen aus einem ganz bestimmten Subnetz, oder
- abgehende Verbindungsaufbaupakete aus bestimmten internen Subnetzen an einen bestimmten externen SMTP-Server zuzulassen, an einen anderen aber zu sperren und
- alle oder manche Aktionen zu protokollieren.

Details folgen weiter unten.

Wenn der Paketfilter darüber hinaus „weiß“, um was für Pakete es sich handelt, z.B. FTP-Datenverbindungen, die in einer bestehenden FTP-Steuerverbindung veranlasst worden sind, dann spricht man von **Stateful Inspection** und nennt den Filter „**Stateful Inspection Firewall**“.

Auf diesem Wege können die Datenflüsse durch den Paketfilter sehr fein „kanalisiert“ werden, nachteilig ist jedoch die mit der Anzahl der Regeln zunehmende Kompliziertheit und die daraus resultierende Fehleranfälligkeit. Daneben können den Nutzern Unannehmlichkeiten entstehen (z.B. bei FTP). Gegen einige Bedrohungen können Firewalls nicht eingesetzt werden:

1

- Angriffe aus dem eigenen Netz
- Kommunikationsbeziehungen, die an der Firewall vorbeigehen, z.B. durch zusätzliche Modem-Einwahl einer Station des eigenen Netzes
- Völlig neuartige Angriffstechniken
- Computerviren, Trojaner etc.

Im BSI-Baustein B 3.301 wird von folgender Gefährdungslage für ein Sicherheitsgateway ausgegangen:

- „Organisatorische Mängel
 - G 2.24 Vertraulichkeitsverlust schutzbedürftiger Daten des zu schützenden Netzes
 - G 2.101 Unzureichende Notfallvorsorge bei einem Sicherheitsgateway
- Menschliche Fehlhandlungen
 - G 3.3 Nichtbeachtung von Sicherheitsmaßnahmen
 - G 3.9 Fehlerhafte Administration von IT-Systemen
 - G 3.38 Konfigurations- und Bedienungsfehler
- Technisches Versagen
 - G 4.8 Bekanntwerden von Softwareschwachstellen
 - G 4.10 Komplexität der Zugangsmöglichkeiten zu vernetzten IT-Systemen
 - G 4.11 Fehlende Authentisierungsmöglichkeit zwischen NIS-Server und NIS-Client
 - G 4.12 Fehlende Authentisierungsmöglichkeit zwischen X-Server und X-Client
 - G 4.20 Überlastung von Informationssystemen
 - G 4.22 Software-Schwachstellen oder Fehler
 - G 4.39 Software-Konzeptionsfehler
- Vorsätzliche Handlungen
 - G 5.2 Manipulation an Informationen oder Software
 - G 5.9 Unberechtigte IT-Nutzung
 - G 5.18 Systematisches Ausprobieren von Passwörtern
 - G 5.24 Wiedereinspielen von Nachrichten
 - G 5.25 Maskerade
 - G 5.28 Verhinderung von Diensten
 - G 5.39 Eindringen in Rechnersysteme über Kommunikationskarten
 - G 5.48 IP-Spoofing
 - G 5.49 Missbrauch des Source-Routing

- G 5.50 Missbrauch des ICMP-Protokolls
- G 5.51 Missbrauch der Routingprotokolle
- G 5.78 DNS-Spoofing
- G 5.143 Man in the Middle Angriff¹

Dagegen steht das Bündel von Maßnahmen-Empfehlungen, hier auszugsweise nur die Qualifizierungsstufe A (Bild 1.180):

■ „Planung und Konzeption“

- M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways
- M 2.71 Festlegung einer Policy für ein Sicherheitsgateway
- M 2.299 Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
- M 2.476 Konzeption für die sichere Internetanbindung

■ „Beschaffung“

- M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways (s.u.)
- M 2.74 Geeignete Auswahl eines Paketfilters
- M 2.75 Geeignete Auswahl eines Application-Level-Gateways

■ „Umsetzung“

- M 2.76 Auswahl und Einrichtung geeigneter Filterregeln
- M 2.77 Integration von Servern in das Sicherheitsgateway

■ „Betrieb“

- M 2.78 Sicherer Betrieb eines Sicherheitsgateways
- M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten
- M 5.39 Sicherer Einsatz der Protokolle und Dienste
- M 5.46 Einsatz von Stand-alone-Systemen zur Nutzung des Internets
- M 5.59 Schutz vor DNS-Spoofing bei Authentisierungsmechanismen
- M 5.70 Adressumsetzung NAT (Network Address Translation)
- M 5.120 Behandlung von ICMP am Sicherheitsgateway²

Exemplarisch wird nun aus der Maßnahme M 2.73 zitiert:

„Im Wesentlichen bieten sich zwei sinnvolle Grundstrukturen (Bild 1.186) an, die als Anhaltspunkt zum Aufbau eines Sicherheitsgateways dienen können. Die grundlegenden Strukturen werden im Folgenden erläutert.“

1. Paketfilter – Application-Level-Gateway – Paketfilter (P-A-P)

Bei dieser Grundstruktur werden ein Paketfilter, ein Application-Level-Gateway (ALG) und ein weiterer Paketfilter „hintereinandergeschaltet“, sodass jeglicher Datenverkehr alle drei Komponenten überqueren muss. In der folgenden Abbildung sind beispielhaft einige Möglichkeiten zur Einrichtung von „demilitarisierten Zonen“ (DMZ) eingezeichnet, in denen weitere Komponenten des Sicherheitsgateways in einer geschützten Umgebung betrieben werden können. [...]“

Die DMZ ist der Bereich zwischen den Grenzen (ein „Niemandsland“). Hier platzierte Servermaschinen heißen auch **Bastion Host** und hosten z. B. einen öffentlich erreichbaren Webserver.

¹ IT-Grundschutz-Kataloge, 2011, S. 190

² IT-Grundschutz-Kataloge, 2011, S. 193

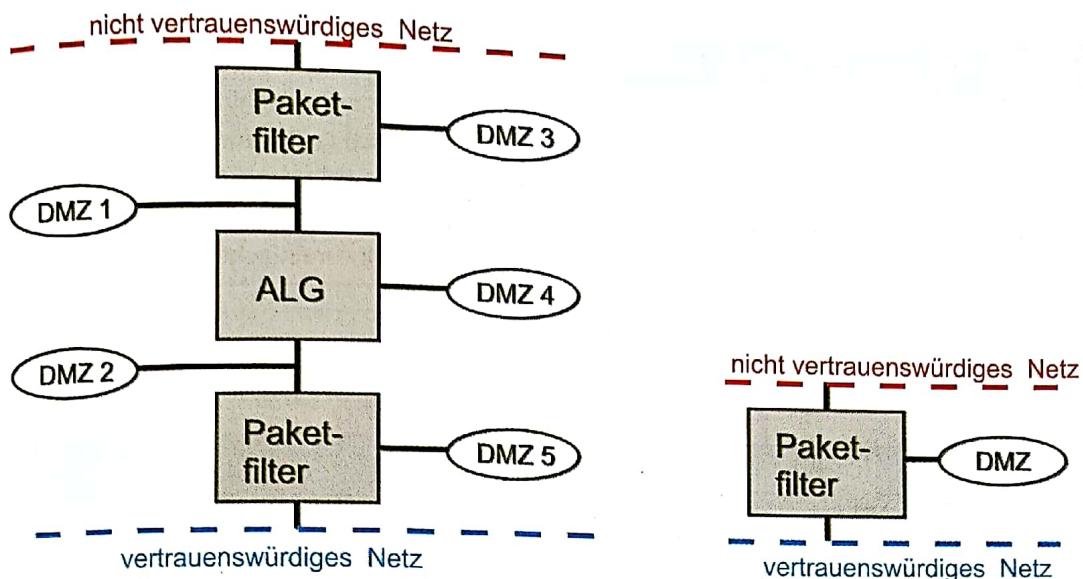


Bild 1.186: Mehrstufiger Aufbau einer Firewall und einstufiger Aufbau

2. Nur Paketfilter

Die einfachste Grundstruktur eines Sicherheitsgateways besteht aus nur einem Paketfilter. Das Grundproblem bei der Filterung der Kommunikation alleine mit einem Paketfilter liegt darin, dass die Entscheidung darüber, ob ein Zugriff erlaubt oder abgewiesen werden soll, anhand der leicht zu fälschenden Daten aus den Headern der verschiedenen IP-basierten Protokolle gefällt wird. Einsatzbereiche sind deshalb vor allem:

- Trennung zweier Netze, falls sich das Maß der Vertrauenswürdigkeit dieser Netze nur wenig voneinander unterscheidet (z. B. Trennung des Internets von einem Intranet mit nur geringem Schutzbedarf)
- Trennung zweier organisationsinterner Netze
- Privater Bereich (Schutz des „heimischen“ Rechners beim Zugriff auf das Internet) [...]¹

Die Eigenschaften dieser Grundtypen werden in Bild 1.187 einander gegenübergestellt:

Paketfilter – ALG – Paketfilter (P-A-P)	Paketfilter
<ul style="list-style-type: none"> – Kann als Grundlage für die Sicherstellung eines hohen Sicherheitsniveaus dienen. – Hohe Komplexität aufgrund der Verwendung mehrerer Module – Nicht in jedem Anwendungszusammenhang einsetzbar. Beispielsweise kann IPSEC-Verkehr nicht über einen TCP/IP-Proxy geleitet werden. – Einfache Erweiterungsmöglichkeiten, z. B. kann ein Virenschanner oder ein Spam-Filter ohne großen Aufwand an das ALG angeschlossen werden. 	<ul style="list-style-type: none"> – Kein hohes Sicherheitsniveau, höchstens für normalen Schutzbedarf ausreichend – Gegenüber einem P-A-P-Aufbau relativ einfache Administration – Geringe Investitionskosten (kostenlose Software unter verschiedenen Betriebssystemen vorhanden) [Anm.d.Verf.: siehe unten] – Keine wesentliche Einschränkung des maximalen Datendurchsatzes am Netzübergang – Einfache, grundlegende Absicherung

¹ IT-Grundschutz-Kataloge, 2011, S. 1262

Paketfilter – ALG – Paketfilter (P-A-P)	Paketfilter
<ul style="list-style-type: none"> – Die Ausnutzung von Sicherheitslücken in Clientsoftware kann teilweise verhindert werden. – Umfangreiche Protokollierungsmöglichkeiten 	<ul style="list-style-type: none"> – Integration auf einem zu schützenden Rechner theoretisch möglich (z. B. kann ein Web-Server gleichzeitig als Paketfilter genutzt werden) – Bereitstellung neuer Dienste gegenüber P-A-P-Aufbau stark vereinfacht

Bild 1.187: Vergleich der Grundstrukturen von Firewalls nach BSI

Darüber hinaus werden „Hinweise zur Auswahl einer Grundstruktur“ gegeben (Bild 1.188):

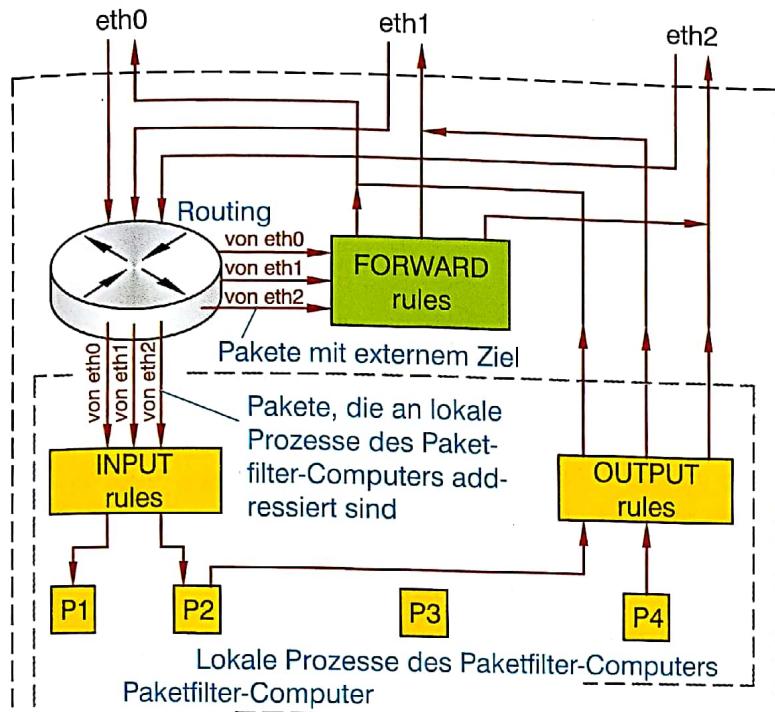
Einsatzgebiet ¹	Empfohlener Aufbau
Trennung zweier Teilnetze des internen Netzes mit gleichem Schutzbedarf	Paketfilter. Bei normalem Schutzbedarf genügt ein Router mit integrierter Paketfilter-Funktion.
Trennung zweier Teilnetze des internen Netzes mit unterschiedlichem Schutzbedarf (insbesondere: Teilnetz mit hohem Schutzbedarf und Teilnetz mit normalem Schutzbedarf)	Mindestens Paketfilter. Falls vom weniger vertrauenswürdigen Netz aus auf einen Dienst im Netz mit hohem Schutzbedarf zugegriffen werden soll, dann ist es empfehlenswert, diesen Zugriff über ein ALG abzusichern.
Trennung eines Teilnetzes mit besonderen Sicherheitsanforderungen von einem anderen internen Netz	Mehrstufiger Aufbau aus Paketfilter – ALG – Paketfilter. Zusätzlich ist in diesem Fall eine ergänzende Sicherheitsbetrachtung notwendig. Der mehrstufige Aufbau kann hier nur als Grundlage für sehr hohe Sicherheit dienen. In der Regel werden zusätzliche Maßnahmen notwendig sein, für die aber keine allgemeinen Empfehlungen möglich sind.
Trennung des eigenen Netzes vom Internet	Grundsätzlich mehrstufiger Aufbau aus Paketfilter – ALG – Paketfilter. In Ausnahmefällen (sehr kleines Netz, kein hoher Schutzbedarf) kann ein Paketfilter (beispielsweise in Verbindung mit einem NAT-Router) ausreichend sein. Zumindest für Dienste wie E-Mail und HTTP wird der Einsatz eines entsprechenden Proxyservers dringend empfohlen. Bei normalem Schutzbedarf kann gegebenenfalls auf den inneren Paketfilter verzichtet werden. Falls kein P-A-P-Aufbau gewählt wird, wird eine zusätzliche Risikobetrachtung dringend empfohlen.

Bild 1.188: Auswahl von Firewall-Strukturen nach BSI

Mit „kostenlose Software unter verschiedenen Betriebssystemen vorhanden“ kann beispielweise der *Netfilter* (Bild 1.189) von Linux gemeint sein, der mit dem Frontend *Iptables* konfiguriert wird. Der Linux-Kernel behandelt IP-Pakete gemäß den Eintragungen in drei Tabellen (daher auch der Name *Iptables*). In jeder Tabelle existieren Regelketten (*Ipchains*), die Verfahrensregeln (*Rules*) für die Paketbehandlung enthalten (können). Treffen Regelmale (*Matches*) zu, wird das Paket einer Zielbestimmung (*Target*) zugeführt (Bild 1.190). Anfangs sind diese Ketten leer, d. h., mangels spezieller Regeln ist alles mög-

¹ IT-Grundschutz-Kataloge, 2011, S. 1261ff.

lich. Eine der drei Tabellen heißt **NAT**, in ihr wird die Network Address Translation durchgeführt (siehe dazu auch Kap. 1.4.3.5). Eine weitere heißt **Mangle**, sie dient für spezielle Paketbehandlungen (to mangle: zerstückeln).



1

Bild 1.189: Vereinfachtes Funktionsmodell des Linux-Netfilters

Für die Paketfilterung dient die Tabelle **Filter**. Sie wird bei Konfigurationsbefehlen standardmäßig verwendet, wenn nicht über die Option `-t` eine andere Tabelle für diesen Befehl festgelegt wird. Die Tabelle besitzt drei Regelketten: INPUT, OUTPUT und FORWARD. Der Einflussbereich geht aus Bild 1.189 hervor.

Wichtigste Paket-Merkmale (Matches) sind: Quell-IP-Adresse/Ziel-IP-Adresse, Protokoll (UDP/TCP), Quell- und Zielport, gesetzte Flags (SYN, ACK ...) etc.

Built-in Targets	Bedeutung
DROP	Das Paket wird ohne Weiteres verworfen.
ACCEPT	Das Paket wird durchgeleitet.
REJECT	Wie DROP, meist mit ICMP-Fehlermeldung an den Absender.
LOG	Es wird ein Vermerk im sogenannten Kernellogging bewirkt.

Bild 1.190: Standardaktionen im Paketfilter

Andere, gerade auch benutzerdefinierte Chains können selbst als Target dienen. Filterregeln für einen einfachsten Paketfilter¹ ohne DMZ könnten so aussehen, wie der nächste Absatz zeigt. Diese Befehlsfolge kann in ein Initialisierungsskript für die Runlevel 3 und 5 eingebunden werden. Auf sie aufbauend können weitere Eigenschaften implementiert werden (siehe weiter oben, # leitet Kommentare ein):

¹ [http://netfilter.org/documentation/HOWTO/de_packet-filtering-HOWTO-5.html](http://netfilter.org/documentation/HOWTO/de	packet-filtering-HOWTO-5.html) [25.6.2013]

```
## Regelkette 'block' erstellen, die neue Verbindungen blockt - \
es sei denn, sie kommen von innen (eth0)
iptables -N block # Neue chain (in Tabelle filter)

# fügt Regel in Kette block ein (-A: ADD)
# -m matches 'state'; hier Zustände ESTABLISHED und RELATED
# ESTABLISHED meaning that the packet is associated with a \
connection which has seen packets in both directions
# RELATED meaning that the packet is starting a new connection\ but is associated with an existing connection,
# such as FTP -data transfer
# -j jumps to a target, hier: ACCEPT
iptables -A block -m state --state ESTABLISHED,RELATED -j ACCEPT

# NEW meaning that the packet has started a new connection
# -i ! eth1: Das in-Interface ist nicht (!) eth1
iptables -A block -m state --state NEW -i ! eth1 -j ACCEPT

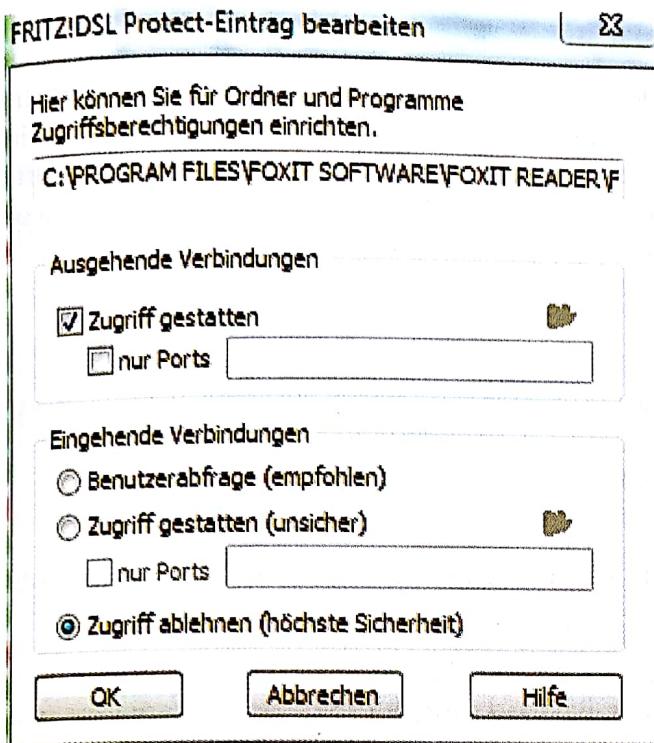
# Letzte Regel in der Kette bestimmt Standardverhalten: Keine \
akzeptable Eigenschaft festgestellt, dann verwerfen!
iptables -A block -j DROP

## Von INPUT und FORWARD Ketten zu dieser Kette springen
iptables -A INPUT -j block
iptables -A FORWARD -j block
```

Appliances und Personal Firewalls

Wenn die komplette Funktionalität einer Firewall (Paketfilter + ALG) in einem (embedded) Gerät zusammengefasst wird, dann spricht man von einer **Firewall Appliance** oder externen Firewall oder – fälschlich – von einer Hardware-Firewall. Dies ist die professionellste Lösung, weil die Firewall-Software in diesem Fall auf proprietären Betriebssystemen oder gehärteten Linuxderivaten aufsetzt.

Im Gegensatz dazu spricht man von einer **Personal Firewall**, wenn diese Software das Betriebssystem des Arbeitsplatzrechners ergänzt, um insbesondere zu verhindern, dass Software unkontrolliert eine Verbindung ins Internet herstellt.



1

Bild 1.191: Akkreditierung einer Anwendung mit einer Personal Firewall

Solche Verbindungen sind aus Sicht einer externen Firewall nämlich meist zulässig. Dazu muss der Anwender entweder jeden Verbindungsaufbau im Netz einzeln akzeptieren oder einzelnen Anwendungen eine Akkreditierung erteilen (Bild 1.191).

In dem seltener werdenden Fall, dass ein (meist privater) Rechner ohne zwischengeschalteten Router ins Internet geht, muss die Personal Firewall natürlich auch Verbindungen von außen nach innen generell abblocken.

VPN

Eines der primären Ziele der Vernetzung ist die Überbrückung von räumlicher Entfernung. Heute besteht vielfach der Wunsch, Außendienstmitarbeiter mit ihren Notebooks, Teleworker mit ihren PCs und entfernte Niederlassungen und Geschäftspartner mit ihren LANs an das firmeneigene Netz anzukoppeln. Dies kann vorteilhaft mit VPNs über das Internet geschehen, wie in Kapitel 3.6.2 beschrieben und in Bild 3.69 dargestellt.

Dem steht allerdings ein großer Nachteil gegenüber: Das Internet ist öffentlich – und damit alles andere als privat!

- Schutzmaßnahmen wie Zugangskontrollen sind nicht durchführbar:
 - Unerlaubter Zugriff auf lokale Einrichtungen von außen muss abgewehrt werden (Firewall).
 - **Authentizität** der Kommunikationspartner und **Integrität** (Unverfälschtheit) der Daten muss gewährleistet sein.
 - Übertragene Daten müssen durch **Verschlüsselung** gegen Ausspähung geschützt werden.

Als Methoden der Netzkopplung bieten sich an:

1. Kopplung auf der Sicherungsschicht: Frames der OSI-Schicht 2 werden komplett in IP-Pakete verpackt. In der Vergangenheit gab es dazu einige proprietäre Ansätze wie das PPTP (Point-to-Point Tunneling Protocol) von Microsoft, welches allerdings nur einen Kanal zuließ, oder das L2F-Protokoll (Layer 2 Forwarding) der Firmen Cisco, Nortel und Shiva, welches mehrere Tunnel bot, aber keine Verschlüsselung.
2. Kopplung auf der Netzwerkschicht durch IPsec.

IPsec ist eine Erweiterung des IP-Protokolls um Schutzfunktionen zur Authentifizierung, Integritätsprüfung und Verschlüsselung. IPsec kann zur aktuellen IP-Version 4 hinzugefügt werden und ist fester Bestandteil der neuen IP-Version 6.

IPsec ist in den RFCs 4301, 4302, 4303 und 4305 definiert und seine zentralen Elemente sind:

- Das AH-Protokoll (Authentication Header, Bild 1.192)
- Das ESP-Protokoll (Encapsulating Security Payload, Bild 1.193)
- Die Schlüsselverwaltung (Key Management)

Dabei ist IPsec nicht auf bestimmte Authentifizierungs- und Verschlüsselungstechniken festgelegt. Zur Erzielung einer minimalen Kompatibilität ist jedoch im AH-Protokoll das Verfahren MD5 (RFC 1321) Pflichtbestandteil jeder Implementation. Dabei wird aus den Nutzdaten und einem geheimen Schlüssel eine Prüfbitfolge erzeugt, die eine Manipulation des Dateninhalts aufdeckt (Integritätsprüfung) und einen Absender authentifiziert. Beim ESP-Protokoll ist das DES-Verfahren (bekannt durch Scheckkarten, RFC 1829) Standard, um die Vertraulichkeit durch Verschlüsselung zu gewährleisten. Beide Protokolle fügen einen neuen Header ein und kennen jeweils einen Transport-Modus und einen Tunnel-Modus.

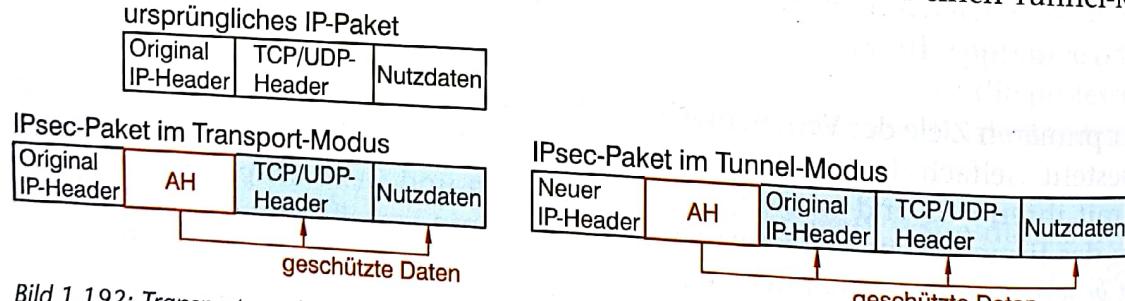


Bild 1.192: Transport- und Tunnel-Modus bei IPsec-Paketen mit AH-Protokoll

Der **Transport-Modus** ist nur für die Host-zu-Host-Kommunikation geeignet, denn es muss jede Station im VPN IPsec beherrschen; die Pakete werden geringfügig größer. Die Kommunikationsbeziehungen können analysiert werden, die Daten sind natürlich nicht einsehbar.

Beim **Tunnel-Modus** wird ein neues IP-Paket erzeugt, die Pakete werden also größer als im Transport-Modus, bei gleichzeitiger Verwendung von AH und ESP um mehr als 60 Byte – es droht Fragmentierung und die damit verbundene Leistungseinbuße. Dafür müssen nur die Gateways an den Tunnelendpunkten IPsec beherrschen. Bei der Durchtunnelung des Internets und innerhalb der Intranets ist nicht mehr erforderlich als die Fähigkeit, IP-Pakete weiterleiten zu können. Nur die Kommunikationsbeziehungen von Tunnelendpunkten können analysiert werden.

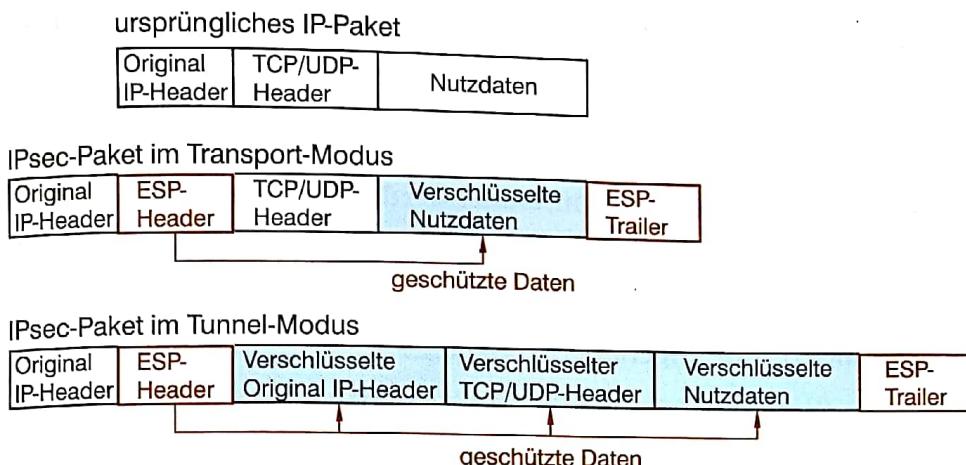


Bild 1.193: Transport- und Tunnel-Modus bei IPsec-Paketen mit ESP-Protokoll

Zum Funktionieren einer gesicherten Punkt-zu-Punkt-Kommunikation ist die Anpassung vieler Parameter erforderlich (Authentifizierung und/oder Verschlüsselung, Verschlüsselungsalgorithmen, Schlüssel etc.), die zumindest bei jedem Verbindungsaufbau neu ausgehandelt werden müssen.

Für jede Richtung einer Punkt-zu-Punkt-Kommunikation und für jedes Protokoll (AH/ESP) wird ein eigener Parametersatz benötigt.

Die jeweils nötigen Parametersätze werden zusammengefasst und als SA (Security Association) bezeichnet und in einer SPD (Security Policy Database) genannten Datenbank abgelegt. Die Verwaltung und die Verteilung der vielen erforderlichen Schlüssel können ein organisatorisches Problem werden, wenn sie „manuell“ durchgeführt werden. Alternativ sollte das IKE (Internet Key Exchange Protocol, RFC 4306) und das ISAKMP (Internet Security Association and Key Management Protocol) eingesetzt werden.

Grundlagen der Verschlüsselung

Der Schutz vor Ausspähung von Informationen durch nicht autorisierte Personen entspricht einem alten Menschheitswunsch. Früher wurden Nachrichten dadurch verschlüsselt, dass ihre Zeichen durch andere Zeichen ersetzt oder nach komplizierten und geheimen Verfahren „durcheinander“ gewürfelt wurden. Ein heute noch gelegentlich verwendetes Verfahren heißt ROT13 und zählt zu den Cäsar-Codierungen, die zur Verschlüsselung eine lineare Verschiebung von Buchstaben im Alphabet durchführen. Die jeweilige Schiebedistanz d stellt dabei den Schlüssel dar.

Beispiel

Beträgt etwa die Distanz $d = 2$, so wird $A \rightarrow C$, $B \rightarrow D$, ..., $Z \rightarrow B$ usw. abgebildet. Aus dem sogenannten Klartext „GEHEIM“ wird der Schlüsseltext „IGJGKO“. Zur Entschlüsselung muss eine Verschiebung um $d' = -2$ bzw. um $d' = 26 - d = 26 - 2 = 24$ durchgeführt werden, weil mit $d = 26$ jeder Buchstabe auf sich selbst abgebildet wird (vollständige Rotation des Alphabets). Am einfachsten in der Handhabung ist somit ROT13, da $d = d'$ einfach zu realisieren ist.



Im Computerzeitalter ist dies nicht ernsthaft als Verschlüsselung aufzufassen; ROT13 dient in News-Groups dazu, bei Scherzfragen die mitgelieferte Lösung nicht gleich offensichtlich zu machen und ist in manche News-Clients integriert (gewesen).

Heutige Verschlüsselungsverfahren sind wissenschaftlich basiert und beruhen auf standardisierten und öffentlich bekannten Algorithmen. Es werden die zu verschlüsselnden Daten nicht mehr zeichenweise, sondern bitweise verschlüsselt. In das Verfahren gehen sowohl der „Klartext“ als auch ein Schlüssel ein (Bild 1.195), der ein möglichst zufälliges und möglichst langes Bitmuster darstellt. Die Erzeugung zufälliger Muster ist mit Digitalrechnern nicht wirklich, sondern nur angenähert möglich.

Den Zusammenhang verdeutlicht die Tabelle in Bild 1.194. Die letzte Spalte nennt die 1995 für erforderlich gehaltene Schlüssellänge. Inzwischen sind 18 Jahre vergangen.

■ Je größer die Schlüssellänge (in Bit), desto stärker ist die Verschlüsselung gegenüber der Kryptanalyse.

Angreifer	Budget	Tools	40 bit	56 bit	1995
Normaler Benutzer	winzig	Rechenzeit	1 Woche	unmöglich	45
Kleine Firma	\$ 400	FPGA	5 Std. (\$ 0.8)	38 Jahre (\$ 5 000)	50
	\$ 10000	FPGA	12 Min. (\$ 0.08)	556 Tage (\$ 5 000)	55
Unternehmen	\$ 300 T	FPGA	24 Sek. (\$ 0.08)	19 Tage (\$ 5 000)	60
	oder	ASIC	18 Sek. (\$ 0.001)	3 Stunden (\$ 38)	
Große Firma	\$ 10 M	FPGA	7 Sek. (\$ 0.08)	13 Tage (\$ 5 000)	70
	oder	ASIC	.005 Sek. (\$ 0.001)	6 Min. (\$ 38)	
Sicherheitsdienste	\$ 300 M	ASIC	.0002 Sek. (\$ 0.001)	12 Sek. (\$ 38)	75

Bild 1.194: Kryptoanalyse-Aufwand¹

Wird, wie in Bild 1.195 dargestellt, mit dem gleichen (oder wie im obigen Beispiel leicht abzuleitenden) geheimen Schlüssel sowohl ver- als auch entschlüsselt, so spricht man von symmetrischer Verschlüsselung.

Zu den bekanntesten Vertretern dieser Art zählen DES (Data Encryption Standard) mit 56 bit (relevanter) Schlüssellänge, Triple-DES mit 108 bit (relevanter) Schlüssellänge und AES (Advanced Encryption Standard, Rijndael-Algorithmus, ab 1998) mit wahlweise 128/192/256 bit Schlüssellänge. Es werden „Klartext“-Blöcke in der Größe der Schlüssellänge nacheinander verarbeitet, daher auch der Name **Blockchiffren**. Die Schutzwirkung ist stark, allerdings haben die Kommunikationspartner das Problem, dass der geheim zu haltende und daher selbst zu schützende Schlüssel gesichert übergeben werden muss.

¹ Eckert, Claudia: IT-Sicherheit - Konzepte, Verfahren, Protokolle, 3. Auflage, München, Oldenbourg, 2004

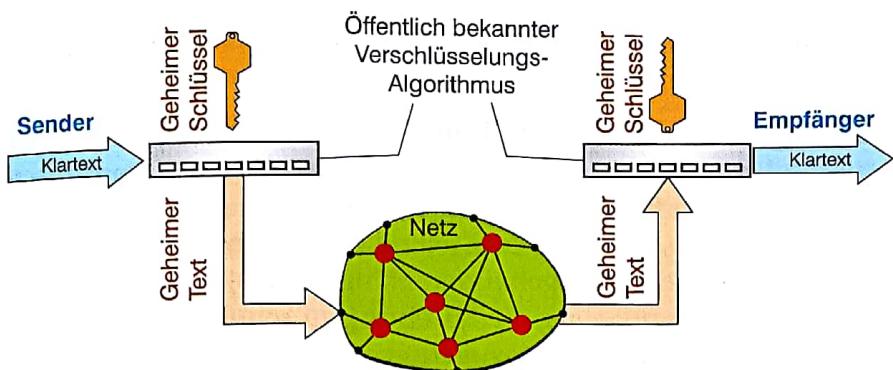


Bild 1.195: Symmetrische Verschlüsselung: Ein Schlüssel zum Verschlüsseln und zum Entschlüsseln

1

Dazu verwendet man zumeist eine asymmetrische Verschlüsselung, etwa das nach seinen Entwicklern (Rivest, Shamir und Adleman, 1978) benannte RSA-Verfahren.

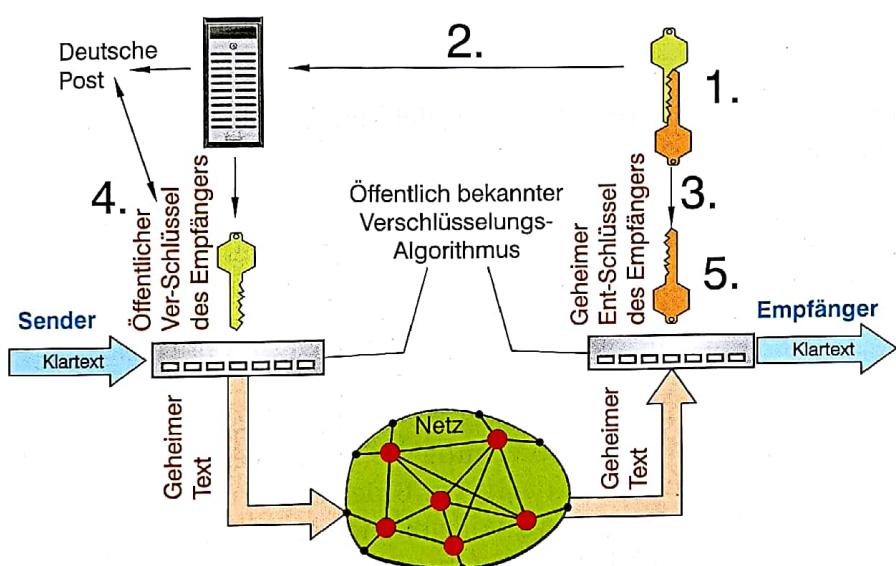


Bild 1.196: Asymmetrische Verschlüsselung: Ein Schlüssel zum Verschlüsseln und einer zum Entschlüsseln

Bild 1.196 skizziert das Verfahren im Groben:

1. Der Empfänger erzeugt ein Paar aus verschiedenen (asymmetrischen), aber exakt **auf einander eingestellten** Schlüsseln.
2. Der öffentliche Schlüssel (**Public Key**) wird allen potenziellen Kommunikationspartnern (z. B. auf einem Schlüssel-Server) zugänglich gemacht und bei einer Zertifizierungsstelle hinterlegt (z. B. Deutsche Post).
3. Der private Schlüssel bleibt Geheimnis des Empfängers.
4. Jeder kann eine Nachricht an den Empfänger mit dessen **öffentliche** Schlüssel verschlüsseln. Zweifel an der Echtheit des Schlüssels beseitigt ein Zertifikat einer vertrauenswürdigen Stelle. In Deutschland werden solche Stellen von der Bundesnetzagentur (vormals RegTP) ihrerseits zertifiziert.
5. Einzig der Empfänger kann mit seinem **geheimen** Schlüssel die Nachricht **entschlüsseln**.

Der **Vorteil** des asymmetrischen Verfahrens besteht darin, dass kein geheimer Schlüssel ausgetauscht werden muss; der **Nachteil**: Es ist um den Faktor 100 bis 1 000 rechenintensiver

(= zeitaufwendiger) als etwa DES und daher weniger gut für größere Datenmengen geeignet.

Die Lösung liegt in einem Kompromiss: Mit dem asymmetrischen Verfahren wird zuerst ein Schlüssel für symmetrische Verschlüsselung geschützt übertragen (Größenordnung: 128 bis 256 bit) und diese anschließend für die eigentliche Datenübertragung eingesetzt. Mit der gleichen Technik – vorzugsweise, aber nicht zwingend mit einem anderen Schlüsselpaar – ist es auch möglich, mit dem eigenen geheimen Schlüssel Dokumente elektronisch zu signieren (zu unterschreiben) und gegen Verfälschung zu schützen. Dabei wird ein Prüfwert (Hash) erzeugt und der Nachricht hinzugefügt. Jeder kann dann mit dem öffentlichen Schlüssel des Absenders dessen Authentizität prüfen. Nicht ganz so aufwendig ist die Erzeugung von Prüfwerten zur Sicherstellung der Unverfälschtheit mit den Verfahren **MD5** (Message Digest Version 5; digest: Auszug, Extrakt) und **SHA-1** (Secure Hash Algorithm).