Paketfilter – Firewall

Grundlagen

Beantworten Sie die folgenden Fragen anhand des Films.

Was ist die grundsätzliche Aufgabe einer Firewall?

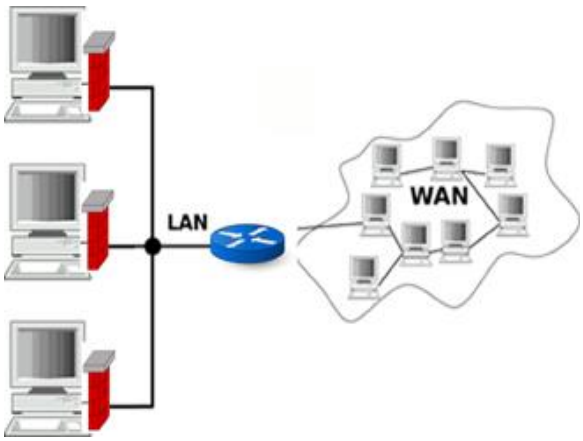
Zu steuern, welche Kommunikation vom netzwerk nach außen und von außen in das Netzwerk erlaubt ist.

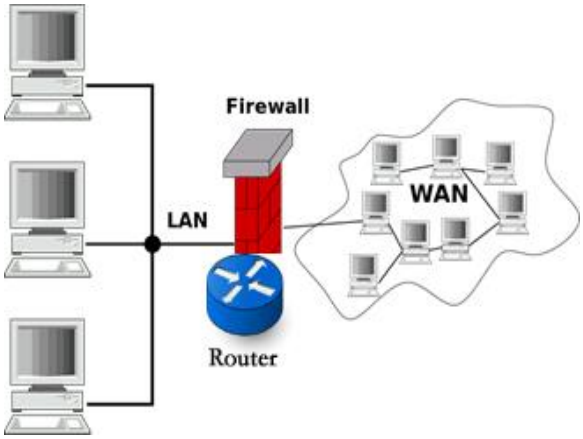
Welche Typen von Firewalls werden unterschieden? Welche Aufgabe hat der jeweilige Typ?

Desktop-Firewalls und Network-Firewalls
Desktop-Firewall: Software, die auf einem PC installiert ist => schützt ein Endgerät
Network-Firewall: Hardware für das gesamte Netzwerk => schützt das gesamte Netzwerk

Braucht man eine Software- bzw. Desktopfirewall, wenn eine Netzwerkfirewall vorhanden ist? Begründen Sie Ihre Antwort.

Ja. Ein hoher Prozentanteil von Sicherheitsverletzungen entstehen innerhalb des Netzwerkes. Gegen diese Bedrohungen kann die Network-Firewall nichts tun.





Desktop-Firewalls müssen auf jedem System konfiguriert werden und stellen somit einen erheblichen administrativen Aufwand dar. Der Einsatz erfolgt somit am Einzelplatzrechner mit Internet oder im SOHO-Bereich (Small Office Home Office). Hier wird die Firewall meist mit weiteren Maßnahmen wie Virenschutz und Web-Proxy kombiniert.

Im Speziellen kann auch ein Server innerhalb des LANs, in der DMZ oder direkt mit WAN-Zugriff geschützt werden.

Netzwerk-Firewalls befinden sich zwischen „sicheren“ und „unsicheren“ Netzen. Sie schützen das sichere Netz gegen unberechtigte Zugriffe von außen. Der Schutz der Rechner im LAN kann lokal somit relativ klein gehalten werden. Durch die zentrale Administration reduzieren sich der Verwaltungsaufwand und das Fehlerpotential.

Der Einsatz erfolgt je nach Netzarchitektur an der Grenze zwischen LAN und DMZ bzw. DMZ und WAN oder zwischen LAN und WAN.

Situation

Sie müssen einen Kunden bezüglich der technischen Möglichkeiten der Umsetzung einer Firewall informieren. Dabei möchte der Kunde von Ihnen über die Unterschiede eines *statischen Paketfilters* und einer *Stateful Inspection Firewall* beraten werden.

Aufgabe: Betrachten Sie das Video und gehen Sie dabei insbesondere auf die folgenden Fragestellungen ein:

	Stateless	**Stateful**
Aktualität	Technik veraltet	Aktueller (aber auch alt)
Wonach werden Pakete akzeptiert (allow) bzw. verworfen (deny)	- Ziel / Quellport, IP - Protokolle (TCP, UDP, IP, ICMP, IGMP, ...) - Richtung des Datenverkehrs (IN / OUT) - ...	- Merkt sich den Status einer Verbindung - IP, Port, Sequenznummer, ... - ....
Nachteile	- Man benötigt viele Filterregeln - Aufwendige Administration - Unsicher, da Ports immer offen sind - Richtung IN alles >1023 als Zielport akzeptieren	- Langsamer - Zugriff von extern nicht ohne interne Anfrage möglich
Vorteile	- Schneller	- Sicherer, da Ports nur für die Dauer der Verbindung offen

Statische und dynamische Paketfilterung

Die **statische Paketfilterung** arbeitet zustandslos, das heißt, die Filterregeln arbeiten unabhängig von vorangegangenen Paketen. Auf jedes Paket wird immer derselbe Satz von Filterregeln (Access Control LIST ACL) angewandt. Für eine TCP-Verbindung werden also mindestens zwei Regeln benötigt, eine für die Hin- und eine für die Rückrichtung.
Die Regelketten werden nach dem Prinzip „first match“ von oben nach unten abgearbeitet. Hierbei gibt es zwei Strategien:

White-List

Alle zugelassenen Übertragungen über die Firewall hinweg werden durch ACCEPT- Regeln zeilenweise festgelegt. Die Regelkette muss mit einer DROP-Regel für alle nicht definierten Zugriffe abschließen Es funktioniert also nur, was explizit erlaubt ist (hohe Sicherheit bei geringer Funktionalität -> meist zwischen LAN und WAN).

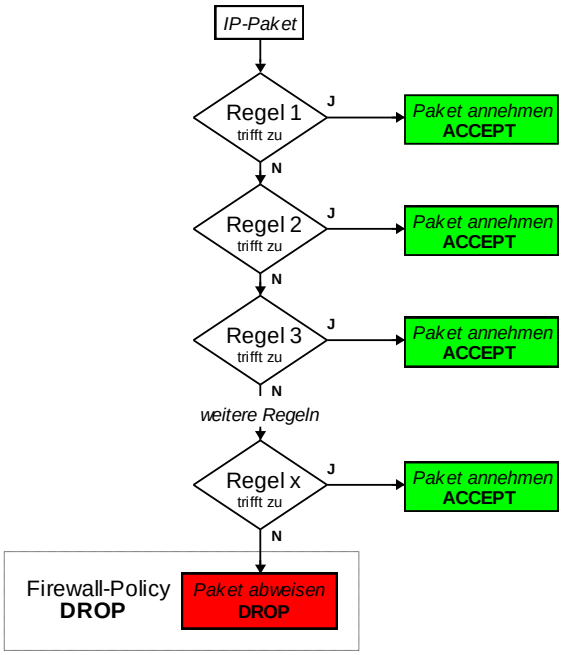
Beispiel mit LINUX:

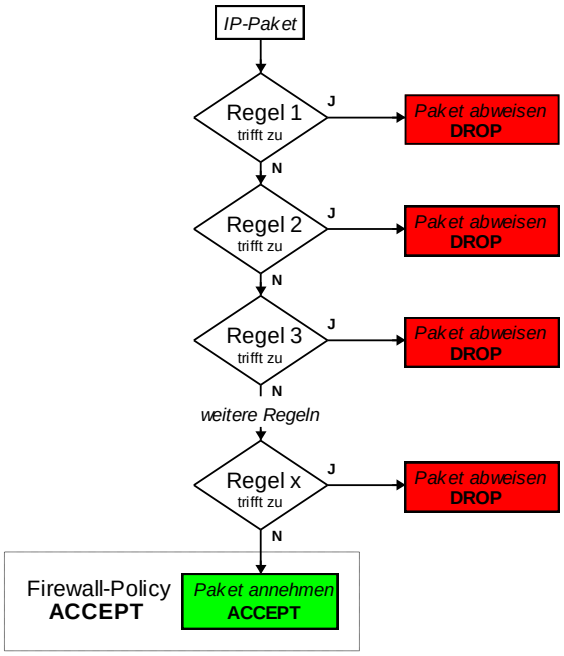
Filtertabelle für SSH bei statischer Paketfilterung

Nr.	Quelle	Ziel	Prot.	Quell-Port	Ziel-Port	Flags	Action	Log
1	Client	Server	TCP	>1023	22	any	ACCEPT	√
2	Server	Client	TCP	22	>1023	!syn	ACCEPT	–
3	any	any	any	any	any	any	DROP	√

Black-List

Alle verbotenen Übertragungen über die Firewall hinweg werden durch DROP- Regeln zeilenweise festgelegt. Die Regelkette muss mit einer ACCEPT-Regel für alle nicht definierten Zugriffe abschließen. Es funktioniert also alles, was nicht explizit verboten ist (hohe Funktionalität bei wenig Sicherheit -> meist innerhalb von LANs).





Die dynamische Paketfilterung, auch „**Statefull Inspection**“ genannt, ist zustandsabhängig und erweitert das Regelwerk temporär um zusätzliche Regeln. Für eine erlaubte Verbindung wird also bei Bedarf die benötigte Rückrichtung für die Dauer der Verbindung freigeschaltet. Die Firewall muss sich dazu jeden Verbindungsaufbau merken, um Folgepakete als zu einer bestehenden Verbindung gehörig zuordnen zu können.

Fragen:

1. Auf welchen OSI-Schichten arbeitet die Paketfilterfirewall?
2. Wie arbeitet eine Paketfilterfirewall die Filterregeln ab? (genaue Beschreibung)
3. Warum gilt eine Firewall mit einer Black-List als unsicher?
4. Beschreibe die Funktion einer Netzwerkfirewall!

1. Auf der Layer 3 und 4

2. Die eingehenden Pakete werden Regel- nach Regel abgearbeitet. Sobald eine Zutrifft (first match), wird das Paket entsprechend behandelt (Accept oder Drop)

3. Weil der Aufwand von allem schädlichen zu blocken viel zu groß und nahezu unmöglich is

4. Diese Firewall wird an forderster Front eingesetzt und verhindert das eindringen von unerwünschten Anfragen oder Antworten. Ist meist als externe Hardware verfügbar.