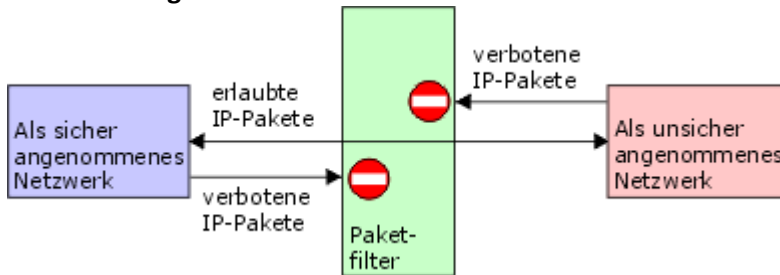


Lernzusammenfassung

Firewall

Definition Firewall: Eine Firewall ist als eine Sicherheitsstrategie zu verstehen, die unerwünschte, unsichere und schädigende Datenübertragung verhindern soll. Eine Firewall ist eine Schutzmaßnahme vor fremden und unberechtigten Verbindungsversuchen aus dem öffentlichen ins lokale Netzwerk

Paketfilterung

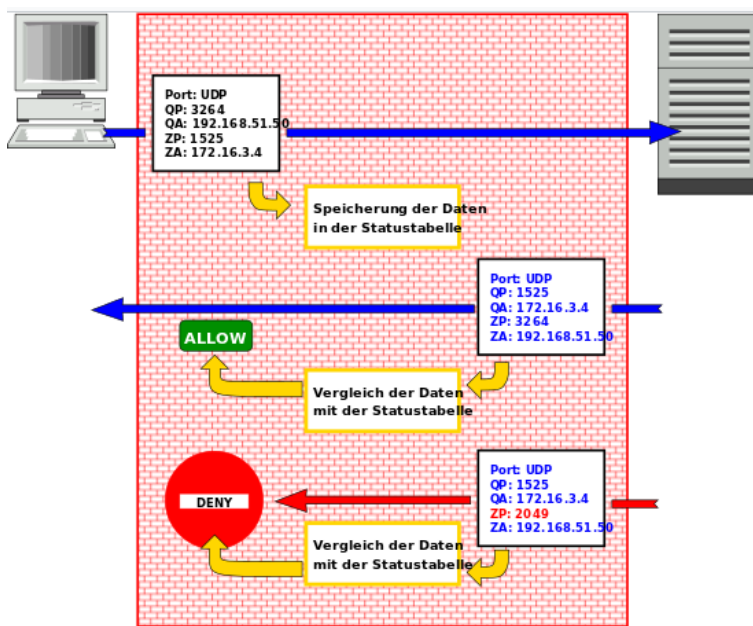


Der Paketfilter kontrolliert den Verkehr mittels Regeln, die sich hauptsächlich auf die Adressierung der Pakete, also die Sockets (IP-Adresse und TCP- oder UDP-Port) der Quelle und des Ziels, beziehen.

Jede Form von gewünschter Verbindungsaufnahme zwischen zwei Sockets sollte explizit erlaubt und jede andere Kommunikation explizit verboten sein.

Für eine Verbindung müssen **zwei** Regeln, eine für eingehende und eine für ausgehende Pakete definiert werden.

Verbindungsorientierte Paketfilterung (Stateful packet filtering)



Führt der Paketfilter eine Tabelle mit dem Status aller aktuellen TCP/IP-Verbindungen (Connection state table), so kann er damit die Kommunikation genauer kategorisieren.

Die Pakete können neue Verbindungen aufbauen (State: NEW), zu bereits existierenden Verbindungen gehören (State: ESTABLISHED), existierenden Verbindungen zugeordnet (State: RELATED) oder ungültig sein (State: INVALID).

Ein solcher "Stateful"-Paketfilter braucht für eine Verbindung im Prinzip nur noch **eine** Regel, da er alle weiteren Pakete dieser Verbindung zuordnen kann.

Offener Port: Ein Port gilt dann als offen, wenn eine Anwendung an einem Port Datenpakete entgegennimmt, die an diesen Port geschickt werden, ohne dass die Anwendung dieses Datenpaket angefordert hat.

Geschlossener Port: Ein Port gilt als „geschlossen“, wenn keine Anwendung an diesem Port „lauscht“

Protokollregel: Definieren das Verhalten der Firewall, z.B. welche Protokolle die Firewall durchlässt bzw. blockieren soll

Blacklist-Strategie: Alles ist erlaubt, außer den verbotenen Adressen.

Whitelist-Strategie: Alles ist verboten, außer der erlaubten Adresse.

Lernzusammenfassung

Firewall

Aufgaben Proxyserver:

- Caching von Webseiten / Filtern von Webseiten
- Inhaltliche Bewertung von Daten, z.B. Benutzerauthentifizierung
- Umfangreiche Protokollierung
- Blockierung von Aktionen bestimmter Anwendungen
- Dienste können Benutzerabhängig erlaubt werden
- Namensauflösung für die Clients

Kurz und knapp:

Paket-Filter: (statische Paketfilterung)

- analysieren nur die IP/TCP/UDP-Header der Datenpakete, **nicht** jedoch den transportierten Inhalt
- Ungewünschter oder unsicherer Datenverkehr kann anhand von IP-Adressen/TCP- und UDP-Ports gefiltert und unterbunden werden.

Anwendungsfiler (Application Gateway / Proxy / Application Level Firewall)

Prüfen zusätzlich den Inhalt der Datenpakete und lehnen abhängig von ihrer Konfiguration Pakete mit bestimmten Inhalten (z.B. ausführbare Mail-Anhänge, Viren) ab.

Stateful Inspection Firewall: (dynamische Paketfilterung)

Bezieht zusätzliche Kriterien (Quellport, Segment-Nummer, Timestap) in die Filterung des Datenverkehrs mit ein. Damit können Antworten, die auf Anfragen aus dem LAN heraus erfolgen, ohne Beachtung weiterer Firewall-Regeln durchgelassen werden.

Port-Liste:

- 25 -> SMTP / 53 -> DNS / 80 -> HTTP
- 110 -> POP3 / 143 -> IMAP / 443 -> HTTPS
- 20+21 -> FTP / 22 -> SSH / 23 -> TELNET

TCP/IP		1.0	2.0	2.1/ 2.2	3.0
4	Anwendungsschicht				Applikations-erkennung
					Protokoll-validierung
				Einige Applikationen	Deep-Paket-Inspection
				AV, IDS/ IPS, Webfilter	AV, IDS/ IPS, Webfilter
3	Transportschicht		Stateful Inspection	Stateful Inspection	Stateful Inspection
2	Vermittlungsschicht	Paketfilter	Paketfilter	Paketfilter	Paketfilter
1	Sicherungsschicht				

Lernzusammenfassung

Firewall

Firewallregeln (Beispiel):

Regel	Richtung	Source IP	Dest. IP	Protokoll		Dest. Port		Aktion
1	Rein	Extern	Intern	TCP		25		Weiterleiten
2	Raus	Intern	Extern	TCP		>1023		Weiterleiten
3	Raus	Intern	Extern	TCP		25		Weiterleiten
4	Rein	Extern	Intern	TCP		>1023		Weiterleiten
5	egal	jede	jede	jedes		jeder		blockieren

Was genau bewirkt nun das Set?

Gehen wir dafür durch die einzelnen Zeilen:

- Die erste Zeile erlaubt hereinkommende Verbindungen, die den Port 25 ansprechen, während die zweite Zeile die Antworten zurück an den Sender erlauben.
 - Zur Erinnerung: Der sendende Computer wird für die Verbindung einen willkürlichen Port oberhalb 1023 nehmen und auf den Zielport 25 zugreifen. Die Rückantworten werden dann vom Port 25 des mailempfangenden Rechners an den vom Sender mitgeteilten Port zurückgesendet. Damit erlauben die Regeln 1 und 2 hereinkommende Mails von außerhalb.
- Die Regeln 3 und 4 realisieren jetzt den gleichen Mechanismus für den Fall, dass ein interner Rechner Mails an einen externen Rechner schicken will.
- Die Regel 5 realisiert jetzt wiederum den „Default-Deny“-Ansatz. Sie verbietet alle Verbindungen außer diejenigen, die durch die vorhergehenden Regeln explizit erlaubt wurden.