Firewall und DMZ

Stand: 03/2020

IT-Team, Elektronikschule Tettnang
A. Grella, H. Müller, W. Heinrich

Definition

- Eine Firewall ist ein System (Konzept) aus software- und hardwaretechnischen Komponenten, um IP-Netze sicher zu koppeln (lt. BSI, Glossar und Begriffsdefinitionen).
- Die umgangssprachliche Trennung in Hardware- und Software-Firewalls ist -technisch gesehen- unsinnig, da jede Firewall aus einem Stück Software besteht, die auf Hardware ausgeführt wird.
- Sinnvoller ist eine Unterscheidung hinsichtlich des Installationsortes der Firewall:
  - Desktop-, Personal-Firewall oder interne Firewall (umgangssprachlich auch Software-Firewall genannt)
  - externe Firewall (umgangssprachlich auch Hardware-Firewall genannt)

Desktop- bzw. Personal-Firewall

- wird lokal auf dem zu schützenden Computer betrieben als Betriebssystemkomponente oder als separate Software (rein softwarebasierte Lösung)
- Aufgaben:
  - Bösartige oder ungewollte Zugriffe auf den Computer von außen verhindern
  - Kommunikation von installierten Programmen mit der Außenwelt ohne das Einverständnis des Anwenders unterbinden. Kann auch einzelne Programme vom Netzwerkverkehr ausschließen (Firefox darf, IE darf nicht).

Desktop-Firewall: Kritikpunkte

- laut BSI empfohlene Sicherheitsmaßnahme für Internetnutzer, obwohl das Konstruktionsprinzip umstritten ist (Nutzer geht evtl. höheres Risiko ein)
- kontrolliert nur den ein- ausgehenden Datenverkehr des einzelnen Endgeräts (nicht den Netzwerkverkehr zwischen den Netzen)
- Überwindet ein Angreifer die Firewall, hat er meist bereits vollständigen Zugriff auf das zu schützende System.
- Schadsoftware kann die Desktop-Firewall kompromittieren, ohne dass der Anwender es merkt, sodass er sich immer noch geschützt fühlt

Externe Firewall

- wird an der Grenze des zu schützenden Netzwerksegments betrieben
- meist sicherheits- und funktionsoptimierte Hardware (Netzwerk-Firewall) oder normaler PC mit "nur Firewall-Funktionalität" (Host-Firewall)
- Aufgaben:
  - Bösartige oder ungewollte Zugriffe auf das Netzwerksegment und somit auf die darin befindlichen Endgeräte von außen verhindern
  - Überwachung des Datenverkehrs zwischen den Netzwerksegmenten

Firewall-Technologien

- Firewalls arbeiten nach unterschiedlichen Verfahren:
  - Paketfilter – Firewall
    (Stateless Packet Firewall, statische Paketfilterung)
  - Stateful Packet Inspection - Firewall
    (SPI – Firewall, dynamische Paketfilterung)
  - Application Layer Firewall
    (Proxy Based Firewall)
  - Next Generation Firewall

Paketfilter - Firewall

- untersucht jedes Datenpaket und wertet die Headerinformationen (Quell-, Zieladresse, Quell-, Zielport, TCP-Flags)
- arbeitet auf OSI-Layer 3 und 4
- statischer Regelsatz mit permit/deny – Einträgen, der sequentiell abgearbeitet wird und über die Zukunft eines jeden Datenpakets entscheidet
- Regelsatz muss für jede Kommunikationsrichtung (Quelle ⇨ Ziel, Ziel ⇨ Quelle) separat formuliert werden
- häufig als Zusatzfeature auf Routern zu finden (ACLs bei Cisco)

Paketfilter-Firewall: Vor-/Nachteile

Vorteile

- kostengünstig, da heute meist standardmäßig im Router enthalten
- recht gute Performance
- ohne großen Aufwand schnell konfigurierbar
- relativ einfach für neue Dienst und Protokolle erweiterbar

Nachteile

- Regelsatz wird schnell unübersichtlich
- Regelwerk für Hin- und Rückweg erforderlich
- für Protokolle mit variablen Portnummern eher ungeeignet (z.B. ftp), da ein großer Portbereich geöffnet werden muss

SPI-Firewall

- basiert auf Paketfilterung
- wertet zusätzlich den Zustand einer Verbindung auf dem Application-Layer dynamisch aus und erweitert das Regelwerk temporär um zusätzliche Regeln (logische Datenströme werden analysiert)
- arbeitet auf OSI-Layer 3, 4 und 7
- Regelsatz muss nur für eine Richtung erstellt werden (Quelle ⇨ Ziel)
- patentiert von Check Point Software Technologies Ltd.

SPI-Firewall: Vor-/Nachteile

Vorteile

- einfache Regelsätze, die nur von der Quelle zum Ziel formuliert werden müssen
- funktioniert auch bei UDP
- höheres Maß an Sicherheit im Vergleich zu Paketfilter, da Rückwege nur zeitlich befristet geöffnet sind und nur einen Port betreffen

Nachteile

- erfordert höheren Rechenaufwand
- ggf. Performanceverlust
- kostenpflichtige Lösung

Application Layer Firewall /Gateway

- erfordert zwei Interfaces zur logischen Trennung der Netze
- nimmt Anfragen vom Client entgegen (wie ein Server), analysiert die Kommunikationsanfragen sowie die Daten und gibt alles –gemäß der Einstellungen- stellvertretend (Proxy) zum Zielsystem (wie ein Client) weiter (ebenso bei externen Anfragen bzw. Antworten).
- Nutzdatenanalyse (Content Filter) möglich, beispielsweise nach bestimmten Schlüsselworten
- arbeitet auf OSI-Layer 7

Proxy-Firewall: Vor-/Nachteile

Vorteile

- sehr hohes Maß an Sicherheit
- umfangreiche Protokollierung möglich
- Dienste können benutzerabhängig erlaubt werden
- völlige Entkoppelung der Netze

Nachteile

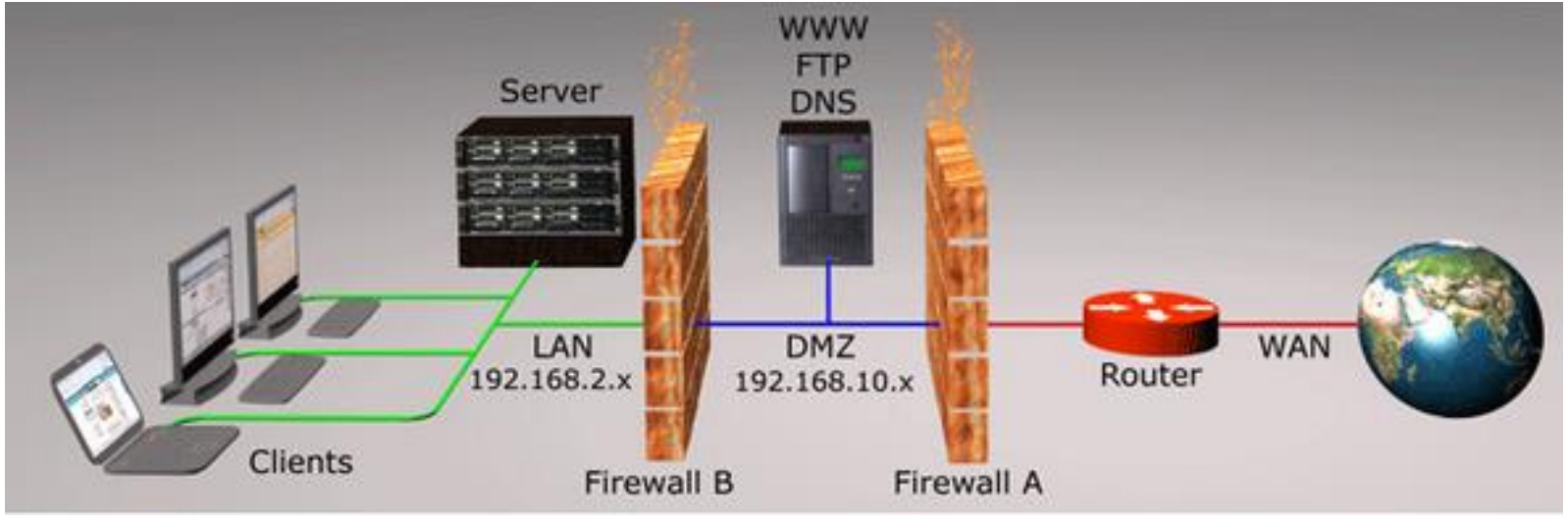
- erfordert sehr hohen Rechenaufwand
- ggf. Performanceverlust
- für jedes Dienst-Protokoll ist ein eigener Filter notwendig

DMZ – Die neutrale Zwischenzone

- DMZ steht für Demilitarized Zone
- DMZ = Rechnernetz mit eigenem IP-Adressbereich, das als Pufferzone zwischen zwei Netzwerken (meist Firmen-LAN und Internet) liegt und diese durch strenge Sicherheitsregeln voneinander abgrenzt.
- DMZ ist sinnvoll und vom BSI empfohlen, wenn Firmenserver aus dem Internet kontaktiert werden sollen (z.B. Web-, Mail-, FTP-, DNS-Server). Diese sog. Bastion-Hosts bieten Hackern eine große Angriffsfläche.

Zweistufiges DMZ-Konzept

- Äußere Firewall schirmt die DMZ vom Internet ab, die innere Firewall trennt die DMZ vom LAN.



Bildquelle: InfoTip

Zweistufiges DMZ-Konzept

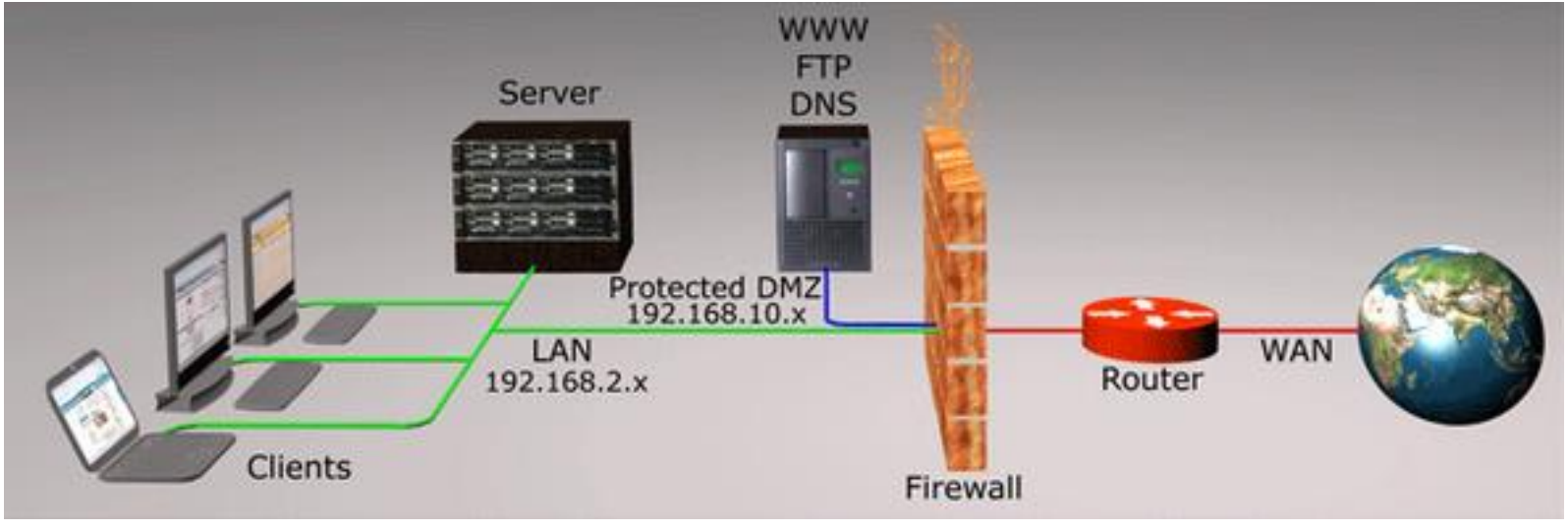
- Dabei sind folgende Zugriffmöglichkeiten einzuhalten:

Nutzer befindet sich…	Zugriff auf DMZ	Zugriff auf LAN	Zugriff auf Internet
…im Internet (WAN)	erlaubt	abgewiesen	-
…im LAN	erlaubt	-	erlaubt
…in der DMZ	-	abgewiesen	abgewiesen

- Empfehlung:
  Firewalls unterschiedlicher Anbieter nutzen
  Weitere Segmentierung der DMZ durch VLANs

Einstufiges DMZ-Konzept

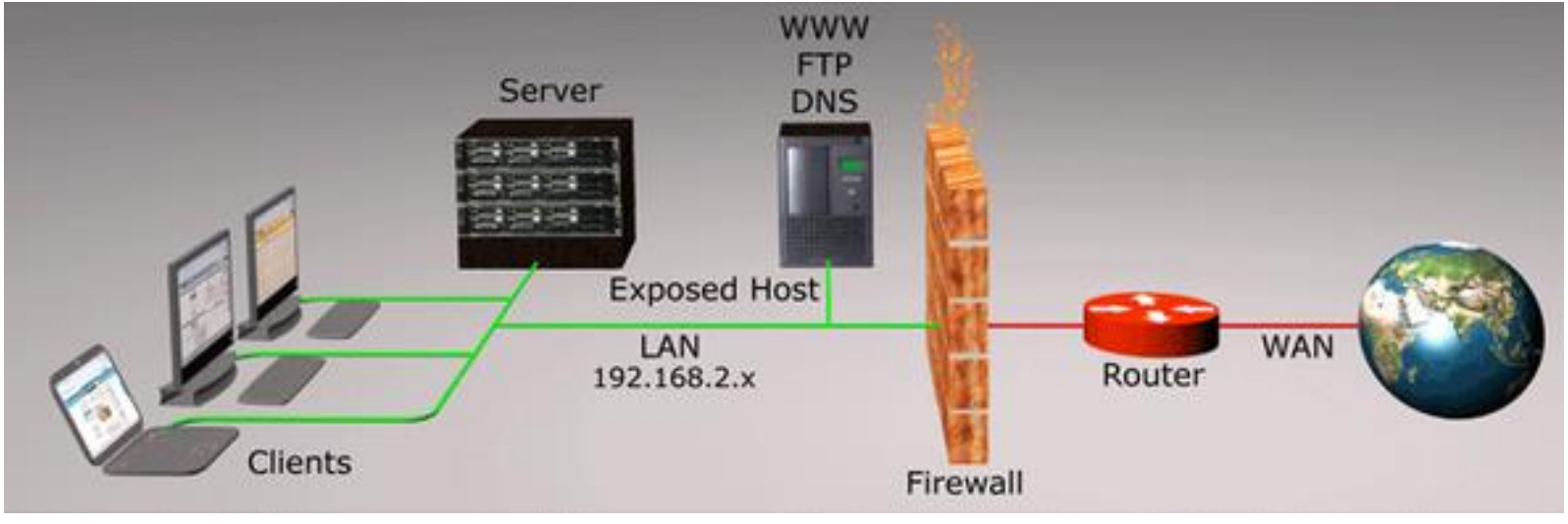
- kostengünstige Variante durch eine Firewall mit drei Interfaces, die auch "Protected DMZ" genannt wird
- Firewall ist aber Single Point of Failure



Bildquelle: InfoTip

Exposed Host als Pseudo-DMZ

- aus Marketinggründen fälschlicherweise als DMZ angepriesen
- Exposed Host ist nicht vom LAN getrennt. Der Router leitet alle Pakete, die nicht zu einem bestimmten Empfänger zugeordnet sind, an den Exposed Host weiter.



Bildquelle: InfoTip