Juventus Technikerschule HF

Hacking Exposed

HE1: Perimeter Security

Ahmet Inci

Die 3 grundlegenden IT-Security Massnahmen

- Starke Passwörter
- Software Updates
- Backup (und Restore)

Wichtiger Hinweis

- Dies ist eine Lehrveranstaltung.
- Die im Rahmen der Hacking-Exposed-Vorlesung vermittelten Kenntnisse sollen dazu beitragen, dass Sie Informationssicherheitsaspekte beachten und in Ihren Projekten berücksichtigen.
- Die HE-Vorlesung ist keineswegs als Anstiftung zum Hacken zu verstehen.

Inhalt heute

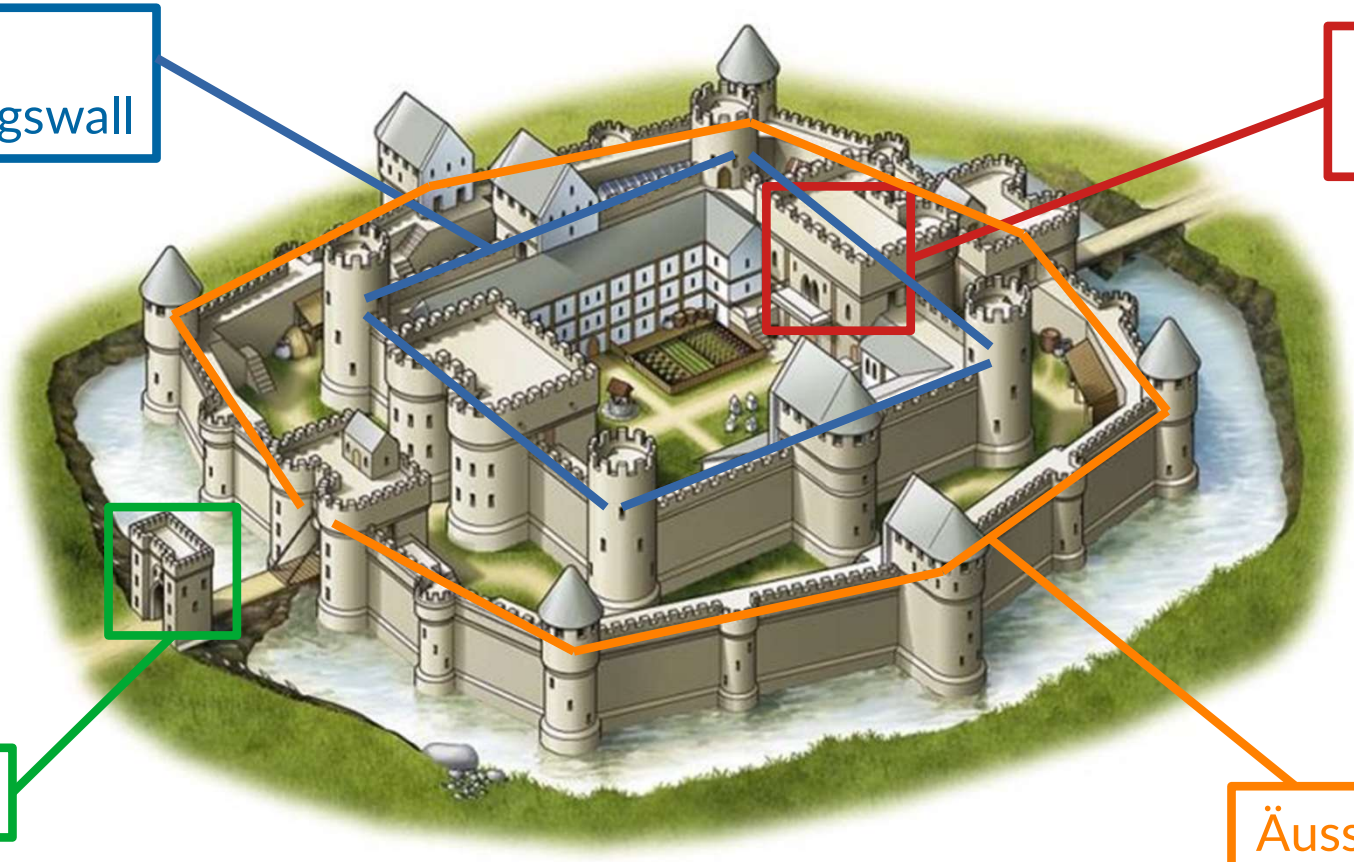
- Perimeter Security Massnahmen
- Firewalling Grundidee
- Firewalling mit Netfilter und Iptables
- Port Scanning

Ziele

- Sie kennen wichtige Komponenten in der Netzwerksecurity und können deren Zweck beschreiben.
- Sie verstehen wieso es wichtig ist ein Netzwerk in Security-Zonen einzuteilen.
- Sie können Firewall-Regeln lesen, verstehen und selbstständig einfache Regeln schreiben.
- Sie können Nmap bedienen um offene Ports zu finden, Applikationsversionen herauszufinden und eigene Firewall-Regeln überprüfen.

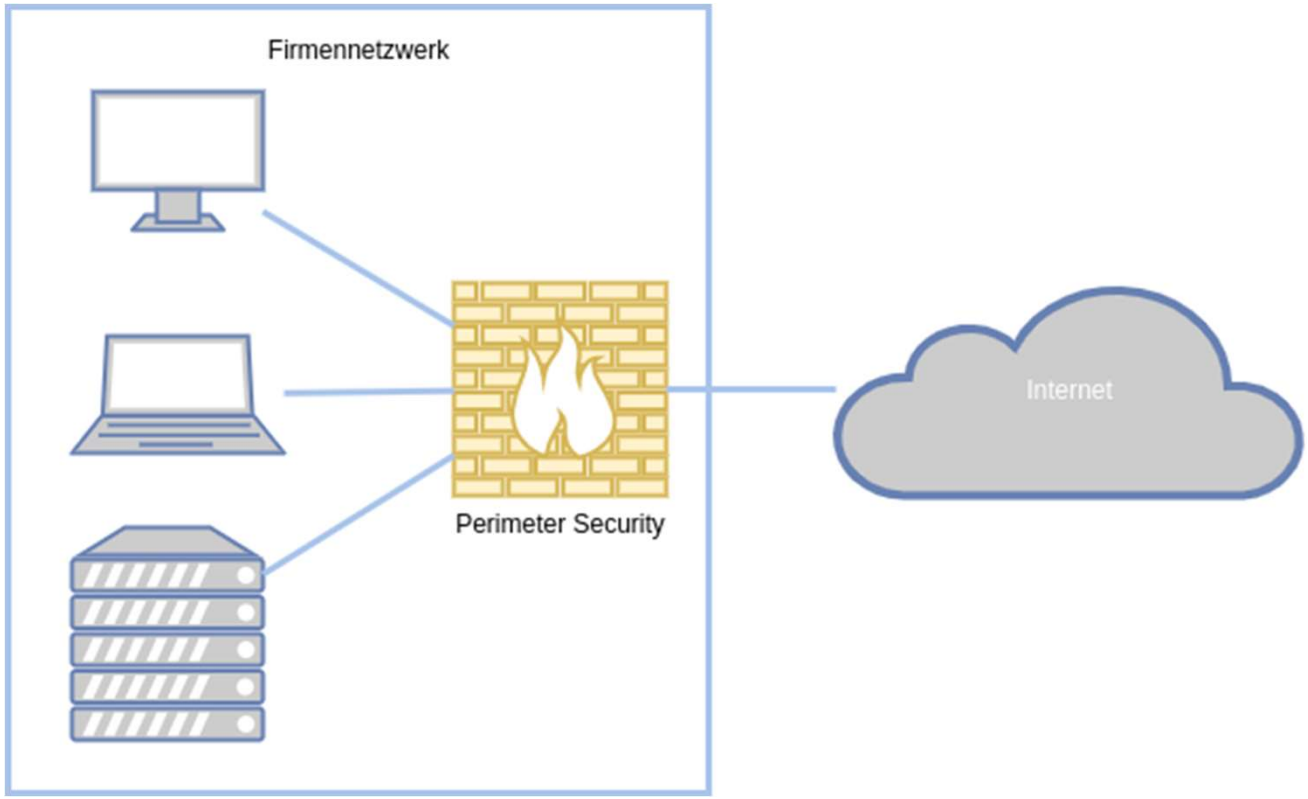
#01 Perimeter Security Massnahmen

Perimeter Security

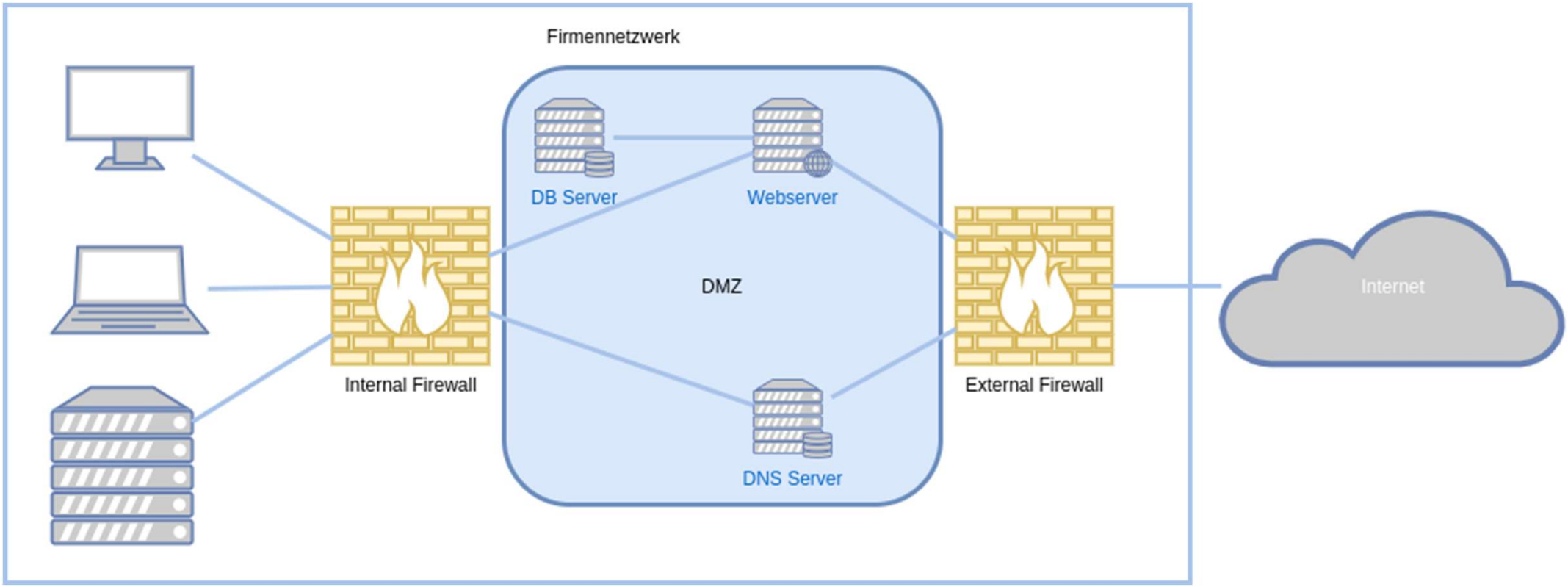


https://julianraxworthy.org/wp-content/uploads/2018/01/Construction-of-a-Castle-in-the-middle-Ages-816x479.jpeg

Firewall als Perimeter Security



Firewall Konzept mit DMZ



Firewall Konzept mit DMZ

- **Szenario/Use Case:** Du bist der IT-Sicherheitsbeauftragte eines mittelständischen Unternehmens, das kürzlich seine Online-Präsenz durch die Einrichtung eines Webshops erweitert hat. Da der Webshop Kundeninformationen und Transaktionsdaten verarbeitet, ist es von höchster Priorität, die Sicherheit dieser Daten zu gewährleisten. Zugleich muss der Webshop im Internet erreichbar sein, um Kunden den Zugriff zu ermöglichen.

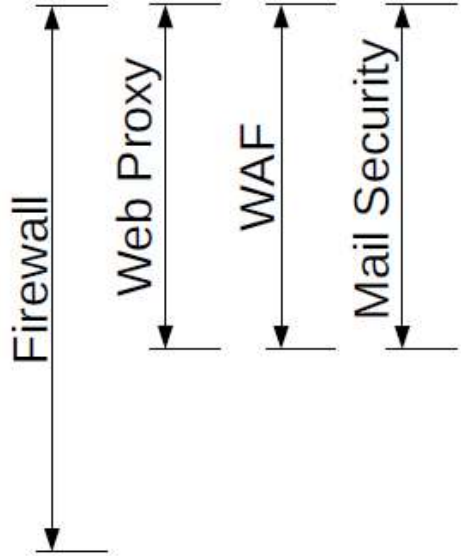
- **Aufgabe:** Deine Aufgabe besteht darin, ein Netzwerksicherheitskonzept zu entwerfen, das den Webshop vor unbefugtem Zugriff und Netzwerkangriffen schützt, während es gleichzeitig den sicheren Zugriff für Kunden und die notwendige Kommunikation mit internen Netzwerkressourcen (z.B. Datenbankserver) ermöglicht.

Firewall

- Ermöglicht Netzwerkszugriffseinschränkung unabhängig von Rechner / Server oder Applikation: Dies bezieht sich auf die Möglichkeit, den Zugang zum Netzwerk zu steuern, ohne dass dies von einem spezifischen Computer, Server oder einer spezifischen Anwendung abhängt. Das bedeutet, dass Zugriffsregeln auf Netzwerkebene definiert werden, die für alle Geräte gelten. Zum Beispiel um den Zugang zu verschiedenen Abteilungsnetzwerken zu kontrollieren, könnte man Netzwerkzugriffslisten (Access Control Lists, ACLs) auf den Routern oder Switches konfigurieren, die den Verkehr zwischen den Netzwerksegmenten vermitteln.
- Segmentierung in verschiedene Netze: Netzwerksegmentierung ist der Prozess der Aufteilung eines Netzwerks in kleinere Teile, oft um Leistung und Sicherheit zu verbessern. Dies kann durch physische Mittel (z.B. separate Switches) oder virtuell (z.B. VLANs) erfolgen.
- IP kontrollieren: Die Kontrolle über IP-Adressen bedeutet, dass der Netzwerkverkehr auf Basis der Quell- oder Ziel-IP-Adresse gefiltert oder geroutet werden kann. Dies kann für Sicherheitsmaßnahmen wie Zugriffssteuerung oder für Routing-Zwecke verwendet werden.
- Vermittlungsschicht, OSI Layer 3: Die Vermittlungsschicht, auch Netzwerkschicht genannt, ist die dritte Schicht des OSI-Modells. Sie ist verantwortlich für das Routing von Datenpaketen über verschiedene Netzwerke hinweg und verwendet dafür Netzwerkadressen (IP-Adressen).
- Ports kontrollieren: Die Kontrolle von Ports bezieht sich auf die Überwachung und Verwaltung des Netzwerkverkehrs basierend auf TCP- oder UDP-Ports. Dies wird häufig verwendet, um den Zugriff auf spezifische Dienste zu erlauben oder zu blockieren. Ein Port ist eine logische Adresse in einem Host, die verwendet wird, um unterschiedliche Anwendungsprozesse oder Dienste zu identifizieren. Zum Beispiel wird der Port 80 üblicherweise für HTTP-Verkehr verwendet und Port 443 für HTTPS. Im Kontext von OSI-Modell und Netzwerkprotokollen sind Ports jedoch ein Konzept der vierten Schicht, der Transportschicht.
- Transportschicht, OSI Layer 4: Die Transportschicht ist die vierte Schicht des OSI-Modells und verantwortlich für die Ende-zu-Ende-Kommunikation und Fehlerkontrolle. Sie sorgt für die korrekte Übertragung von Daten zwischen Hosts.
- NAT: NAT ist ein Verfahren, bei dem IP-Adressen und Ports von Netzwerkpaketen beim Durchgang durch einen Router oder eine Firewall geändert werden. Dies wird oft eingesetzt, um private IP-Adressen in öffentliche Adressen umzuwandeln, was die Anzahl der benötigten öffentlichen Adressen reduziert und die Sicherheit erhöht.
- Logging von Netzwerkaktivitäten: Das Logging ist der Prozess der Aufzeichnung von Ereignissen im Netzwerk. Dies kann den Datenverkehr, Zugriffsversuche, Systemereignisse und mehr umfassen. Logging ist entscheidend für die Überwachung und das Nachvollziehen von Aktivitäten im Netzwerk für Sicherheits- und Diagnosezwecke.
- Netfilter, CheckPoint, Fortinet etc: Dies sind Beispiele für Netzwerksicherheitsprodukte und -technologien. Netfilter ist ein Teil des Linux-Kernels, der das Filtern und Manipulieren von Netzwerkpaketen ermöglicht. CheckPoint und Fortinet sind Unternehmen, die Netzwerksicherheitsgeräte und -services wie Firewalls, VPNs und Intrusion Prevention Systems (IPS) anbieten

Weitere Security Massnahmen

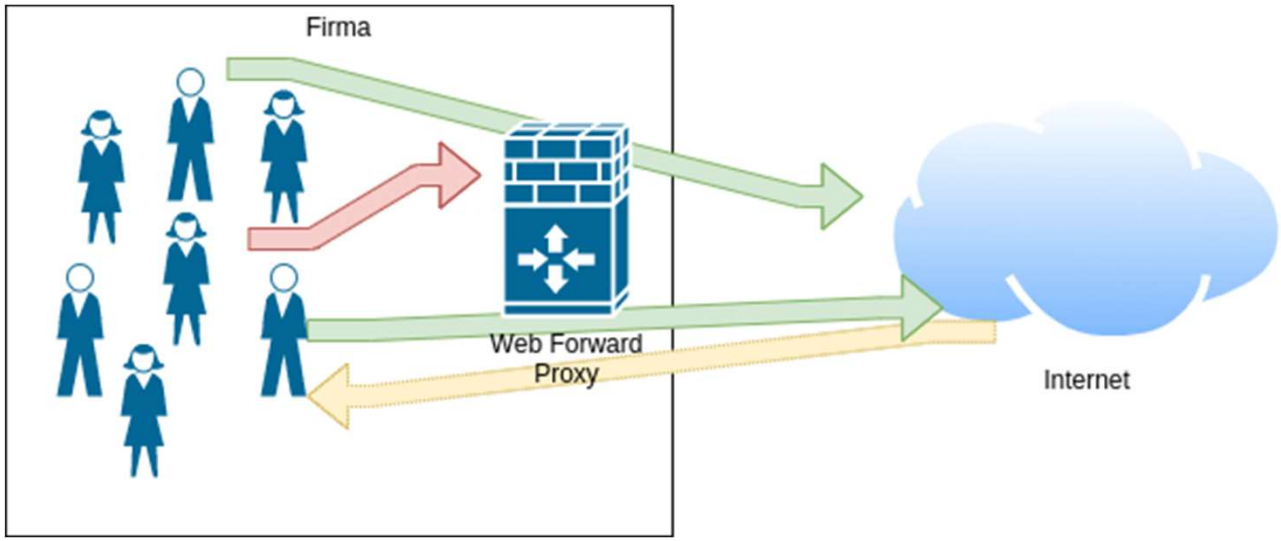
OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, UDS, FTP, SMTP, POP, Telnet, DHCP, OPC UA
Darstellung (6)		
Sitzung (5)		TLS, SOCKS
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6), ICMP (über IP)
Sicherung (2)	Netzzugang	Ethernet, Token Bus, Token Ring, FDDI
Bitübertragung (1)		



Weitere Security Massnahmen

- **Firewall:** Operiert typischerweise auf den Schichten 3 und 4, um den Verkehr basierend auf IP-Adressen und Ports zu filtern.
- **Web Proxy:** Arbeitet auf Anwendungsebene (Schicht 7 im OSI-Modell), um Webanfragen zu filtern und zu überwachen.
- **WAF (Web Application Firewall):** Schützt Webanwendungen, indem es auf Anwendungsebene arbeitet und speziell auf Webverkehr ausgerichtet ist.
- **Mail Security:** Schützt E-Mail-Dienste, indem es auf Anwendungsebene nach Bedrohungen wie Spam und Malware filtert.

Web Proxy

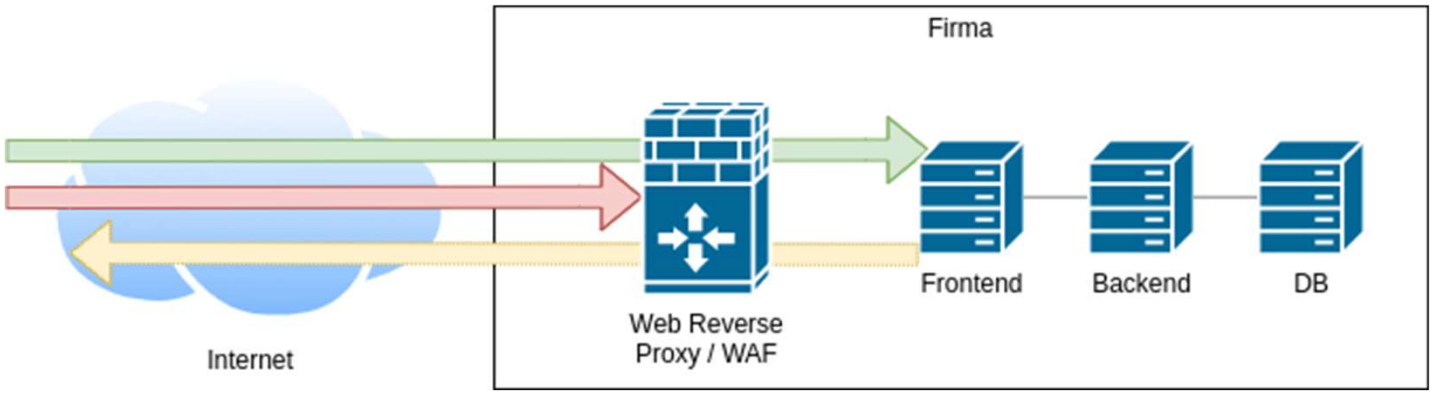


- Anti-Virus Scanning
- URL Filtering
- Connection- & Content-Rating
- Caching
- Logging
- User / Group Verwaltung
- Bandwidth Management

Web Proxy

- Anti-Virus Scanning: Überprüft den eingehenden und ausgehenden Webverkehr auf Viren und Malware, um das interne Netzwerk zu schützen.
- URL Filtering: Blockiert oder erlaubt den Zugriff auf bestimmte Websites basierend auf einer Liste von URLs, was dazu beitragen kann, Richtlinien zur Internetnutzung durchzusetzen und die Netzwerksicherheit zu verbessern.
- Connection- & Content-Rating: Bewerten und filtern Verbindungen und Inhalte, oft basierend auf Kategorien oder Reputationsscores, um unangemessene oder riskante Inhalte zu blockieren.
- Caching: Speichert lokal Kopien von häufig angeforderten Webinhalten, um die Ladezeiten zu beschleunigen und die Bandbreitennutzung zu reduzieren.
- Logging: Zeichnet Details über den Webverkehr auf, wie besuchte Websites, Zeitstempel und möglicherweise Benutzerinformationen, was für Überwachung, Analyse und Compliance wichtig sein kann.
- User / Group Verwaltung: Ermöglicht die Verwaltung von Zugriffsrechten und -regeln basierend auf Benutzer- oder Gruppenidentitäten.
- Bandwidth Management: Regelt die verfügbare Bandbreite für verschiedene Benutzer oder Dienste, um sicherzustellen, dass kritische Anwendungen ausreichend Netzwerkressourcen erhalten.

Web Reverse Proxy / Web Application Firewall (WAF)



- TLS-Termination
- Anti-Virus Scanning
- Logging
- Policy Enfocement bspw. OWASP Top 10
- Connection- & Content-Rating
- Caching
- Load Balancing

Web Reverse Proxy / Web Application Firewall (WAF)

Web Reverse Proxy / WAF

- Ein Web Reverse Proxy nimmt Anfragen aus dem Internet entgegen und leitet sie an interne Server (Frontend, Backend, Datenbanken) weiter. Wenn es mit einem WAF kombiniert wird, bietet es zusätzlichen Schutz für Webanwendungen.
- **TLS-Termination:** Der Proxy beendet die TLS-Verschlüsselung, was bedeutet, dass der verschlüsselte Verkehr vom Internet hier entschlüsselt wird, damit er intern analysiert werden kann, bevor er an das Backend weitergeleitet wird.
- **Anti-Virus Scanning:** Der eingehende Traffic wird auf Viren und Malware gescannt, um zu verhindern, dass schädliche Inhalte das interne Netzwerk erreichen.
- **Logging:** Alle durchgehenden Anfragen werden protokolliert, was für Sicherheitsüberwachung, Audits und Analysen wichtig ist.
- **Policy Enforcement:** Der WAF setzt Sicherheitsrichtlinien durch, wie zum Beispiel die OWASP Top 10, die eine Liste der häufigsten Webanwendungssicherheitsrisiken darstellt.

Web Reverse Proxy / Web Application Firewall (WAF)

Zusätzliche Funktionen

- **Connection- & Content-Rating:** Bewertet die Verbindungen und Inhalte, möglicherweise basierend auf Reputation oder Verhaltensanalysen, um gefährlichen oder unerwünschten Traffic zu identifizieren.
- **Caching:** Temporäres Speichern von häufig angeforderten Daten, um die Antwortzeiten zu verbessern und die Belastung der Backend-Server zu verringern.
- **Load Balancing:** Verteilt den eingehenden Traffic gleichmäßig auf mehrere Server, um die Last zu verteilen und die Verfügbarkeit und Zuverlässigkeit zu erhöhen.

Netzwerkstruktur

- **Frontend:** Der Teil der Webanwendung, der mit dem Benutzer interagiert, üblicherweise Webserver, die statische Inhalte und Anwendungslogik präsentieren.
- **Backend:** Server, die für die Verarbeitung der Geschäftslogik zuständig sind, oft Anwendungsserver oder APIs.
- **DB (Datenbank):** Hier werden Daten gespeichert und abgefragt, die für die Webanwendung notwendig sind.

Web Reverse Proxy / Web Application Firewall (WAF)

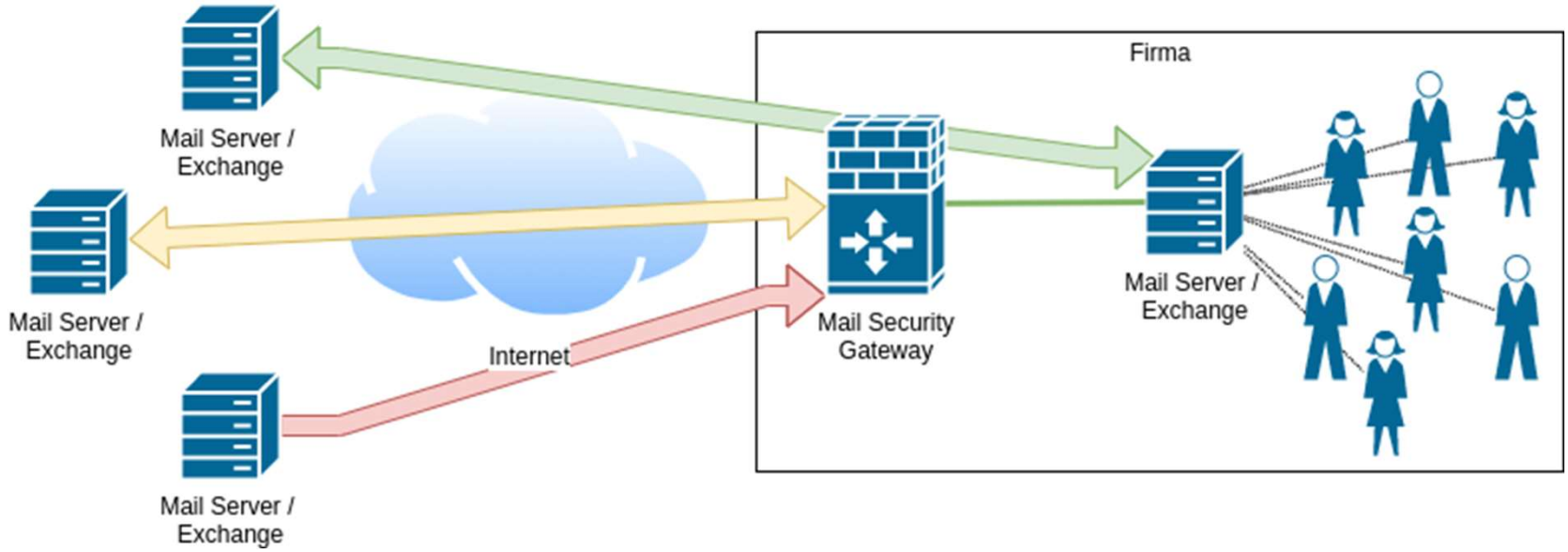
Beispiel: Verhinderung von SQL-Injection (OWASP Top 10 - A1: Injection)

Szenario: Eine Webanwendung nimmt Benutzereingaben über ein Formular entgegen und verwendet diese Eingaben, um eine Datenbankabfrage zu konstruieren. Ein Angreifer könnte versuchen, schädlichen SQL-Code in das Formular einzugeben, in der Hoffnung, dass die Anwendung diesen Code in die Datenbankabfrage einfügt und ausführt. Dies ist bekannt als SQL-Injection.

Lösung durch WAF: Ein WAF, der auf OWASP Top 10 basierende Regeln implementiert hat, würde wie folgt vorgehen:

- Anfrageüberwachung: Der WAF überwacht alle eingehenden HTTP-Anfragen an die Webanwendung.
- Erkennung von Anomalien: Wenn ein Benutzer eine Anfrage absendet, untersucht der WAF die Benutzereingaben auf Muster, die auf eine SQL-Injection hinweisen könnten. Zum Beispiel würde der WAF nach SQL-spezifischen Befehlen und Operatoren in den Eingabedaten suchen.
- Durchsetzung von Regeln: Der WAF wendet spezielle Regelsätze an, die entworfen wurden, um Injection-Angriffe zu erkennen. Diese Regeln können spezifisch für die Erkennung von unerwarteten oder bösartigen SQL-Befehlen in der Benutzereingabe sein.
- Blockierung oder Säuberung: Alerting: Der WAF kann zusätzlich Alarme auslösen, um die Administratoren zu benachrichtigen, dass eine mögliche Injection-Attacke erkannt wurde.
- Logging: Der WAF protokolliert den Vorfall für eine spätere Analyse und Überprüfung.

Mail Security Gateway



- Anti-Virus Scanning
- Deny- & Allow-Listing
- Anti-Spam
- Adress Harvesting Protection
- Logging
- Mail Routing

Mail Security Gateway

- **Anti-Virus Scanning:** Überprüft eingehende und ausgehende E-Mails auf Viren, Malware und andere schädliche Inhalte, um zu verhindern, dass diese das Netzwerk infizieren.
- **Deny- & Allow-Listing (auch als Blacklisting & Whitelisting bekannt):** Ermöglicht es Administratoren, bestimmte E-Mail-Adressen oder Domains zu blockieren (Deny-List) oder zu erlauben (Allow-List), um unerwünschte E-Mails zu filtern.
- **Anti-Spam:** Filtert Spam-E-Mails, um zu verhindern, dass unerwünschte oder potenziell schädliche Nachrichten die Posteingänge der Benutzer erreichen.
- **Adress Harvesting Protection:** Schützt vor Angriffen, bei denen versucht wird, gültige E-Mail-Adressen von einem Mailserver zu sammeln, um sie für Spam oder andere böswillige Aktivitäten zu nutzen.
- **Logging:** Protokolliert E-Mail-Aktivitäten, um Überwachung, Nachverfolgung und die Einhaltung von Compliance-Anforderungen zu unterstützen.
- **Mail Routing:** Bestimmt den Weg, den E-Mails nehmen, wenn sie in das oder aus dem Netzwerk gesendet werden, und leitet E-Mails entsprechend um, beispielsweise durch die Anwendung von Routing-Regeln oder die Verwendung von Failover-Mechanismen.

#02 Firewalling Grundidee

Server-Applikation und Betriebssystem

- Server-Applikationen hören auf einem Port auf eingehende Anfragen
  - Beispiel: Der Prozess Apache Webserver kann auf allen IPv4 Interfaces (0.0.0.0) für die Ports 80, 443 und 9000 hören. Eine andere Applikation kann dann nicht mehr auf derselben IP/Port Kombination hören.
- Eine Applikation/Prozess pro Port
  - Applikation fordert diesen vom Betriebssystem an
- Well-Known Ports setzen Root-/Administratorenrechte voraus
- Mehrere Applikationen pro IP-Adresse

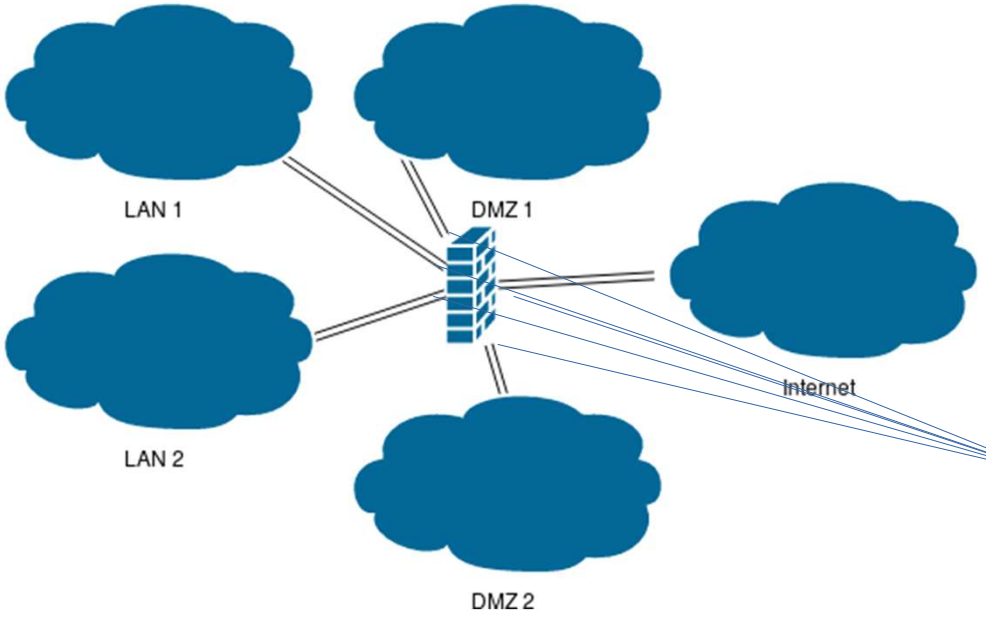
	IPv4	IPv6
Localhost	127.0.0.1	::1
Spezifisches Interface	129.168.1.210	2a02:168:4090::196
Alle Interfaces	0.0.0.0	:::

Prozesse und deren Sockets unter Linux anzeigen

```
$ sudo netstat -tulpn

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address          Foreign Address        State       PID/Program name

tcp        0      0 127.0.0.1:5433         0.0.0.0:*              LISTEN      1385/postgres

tcp        0      0 127.0.0.1:5434         0.0.0.0:*              LISTEN      1382/postgres

tcp        0      0 127.0.0.1:5435         0.0.0.0:*              LISTEN      1383/postgres

tcp        0      0 127.0.0.1:53           0.0.0.0:*              LISTEN      1944/stubby

tcp        0      0 127.0.0.1:8853         0.0.0.0:*              LISTEN      1333/stunnel4

tcp        0      0 127.0.0.1:631          0.0.0.0:*              LISTEN      1189/cupsd

tcp        0      0 127.0.0.1:5432         0.0.0.0:*              LISTEN      1388/postgres

tcp6       0      0 ::1:53                 :::*                   LISTEN      1944/stubby

...
```

Segmentierung von Netzen

- Verschiedene Bereiche eines Netzwerkes haben unterschiedliche Sicherheitsstufen
- Nicht jeder Rechner soll jeden anderen Rechner «sehen»



Firewall mit 5 Interfaces

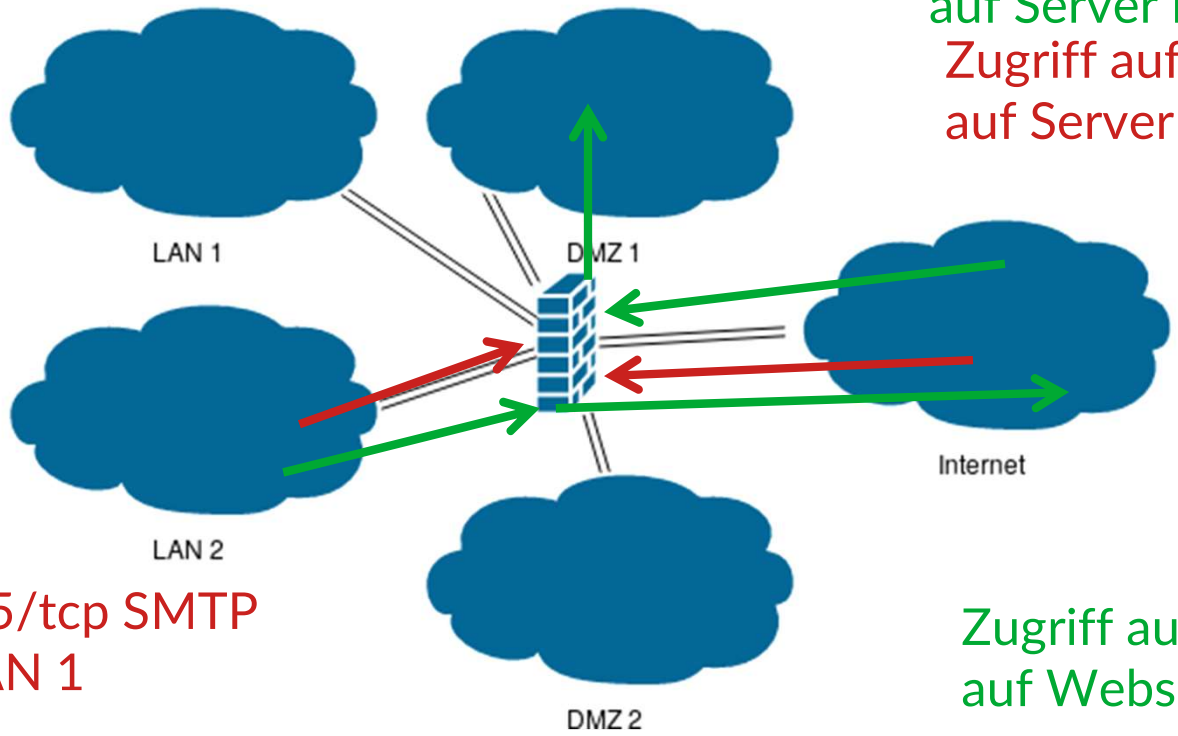
Typische Segmente

- Im Firmenumfeld wird das Netzwerk meist in verschiedene Teilbereiche aufgeteilt:
  - Internet: Nicht vertrauenswürdige Zone grösste Restriktion
  - DMZ: Demilitarisierte Zone mit strengen Zugriffskontrollen
    - «Was von extern und von intern erreichbar ist»
    - Server, Proxy, Mail-Gateway etc.
  - LAN: Interne Zone die aus dem Internet nicht erreichbar ist
    - Arbeitsplatzrechner, Drucker etc.
  - Server Netz: Interne Zone mit internen Servern die nicht (direkt) aus dem Internet erreichbar sind
    - AD, Exchange, File Share etc.

Firewalling Überblick

Zugriff auf Port 443/tcp HTTPS
auf Server in DMZ 1

Zugriff auf Port 445/tcp SMB
auf Server in DMZ 1



Zugriff auf Port 25/tcp SMTP
Auf Rechner in LAN 1

Zugriff auf Port 80/tpc HTTP
auf Webserver

Allgemeine Funktionsweise einer Firewall

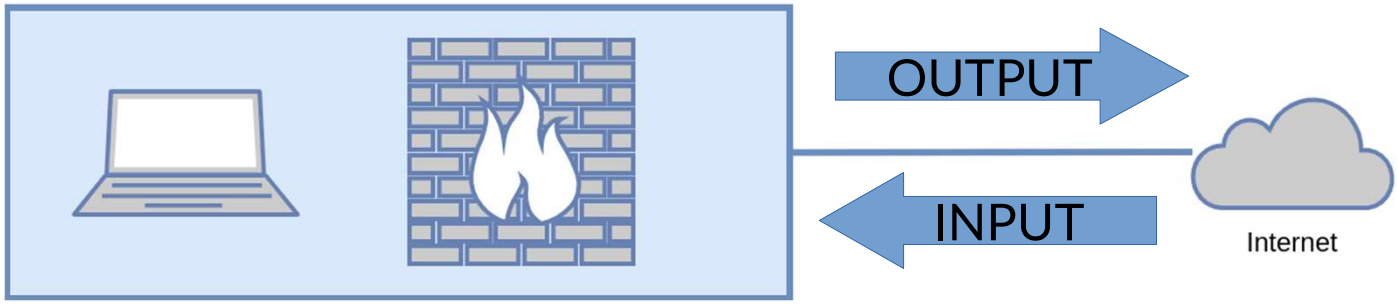
- Anwenden einer Regel eines Regelsets auf eintreffende Netzwerkpakete

Interface	INPUT / OUTPUT	Source	Destination	Port

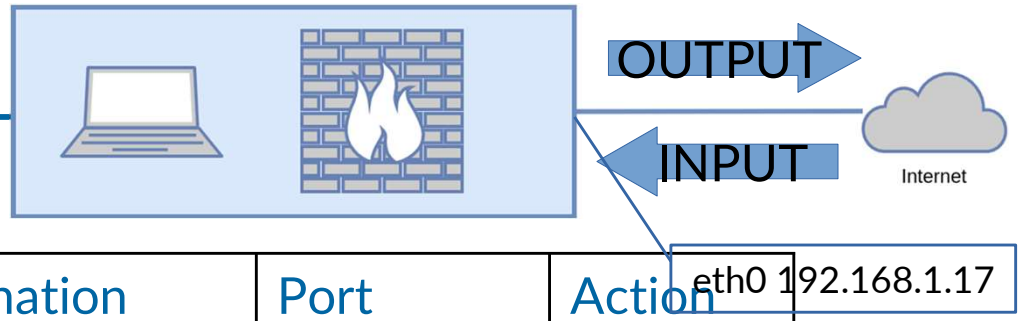
- Logisch-UND verknüpft
- Inbound: Aus Sicht des Gerätes kommt der Pfeil von extern auf das Gerät
- Outbound: Aus Sicht des Gerätes geht der Pfeil Richtung extern
- Ausführen einer Aktion
- Allow: Verbindung zulassen
- Deny/Block: Verbindung blockieren und keine Antwort zurücksenden
- Reject: Verbindung blockieren und Sender informieren
- Bspw. TCP Reset Paket oder ICMP Fehlermeldung
- Firewall allgemein gilt: First Match Action und Deny-All-Rule als Clean-up Rule

Fokus: Firewall auf lokalem System

- Wir konzentrieren uns auf ein Setup, in dem die Firewall direkt auf dem Server / Notebook konfiguriert wird:



Beispiel



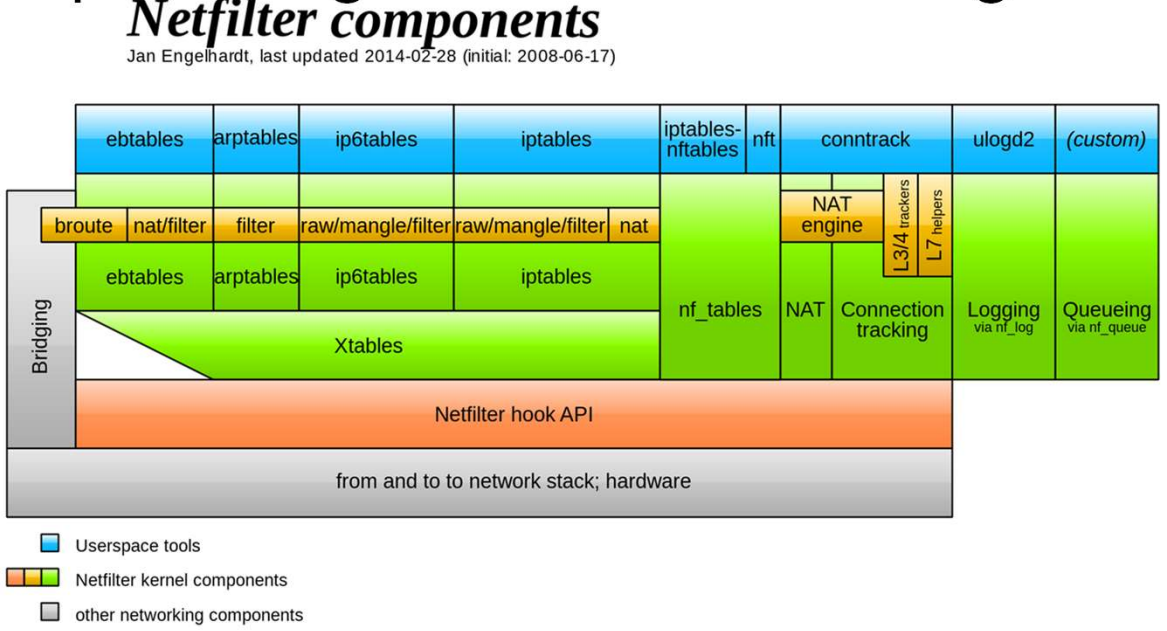
Interface	INPUT / OUTPUT	Source	Destination	Port	Action
eth0	INPUT	192.168.1.0/24	192.168.1.17	80/tcp	Allow
eth0	INPUT	192.168.1.0/24	192.168.1.17	443/tcp	Allow
eth0	INPUT	Any	Any	Any	Deny
eth0	OUTPUT	192.168.1.17	Any	443/tcp	Allow
eth0	OUTPUT	192.168.1.17	Any	53/udp	Allow
eth0	OUTPUT	Any	Any	Any	Reject

#03 Firewalling Netfilter und Iptables

Juventus
Technikerschule HF

Netfilter und Iptables

- Netfilter ist die Linux Firewall
- Iptables das Userspace Programm zur Verwaltung des Regelsets



Netfilter und Iptables

- **Iptables** ist ein Userspace-Werkzeug, das zur Konfiguration der Netfilter-Regeln verwendet wird. Administratoren nutzen iptables, um Regeln für das Filtern des Verkehrs, das NAT und andere Firewall-Aufgaben zu definieren**.**
- **Ebtables/Arptables/ip6tables:** Diese sind ähnlich wie iptables, aber für unterschiedliche Arten von Verkehr (Ethernet, ARP, IPv6).
- **Xtables:** Ein gemeinsamer Name für ebtables, arptables und iptables, der die vereinheitlichte Schnittstelle für diese Werkzeuge beschreibt.
- **NAT Engine:** Dies ist die Komponente, die für die Durchführung von NAT verantwortlich ist, was es privaten Netzwerken ermöglicht, eine öffentliche IP-Adresse für die Internetkommunikation zu verwenden.
- **Connection Tracking (conntrack):** Dies ist eine Funktion von Netfilter, die es ermöglicht, den Zustand von Netzwerkverbindungen zu verfolgen, was wichtig für fortgeschrittene Firewall-Regeln und NAT ist.
- **Logging (ulogd):** Ein Userspace-Daemon, der detailliertes Logging von Netzwerkverkehr ermöglicht, der durch Netfilter geht.
- **Queuing:** Eine Komponente, die es externen Programmen erlaubt, Netzwerkpakete zu empfangen und zu verarbeiten, möglicherweise für detaillierte Inspektion oder für User-Space-Implementierungen von Paketverarbeitung.

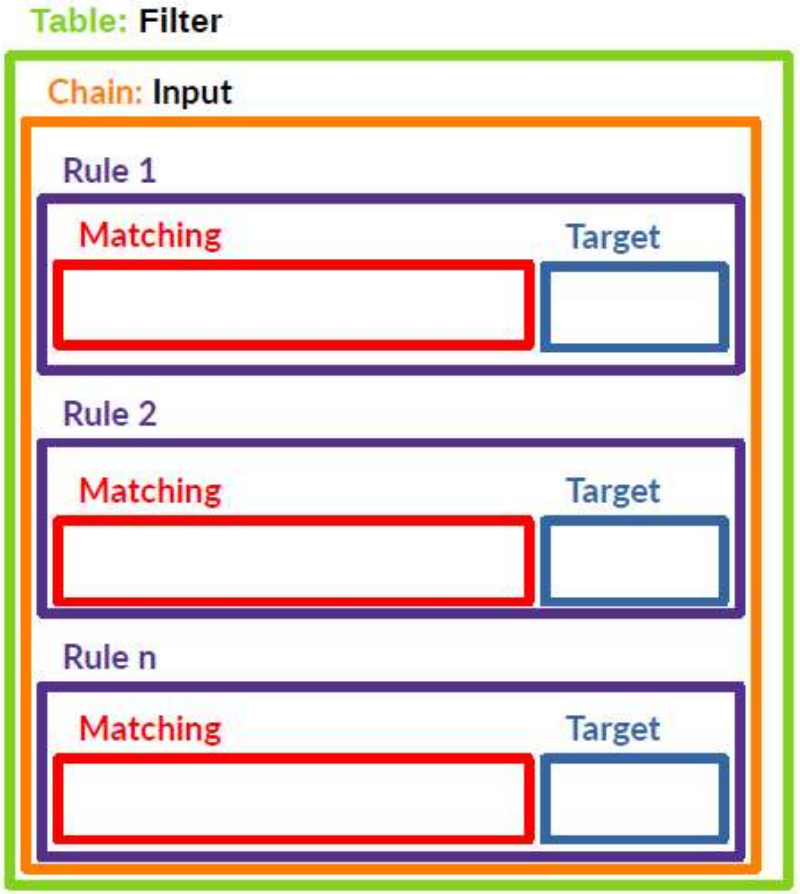
Netfilter und Iptables

Iptables ist ein Userspace-Werkzeug, das zur Konfiguration der Netfilter-Regeln verwendet wird. Administratoren nutzen iptables, um Regeln für das Filtern des Verkehrs, das NAT und andere Firewall-Aufgaben zu definieren.

- Iptables das Userspace Programm zur Verwaltung des Regelsets

Iptables Komponenten

- Tables
  - Verschiedene Tabellen beherbergen verschiedene Rule-Typen
  - Filter, NAT, Mangle, RAW & Security
- Chains
  - Punkt im Traffic-Flow an welchem eine Rule aktiv sein kan
  - Prerouting, Input, Forward, Output & Postrouting
- Rules
  - Bestimmt welche Action für ein Paket vorgesehen ist
  - Matching-Component
    - Protokoll, IP-Adresse, Port, Interface, Headers etc.
  - Target-Component
    - Terminating Targest: Accept, Drop, Reject und einige andere



Iptables Chain

- Jedes Netzwerkpaket (Inbound und Outbound) durchläuft mindestens eine Chain
  - INPUT – eingehende Pakete die für lokalen Socket vorgesehen sind
  - FORWARD – eingehende Pakete die für ein anderes System vorgesehen sind
  - OUTPUT – lokal generierte Pakete welche dieses System verlassen
- Jede Chain hat eine Policy
  - ACCEPT – Paket wird akzeptiert, Standardeinstellung
    - # iptables --policy INPUT ACCEPT
  - DROP – Paket wird verworfen
    - # iptables -P INPUT DROP

Regelset für einfachen, lokalen Webserver

- Port 80 eingehend erlauben

–# iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

- FORWARD und INPUT Chain alle Pakete verwerfen

–# iptables -P FORWARD DROP

–# iptables -P INPUT DROP

Regeln

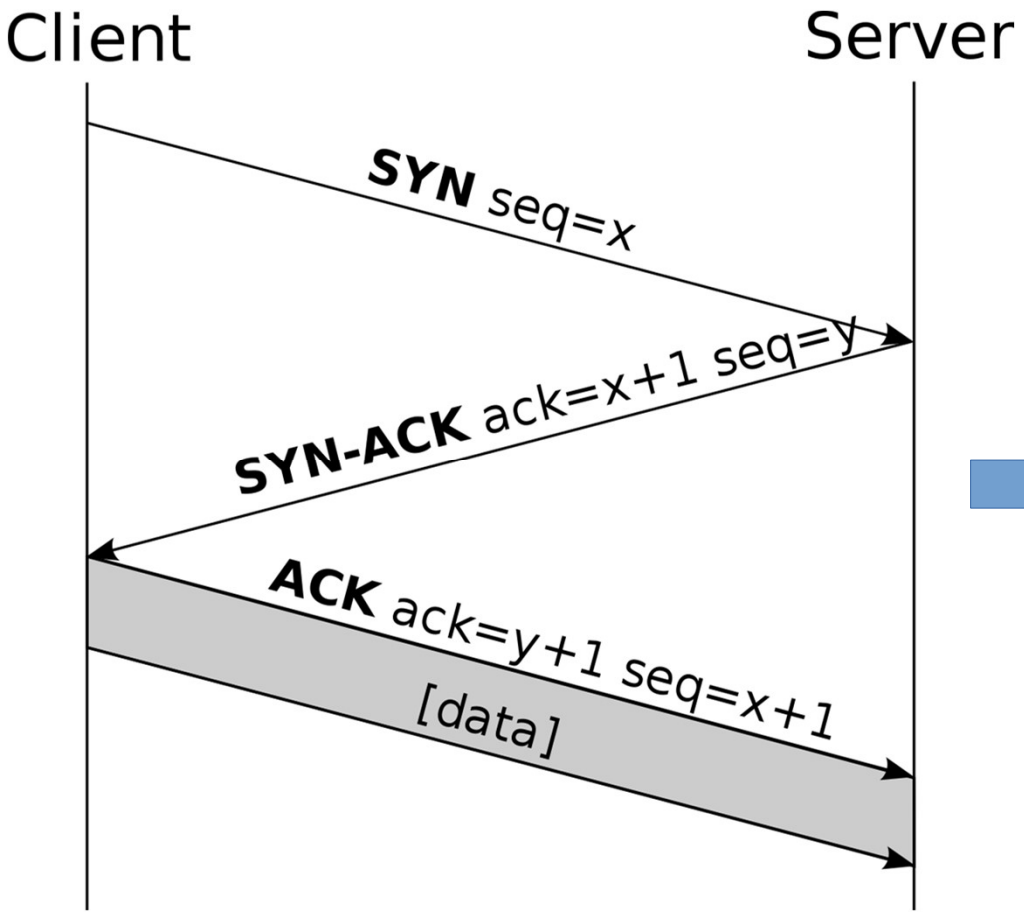
- Gehören zu einer Chain
  - Werden an diese angehängt -I am Anfang und mit -A am Ende des Regelsets
  - Und mit -D gelöscht (selber Befehl)
- Steuern Protokoll, Port und IP-Adressen
- Haben eine Aktion -j (für Jump)
  - ACCEPT
  - DROP
  - REJECT
- Ganzes Regelset kann mit iptables -L angezeigt werden
- Alle Regeln löschen mit iptables -F (ausser Chain Policy)

#04 Port Scanning

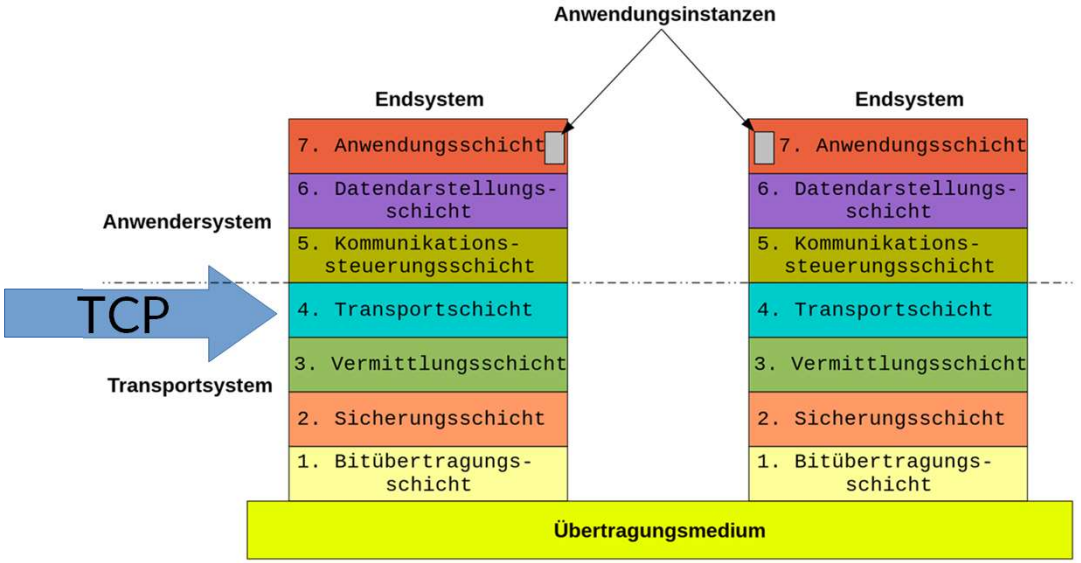
Netzwerk Port

- Ein Port ist der Bestandteil einer Netzwerk-Adresse auf dem Transport Layer (TCP und UDP)
  - Well-Known Ports: 0 bis 1023
  - Registered Ports: 1024 bis 49151
  - High Ports: 49152 bis 65535 (2^{16}-1)
- Server Applikationen sind an einen oder mehrere Ports gebunden (bind) und warten auf Anfragen (listen)
- Client Applikation wird vom OS ein Source Port zugeordnet

TCP Handshake



OSI-Modell



Quelle: Wikipedia

Der Port-Scanner Nmap

- Ziel ist Finden von offenen Ports
  - Jeder offene Port ist eine mögliche Bedrohung
- Einsatzzweck
  - Security Audits von Netzwerkgeräten
  - Finden von offenen Ports
  - Erstellen eines Netzwerkinventars
  - Finden von Schwachstellen in Software oder Systemen
- Vergewissern Sie sich stets, dass Sie den richtigen Host scannen und scannen Sie nie Systeme die Ihnen nicht gehören

Port Zustände

- Nmap ist in der Lage, Remote Ports in unterschiedliche Zustände einzuteilen. Die wichtigsten sind:
  - **open** – Applikation akzeptiert TCP Verbindungsaufbau
  - **closed** – Port ist erreichbar aber keine Applikation hört auf dem Port (TCP RST) → Host ist online!
  - **filtered** – Firewall blockiert Zugriff auf Port, kein TCP RST

Nmap Usage

- $ nmap scanme.nmap.org
  - Scan der 1000 häufigsten Ports
- $ nmap www.addere.ch -p 1,2,4-8,16
  - Scannt Ports 1, 2, 4, 5, 6, 7, 8 und 16

Scan-Techniken

- Nmap unterstützt eine Vielzahl unterschiedlicher Scan-Methoden mit spezifischen Einsatzzwecken
- TCP SYN scan (-sS) ist Standard-Scan
  - Nur SYN-Pakete, kein TCP Handshake, sehr schnell, erweiterte Rechte notwendig
- TCP connect scan (-sT)
  - Verwendet OS Network API und baut TCP Verbindung auf, weniger schnell und genau
- Weitere Scan-Methoden: UDP scan (-sU), TCP NULL, FIN und Xmas scan (-sN, -sF, -sX), TCP ACK scan (-sA), etc.

Service & Version Detection

- Service-DB mit ca. 2200 Port und Service Kombinationen
  - 25/tpc ist SMTP
- Schnell
- Ungenau respektive kann falsch sein
  - Webserver kann auch auf Port 25/tcp hören
- Keine Informationen über Service/Daemon
  - Jedoch nötig für Vulnerability Suche

Service & Version Detection

- Version detection mit -sV starten
- Verschiedene Anfragen werden auf Port geschickt und Antworten/Reaktionen ausgewertet
  - Service Protocol
    - FTP, SSH, Telnet, HTTP etc.
  - Application Name
    - ISC BIND, Apache httpd, Solaris telnetd etc.
  - Version Number
  - Hostname
  - Device Type
    - Printer, Router etc.
  - OS Family
    - Windows, Linux

Übungen & Labor

Übungen: HE1

Labor: hexposed/Lab: Hacking Exposed Juventus LAB (github.com)

Videoempfehlungen fürs Selbststudium

- Hirne Hacken (43 Min)