Aspect der Sicherheit von verteilten Systemen: Firewalls

Dozent: Prof. Dr. Michael Eichberg
Kontakt: michael.eichberg@dhbw.de

Version: 1.3.7

Quellen: Folien von Prof. Dr. Henning Pagnia bzgl. Netzwerksicherheit

---

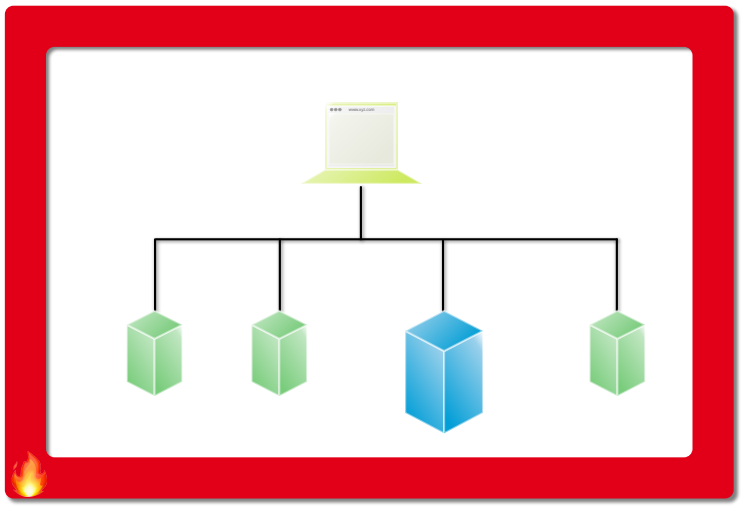
Folien: [HTML] https://delors.github.io/sec-firewalls/folien.de.rst.html
[PDF] https://delors.github.io/sec-firewalls/folien.de.rst.html.pdf

Fehler melden: https://github.com/Delors/delors.github.io/issues

1. Firewalls

2

Unabhängiges Netz - „Ideale Situation“



Vorteile:
- keinerlei Angriffsmöglichkeiten von außen

Nachteile:
- kein Schutz gegen Insider
- kein Zugang zum Internet

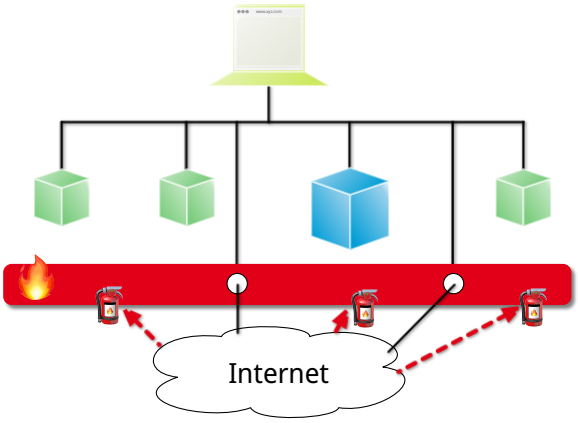
Wie bereits diskutiert gibt es auch Angriffsmuster gegen Air-Gapped-Systeme. Ein Beispiel ist der Stuxnet-Wurm, der sich initial über USB-Sticks verbreitet.

Wenn man kein Zugang zum Internet hat, dann hat man zum Beispiel kein Zugriff auf externe Dienste wie NTP und das Einspielen von Updates ist nur über Umwege möglich.

Von der Notwendigkeit des Schutzes von Rechnern

> [...] Züger und sein Team hätten [...] erst kürzlich ein Experiment durchgeführt, [...]. Sie hätten einen Computer "ohne jeglichen Schutz" mit dem Internet verbunden, um zu sehen, wie lange es dauere, bis er befallen sei. Konkrete Details zur Konfiguration dieses Systems werden zwar nicht genannt, angeblich war der Rechner aber schon nach 20 Minuten infiltriert.
>
> —Golem.de 6.2.2024

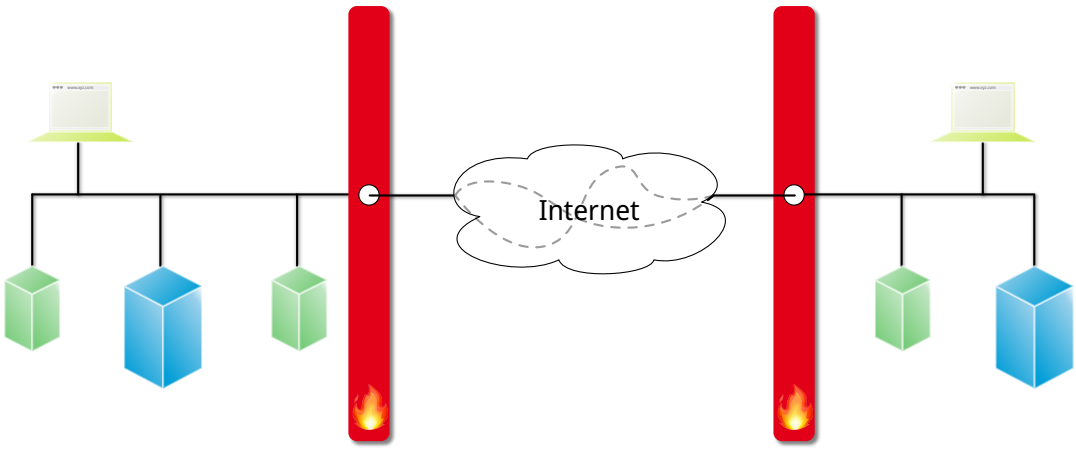
Schutzschicht zwischen internem und externem Netz



- Kontrolle des Nachrichtenverkehrs durch Filterung
- begrenzte Isolation mit begrenztem Schutz

Eine Firewall schafft zwischen verbundenen Netzen Sicherheitsdomänen mit unterschiedlichem Schutzbedarf. Eine wichtige Teilaufgabe ist das Ausarbeiten von Sicherheitsrichtlinien.

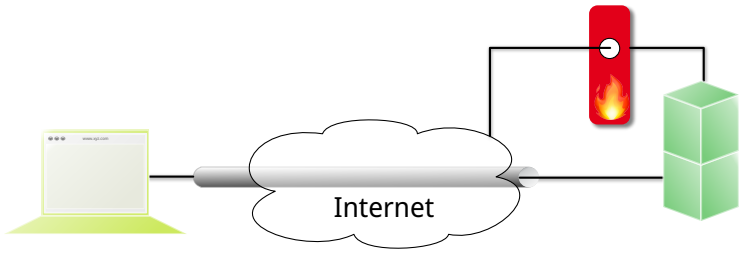
Realisierung von Virtual Private Networks (VPN)



- Aufbau einer scheinbar privaten Verbindung von Firmenteilnetzen über das (öffentliche) Internet.
- Zusätzliche Verbindungsverschlüsselung zwischen den Firewalls.

Ziel ist es aktive und passive Angriffe zu unterbinden. Selbst bei verschlüsselten Verbindungen kann die Verkehrsflussanalyse noch Informationen liefern über die Verbindungen liefern.

Kommerzielle VPNs für Endnutzer



Motivation

- Schutz der Privatsphäre; der ISP kennt nicht mehr die Webseiten, die man aufruft.
- Die IP-Adresse des Nutzers ist den aufgerufenen Webseiten nicht mehr bekannt und kann deswegen der Umgehung von Geo-Blocking dienen.

Nachteile?

- Vertrauen in den VPN-Anbieter muss vorhanden sein. Insbesondere, beim Einsatz zum Stärken der Privatsphäre, muss der VPN-Anbieter vertrauenswürdig sein und sollte ein so genannter „no-log“ Anbieter sein.
- Es gibt auch (scheinbar kostenlose) VPN-Anbieter, die die Daten der Nutzer dann aber verkaufen (ehemals: Facebook Onavo).

Schutz auf den Schichten des TCP/IP Stacks

Zentraler Schutz des gesamten internen Netzwerks durch:

- Paket Filter ( *Packet Filtering*)
  - Blockieren bestimmter IP-Empfänger-Adressen (extern / intern)
  - Blockieren bestimmter IP-Absender-Adressen (extern / intern)
    (z. B. aus dem Internet mit internen IP-Absender-Adressen)
  - Blockieren bestimmter Dienste; ggf. nur für bestimmte IP-Adressen
- Filter auf Anwendungsebene ( *Application-level Filtering*)
  - inhaltsbezogene Filterung der Verkehrsdaten eines Dienstes
    (z. B. Virenfilter oder Spamfilter)
  - wirkungslos bei verschlüsselten Verkehrsdaten
- Protokollierungsmöglichkeit der Kommunikation von / nach extern

---

Firewalls (alleine) können die Struktur des Netzwerks nicht verbergen.

DoS Attacke auf Anwendungsebene

> […] Angriff auf die Kleinen
>
> Waren bei früheren Spamangriffen massenhaft Accounts auf der größten Mastodon-Instanz `mastodon.social` angelegt worden, die dann von dort ihre Inhalte verbreiteten, trifft es nun nicht die größte, sondern die kleinsten. Automatisiert werden dabei Instanzen ausgesucht, auf denen eine Registrierung ohne Überprüfung und sogar ohne ein Captcha möglich ist. Das können etwa solche mit wenigen Accounts sein, die von Enthusiasten etwa für eine Gemeinde betrieben werden. Waren die Verantwortlichen in den vergangenen Tagen nicht aufmerksam, wurden diese Instanzen dann regelrecht überrannt. Die Spam-Accounts verschickten massenhaft Nachrichten mit einem Bild des namensgebenden Frühstücksfleischs und Links zu Discord-Servern, die wohl lahmgelegt werden sollten.
>
> —Mastodon: Spamwelle zeigt Schwächen auf […]

Realisierungsmöglichkeiten von Firewalls

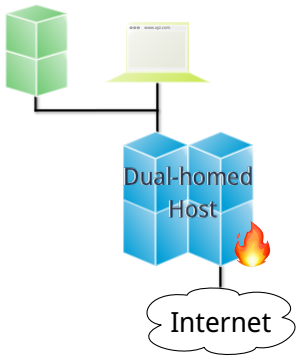
- Hardware-Firewall
  - Screening Router
  - Application Gateway (auch Bastion Host)
    - (Reverse-)Proxy-Server für bestimmte Dienste
    - Endpunkt aus Sicht von Client-Software (HTTP-Browser, EMail, ...)
    - spezialisierte Server-Software
- Software-Firewall (*Personal Firewall*)

Im Falle eines  *Bastion Host*, ist dies der einzige unmittelbar aus dem Internet erreichbare Rechner.

Dual-Homed Host

Aufbau

- zwei Netzwerkkarten: ggf. private interne Adressen
- Screening Router & Gate: Packet Filter und Application-Level Filter
- Proxy-Dienste installieren
- Benutzer-Logins von extern



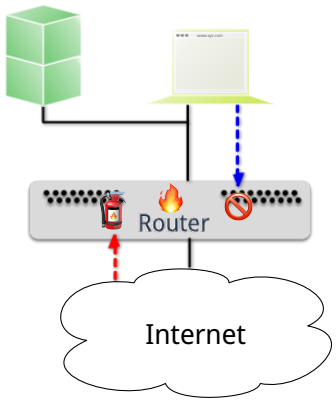
!! Wichtig

Bei der Konfiguration der Netzwerkkarten gilt:

IP-Pakete nicht automat. weiterleiten

Screening Router

Aufbau



Programmierbarer Hardwarerouter mit simplen Filterfunktionen:

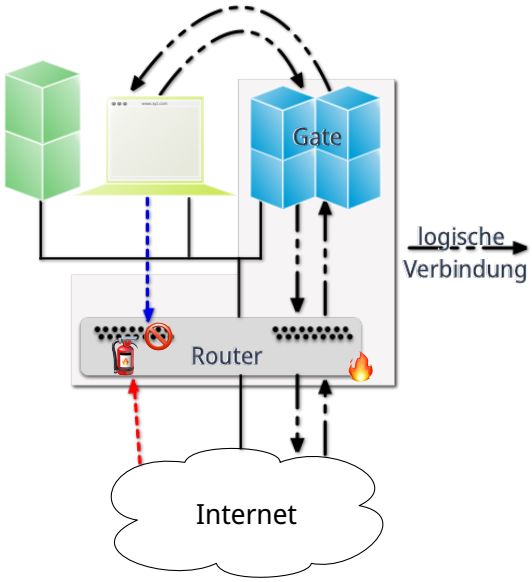
- nur Paket-Header prüfen
- schnelle Auswertung ermöglicht hohen Durchsatz
- Realisierung eines Packet Filters

Bewertung	
✓einfach und billig	! schwer zu testen
✓flexibel	! Protokollierung
	! Fernwartung
	! keine Inhaltsfilterung

Screened Host

Aufbau

- Screening Router blockiert:
  - Pakete von / an interne Rechner (nicht Gate)
  - Source-Routed Pakete
- von extern nur Gate sichtbar
- Pakete von intern nur via Gate
- Gate bietet Proxy-Server (z. B. für E-Mail)



Source-Routed Pakete sind Pakete, die den Weg durch das Netzwerk explizit angeben. (*Source-routing* wird auch als *Path Addressing* bezeichnet und wird im Allgemeinen als Sicherheitsproblem angesehen.)

Gibt es für eine bestimmte Anwendung kein Application-level Proxy, dann kann auf einen für TCP/UDP generischen Proxy zurückgegriffen werden. Dieser arbeitet auf dem Session Layer und kann nur die Header-Informationen auswerten. Es handelt sich dann um ein *Circuit-level Proxy/Gateway*. Im Vergleich zu einem Application-level Proxy ist die Sicherheit geringer, da der Circuit-level Proxy nicht in der Lage ist, die Daten zu interpretieren.

Ein allgemeines Problem ist, dass viele Anwendungen auf generische Protokolle wie HTTP aufsetzen. Weiterhin betreiben einige Anwendungen „Port Hopping“, d. h. sie wechseln den Port wenn der Standardport nicht offen ist.

Eine Anforderung an „Next-generation Firewalls“ ist, dass diese die Analyse von den Daten einer Anwendung unabhängig vom Port und Protokoll ermöglichen.

Konfiguration eines Gateways

Das Ziel der Konfiguration muss eine minimale angreifbare Oberfläche sein.

- Abschalten aller nicht-benötigten Netzdienste
- Löschen aller nicht benötigter Programme
- Rechte von `/bin/sh` auf 500 setzen
- Rechte aller Systemverzeichnisse auf 711 setzen
- keine regulären Benutzerkennungen
- root-Login mit Einmal-Passwortsystem bzw. 2-Faktor Authentifizierung
- setzen von Platten- und Prozess-Quotas
- volle Protokollierung, möglichst auf Hardcopy-Gerät
- möglichst sichere, stabile und regelmäßig aktualisierte Betriebssystemversion einsetzen

---

Die Rechte von `/bin/sh` auf 500 setzen bedeutet, dass nur der Eigentümer (root) es ausführen kann.

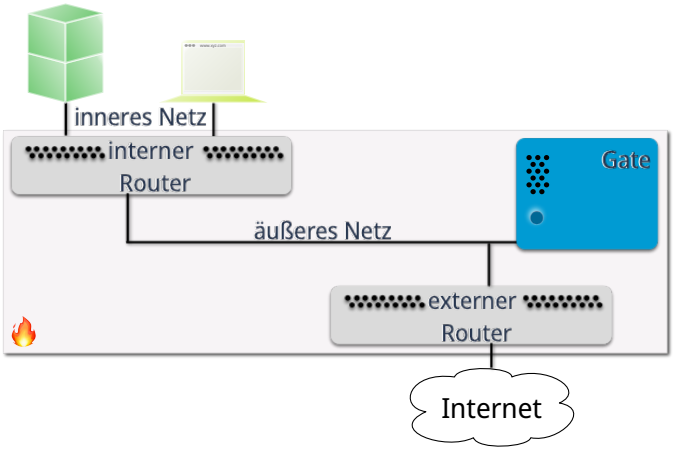
Default:

```
$ ls -al /bin/sh
-rwxr-xr-x  1 root  wheel  101232 Oct  1 06:10 /bin/sh
```

Screened Subnet

Aufbau

- interner Screening Router als weiterer Schutzwall
  - blockiert Dienste, die nicht einmal bis zum Gate gelangen sollen
  - lässt nur Pakete zum / vom Gate durch
- äußeres Netz realisiert Demilitarisierte Zone (DMZ) für HTTP-Server, Mail-Server, ...



2. Intrusion Detection Systeme (IDS)

Intrusion Detection Systeme (IDS)

Definition

Ein IDS ist ein Gerät (meist ein speziell konfigurierter Rechner), das vielfältige Techniken zur Erkennung von Angriffen anwendet und Angriffe meldet und ggf. abwehrt, in dem (z. B.) die Firewall automatisch umkonfiguriert wird.

Motivation

- Firewalls alleine sind zu statisch und deswegen häufig nicht ausreichend
- bessere Aufzeichnung und flexiblere Erkennung notwendig
- angepasste Reaktion notwendig

Umsetzung

An verschiedenen, neuralgischen Stellen werden spezielle Sensoren platziert, die (hier) den Netzwerkverkehr überwachen und verdächtige Aktivitäten melden.

Miteinander verwandt bzw. typischerweise in einem Produkt zu finden:

- Intrusion Detection (IDS)
- Intrusion Response (IRS)
- Intrusion Prevention (IPS)

IDS-Erkennungstechniken

- Signaturerkennung
- statistische Analyse
- Anomalieerkennung

Probleme

- Fälschlicherweise gemeldete Angriffe (false positives)
- nicht gemeldete Angriffe (false negatives) (insbesondere bei neuartigen Angriffen)
- Echtzeitanforderung, insbesondere bei Hochgeschwindigkeitsnetzen
- Aufzeichnung bei Netzwerken mit Switches (⇒ spez. SPAN Port)
- Sensoren sollen unbeobachtbar sein (*stealth*)

SPAN ( *Switched Port Analyzer*) Ports sind spezielle Ports auf Switches, die bestimmten Verkehr (z. B. bestimmte Pakete) die über ein Switch gehen, an einen definierten Port weiterleiten können. An diesem Port kann dann eine Analyse des Verkehrs durchgeführt werden / ein Sensor angeschlossen werden.

Übung

2.1. Firewalls

1. Was sind Vorteile eines Dual Homed Host gegenüber einem Paketfilter? Was sind die Nachteile?
2. Benennen Sie zwei konzeptionelle Grenzen von Firewalls. D. h. zwei Szenarien gegen die Firewalls nicht schützen können.
3. Für welche der folgenden Cybersicherheitsstrategien können Firewalls eingesetzt werden:
    1. Angriffe vermeiden
    2. Angriffe erkennen
    3. Angriffe abwehren/Angriffen entgegenwirken
    4. Reaktion auf Angriffe
4. Sie werden beauftragt die Firewall so einzurichten, dass Mails mit Schadsoftware nicht durchgelassen werden. Wie reagieren Sie?