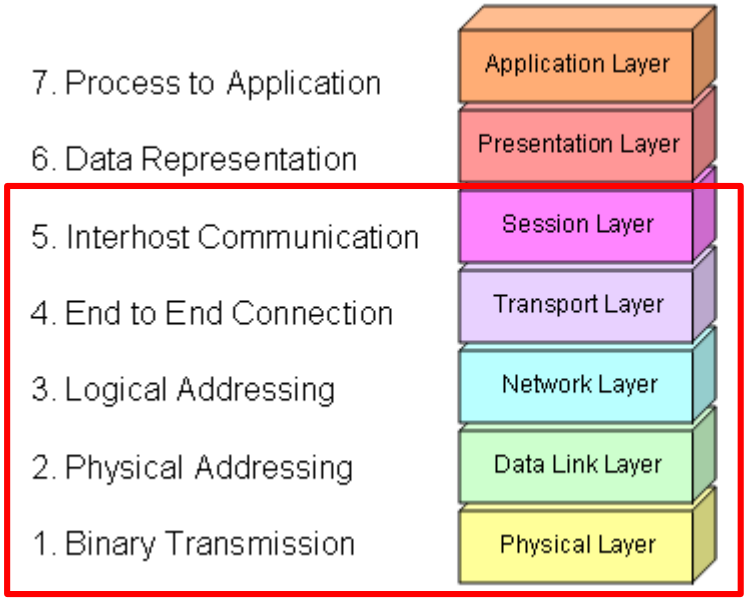
IT-SICHERHEIT UND DATENSCHUTZ

KAPITEL 6 - NETZWERK-SICHERHEIT

buchmann@hft-leipzig.de

LERNZIEL UND AUFBAU DIESES KAPITELS

- Internet-Protokolle
  - Kommunikation in Netzwerken und nach „außen“ ins Internet
- Angriffe
  - belauschen der Kommunikation
  - unsichere Protokolle und Architekturen
- Firewalls
  - Paketfilter und Firewall-Architekturen



- Lernziele
  - Sie können erklären, welche unterschiedlichen Arten von Angriffe auf die Netzwerkkommunikation existieren
  - Sie sind in der Lage, für ein einfaches Szenario eine Firewall-Architektur auszuwählen und einen Regelsatz für einen Paketfilter aufzustellen

ZIELE DER IT-SICHERHEIT

- „Security triad“
  - **Vertraulichkeit**: Asset ist nur Autorisierten zugänglich
  - **Integrität:** Asset kann nur von Autorisierten modifiziert werden
  - **Verfügbarkeit**: Asset kann von Autorisierten genutzt werden

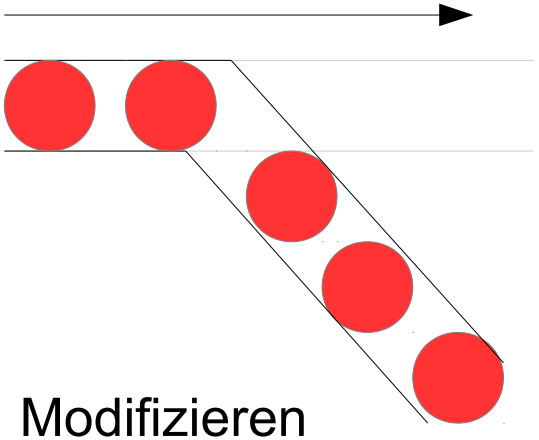
- ISO 7498-2 fügt hinzu
  - **Authentisierung**: Identität eines Senders wird überwacht
  - **Nichtabstreitbarkeit**: Sender kann nicht abstreiten, das eine Nachricht von ihm kam
- US Department of Defense fügt hinzu
  - **Auditierbarkeit**: Alle Aktionen mit dem Asset sind nachvollziehbar

ANGRIFFE AUF DIE NETZWERK-SICHERHEIT

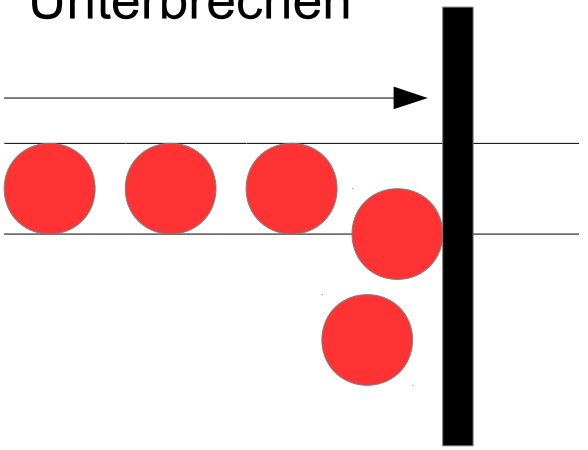
MÖGLICHKEITEN, UM SCHADEN ZU VERURSACHEN

Wiederholung

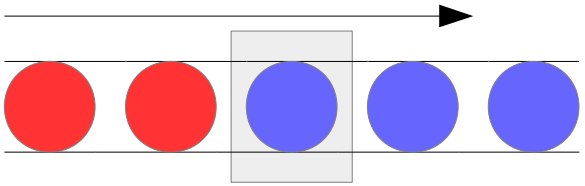
- Abfangen



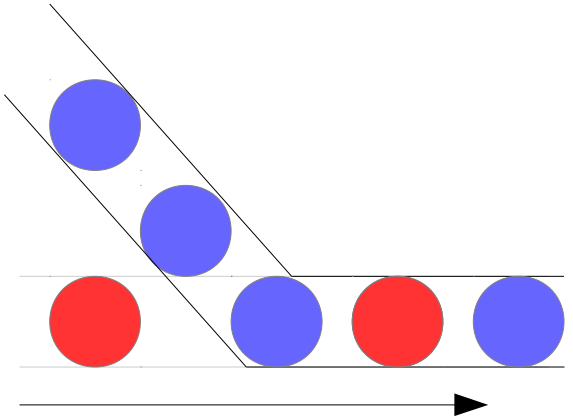
- Unterbrechen



- Modifizieren



- Einschleusen



HERAUSFORDERUNGEN IN DEN OSI-LAYERN 1-5

- **Vertraulichkeit**
  - Belauschen vertraulicher Datenpakete (ganz besonders drahtlose Protokolle wie WLAN/Bluetooth/etc. mit Richtfunkantennen)
  - Man-in-the-middle-Angriffe, sowohl physikalisch (Angriff/Tausch eines Routers) als auch logisch (s. Kapitel 6)

- **Integrität**
  - Datenübertragungen sind sehr leicht störbar (physikalisch → Sonennflecken, logisch → Services wie ARP, DNS,...)
  - Einschleusen von gefälschten Datenpaketen ebenfalls leicht

- **Verfügbarkeit**
  - Denial of service, z.B. durch Dienstüberlastung, stören von Routingtabellen, unvorsichtige Baggerfahrer

WAS MACHT NETZWERKE ANFÄLLIG? (1/2)

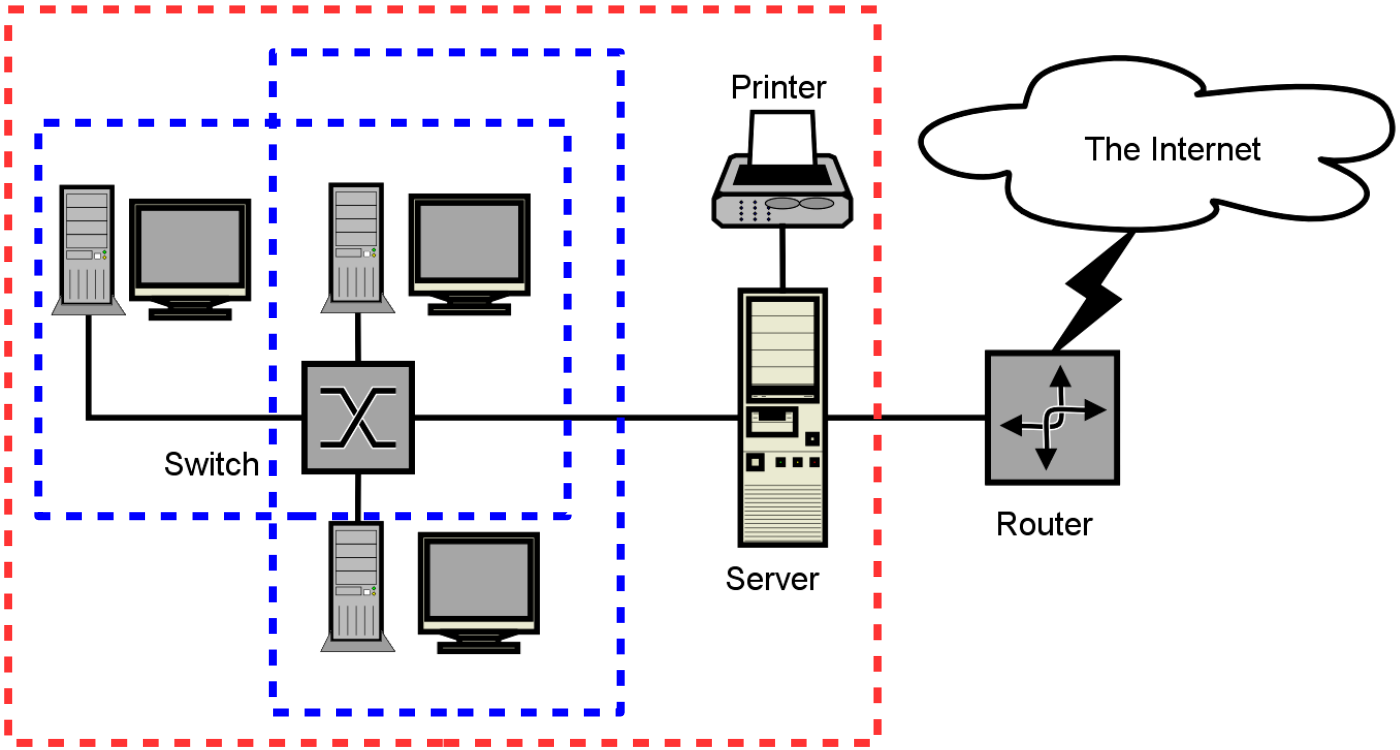
- Anonymität, Angriffe aus Sicherheitsabstand
  - Angreifer kann weit entfernt von den physischen Netzwerkgeräten sein
  - Angriff lässt sich über mehrere Stationen routen (s. Kapitel 9)

- Systemkomplexität
  - Viele potentielle Schwachstellen
  - Zahllose Rechner, Kabel, Switches, Protokolle, Dienste etc., die alle gleichzeitig funktionieren müssen

- „Mischbetrieb“
  - Netzwerke und insbes. Netzwerkbandbreite sind eine endliche Ressource, die von vielen gleichzeitig beansprucht wird

WAS MACHT NETZWERKE ANFÄLLIG? (2/2)

- Unbekannte Perimeter
  - Prinzipiell könnte jeder Rechner im Netz als WLAN-Hotspot oder Bridge in ein anderes Netzwerksegment dienen
  - Neue Rechner können prinzipiell überall im Netz hinzugefügt werden
- Unbekannte Pfade
  - Es ist nicht festgelegt, welchen Weg Datenpakete nehmen sollen



Metropolitan.fi
News from Finland in English

DDoS attack halts heating in Finland amidst winter

A Distributed Denial of Service (DDoS) attack halted heating distribution at least in two properties in the city of Lappeenranta, located in eastern Finland. In both of the events the attacks disabled the computers that were controlling heating in the buildings.

Both of the buildings where managed by Valtia. The company who is in charge of managing the buildings overall operation and maintenance. According to Valtia CEO, Simo Rounela, in both cases the systems that controlled the central heating and warm water circulation were temporarily disabled.

In the city of Lappeenranta, there were at least two buildings whose systems were knocked down by the network attack. In a DDoS attack the network is overloaded by traffic from multiple locations with the aim of causing the system to fail.

In an interview with Etelä-Saimaa, Rounela estimated the attack in Eastern Finland lasted from late October to Thursday the 3rd of November. The systems that were attacked tried to respond to the attack by rebooting the main control circuit. This was repeated over and over so that heating was never working.

At this time of the year temperatures in Finland are below freezing and a long-term disruption in heat will cause both material damage as well as the need to relocate residents elsewhere. Thankfully in this case the fix was easy to do by limiting network traffic.

News from Finland

Read more »

Recent Entries

- DDoS attack halts heating in Finland amidst winter
- Finland preparing a radical car taxation reform to lower emissions
- Finland in mid-tier when it comes to European software developer salaries
- "Finland could employ some 2000-3000 developers immediately"
- Estonia the first country in Europe to legalize Uber

Entries overview »

Recent Formula 1 Facts

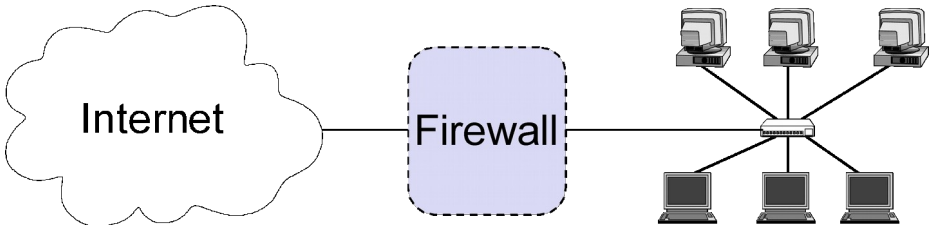
- Why does the red rear light of a F1 car blink/flash in dry conditions?
- How long does it take to assemble a Formula 1 car?
- Does the use of fuel during the race change the balance of a Formula 1 car?

FIREWALLS

WAS SIND FIREWALLS?

- Vergleichbar mit einem Stadttor
  - Leute dürfen nur an Kontrollpunkt die Stadt betreten oder verlassen
  - Angreifer kommen gar nicht erst in die Nähe anderer Verteidigungspunkte in der Stadt

- Üblicherweise separiert eine Firewall zwei Netzwerk-Segmente mit unterschiedlichen Sicherheitsniveaus
  - Offensichtliches Beispiel: Firewall zwischen Internet und Firmennetz



  - Weniger offensichtliches Beispiel: Firewall zwischen der Testumgebung der Entwickler und dem Netzbereich der Firmenleitung

WAS LEISTEN FIREWALLS FÜR DIE IT-SICHERHEIT?

- Eine Firewall dient als Fokus für Sicherheitsentscheidungen
  - Wo sind eigentlich meine sensiblen Daten?
- Eine Firewall kann Sicherheitsregeln durchsetzen
  - Wer darf überhaupt mit wem kommunizieren?
- Eine Firewall kann Aktivitäten mitloggen
  - Wer kommuniziert wann mit wem über welches Protokoll?
- Eine Firewall kann Sicherheitsprobleme auf ein Teilnetz beschränken
  - Welche Rechner oder Dienste müssen von jedermann aus dem Internet erreichbar und damit potentiell angreifbar sein?

WAS KÖNNEN FIREWALLS NICHT LEISTEN?

- Eine Firewall schützt nicht gegen Angreifer von Innen
- Eine Firewall überwacht keine Verbindungen, die an ihr vorbei gehen
  - Wenn ein Angestellter einen LTE-Surfstick in seinen Rechner steckt, kann prinzipiell jeder Datenverkehr darüber laufen
- Eine Firewall schützt nicht zuverlässig gegen neue Bedrohungen
- Eine Firewall schützt nicht zuverlässig vor Viren, Trojaner, Malware
- Eine Firewall kann sich nicht von allein konfigurieren
  - Regeln benötigen Hintergrundwissen über erlaubte Datenströme

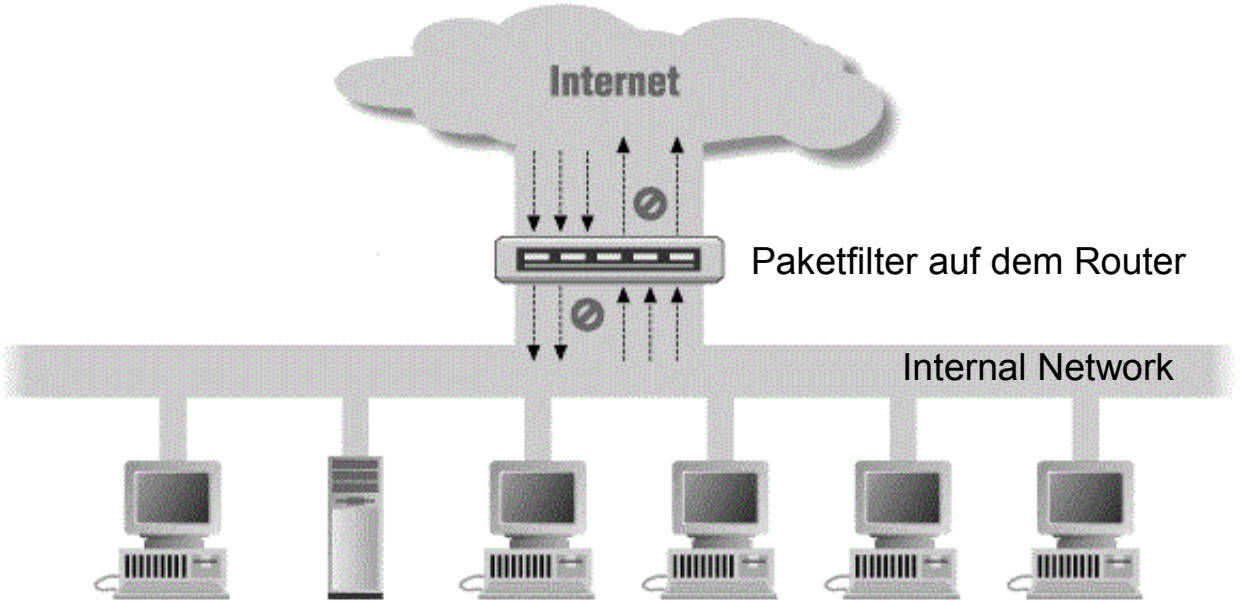
FIREWALL-ARCHITEKTUREN

- Simple Packet Filter
- Dual-Homed Host
- Screened Host
- Screened Subnet
- Split Screened Subnet

BEGRIFFE IM FOLGENDEN

- **Subnetz, Teilnetz**
  - Durch Router, Firewalls etc. abgegrenzter Teil eines internen Netzes
- **Paketfilter**
  - Programm (ggf. auf eigenständigen Rechner oder Router), welches Netzwerkpakete nach bestimmten Filterregeln filtert oder loggt
- **Dual-homed Host**
  - Rechner mit (mindestens) zwei getrennten Netzwerk-Schnittstellen, der Netzsegmente physisch trennt
- **Bastion Host**
  - Ein besonders geschützter und überwachter Rechner für sicherheitskritische Aufgaben
    - z.B. Rechner auf dem eine Application Level-Firewall oder ein Virenscanner laufen, oder der einen vom Internet aus sichtbaren Server betreibt

SIMPLE PACKET FILTER-ARCHITEKTUR (1/2)



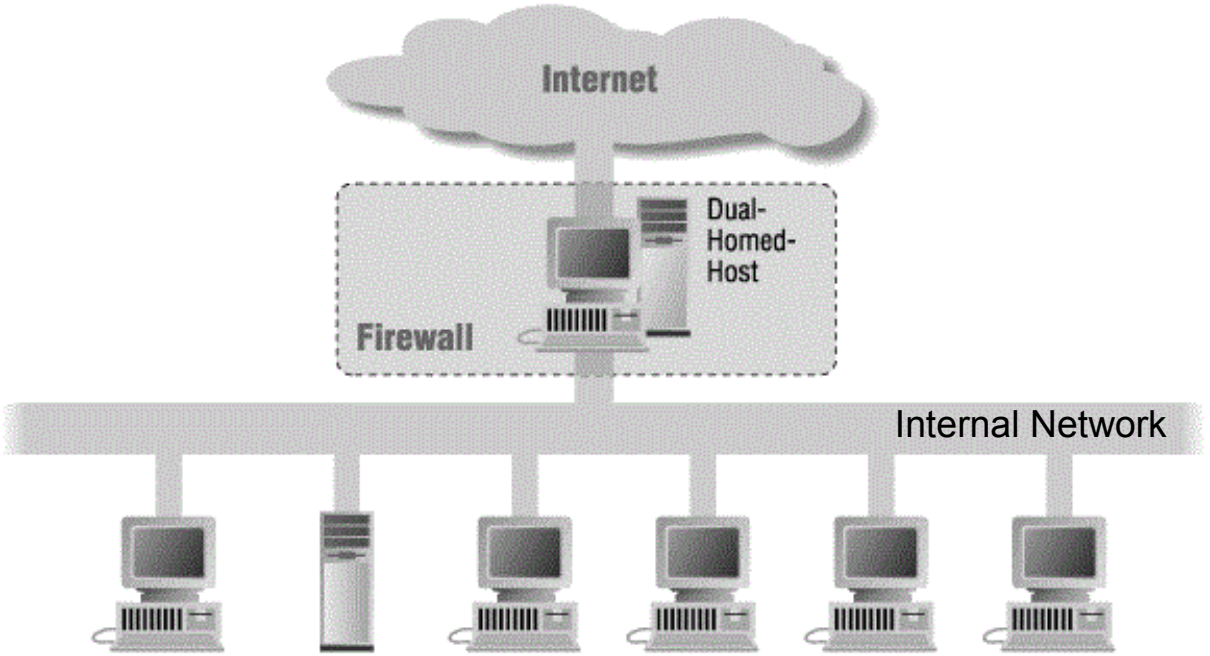
- Ein Paketfilter auf dem Router …
  - ist die einfachstmögliche Architektur
  - filtert Pakete anhand eines definierten Regelwerks aus dem Datenstrom
  - loggt Pakete mit, ebenfalls anhand eines Regelwerks
  - sendet alle erlaubten Pakete von einem Subnetz in ein anderes

SIMPLE PACKET FILTER-ARCHITEKTUR (2/2)

- Pro‘s
  - Kostengünstiger Aufbau
  - Konfiguration und Wartung sind einfach
    (Sie müssen aber trotzdem wissen was Sie tun)

- Con‘s
  - Eine einzelne Komponente schützt das ganze Subnetz
    - Single Point of Failure, attraktives Angriffsziel
    - Wenn der Angreifer die Firewall überwunden hat, sieht er alles
  - Die Filterregeln können sehr umfangreich und sehr komplex werden
    - Abhängig von den Anwendungen im Subnetz

DUAL-HOMED HOST-ARCHITEKTUR (1/2)



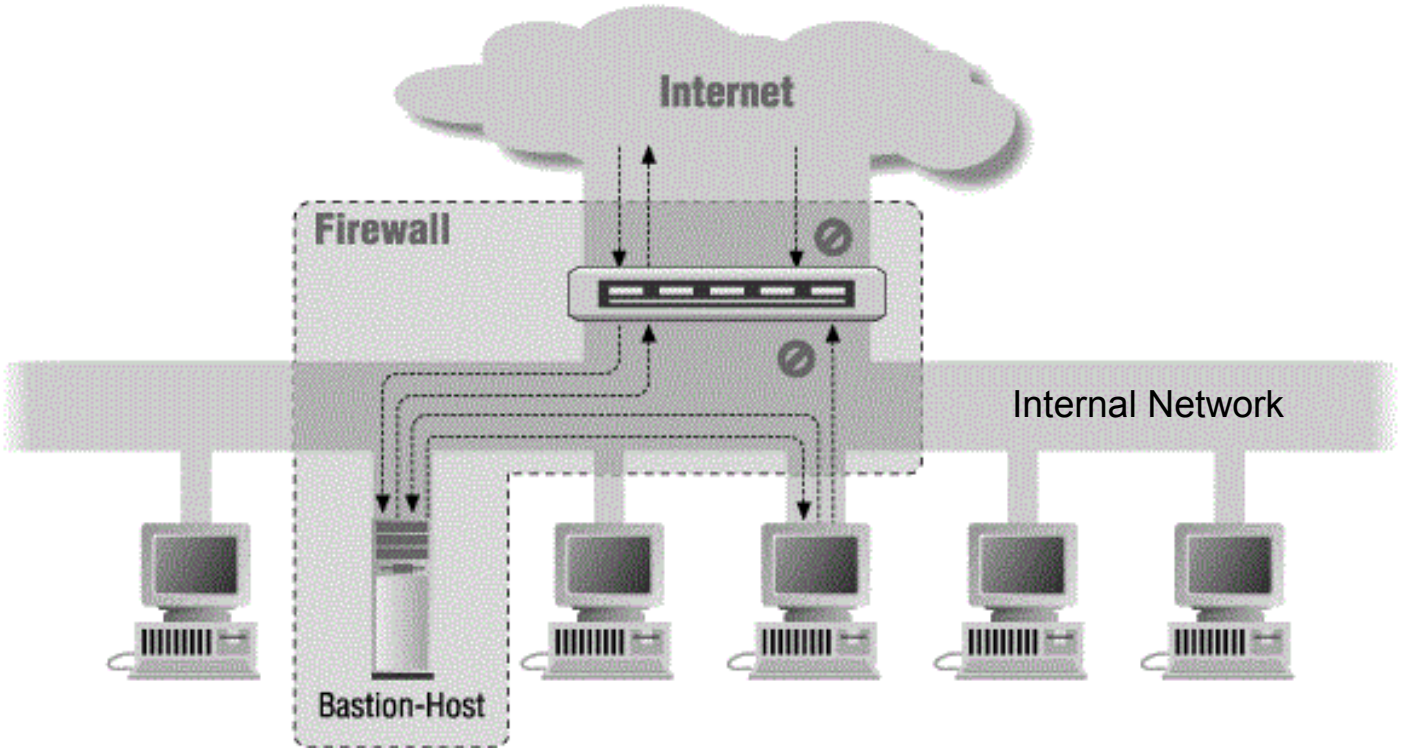
- Dual-homed Host hat eigene physische Netzwerkschnittstelle für ein- und ausgehenden Datenverkehr
  - mehr Rechenleistung als ein Router, komplexere Filteraufgaben
    - Virenscanner, WWW-Proxy, etc.
  - Kann nicht im Router „wegkonfiguriert“ werden
- Arbeitet als Internet-Router für das interne Netzwerk (Network Address Translation)

DUAL-HOMED HOST-ARCHITEKTUR (2/2)

- Pro‘s
  - Kann allen Datenverkehr mitloggen und potentielle Angriffe erkennen
  - Es gibt keine direkte Verbindung zu dem internen Netzsegment, das der Dual-Homed Host schützt
  - Details des internen Netzsegments werden nicht nach außen sichtbar (ARP, DNS etc., von jedem Rechner läuft immer über den Host)

- Con‘s
  - Da jeder Datenverkehr durch den Dual Homed Host muss, ist dieser ein potentieller Performanz-Flaschenhals
  - Dual Homed Host ist attraktives Angriffsziel, „sieht“ das gesamte geschützte Subnetz und allen Datenverkehr nach außen

SCREENED HOST-ARCHITEKTUR (1/2)



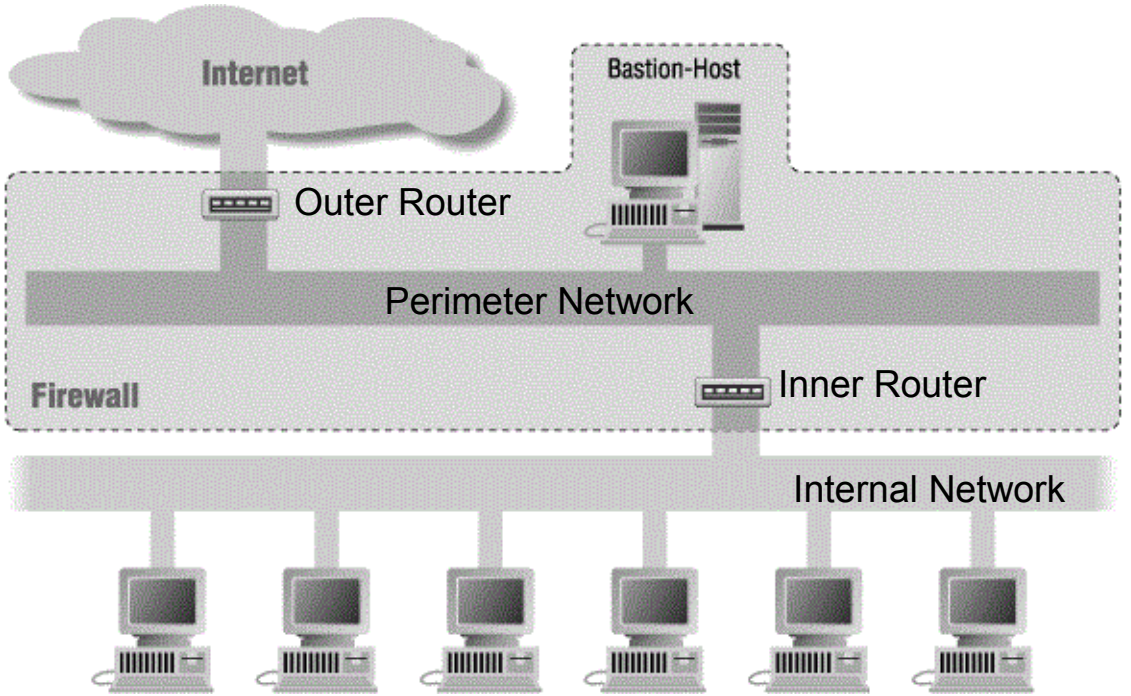
- Paketfilter auf dem Router
  - Erlaubt Datenverkehr zwischen Bastion Host und Internet sowie zwischen internem Netz und Bastion Host, blockiert alles andere
- Bastion Host bietet Proxy-Dienste
  - Beispielsweise kann der Paketfilter auf dem Router erzwingen, dass alle Emails durch den Virenscanner auf dem Bastion Host laufen müssen

SCREENED HOST-ARCHITEKTUR (2/2)

- Pro‘s
  - Nur der Router und der Bastion Host sind aus dem Internet sichtbar
  - Es ist möglich, internen Rechnern für bestimmte Dienste Internet-Zugang zu geben, z.B. auf einen externen Zeitserver oder DNS-Server
  - Zwei Sicherheitskomponenten statt einer erhöhen Sicherheit
  - Performanter als Dual Homed Host, da es möglich ist, für jeden Dienst einen eigenen Bastion Host bereitzustellen (Email-Filter, Virenscanner, Web-Proxy, Application-Level Firewall, ...)

- Con‘s
  - Ein vom Angreifer übernommener Bastion Host kann internen Datenverkehr ablauschen
  - Ein vom Angreifer übernommener Router kann Datenverkehr am Bastion Host vorbeileiten
  - Konfigurationsaufwand/Wartung für zwei Komponenten ist höher als für eine Komponente

SCREENED SUBNET-ARCHITEKTUR (1/2)



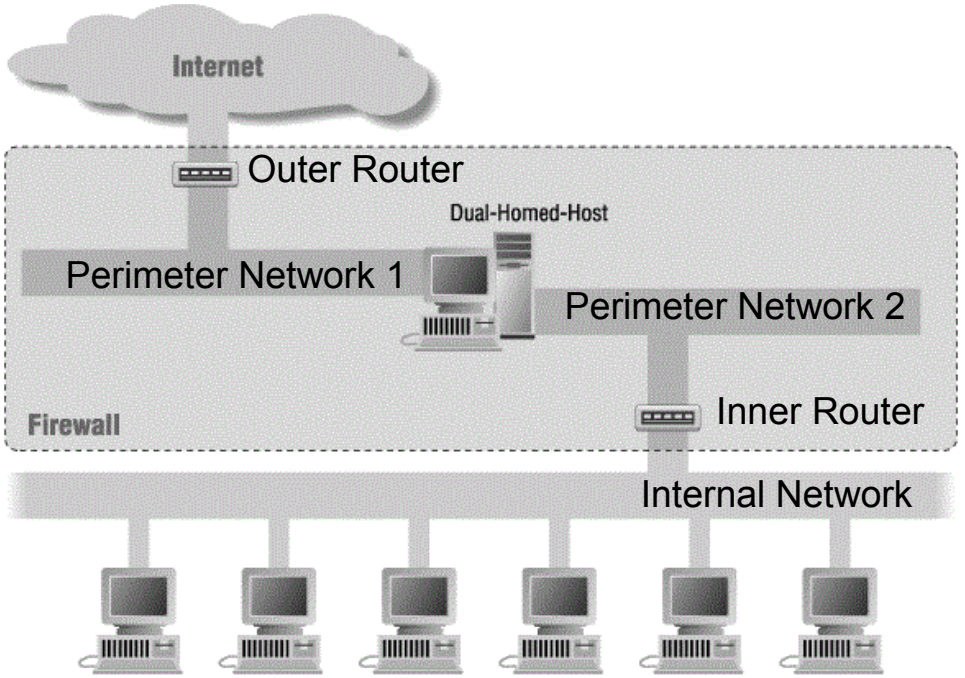
- Bastion Host in einem Perimeter-Network zwischen zwei Paketfiltern
  - auch als Demilitarized Zone (DMZ) bekannt
- Bastion Host sowohl im inneren Teilnetz als auch im Internet sichtbar
  - Dienste in beide Richtungen
- Paketfilter auf beiden Routern

SCREENED SUBNET-ARCHITEKTUR (2/2)

- Pro‘s
  - Hohes Sicherheitslevel für praktisch alle Anwendungen
    - Inneres Netz nicht nach außen sichtbar
    - Wer den äußeren Router überwindet sieht nur Bastion Host
    - Wer den Bastion Host erobert sieht nur zwei Router
    - Wer in das interne Netz will muss an zwei Routern vorbei
  - Performant wie Screened Host, da nur der Datenverkehr an den Bastion Host geschickt wird, den dieser benötigt
    - Es ist möglich, internen Rechnern für bestimmte Dienste Internet-Zugang zu geben, z.B. auf einen externen Zeitserver oder DNS-Server
    - Es kann mehrere Bastion Hosts für unterschiedliche Aufgaben geben

- Con‘s
  - Hoher Konfigurationsaufwand

SPLIT SCREENED SUBNET-ARCHITEKTUR (1/2)



- Dual Homed Host teilt das Perimeternetzwerk zwischen zwei Routern in zwei Hälften
  - Physische Trennung zwischen internem und externem Netz durch den Dual Homed Host, jede Datenübertragung wird kontrolliert
  - Jeder Router schützt über Paketfilter den Dual Homed Host, jeweils ins interne Netz und ins Internet

SPLIT SCREENED SUBNET-ARCHITEKTUR (2/2)

- Pro‘s
  - Nochmal sicherer als Screened Subnet, weil es nicht möglich ist Datenverkehr am Dual Homed Host vorbeizurouten
  - Damit ein Angreifer Zugriff auf das interne Netz bekommt, muss er zwei Router und den Dual Homed Host überwinden

- Con‘s
  - Sehr hoher Konfigurationsaufwand
  - Dual Homed Host als Flaschenhals für die Performanz, weil es nicht möglich ist unverdächtigen Datenverkehr vorbeizurouten

WAS LEISTET EIN PAKETFILTER?

- Einfachste Form einer Firewall

WELCHE MÖGLICHKEITEN HAT EIN PAKETFILTER?

- **Pass**
  - Das Paket passieren lassen, also vom Input-Interface an das Output-Interface weitergeben
- **Drop**
  - Das Paket verwerfen
- **Reject**
  - Das Paket verwerfen und den Absender darüber informieren
- **Log**
  - Das Paket loggen (egal ob pass oder drop), Statistiken fortschreiben

- **Network address translation**
  - Das Paket an einen anderen Empfänger/anderes Netzwerksgement weiterleiten *(genau genommen ist das kein Filtern)*

ZWEI FUNDAMENTALE STRATEGIEN

- **Default deny-Strategie:**
  - "Alles was nicht explizit erlaubt wurde ist verboten"
  - Finde heraus, welche Dienste die Nutzer im Netzwerksegment brauchen
  - Treffe eine Entscheidung, ob und unter welchen Umständen diese Dienste mit einem unsicheren Netzwerksegment kommunizieren dürfen
  - Erlaube nur „sichere" Dienste, die im Unternehmensinteresse liegen
  - Verbiete alles andere

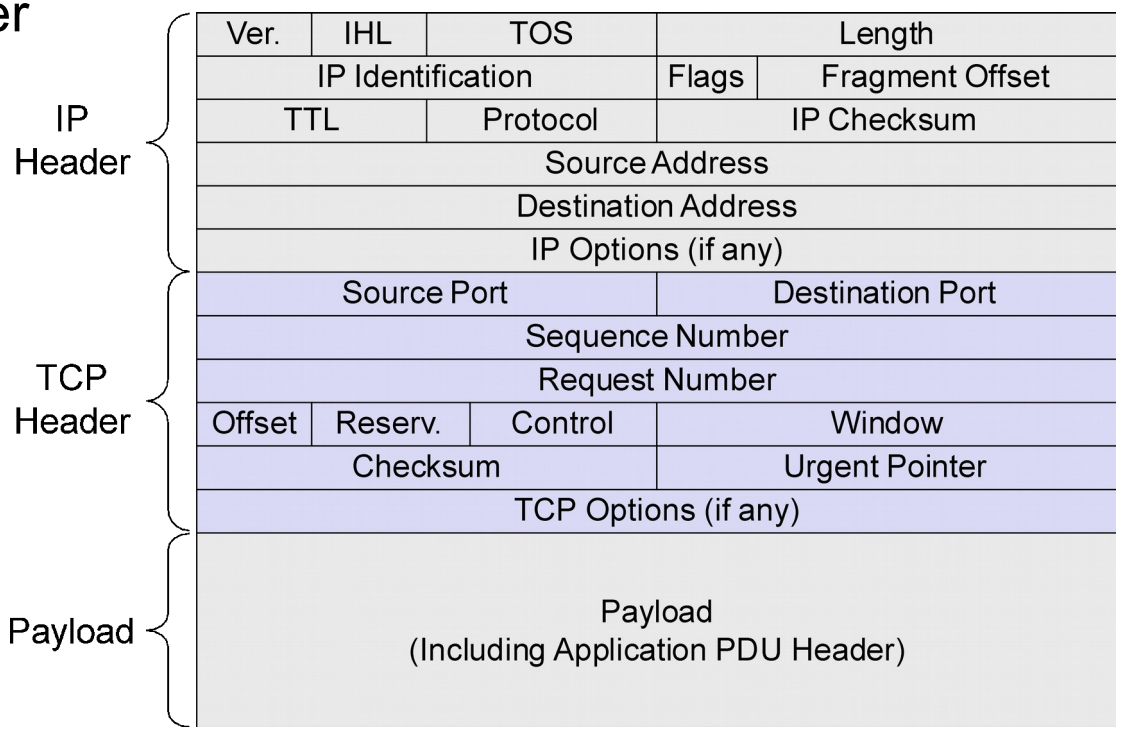
- **Default permit-Strategie:**
  - "Alles was nicht explizit verboten wurde ist erlaubt"
  - Verbiete jeden Dienst, der als gefährlich oder unsicher eingestuft wird
    - z.B. Pakete des Network File System (NFS) nicht in andere Netze weiterleiten, (unverschlüsselte) Telnet-Verbindungen nur zu einem Rechner

- *Welchen Grund könnte es für eine Default Permit-Strategie geben?*

TECHNISCHER HINTERGRUND FÜR DAS FOLGENDE

(SOLLTE IHNEN EIGENTLICH BEKANNT SEIN)

- Internet: Client-Server-Architektur, Client redet über den TCP/IP- Protokollstack mit dem Server
- TCP (verbindungsorientierte) oder UDP (verbindungslose) Pakete
- Ein TCP-Datenpaket enthält
  - Internet Protocol (IP)-Header
    wohin geht das Paket
  - Transmission Control Protocol (TCP)-Header
    wie werden die Daten ausgetauscht
  - Payload
    die Inhalte, App-Protokolle wie HTTP, POP3, IMAP
- UDP-Header ist einfacher (Source Port, Dest. Port, Length, Checksum)



INTERESSANT FÜR DIE FIREWALL (1/3)

- **Media Access Protocol**
  - Welches Protokoll? IP, Appletalk, IPX (Novell), DecNet, etc.
  - Welche Adressen? MAC-Adr. (Ethernet, WLAN), IMEI (Mobilfunk), etc.
    - Adressen beziehen sich auf die Sender- und Empfängerhardware
- **IP**
  - Source-Adresse
  - Destination-Adresse
  - Protokolltyp: TCP, UDP, ICMP, ...

INTERESSANT FÜR DIE FIREWALL (2/3)

- **TCP**
  - Source-Port, Destination-Port:
    - An welchen Dienst auf dem Rechner mit der Destination-Adresse im IP-Header ist das Paket gerichtet?
      (s. https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports
    - Von welchem Dienst kommt das Paket (Ports < 1024 sind Systemdienste, alle höheren Ports sind Anwendungen des Users, z.B. Webbrowser)
  - Steuerungsflags:
    - **ACK**: False im allerersten Paket bei Verbindungsaufbau, sonst immer true
    - **SYN**: Im jeweils ersten Paket vom Sender zum Empfänger und zurück vom Empfänger zum Sender true, sonst false
    - **RST**: True: Irgendwas ist schiefgegangen (z.B. Paket an eine vom Empfänger eigentlich geschlossene Verbindung gesendet), zurücksetzen

      → Wichtig für Stateful Inspection, ermöglicht Regeln wie „Externe Rechner dürfen Verbindung mit Webserver aufbauen, aber nicht umgekehrt)

INTERESSANT FÜR DIE FIREWALL (3/3)

- **Anwendungsprotokoll**
  - Beschreibt, wie die Payload im TCP/IP-Paket strukturiert ist, z.B.
    - HTTP: Abruf von Webseiten
    - POP3: Abruf von Email
    - SMTP: Senden von Email
    - DNS: Namensauflösung für IP-Adressen
    - …

- Anwendungsspezifisch, daher in dieser Vorlesung außen vor.

  Wenn Sie googeln wollen: „deep packet inspection“, z.B.: „Blockiere Pakete an UDP-Port 53, wenn sie nicht wie DNS-Pakete aufgebaut sind“

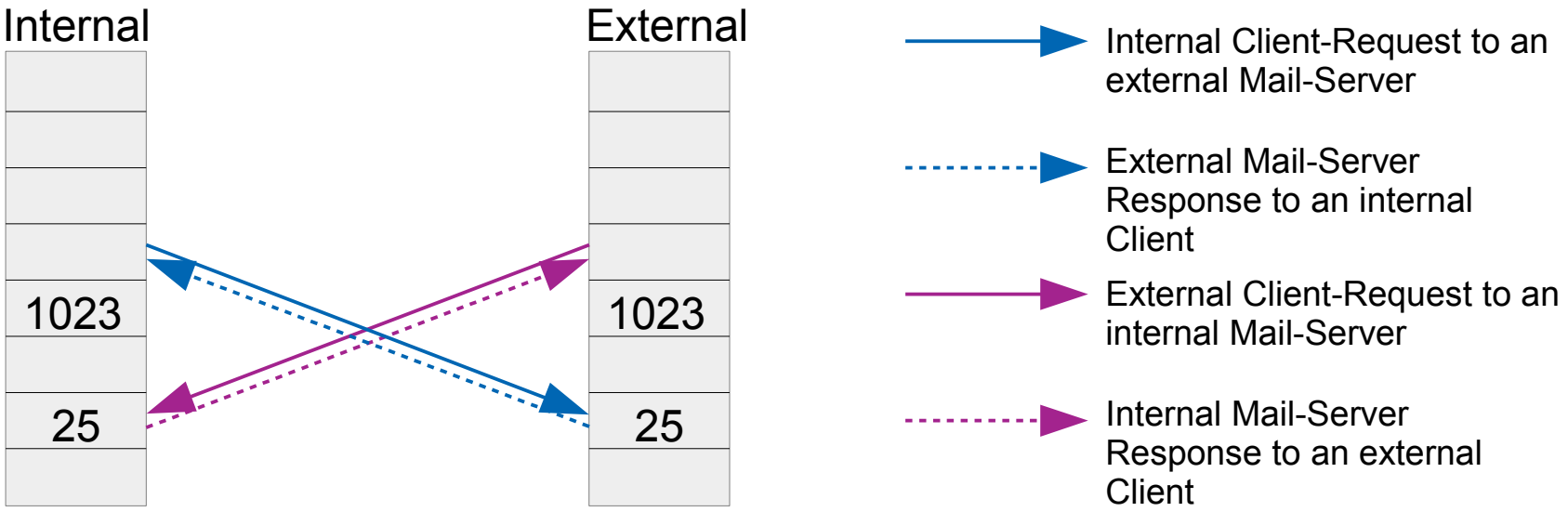
DIE ÜBERTRAGUNGSRICHTUNG

Da Paketfilter immer an den Grenzen eines Netzwerksegments sitzen, gibts eine implizite Festlegung für die Übertragungsrichtung beim Filtern:

- **Outbound** *(herausgehend)*
  - Das Datenpaket ist über eine Schnittstelle in den Rechner gelangt, die *innerhalb* des geschützten Netzwerksegments liegt
  - Beispiel: Ein Rechner aus dem internen Netz sendet eine Anfrage an einen Webserver im Internet.
- **Inbound** *(hereinkommend)*
  - Das Datenpaket ist über eine Schnittstelle in den Rechner gelangt, die *außerhalb* des geschützten Netzwerksegments liegt
  - Beispiel: Antwort dieses Webservers an den internen Rechner.

- Für jede Regel eines Paketfilters muss die Übertragungsrichtung angegeben werden, “*inbound*”, “*outbound*”, “*either*” (beide Richtungen)

BEISPIELSZENARIO



- Im geschützten Netzwerksegment (Internal) steht ein Email-Server und wartet an TCP-Port 25 (SMTP) auf eingehende Verbindungen.
- Wenn der Server als Email-Relay selber Emails an externe Server weitergibt, agiert er als Client, d.h., öffnet ausgehend von einer Portadresse >1023 eine Verbindung zu Port 25 auf dem anderen Server.
- Wenn der Server eine Email von einem externen Server erhält, dann ist es genau andersherum.

BEISPIEL-REGELSATZ

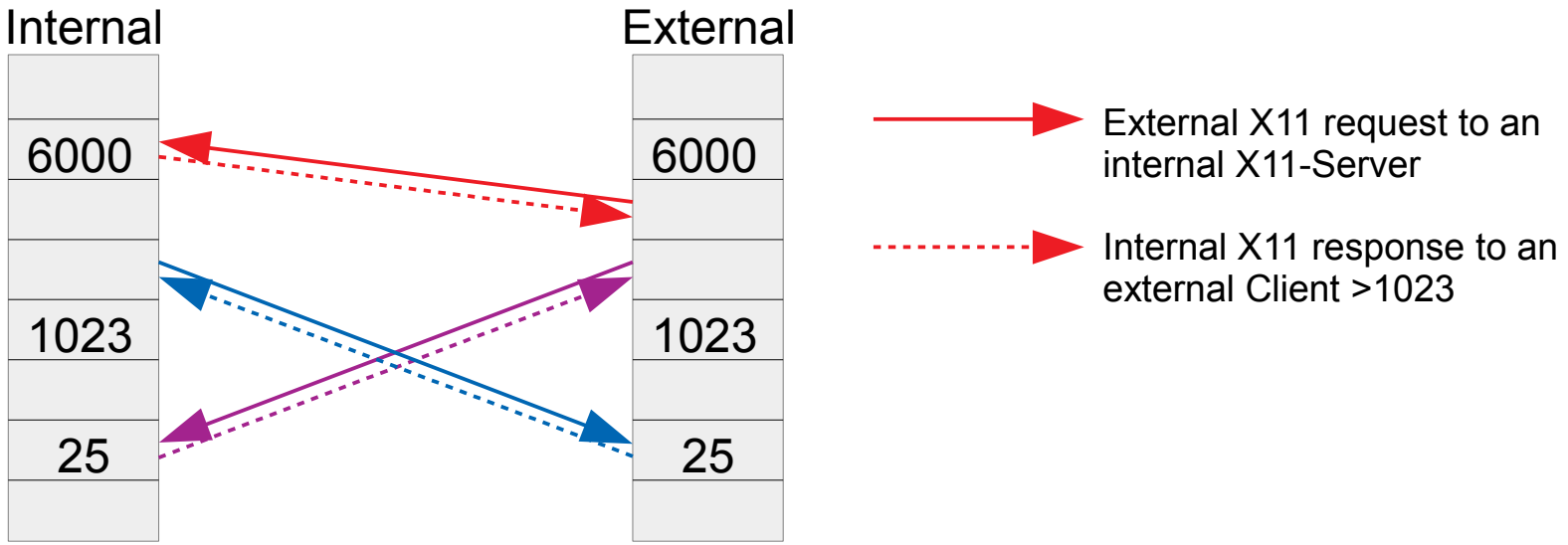
Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP		25		Permit
B	Outbound	Internal	External	TCP		>1023		Permit
C	Outbound	Internal	External	TCP		25		Permit
D	Inbound	External	Internal	TCP		>1023		Permit
E	Either	Any	Any	Any		Any		Deny

- Annahme: Nur eingehende und ausgehende Email ist erlaubt.
- Regel A erlaubt eingehende TCP-Datenpakete von einer externen Quelle, die an Port 25 einer internen Adresse gerichtet ist (eingehende Email)
- Regel B erlaubt das Senden einer Bestätigung an den externen Server, von dem die Email kam.
- Regel C und D sind analog für herausgehende Email.
- Regel E verbietet alle anderen Datenpakete
  (Die Reihenfolge ist wichtig!)

FUNKTIONIERT DER BEISPIEL-REGELSATZ? (1/2)

- Angreifer 1: Versucht, von außen eine SSH-Verbindung (TCP Port 22) zu dem Email-Server zu öffnen
  - Jedes inbound-Datenpaket muss entweder an den TCP-Port 25 gerichtet sein (Regel A) oder an einen TCP-Port > 1023 (Regel D).
  - Zugriff wird erfolgreich blockiert.
- Angreifer 2: Versucht, mit einer gefälschten internen Source-Adresse von außen in das geschützte interne Subnetz zu kommen
  - Ein Datenpaket, das an eine interne Destination-Adresse gerichtet ist, muss über die „inbound“-Schnittstelle kommen. (Regel A,B,C,D)
  - Zugriff wird erfolgreich blockiert
- Angreifer 3: Mitarbeiter hat den Email-Server übernommen und will von diesem aus einen externen Rechner mittels Telnet (TCP-Port 23) erreichen
  - Jedes outbound-Datenpaket muss entweder an den TCP-Port 25 gerichtet sein (Regel C) oder an einen TCP-Port > 1023. (Regel B)
  - Zugriff wird erfolgreich blockiert

FUNKTIONIERT DER BEISPIEL-REGELSATZ? (2/2)



- X11-Protokoll für Unix-Bildschirmweiterleitung
  - X11-Server läuft im User-Space, standardmäßig TCP-Port 6000
  - X11-Client läuft ebenfalls im User-Space, benutzt TCP-Ports >1024

- Angreifer 4: will von außen eine X11-Bildschirmweiterleitung aufmachen
  - Regel D erlaubt TCP-Pakete von außen an Port >1023 (Requests)
  - Regel B erlaubt TCP-Pakete nach außen an Port >1023 (Antworten)
  - Zugriff ist erlaubt

BLOCKIEREN DES X11-SERVERS

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25		Permit
B	Outbound	Internal	External	TCP	25	>1023		Permit
C	Outbound	Internal	External	TCP	>1023	25		Permit
D	Inbound	External	Internal	TCP	25	>1023		Permit
E	Either	Any	Any	Any	Any	Any		Deny

- Im Regelsatz die Source-Ports ergänzen
  - Outbound-Pakete sind nur erlaubt, wenn sie von Port 25 kommen (Regel B) oder an Port 25 gerichtet sind (Regel C)
  - Inbound-Pakete sind nur erlaubt, wenn sie von Port 25 kommen (Regel D) oder an Port 25 gerichtet sind (Regel A)
  - X11-Server wird blockiert

- Angreifer 5: Hat root-Rechte auf dem Emailserver, ändert die Standardports und startet Verbindungen mit Source-Port 25
  - Zugriff ist erlaubt

WER DARF VERBINDUNGEN ÖFFNEN?

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Internal	TCP	>1023	25	Any	Permit
B	Outbound	Internal	External	TCP	25	>1023	Yes	Permit
C	Outbound	Internal	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Internal	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny

- *ACK: No im ersten Paket bei Verbindungsaufbau, sonst immer Yes*

- Im Regelsatz das ACK-Flag in den Regeln B, D ergänzen
  - Regel B erlaubt nur Outbound-Datenpakete *als Antwort* auf eine eingehende Verbindung
  - Regel D erlaubt nur Inbound-Datenpakete *als Antwort* auf eine ausgehende Verbindung

(Anm.: Spätenstens wenn der Angreifer bereits Root-Rechte hat, versagt eine Firewall, die auf dem selben Rechner läuft wie der zu schützende Server)

ABSCHLUSS

ZUSAMMENFASSUNG

- In hinreichend komplexen Netzwerk-Infrastrukturen ist es praktisch unmöglich zu verhindern, dass jemand physikalisch Daten ablauscht
  - viel zuviele Gelegenheiten für interne und externe Angreifer

- Beste Möglichkeit
  - Verschlüsselte Protokolle und Netzwerkauthentifizierung wann immer möglich
  - Von Hause aus unsichere Protokolle sowie nicht benötigte Dienste konsequent abschalten
  - Firewalls helfen bei der Einteilung des Netzwerks in Sicherheitszonen
    - Geräte/Daten mit ähnlichen Sicherheitsanforderungen in derselben Zone
    - Firewalls kontrollieren Zonengrenzen

- *Verlassen Sie sich nicht auf vorkonfigurierte Personal Firewalls!*

MÖGLICHE PRÜFUNGSFRAGEN

- Eine kleine Fabrik hat eine Verwaltung, ein Produktivsystem mit Industriesteuerungsanlagen sowie vom Internet sichtbare Web- und Email-Server. Welche Argumente sprechen für oder gegen die Aufteilung in 1, 2 oder 3 durch Firewalls voneinander getrennte Subnetze?

- Welche Vor- und Nachteile hat eine Personal Firewall (d.h., eine auf dem Arbeitsplatzrechner selbst installierte Firewall, wie in Windows 10 enthalten)

- Auf einem Bastion-Host laufen ein HTTP-Proxy, ein Web-Server und ein Email-Server (TLS/SSL). Der Bastion Host ist durch einen Router mit dem Internet verbunden (Screened Host-Architektur). Die Firewall läuft auf dem Router. Die anderen Rechner im internen Netz dürfen nur über den HTTP-Proxy auf dem Bastion-Host mit dem WWW kommunizieren. Der DNS-Server hat die IP-Adresse 80.153.199.210 und muss von jedem Rechner erreichbar sein. Wie sehen die Paketfilterregeln für die Firewall aus?

LITERATUR

[Zwi00a]	E. Zwicky, S. Cooper, B. Chapman. *Building Internet Firewalls.* Second Edition, O'Reilly, 2000.
[Sem96a]	C. Semeria. *Internet Firewalls and Security.* 3Com Technical Paper, 1996.
[Wack95a]	J. P. Wack, L.J. Carnahan. *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls.* NIST Special Publication 800-10, 1995.

(Literaturquellen danach ausgesucht, dass sie im Internet verfügbar sind.
Achten Sie bei der 1. Quelle bitte selbst auf Urheberrechtsangaben)