NW: Firewall

Vorlesung von Reto Burger

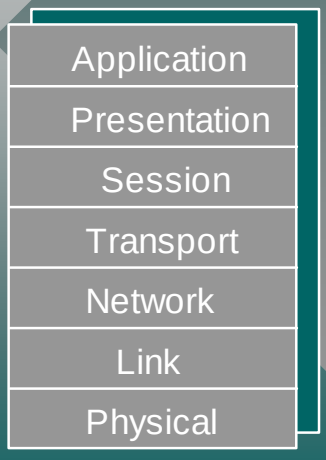
0 Übersicht

- Persönliche Kurzvorstellung
- Ihre Erwartungen
- Vorstellung des Fachs: Kapitel, Ziele, Prüfungen
- Allgemeines

Kapitel 1: Einführung

- 1.1 Grundlagen OSI-Modell
- 1.2 TCP/IP Kurzübersicht
- 1.3 Konzepte
- 1.4 Strukturen
- 1.5 Beispiele

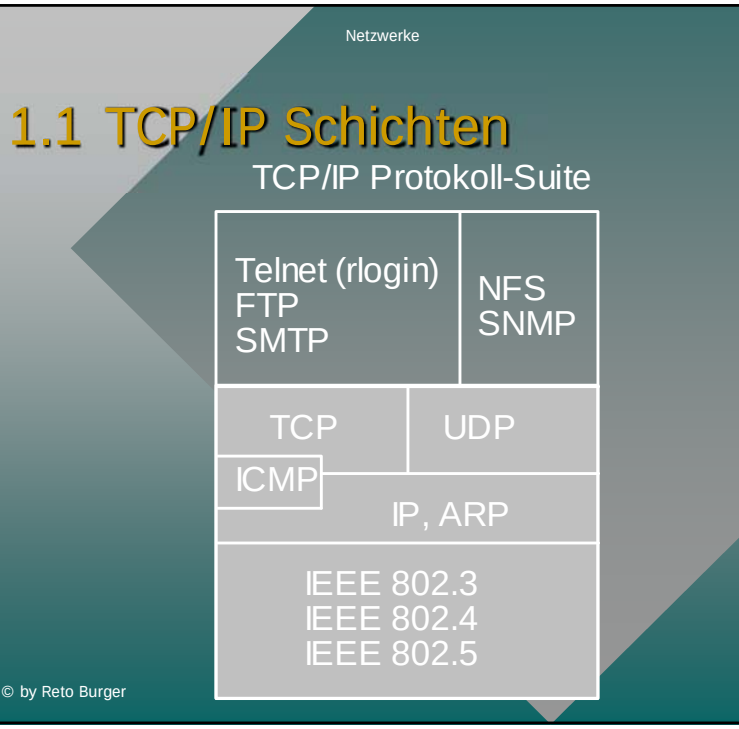
1.1 OSI-Referenzmodell



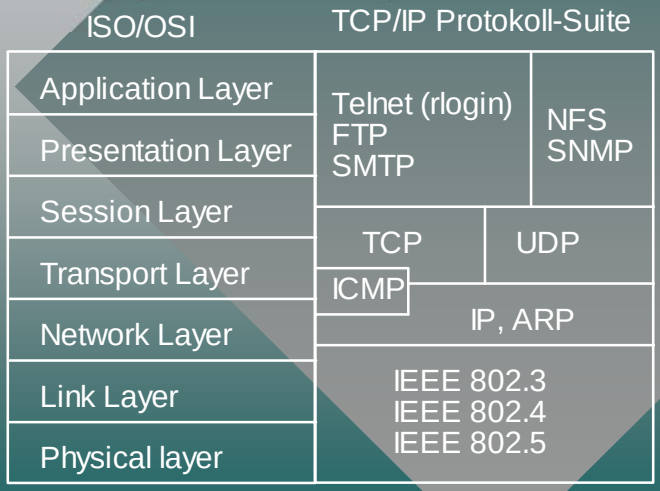
Schichten:

Anwendung
Darstellung
Kommunikation
Transport
Vermittlung
Sicherung
Bitübertragung

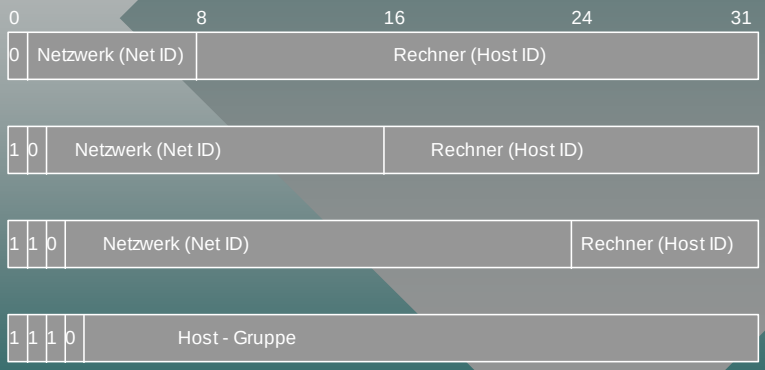
1.1 TCP/IP Schichten



1.1 Vergleich OSI / TCP-IP



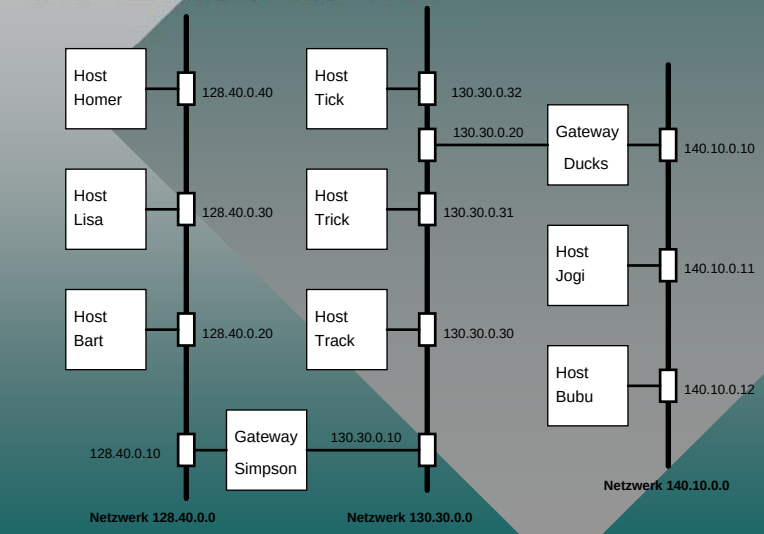
1.1 Aufteilung der NW in Klassen



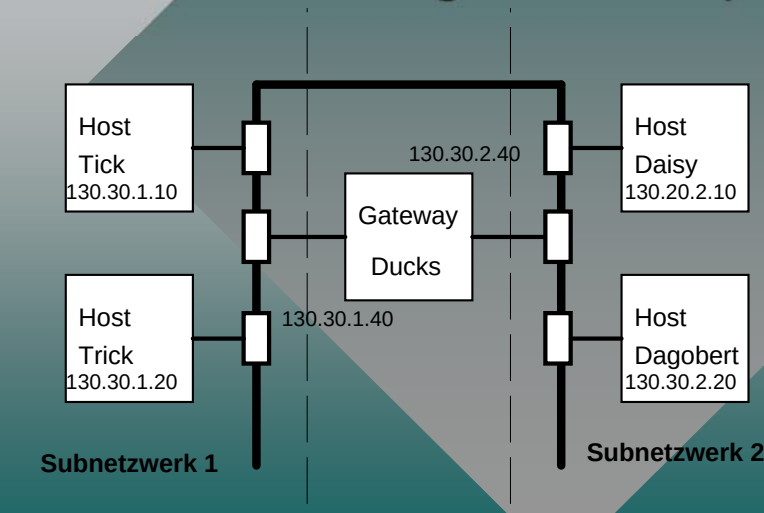
1.1 Subnetze

	1. Byte	2. Byte	3. Byte	4. Byte
Klasse A Netzwerk	Netzwerknummer (1-126)	Hostnummer		
Netzwerk Maske	255	255	0	0
Subnetzwerk	Netzwerknummer	Subnetzwerk- Nummer	Hostnummer	

1.1 Einfaches NW



1.2 Zwei NW auf gleichem Phy



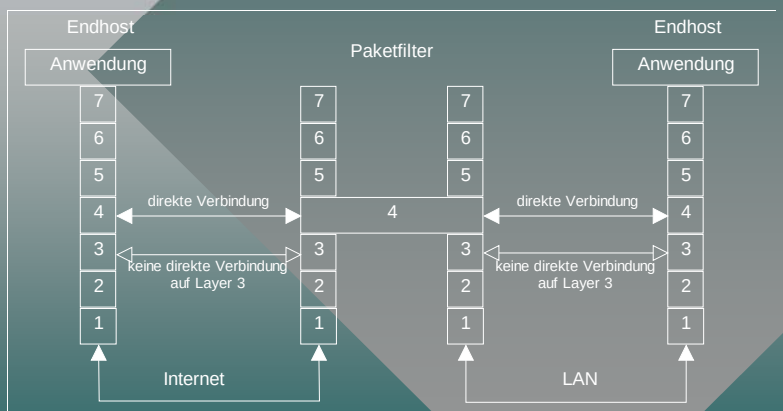
1.2 Portnummern

Internetsockets	Telefon
Netzwerknummer	Ortsvorwahl
Host-ID	Telefonnummer
Portnummer	Nebenstelle

1.3 Firewalltypen

Bezeichnung	*Art*	*Eigenschaften*
• *Paketfilter*	Router- and host-based packet filters	Schnell, relativ günstig. Immer direkte Verbindung zwischen Kommunikationspartnern Untertypen: Screening Router, Screening Host
• *Vermittler- oder Transportschicht-Gateway (circuit level gateway)*	Host-based „smart“ filter	Arbeitet auf Layer 4 als TCP-Relais. Während die Verbindung besteht, kopiert Gateway die Daten zwischen den Schnittstellen hin und her. Läuft auf der Benutzerworkstation, keine Teile auf der Firewall.
• *Anwendungsschicht-Gateway (application level gateway)*	Host-based application gateway	Gelten als die sichersten Firewalls, da höchster Grad der Kontrolle. Für jeden angebotenen Dienst besteht eigenes Gateway-Programm. Kommunikationspartner kennen die IP-Adresse ihres Gegenüber nicht.

1.3 Paketfilter (Router)



1.3 Filtertabelle

Obwohl sich die verschiedenen Produkte unterscheiden, so können doch die wesentlichen Kriterien für eine Filterung und somit für die Filtertabelle angegeben werden. Die Regeln basieren also auf den folgenden Kriterien :

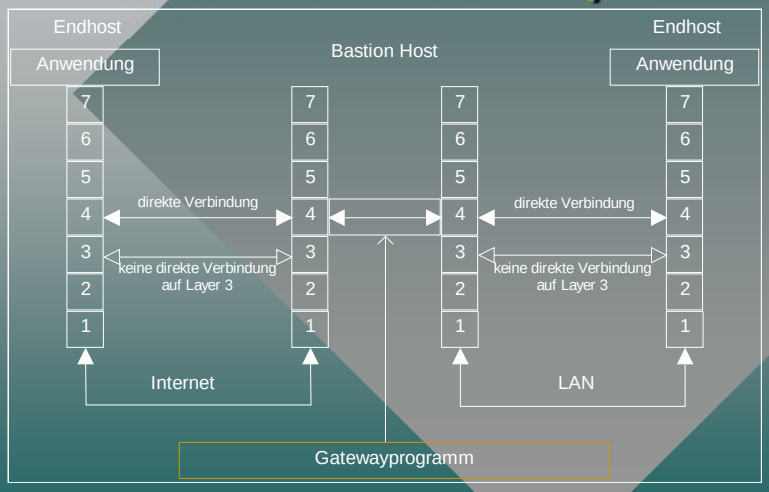
- Verkehrsrichtung
- Interface, von welchem ein Paket erhalten wurde, oder zu welchem es geschickt werden soll
- Protokolltyp (IP, ICMP, TCP, UDP, IPX)
- Quell- oder Zielport einer TCP oder UDP Verbindung
- TCP Status Information

1.3 Circuit Level Gateway Funktionsweise

Die Funktionsweise des Circuit Level Gateways kann folgendermassen beschrieben werden:

- Der interne Host sendet seine TCP-Pakete an einen Zielhost im externen Netz
- Der Gatewayrechner nimmt das Paket entgegen, uns sendet es – mit seiner eigenen IP-Adresse als Absender (IP-Sourceadresse im TCP-Header) – ins öffentliche Netz
- Der externe Host sendet seine Pakete zurück an das Gateway. Dieser nimmt das Paket entgegen und leitet es an den internen Host weiter. Der Gateway-Rechner muss also wissen, welcher interne Rechner der Kommunikationsparter des externen Rechners ist.

1.3 Circuit Level Gateway



1.3 Application Level Gateway

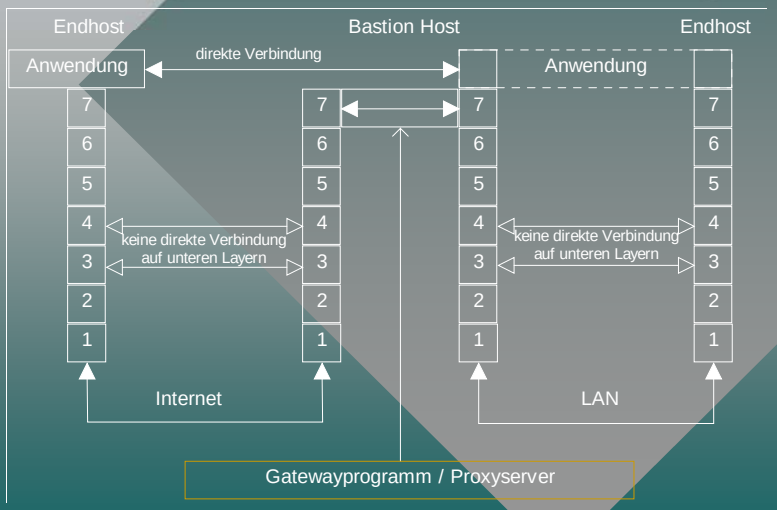
Weiter haben Application Level Gateway folgende Eigenschaften und Vorteile vorzuweisen:

- Der gesamte ein- und abgehende Verkehr kann kontrolliert und protokolliert werden, was das Auffinden von Sicherheitslücken wesentlich erleichtert.
- Die internen Host sind gegen aussen unsichtbar.
- Es sind keine komplexen Regeln notwendig.

Als Nachteile sind folgende Punkte zu erwähnen:

- Für die meisten Dienste sind spezielle Anwendungen nötig.
- Zwischen den internen und externen Hosts besteht keine direkte Verbindung. Es ist ein Proxy-Server notwendig, welcher als Vermittler funktioniert.

1.3 Application Level Gateway



1.3 Application Level Gateway

Wie schon einleitend erwähnt wurde, gelten Application Level Gateways allgemein als sicherster Typ von Firewalls. Dies setzt aber voraus, dass sie von einem fähigen Netzwerkadministrator betrieben werden. Für Unternehmen mit strengen Sicherheitsvorschriften, welche über genügend Geld und Personal verfügen um die Firewall korrekt zu implementieren und zu warten, sind Application Level Gateways sehr empfehlenswert.

2 Architektur

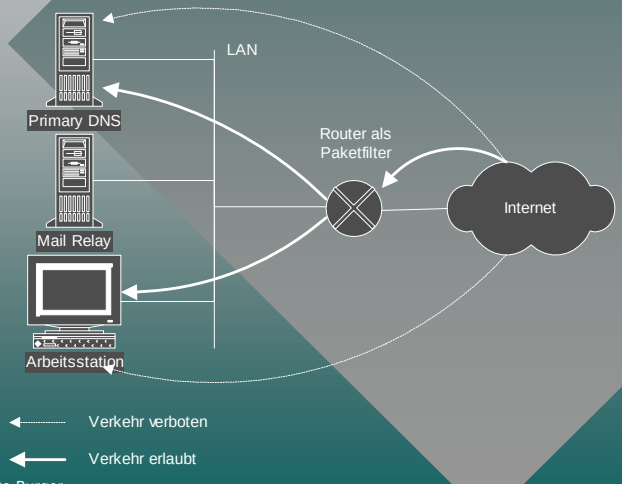
- Screening Router
- Dual-Homed
- Screened Host Gateway
- Gateway Screened Subnet

2.1 Screening Router

Der Screening Router wird oft als erste Abschirmung gegen das öffentliche Netz eingesetzt. Das interne und externe Netz sind lediglich durch einen als Paketfilter arbeitenden Router getrennt. Durch diese Blockade können Pakete zu bestimmten Hosts oder Netzwerken gefiltert werden.

2.1 Screening Router

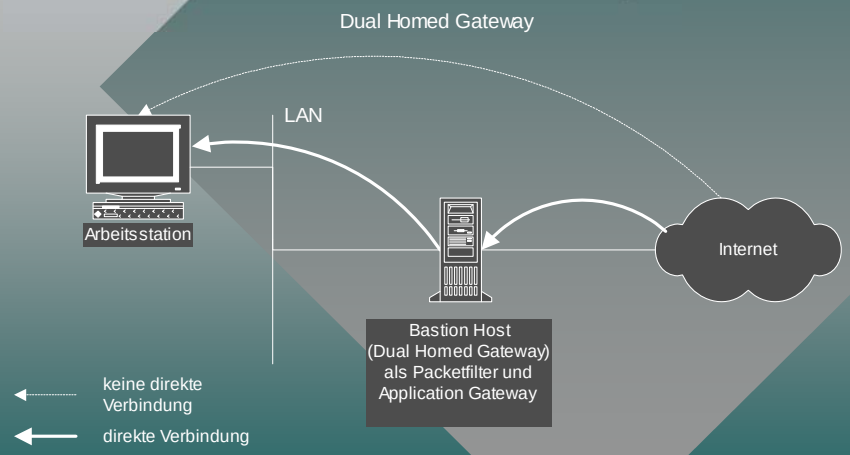
Screening Router Firewall



2.2 Dual Homed Gateway

Der Dual-Homed Gateway ist ein Rechner mit zwei Netzwerkkarten, der sich zwischen den beiden Netzen befindet. Er stellt eine sehr häufige und leicht einzurichtende Firewall dar

2.2 Dual Homed Gateway

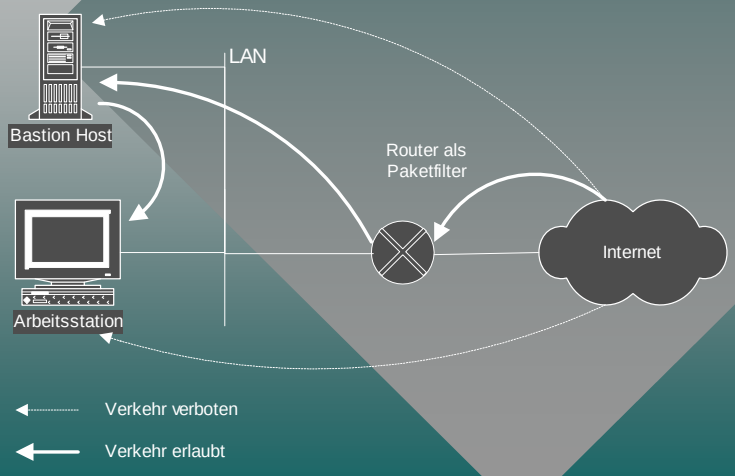


2.3 Screened Host Gateway

Screened Host Gateways (Screening Hosts) gelten als sicher und sind gleichzeitig leicht einzurichten. Wie bei den Screening Routern sind die beiden Netze durch einen als Paketfilter arbeitenden Router getrennt. Der Router erlaubt aber nur den Verkehr zu einem einzigen internen Host, dem sogenannten Bastion Host. Dieser Bastion Host wird durch spezielle Sicherheitsmassnahmen geschützt.

2.3 Screened Host Gateway

Screened Host Firewall



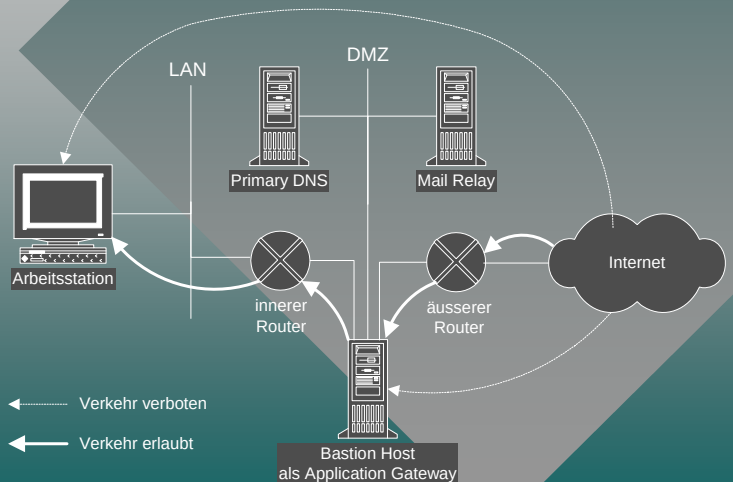
2.4 Screened Subnet

Screened Subnet Firewalls sind in einigen Fachbüchern auch unter dem Namen Belt-and-Suspenders Firewalls geführt.

Das Screened Subnet ist ein Segment zwischen dem internen und dem externen Netz. Es wird als demilitarisierte Zone (DMZ) bezeichnet. In dieser DMZ befindet sich der Bastion Host, der als einziger den Datenverkehr zwischen dem internen und dem externen Netz weiterleiten kann. Während der äussere Router also nur den Datenverkehr zwischen dem Bastion Host und dem öffentlichen Netz erlaubt, so leitet der innere Router nur den Datenverkehr zwischen dem Bastion Host und dem internen Netz weiter.

2.4 Screened Subnet

Screened Subnet mit zwei Router, einer davon als Paketfilter

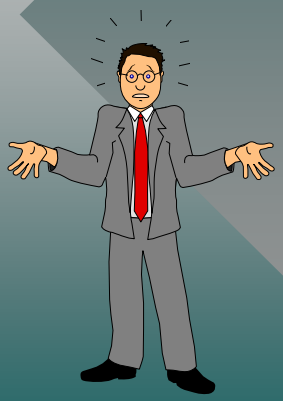


3 Angriffsarten

Es lassen sich verschiedene Unterscheidungskriterien angeben. Allgemein geht man davon aus, dass Attacken (auch als Threads bezeichnet) auf Datenkommunikationssystemen folgende Ziele anstreben :

- Lahmlegen eines Services
- Zerstörung von Daten und/oder anderen Ressourcen (Verfügbarkeit)
- Änderung von Daten (Integrität)
- Diebstahl von Daten und/oder anderen Ressourcen (Verfügbarkeit)
- Bekanntmachen von geheimen Daten (Vertraulichkeit)

Danke



- Sind noch Fragen ???