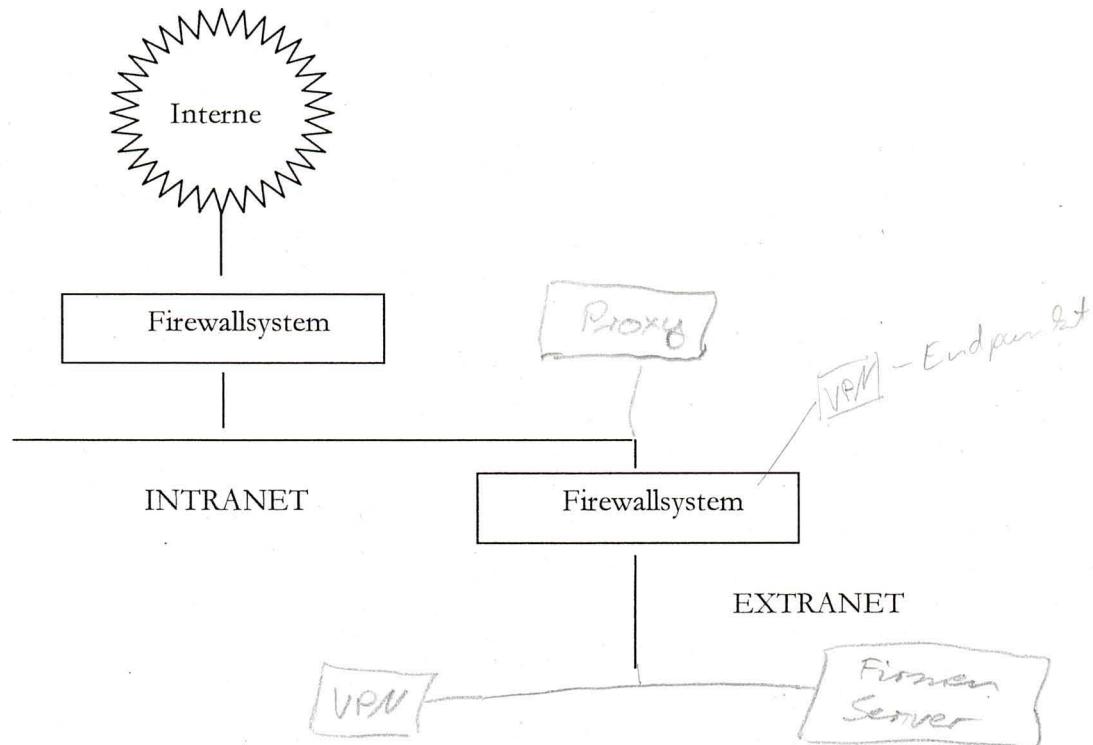


FIREWALLS	2
HAUPTFUNKTIONEN EINER FIREWALL	2
FIREWALL KONFIGURATIONSARTEN.....	3
1.) <i>Dual – Homed – Host</i>	3
2.) <i>Aufbau mit überwachtem Host</i>	4
3.) <i>Überwachtes Teilnetz</i>	5
Überwachtes Teilnetz : Innerer Router.....	5
Erzwingt, dass die Benutzer aus dem Intranet die Proxy-Dienste des Bastion Host verwenden Überwachtes Teilnetz : Äußerer Router	6
Überwachtes Teilnetz : Bastion Host.....	7
Richtlinien für die Konfiguration von Bastion Hosts.....	8
VON FIREWALL- SYSTEMEN VERWENDETE SICHERUNGSMETHODEN	9
<i>Paketfilter -Firewall</i>	10
Grundlagen	10
Welche Protokollfelder muss eine Paketfilter- Firewall beachten?.....	11
Aufgabe Paketfilter- Firewall.....	12
Filterung nach Adressen.....	13
Filterung nach Diensten.....	15
PROXY-SYSTEME	16
Application – Level Proxy (dedizierter Proxy)	16
Circuit- Level Proxy (generischer Proxy).....	16
Der Internetexplorer als Proxy-Client	18
Socks : Ein generischer Proxy	19
NAT	20
Basic NAT.....	20
Static NAT.....	21
Dynamic NAT	21
Network Address Port Translation (NAPT).....	21
Aufgabe NAT 1.....	23
Aufgabe NAT 2.....	24
CISCO ACCESS CONTROL LISTS (ACLs).....	25
ACL GRUNDLAGEN.....	25
Bearbeitung der ACL- Regeln.....	26
Zuweisen von ACLs an Interfaces.....	27
Erstellen von ACLs.....	27
Wildcard mask bits.....	28
STANDARD ACLS.....	29
Aufgabe: Standard- ACL.....	33
EXTENDED ACL.....	34
Aufgabe Extended ACL	37
NAMED ACLS.....	38
Eigenschaften von named ACLs.....	39
Syntax zum Anlegen von named ACLs.....	39
Überprüfung von ACLs	39
OPTIMALE PLATZIERUNG VON ACLS	40
AUFGABEN ACL	41

Firewalls

Hauptfunktionen einer Firewall



Ein Teil des Intranet Daten werden einem Teil der Benutzer zur Verfügung gestellt

- Zutritt zum eigenen Netz nur an einem stark kontrollierten Punkt möglich
→ Einschränkung der Zugriffe

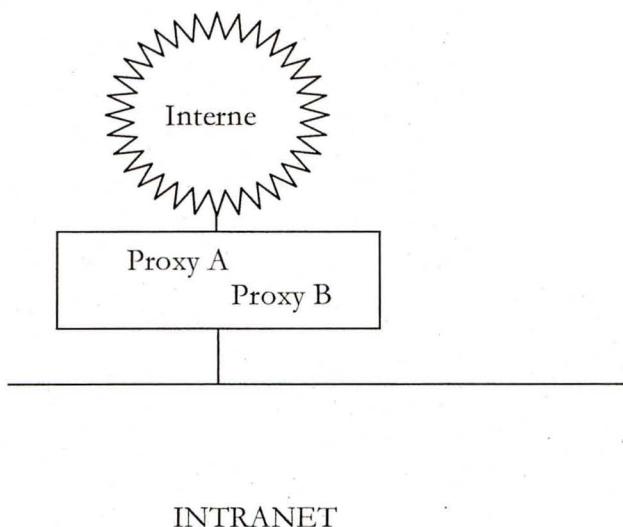
- Schutz vor äußeren Angreifern

- Das interne Netz kann nur an einem Punkt verlassen werden.

→ zwingt dass Internetclients
z.B. Internet-Proxy's verwendet
zentral loggen

Firewall Konfigurationsarten

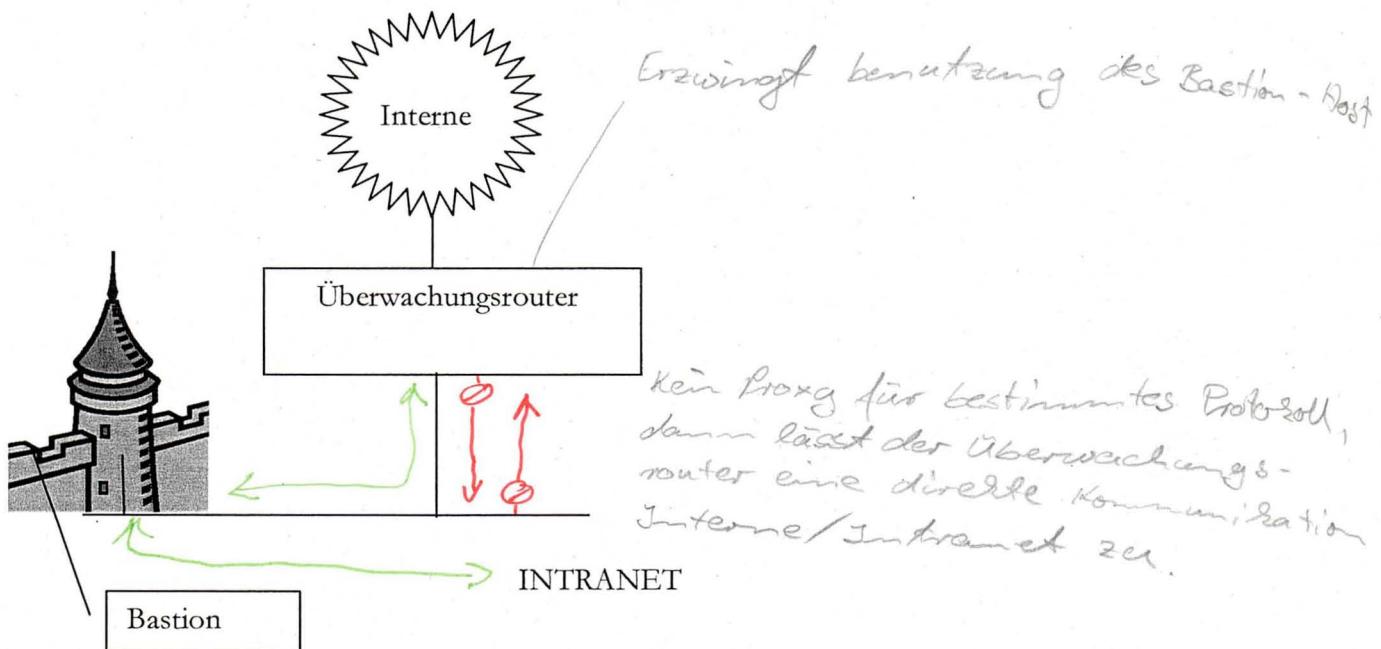
Dual – Homed – Host



Ein Dual –Homed –Host besitzt zwei Interfacekarten: Er ist mit einem Interface am Internet angeschlossen mit dem anderen am Intranet. Er bietet Internetdienste an durch:

- Proxy Server
 - Web-Proxy: Cache für häufig abgerufene Seiten
 - Kennt höhere Protokolle
 - Ist Stellvertreter bei Anfragen ins Internet
 - ↳ Client → gelangt nicht ins Internet
- Benutzer müssen sich hier einloggen* um auf das Internet zugreifen zu können
 - * bei Diensten für die es keinen Proxy gibt.

Aufbau mit überwachtem Host



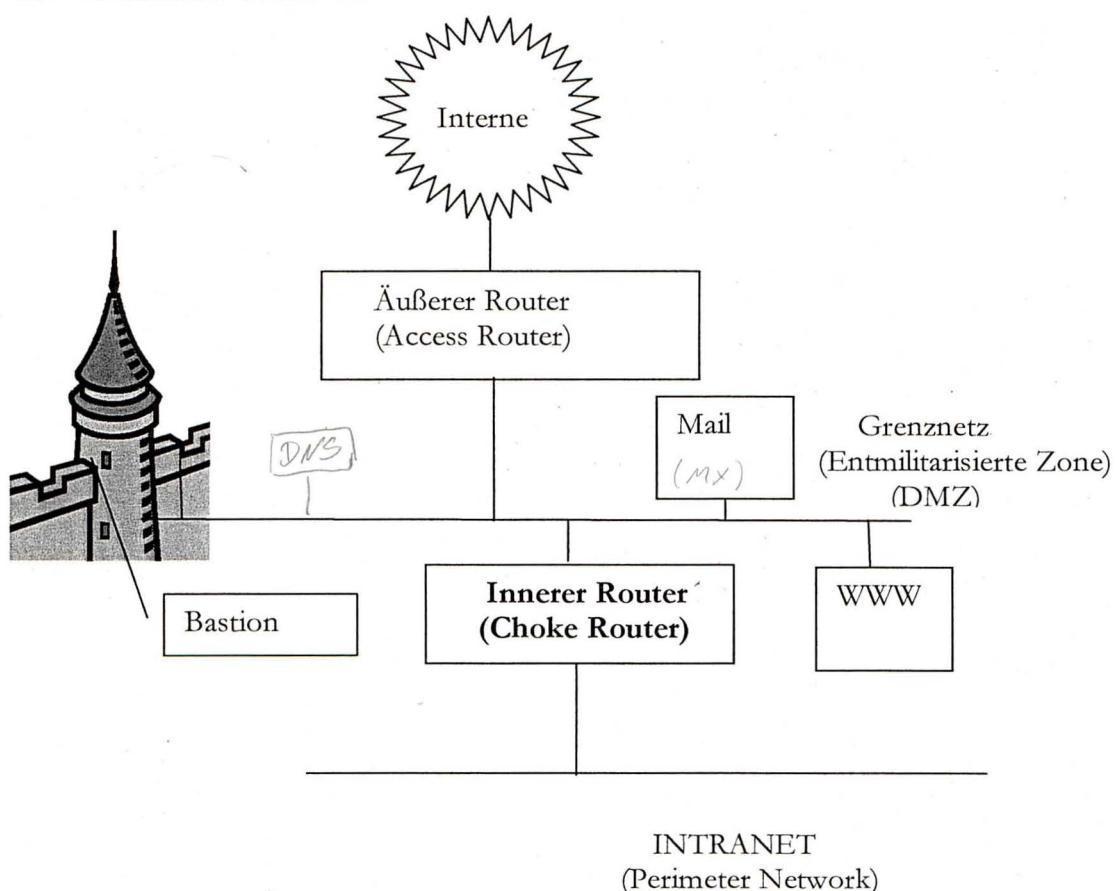
Der **Bastion Host** bietet den Rechnern des Intranet die externen Internetdienste an.

Der **Überwachungsrouter** verhindert durch Paketfilterung, dass die Nutzer aus dem Intranet den Bastion Host umgehen und direkte Verbindungen mit Rechnern im Internet aufnehmen können. Der Bastion Host wickelt die Kommunikation mit dem Internet ab. Der Überwachungsrouter wird so konfiguriert, dass Rechner aus dem Internet Verbindungen nur mit dem Bastion Host aufnehmen können.

Mögliche Konfigurationen des Paketfilters des Überwachungsrouter:

- Rechner aus dem Intranet dürfen einige Dienste im Internet direkt ansprechen, die anderen Dienste müssen über Proxy-Server des Bastion-Host verwendet werden
- Die Rechner aus dem Internet dürfen ausschließlich über den Bastion-Host Verbindung mit Rechnern aus dem Intranet aufnehmen.

Überwachtes Teilnetz

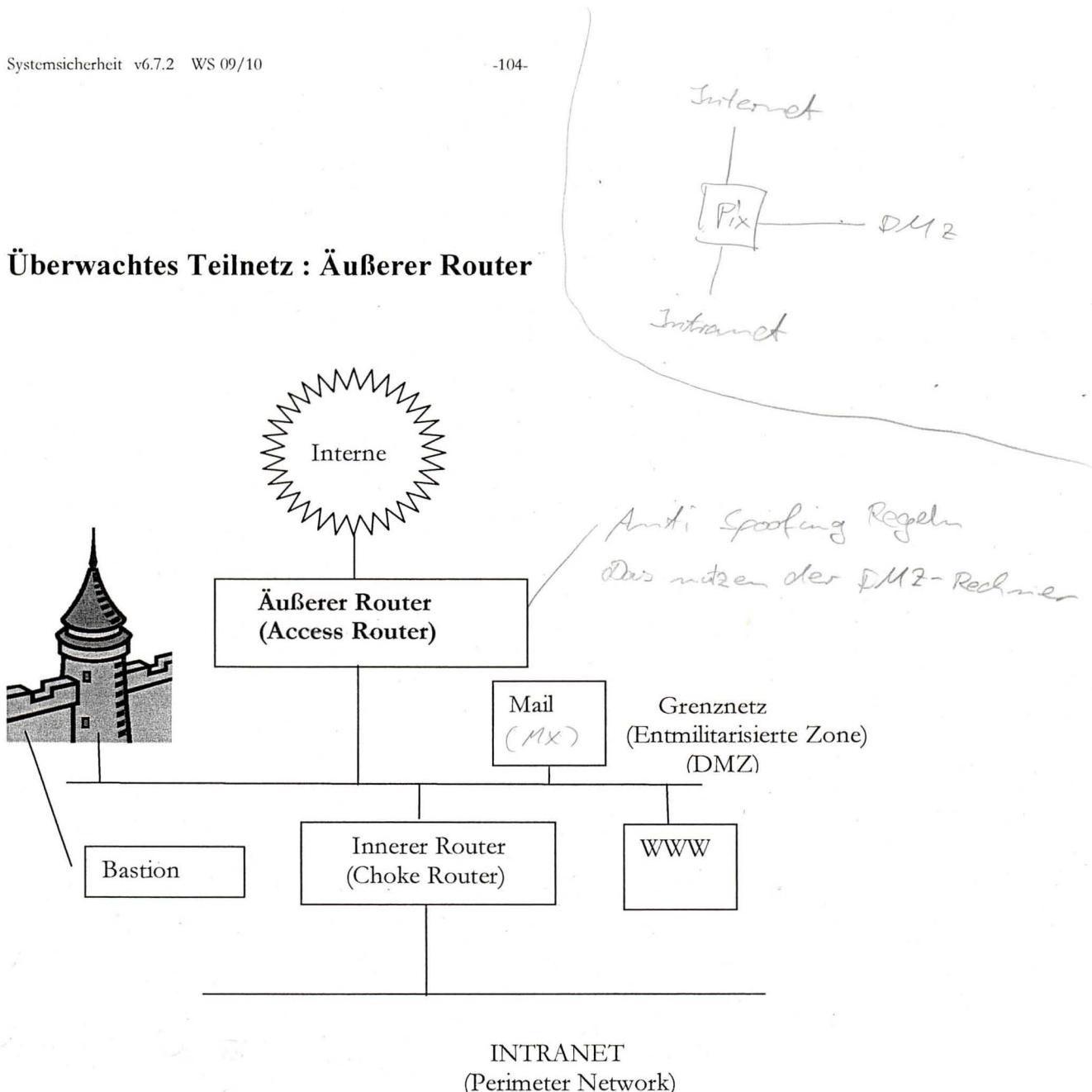


Bei dieser Konfiguration ergibt sich eine zusätzliche Sicherung, weil ein Eindringling zwei Router und den Bastion Host überwinden muss, um ins Intranet zu gelangen.

Überwachtes Teilnetz : Innerer Router

- Übernimmt den Großteil der Pakettfiltrierung
- Ermöglicht es ausgewählte Diensten, direkt auf das Internet zugreifen zu können.
- Erzwingt, dass die Benutzer aus dem Internet die Proxy-Dienste des Bastion-Host verwenden

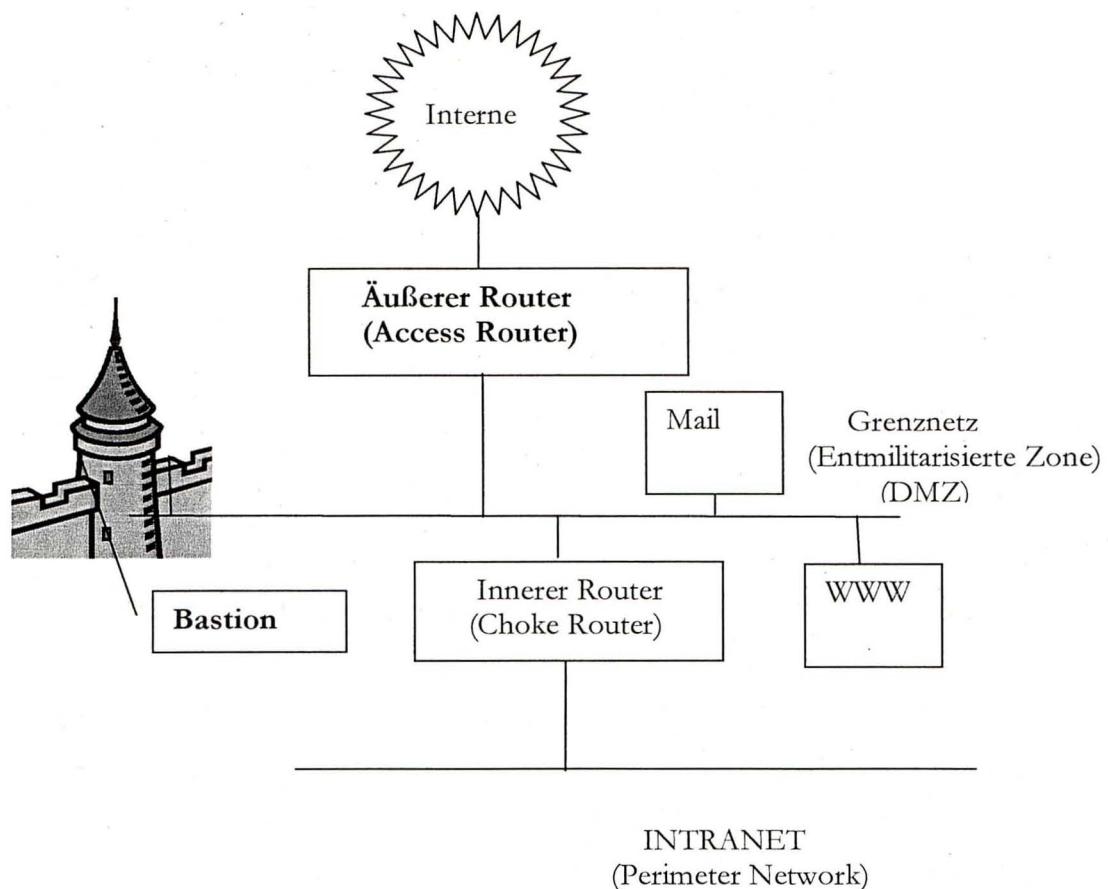
Überwachtes Teilnetz : Äußerer Router



Überwachtes Teilnetz : Äußerer Router

- Es schützt davor, dass Rechner von außen hinzugefügt werden, um zum Intranet zu gehören.
- Es zwingt, dass nur die Server der DMZ genutzt werden.

Überwachtes Teilnetz : Bastion Host



Überwachtes Teilnetz: Bastion - Host

- Stellt Proxy-Dienste zur Verfügung
- Kann als Anlaufstelle aus dem Internet dienen für E-Mail, FTP, DNS, ...
Bei hohem Datenverkehr können diese Dienste auf andere Rechner in der DMZ angelagert werden

Richtlinien für die Konfiguration von Bastion Hosts (Rechner in der DMZ)

Um es einem Angreifer schwer zu machen, sollten folgende Richtlinien für die Realisierung eines Bastion-Host eingehalten werden:

- ① Keine Benutzer-Accounts auf dem Host
(Schwache Passwörter)
- ② Deaktivieren überflüssiger Dienste
(keine überflüssigen Programme)
- ③ Abhalten des Routing
 - ip forwarding deaktivieren
 - alle Programme deaktivieren die Pakete weiterleiten können.
 - IPv6
- ④ z.B. Einsatz von Wrappers zum Schutz von Diensten
 - ↑
tcpd mit inetd
 - xinetd → Rate von Dienstanfragen festlegen
- ⑤ Auditing - Pakete aktivieren
 - ↑
Sicherheitsprüfung (→ Nessus von BSI)
 - Auditing-Pakete verfolgen zwei Ziele
 - Testen von Sicherheitslücken
 - Erkennung von unerlaubten Änderungen (Tripwire) von Dateien (Prüfsummen von sauberen Programmen werden in Datenbank abgelegt)
zyklische Überprüfung
- ⑥ Dateisystem soweit möglich als nur lesbar konfigurieren

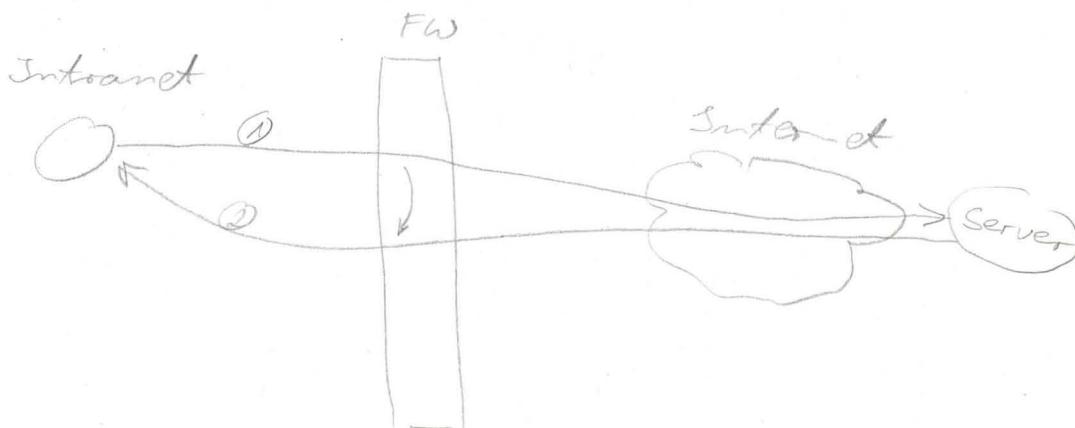
Von Firewall- Systemen verwendete Sicherungsmethoden

- Paketfilter
- Proxy- Systeme
- NAT

Paketfilter -Firewall

Grundlagen

- Ist ein Router, der alle Pakete nach vorgegebenem Regelwerk (rule-set) filtert
- Ist transparent gegenüber den Kommunikationspartnern
- Arbeitet auf den Schichten 3 und 4
- Arten von Paketfilterung
 - statische Paketfilterung
Die Filterregeln arbeiten unabhängig von vorangegangenem Datenpaket
 - dynamische Paketfilterung
(stateful inspection)
Erweitert z.B. Regelwerk temporär um zusätzliche Regeln für den Rückkanal



FW schaltet mit temporären Regeln den Weg für die Server-Antwort frei.

Welche Protokollfelder muss eine Paketfilter-Firewall beachten?

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1
+-----+-----+-----+-----+			
Version IHL Type of Service Total Length			
+-----+-----+-----+-----+			
Identification Flags Fragment Offset			
+-----+-----+-----+-----+			
Time to Live Protocol Header Checksum			
+-----+-----+-----+-----+			
Source Address			
+-----+-----+-----+-----+			
Destination Address			
+-----+-----+-----+-----+			
Options Padding			
+-----+-----+-----+-----+			

IP

2. für ICMP-Pakete
auf 1 gesetzt

0	7 8	15 16	23 24	31
+-----+-----+-----+-----+				
Source Port Destination Port				
+-----+-----+-----+-----+				
Length Checksum				
+-----+-----+-----+-----+				
data octets ...				
+-----+-----+-----+-----+				

UDP

3. Pakete mit dem
ACK-Flag = 0 aus
dem Internet
sperren/filtern

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1 2 3 4 5 6 7 8 9 0	1
+-----+-----+-----+-----+			
Source Port Destination Port			
+-----+-----+-----+-----+			
Sequence Number			
+-----+-----+-----+-----+			
Acknowledgment Number			
+-----+-----+-----+-----+			
Data U A R S F			
Offset Reserved R C S S Y I Window			
G K H T N N			
+-----+-----+-----+-----+			
Checksum Urgent Pointer			
+-----+-----+-----+-----+			
Options Padding			
+-----+-----+-----+-----+			
data			
+-----+-----+-----+-----+			

TCP

Zulassen: Intranet

①
P-Dest
CP-Dest Port

141.69.1.22

Telnet
②

③
P-Dest
CP-Dest Port

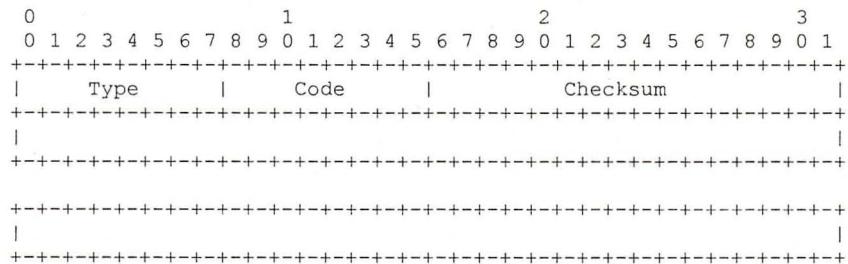
141.69.1.1

DNS, UDP
④

FW Internet
TCP-Dest-Port > 1023
ACK-Flag = 1

ICMP V4

ICMP-Nachrichten werden in IP-Paketen transportiert. Das IP-Header-Feld enthält den Wert 1.



Type:

Das Feld Type gibt darüber Aufschluss, um welche ICMP-Nachricht es sich handelt. Es sind die folgenden Type-Werte definiert:

Werte für das Type-Feld:

0 Echo Reply	3 Destination Unreachable	12 Parameter Problem
4 Source Quench		13 Timestamp
5 Redirect		14 Timestamp Reply
8 Echo		15 Information Request
11 Time Exceeded		16 Information Reply

Code:

Das Feld Code gibt eine weitere Beschreibung der ICMP-Nachricht. Es gibt z.B. bei der Nachricht "Destination Unreachable; Type=3" Gründe an, warum ein System nicht erreichbar ist.

Aufgabe Paketfilter- Firewall

Welche Header-Felder muss eine Paketfilter-Firewall interpretieren, wenn folgende Filterregeln gelten sollen?

- 1.) Als Ziel für einkommende Telnet-Verbindungen nur den Rechner 141.69.1.22 zulassen.
- 2.) Alle ICMP-Pakete ausfiltern.
- 3.) Den Verbindungsaufbau aus dem Internet auf jeden Intranetrechner sperren.
- 4.) DNS-Anfragen aus dem Internet nur auf den DNS-Server 141.69.1.1 zulassen.

② IP-Protokoll = ICMP

③ Verbindungsauflösung



Paketfilterung ist ein Sicherheitsmechanismus, der aufgrund des Inhaltes von Datenpaketen (im wesentlichen **IP-Adressen und Port-Nummern**) überprüft, ob Daten in ein Netz oder aus einem Netz weitergeleitet werden dürfen. Die Paketfilterung wird auf Routern verwendet.

Einige mögliche Einschränkungen, die sich durch Paketfilter realisieren lassen:

Telnet aus dem Internet auf einen beliebigen Rechner des Intranet sperren

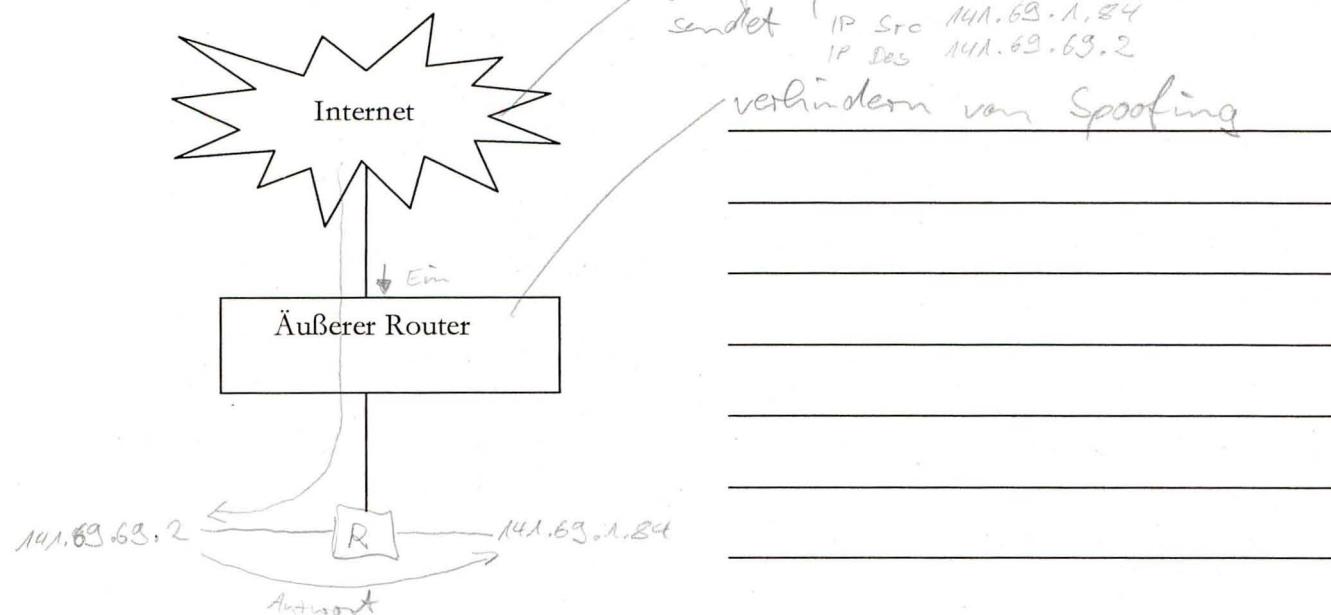
Beliebige Rechner aus dem Internet dürfen eine Verbindung zum SMTP-Port des Mail-Exchangers aufbauen

Ein bestimmter Rechner aus dem Internet darf Daten mit einem bestimmten Protokoll an einen Rechner des Intranet senden

Ein Paketfilter kann jedoch nicht eine Datei- oder Benutzer-orientierte Filterung durchführen.

Eine Paketfilterung ist bei Firewallsystemen auf dem äußeren und auf dem inneren Router sinnvoll einsetzbar.

Filterung nach Adressen



Regel zum Abblocken von IP-Paketen mit gefälschter Quelladresse:

Regel	Richtung	Quelladresse	Zieladresse	Aktion
1	Ein	intern	beliebig	verbieten
2	Ein	extern	intern	zulassen

Diese Filterregel schützt vor Angriffen, bei denen der Angreifer vortäuscht, seine Datenpakete würden von einem vertrauenswürdigen Rechner aus dem Intranet stammen. Für diese Art des Angriffs gibt es die folgenden Voraussetzungen:

Der Angreifer benötigt keine Antwortpakete (z.B. wenn er sich die Passwort-Datei per E-Mail zusenden lassen will)

Der Angreifer errät die Antwortpakete (die kommen natürlich nicht bei ihm an, da sie nicht aus dem Intranet heraus geroutet werden) und quittiert diese.

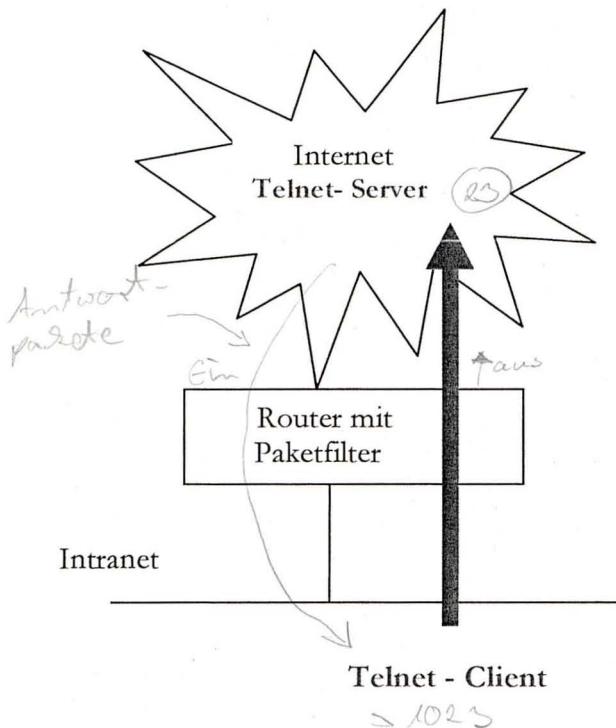
Das bei diesen Angriffen auftretende Problem besteht darin, dass der „echte“ Rechner aus dem Intranet die Antwortpakete erhält und ggf. auf diese antwortet.

Lösung:

- Der Angriff wird durchgeführt, wenn der echte Rechner nicht einsatzbereit ist
- Vor oder während des Angriffs wird der Echte Rechner lahmgelegt (DoS)
- Das Routing wird zwischen dem Angreifer und dem echten Rechner geändert.
z.B. Source Route Option von IP verwenden.
- Der Angreifer verwendet eine Internetadresse die nicht vergeben ist

Filterung nach Diensten

Es wird nur dann ausschließlich nach Adressen gefiltert, wenn gefälschte Pakete abgewehrt werden sollen. In den meisten anderen Fällen bezieht die Paketfilterung die Überprüfung von Diensten mit ein.



Spooing
Beispiel: Telnet vom Intranet ins Internet erlauben
Telnet aus dem Internet auf einen Server ins Intranet verbieten.

* Beim ersten Paket einer TCP-Verbindung ist das ACK-Flag nicht gesetzt, somit immer:

Regeln, wenn nur nach außen gerichtetes Telnet zugelassen sein soll:

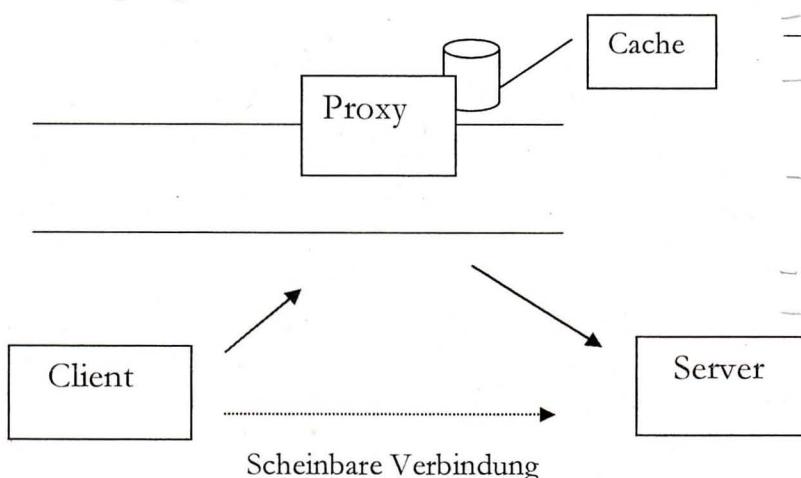
Regel	Richtung	Quell-adresse	Ziel-adresse	Protokoll	Quell-port	Ziel-port	ACK gesetzt?	Aktion
1	aus	intern	beliebig	TCP	>1023	23	beliebig ja	zulassen
2	ein	extern	intern	TCP	23	>1023	ja	zulassen
3	beliebig	bel.	bel.	bel.	bel.	bel.	bel.	verbieten

Regel 1: Erlaubt Pakete zu Telnet- Servern im Internet.

Regel 2: Lässt Antwortpakete von den Telnet-Servern zu.

Regel 3: Wenn die Regeln 1 oder 2 nicht greifen, wird das betreffende Paket blockiert.

Proxy-Systeme



- Caching von Inhalten
- muss höheres Protokoll kennen.
- Untersucht Inhalte: Schutz vor Angriffen.
- Inhaltsproxys
- Logging

Ein Proxy ist ein Rechner, der sich als Vermittler in den Kommunikationspfad zwischen einem Client im Intranet und einen Server im Internet einschaltet. Zum Internet erscheint nur dieser Rechner mit seiner IP- Adresse. Rechner aus dem Internet können also nicht auf die hinter dem Proxy verborgenen Client-Rechner zugreifen.

Man teilt Proxy-Server in die folgenden Gruppen ein:

Application – Level Proxy (dedizierter Proxy)

Dieser **interpretiert** das von der Anwendung verwendete Protokoll

- für jedes Protokoll ist ein eigener Proxy erforderlich
- kann die Inhalte überprüfen

Circuit- Level Proxy (generischer Proxy)

Dieser Proxy- Typ führt ebenfalls für Client-Rechner aus dem Intranet Anfragen an Server im Internet durch. Er **interpretiert** das Anwendungsprotokoll jedoch **nicht**. Die Client- Rechner müssen **modifizierte Zugriffsprogramme** für den Zugriff auf Server verwenden.

- Nimmt die Applikationsdaten eines Client entgegen und gibt sie als TCP- Verbindung umgehängt an den Server im Internet weiter.
- Bsp.: Socks!

Proxy- Systeme beugen Sicherheitsproblemen vor:

Keine Benutzer - Accounts auf einem aus dem Internet erreichbaren Rechner (damit auch keine schwachen Passwörter)

Es ist den Clients im Intranet nicht möglich unkontrolliert Software für den Internetzugang zu verwenden (sie müssen die Programme des Proxy verwenden)

Die Client-Rechner, die den Proxy verwenden, bleiben den Rechnern des Internet verborgen, weil der Proxy die Internetanfragen mit seiner IP-Adresse durchführt.

Vorteile von Proxy - Diensten:

Proxies bieten Nutzern Zugriff auf Internetdienste

Effektive Möglichkeit zur Protokollierung

Untersuchung der Datenpaketinhalte möglich (Entfernen von gefährlichem Inhalt)

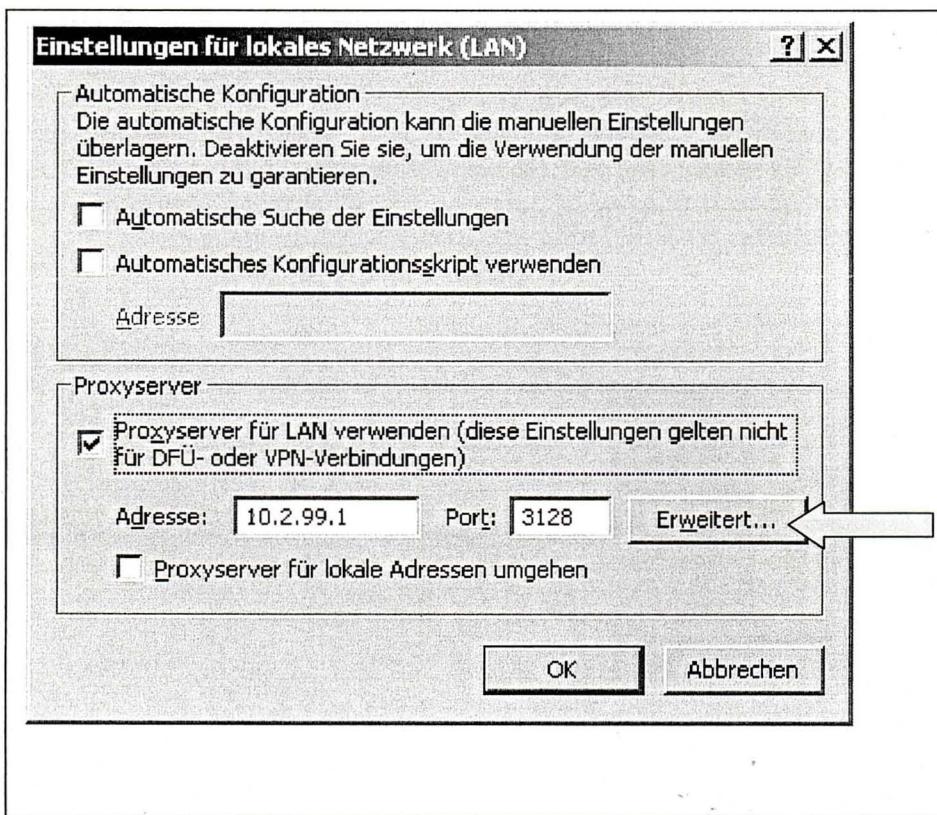
Caching von z.B. Webinhalten möglich

Nachteile von Proxy- Diensten:

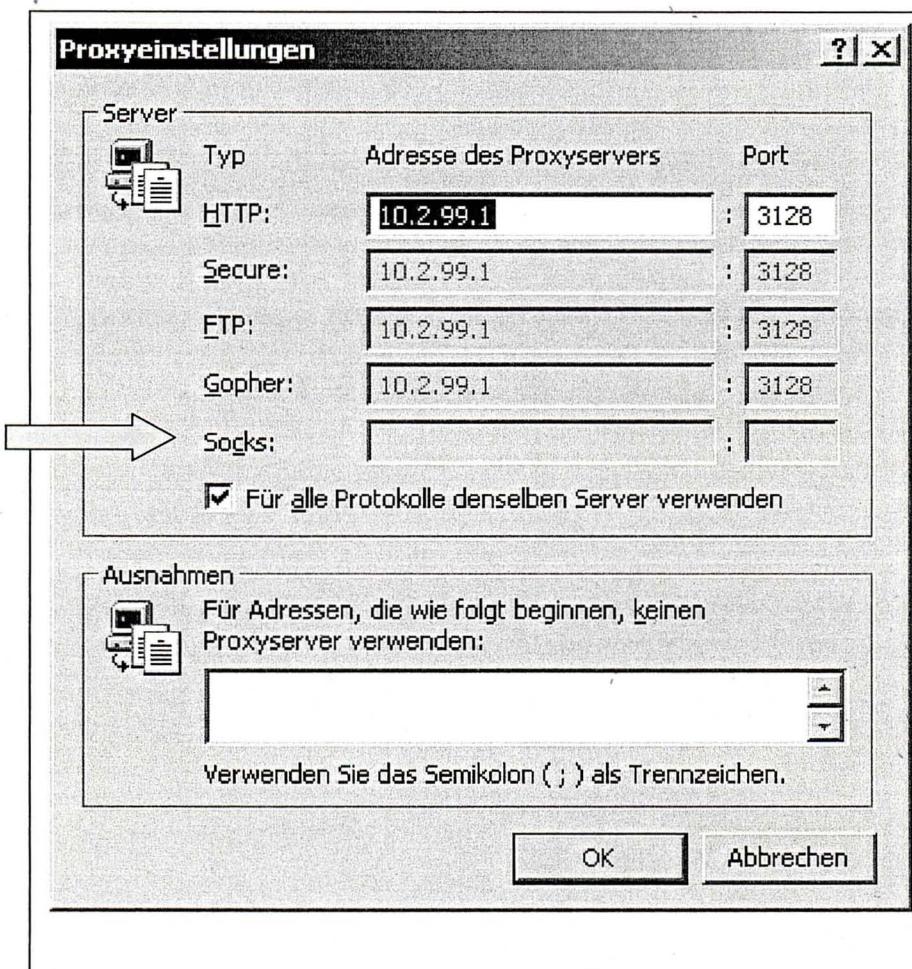
- hindern neuen Applikationen hinterher
- Bei Application-level Proxies benötigt man für jeden Dienst einen eigenen Proxy
- für solche verwendete Dienste gibt es keinen Proxy
- Client-Software muss angepasst werden!
- Ablauf wird langsamer

Der Internetexplorer als Proxy-Client

Internetexplorer: Extras → Internetoptionen → Verbindungen → LAN- Einstellungen:



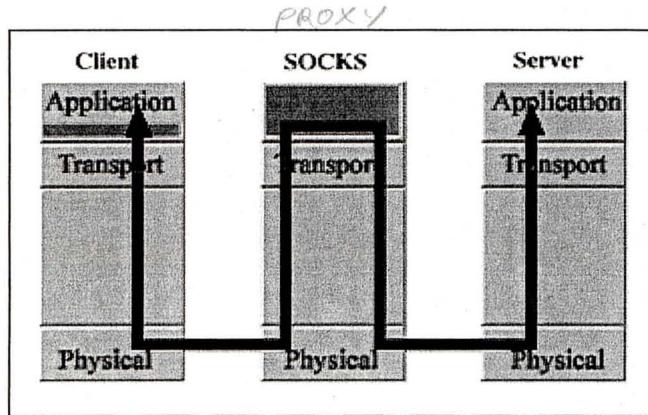
Erweitert:



Socks : Ein generischer Proxy

SOCKSv5 is an IETF (Internet Engineering Task Force) approved standard (RFC 1928) generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies.

SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct IP-reachability.



When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server. For the application server, the proxy server is the client.

Application-Independent Proxy

As a generic proxy, the SOCKS protocol establishes communication channels, and manages and protects the channel for any application. As new applications come to market, SOCKS can protect them without requiring additional development. IP layer stateful inspection proxies require a new script for protocol inspection, and application layer proxies require new proxy software for each new application.

NAT

RFC3022

Die RFC 3022 trägt den „Titel Traditional IP Network Translator (Traditional NAT)“.

Der Network Address Translator ist dabei das Gerät, welches eine Übersetzung von Netzwerkadressen vornimmt. Im weiteren Text dieser RFC wird dann NAT zusätzlich als Abkürzung für Network Address Translation verwendet. Dies ist der sonst übliche Sprachgebrauch, der sich eingebürgert hat. Diese Verwendung der Abkürzung NAT wird auch in diesem Skript verwendet. Mit NAT ist also im Folgenden der Vorgang der Adressübersetzung (Translation) gemeint.

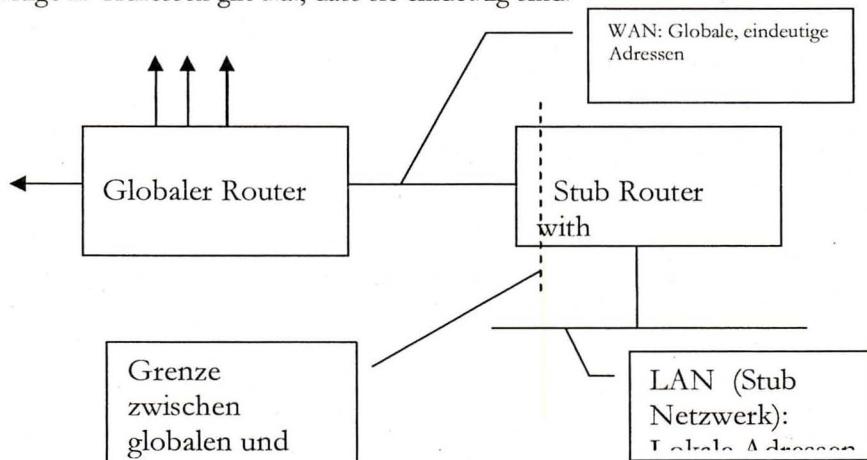
Es gibt zwei Arten von NAT(Basic NAT, NAPT), die zusammen als „Traditional NAT“ bezeichnet werden.

Unter dem Begriff „Basic Network Address Translation“ (Basic NAT) versteht man eine Methode mit der eine Gruppe von IP-Adressen auf eine andere Gruppe von IP-Adressen abgebildet wird. Dieser Vorgang wird transparent für den Anwender durchgeführt.

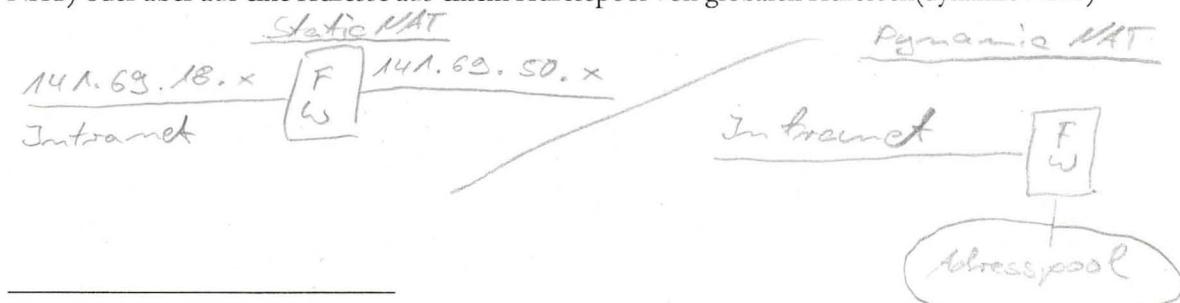
„Network Address Port Translation“ (NAPT) bezeichnet ein Verfahren bei dem viele IP-Adressen auf **eine** IP-Adresse abgebildet werden. Um die Abbildung umkehrbar zu machen, wird zusätzlich zur Quell-IP-Adresse das Quell TCP- oder UDP- Port vom Network Address Translator (Das ist die Netzkomponente, die die Network Address Translation durchführt) umgeschrieben.

Basic NAT

Ein Stub – Netzwerk¹ mit einer Reihe von privaten oder zu modifizierenden Adressen erhält mit diesem Verfahren die Möglichkeit mit einem externen Netzwerk zu kommunizieren. Die Adressen des externen Netzwerkes werden als globale Adressen bezeichnet. Globale Adressen sind gültige IP- Adressen. Für gültige IP-Adressen gilt u.a., dass sie eindeutig sind.



Die Übersetzung der lokalen Adressen kann entweder immer auf dieselbe globale Adresse erfolgen (static NAT) oder aber auf eine Adresse aus einem Adresspool von globalen Adressen(dynamic NAT).



¹ Ein Stub-Netzwerk ist ein Netz, bei dem Datenpakete aus dem lokalen Netz und in das lokale Netz nur über einen Router (=Stub-Router) gesendet werden.

Static NAT

Beim static NAT ist die Zuordnung der lokalen IP- Adressen (l) zu globalen Adressen (g) fest vorgegeben. Man benötigt also genauso viele globale Adressen wie genutzte lokale Adressen.

1 : g - Translation
 $l, g \geq 1$ und $l = g$
 l: Anzahl der lokalen Adressen; g: Anzahl der globalen Adressen

Für die Zuordnung zwischen globalen und lokalen Adressen gilt:
 global-address = global-network-ID OR (local-address AND (NOT

Beim static NAT bleibt die host-ID erhalten, die net-IDs ändern sich.

Static NAT wird dann eingesetzt, wenn die lokalen Adressen nicht im globalen Netz verwendet werden dürfen. Das kann dann der Fall sein, wenn es sich bei den lokalen Adressen um private IP-Adressen handelt, oder wenn etwa nach einem ISP-Wechsel die bisher verwendeten IP-Adressen des alten ISPs weiter verwendet werden sollen, weil der Umstellungsaufwand auf die Adressen des neuen ISP zu groß ist. Static NAT kann ferner erforderlich sein, wenn aus dem globalen Netz auf Server innerhalb des lokalen Netzes zugegriffen werden soll.

Dynamic NAT

Dynamic NAT wird dann benötigt, wenn die Anzahl der lokalen Adressen größer ist als die Anzahl der zur Verfügung stehenden globalen Adressen, oder wenn die IP-Adressen des lokalen Netzes verschleiert werden sollen.

1 : g - Translation
 $l \geq 1$ und $l \geq g$
 l: Anzahl der lokalen Adressen; g: Anzahl der globalen Adressen

Für die Zuordnung zwischen globalen und lokalen Adressen gilt:

- Die lokalen Adressen werden auf globale Adressen aus einem Adresspool abgebildet.
- Jede neue Verbindung aus dem lokalen Netz erhält eine neue IP- Adresse aus dem globalen Adresspool zugeordnet.
- Wenn eine Adresszuordnung für einen lokalen Rechner besteht, wird diese Zuordnung verwendet.
- Solange die Zuordnung besteht, kann der betreffende Rechner aus dem globalen Netz unter seiner zugeordneten globalen Adresse erreicht werden.

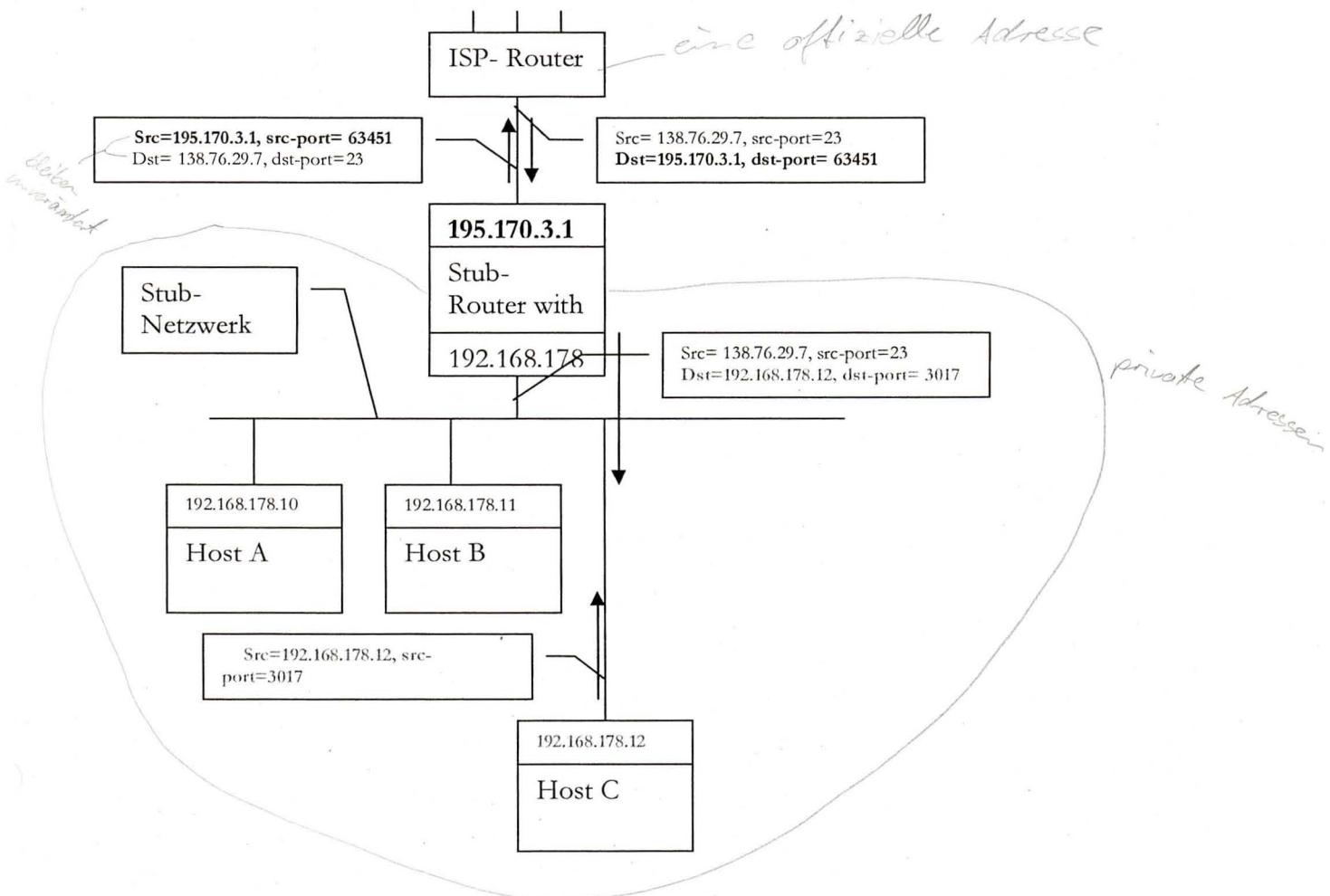
Network Address Port Translation (NAPT)

Der Anschluss von kleineren Institutionen an das Internet über einen ISP erfolgt häufig so, dass der ISP der Organisation nur eine offizielle IP- Adresse zuweist. In der Regel soll jedoch auch bei kleineren Institutionen mehreren Rechnern im LAN der Internet-Zugriff gestattet werden. NAPT ermöglicht eine Zuordnung von vielen lokalen IP- Adressen auf eine offizielle IP- Adresse, so dass von allen lokalen Rechnern ausgehender Internetverkehr möglich ist. NAPT ist die am häufigsten verwendete NAT- Technik. Sie wird auch mit dem Begriff „Masquerading“ bezeichnet. Die lokalen Adressen sind versteckt, so dass aus dem globalen Netz in der Regel nicht auf die Rechner des lokalen Netzes zugegriffen werden kann.

Diese Situation ist bei den im Heimbereich eingesetzten DSL-Anschlüssen die Regel. NAPT kann so erweitert werden, dass eingehender Verkehr statisch aufgrund seiner Zielportnummer auf einen der lokalen Rechner geleitet wird (port forwarding).

1 : g - Translation
 $1 \geq l$ und $g = 1$
 l: Anzahl der lokalen Adressen; g: Anzahl der globalen Adressen

Im folgenden Beispiel nutzt das interne Stub-Netzwerk den privaten Adressblock 192.168.178.0/24. Die dem Stub-Router an seinem WAN-Interface vom ISP zugewiesene offizielle IP-Adresse ist 195.170.3.1.



Wenn der Host C innerhalb des Stub-Netzwerks ein Telnet-Paket an den Rechner 138.76.29.7 sendet, verwendet er dessen Adresse als Zieladresse (dst) im IP-Header. Im TCP-Header gibt er 23 (=well known port für den Telnetdienst) als Zielport (dst-port) an. Als Quelladresse gibt er in diesem Paket seine IP-Adresse (src=192.168.178.12) an. Als TCP-Quellport (src-port) verwendet er in diesem Beispiel 3017.

Der Stub-Router hat den Router des ISP als Standard-Gateway eingetragen. Er leitet das Paket an das Ziel 138.76.29.7 über dieses Standard-Gateway weiter. Vorher tauscht er im Paket jedoch die Quelladresse und den Quellport aus. Der Stub-Router gibt im weitergeleiteten Paket seine IP-Adresse (195.170.3.1) als

Quelladresse im IP-Header an. Als Quellport im TCP-Header gibt er aus seinem NAT-Portbereich eine freie Portnummer an. Er trägt diese Zuordnung in einer internen Tabelle ein, damit er beim Antwortpaket des Telnet-Servers die Veränderungen wieder rückgängig machen kann, bevor er das Paket an den Host C ausliefert. Die Tabelle hat den folgenden prinzipiellen Aufbau.

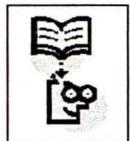
Masquerading-Table		
Stub-Netzwerk IP	Quellport des betreffenden Stub-Rechners	Zugewiesene Quellportnummer
192.168.178.12	3017	63451
...		

Der Stub-Router muss den zugewiesenen Quellport eindeutig vergeben. Im Antwortpaket wird dieser Port dann als Zielpunkt angegeben. Aus der obigen Tabelle erkennt der Stub-Router, an welchen lokalen Rechner und an welchen lokalen Port er das Datenpaket weiterleiten muss.

Wenn aus dem Internet auf einen bestimmten Dienst im Stub-Netzwerk zugegriffen werden soll, so ist es möglich eingehenden Datenverkehr, der an ein well known port gesendet wird, an einen bestimmten Rechner im Stub-Netzwerk weiterzuleiten.

Aufgabe NAT 1

Fragen zum Kapitel „NAT“



- a) Welche Verfahren kennen Sie für eine Network Address Translation?
- b) Mit welchen Verfahren „spart“ man offizielle IP-Adressen?
- c) Wann kann ein Stub-Router mit NAPT eine zugewiesene Quellportnummer wieder freigeben?
- d) Wie können ICMP-Pakete korrekt ausgeliefert werden?
- e) Welche Felder muss ein Stub-Router mit NAT/NAPT im IP-, TCP- und UDP-Header modifizieren?

Aufgabe NAT 2

Auf einem Rechner hinter einem NAT-Router wird ein ping -Kommando abgesetzt. Dabei wird der folgende Datenrahmen auf diesem Rechner aufgezeichnet.

0000 00 17 9a 59 2d 55 | 00 15 58 7c d5 25 | 08 00 45 00 ... Y-U..X|.%.E.

DA SA Type TOS
=1Pv4

0010 00 3c 5e 59 00 00 80 01 8d 06 c0 a8 00 73 8d 45 .<^Y.....s.E

Length IP Flag TTL F Σ SA
Fragment offset = ICMP 192.168.0.15

0020 01 01 08 00 35 5c 05 00 13 00 61 62 63 64 65 66 5\....abcdef

DA T C Σ ID SEQ
Echo = P d e

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuvwxyz

0040 77 61 62 63 64 65 66 67 68 69 wabcdefghijklm

Hinter dem NAT-Router wird der folgende modifizierte Datenrahmen aufgezeichnet.

0000 00 00 0c 07 ac 34 | 00 17 9a 59 2d 54 | 08 00 45 00 4...Y-T..E.

DA SA Type TOS

0010 00 3c 5e 59 00 00 7f 01 8d 66 8d 45 34 76 8d 45 .<^Y.....f.E4v.E

Length IP Flag TTL F Σ SA
192.168.52.118

0020 01 01 08 00 9e 73 9b e8 13 00 61 62 63 64 65 66 s....abcdef

DA E ID SEQ

192.168.1.1

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmnopqrstuvwxyz

0040 77 61 62 63 64 65 66 67 68 69 wabcdefghijklm

a.) Wie setzt der NAT-Router die ICMP-Pakete um?

b.) Wie werden die IP-Adressen umgesetzt?

Cisco Access Control Lists (ACLs) \triangleq Paketfilterung

ACL Grundlagen

ACLs sind Anweisungslisten denen der Router entnehmen kann, welche Datenpakete er weiterleiten (permit) und welche er blockieren (deny) soll

Eine permit- oder deny- Anweisung untersucht die folgenden Parameter:

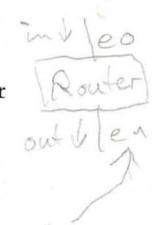
- Source Address
- Destination Address
- Port-Numbers
- Flags (TCP)
- Upper Layer Protocols

ACLs werden an die Schnittstellen **gebunden**, bei denen Sie die Pakete untersuchen sollen. Es wird bei Cisco-ACLs eine Richtung für die ACLs angegeben (**in / out**). "In" bezeichnet dabei Datenpakete, die zum Router gesendet werden, out bezeichnet die Pakete, die den Router verlassen.

Sämtlicher Datenverkehr, der die Routerschnittstellen in der durch die Bindung vorgegebenen Richtung passiert, wird gegen die Anweisungen der gebundenen ACL getestet.

ACLs können für **jedes routbare Protokoll** erzeugt werden. Sie können den **Zugriff** auf ein Netz, ein Subnetz oder einzelne Rechner kontrollieren. Sie werden für jedes Protokoll separat definiert.

IP, IPX, AppleTalk



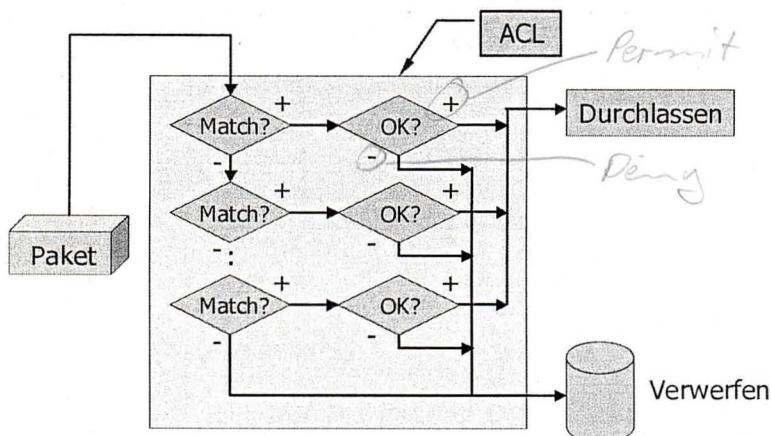
Gründe warum ACLs eingesetzt werden

-
- Netzwerksicherheit soll erhöht werden
 - Zugriffskontrolle auf einzelne Netze oder Rechner
 - Sperren von Protokollen
↳ Dial on Demand (ISDN)
-

Bearbeitung der ACL-Regeln

Eine ACL besteht im Normalfall aus einer ganzen Reihe von **Regeln (rules)**. Jedes Datenpaket wird gegen diese ACL-Regeln in der **Reihenfolge** getestet, in der sie in die betreffende ACL eingetragen sind. Wird eine **Übereinstimmung (match)** gefunden, wird das betreffende Paket - wie in dieser ACL-Anweisung angegeben - entweder zur Weiterleitung zugelassen (permit) oder verworfen (deny).

Die Regeln, die auf die Anweisung mit einer Übereinstimmung (Match) folgen werden nicht mehr ausgeführt. Falls in der ACL kein Match gefunden wurde, wird ein implizites "deny any" Statement durchgeführt.



interface ethernet 0

ip address 1.1.1.1 255.0.0.0

} IP-Addresse festlegen
ip access-group 1 in Binden der ACL mit der Nr. 1 an dieses Interface
ip access-group 2 out Richtung: in dieses Interface

! Numerenzbereich legt fest: Standard oder Extended ACL
access-list 1 permit 5.6.0.0 0.0.255.255 ↗ überprüft nur Quelladressen
access-list 1 deny 7.9.0.0 0.0.255.255 ↗ Wildcard

access-list 2 permit 1.2.3.4

access-list 2 deny 1.2.0.0 0.0.255.255 ↗ 0.0.0.0 kann weggelassen werden

!

Zuweisen von ACLs an Interfaces

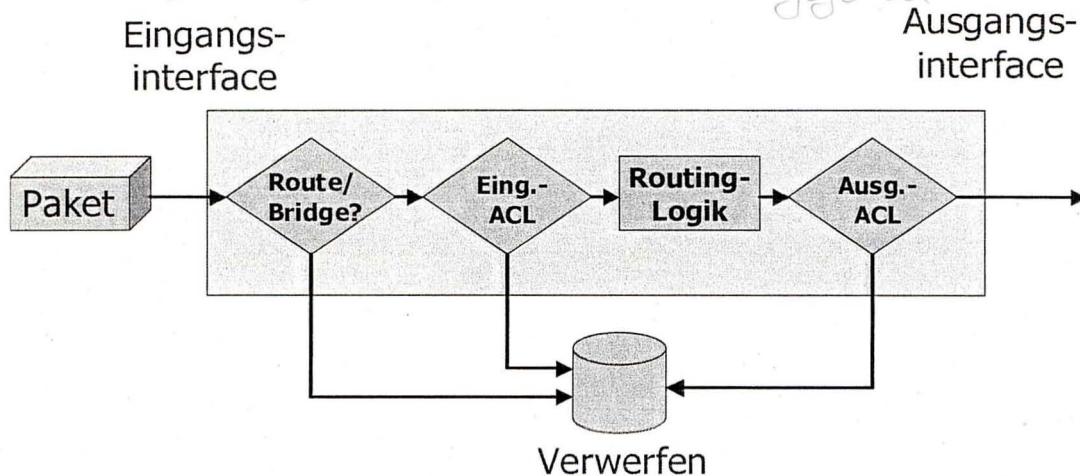
Die ACLs werden angewendet beim Eintreten eines Paketes in den Router (inbound)

oder beim Verlassen des Routers (outbound).

Damit die bereits definierten ACLs wirken werden, müssen sie an die Interfaces gebunden werden, für diese angezeigt werden sollen.

Beim Binden an ein Interface wird die

Wirkrichtung bezogen auf den Router angegeben (in/out)



Pro Interface kann **pro Richtung** und Protokoll jeweils nur eine ACL gebunden werden.

Regelwerke für ausgehenden Datenverkehr (**outbound ACL's**) sind **effizienter** und daher zu bevorzugen.

Erstellen von ACLs

Im ersten Schritt werden die **ACLs definiert**, im zweiten Schritt werden sie an ein **Interface gebunden**. Weil outbound ACLs effizienter als inbound ACLs sind, werden sie bevorzugt eingesetzt. Cisco - ACLs werden durch eine Nummer (**„numbered ACL“**) oder einen Namen (**„named ACL“**) eindeutig identifiziert.

Für die einzelnen Protokolle sind Gültigkeitsbereiche für die ACL- Nummern fest vorgegeben.

Protokoll	Nummernbereiche für die ACL
IP (Standard ACLs)	0 – 99 <i>Nur Source - Adress prüfen</i>
Extended IP (Extended ACLs) <i>(*)</i>	100 – 199
Apple Talk	600 – 699
IPX	800 - 899
Extended IPX	900 - 999
IPX SAP	1000 - 1099

Wenn eine Anweisung in einer „numbered ACL“ geändert werden soll, muss die gesamte ACL gelöscht werden:
`no access-list <list number>`

`Router(config)# access-list access-list-number {permit|deny} {test-conditions}`

`Router(config-if)# [protocol] access-group access-list-number` | Interface-Config-Modus

Beispiel:

```
interface ethernet 0
ip address 1.1.1.1 255.0.0.0
ip access-group 1 in
ip access-group 2 out
!
access-list 1 permit 5.6.0.0 0.0.255.255
access-list 1 deny 7.9.0.0 0.0.255.255
!
! diese Wildcard kann weg gelassen werden
access-list 2 permit 1.2.3.4 0.0.0.0
access-list 2 deny 1.2.0.0 0.0.255.255
!
```

Konfigurationsdatei
wird beim Start
des Routers geladen.

0-99 Standard IP-ACLs

Bit = 0 prüfen
Bit = 1 nicht prüfen

Wildcard mask bits

werden eingesetzt, um anzugeben ob eine ACL eine Subnetzadresse einen Addressbereich oder eine Hostadresse überprüfen soll.
 Eine Wildcard Mask besteht aus 32 Bit, die in 4 Byte aufgeteilt und dezimal angegeben werden.

ACHTUNG: Obwohl eine Wildcard eine gewisse Ähnlichkeit zu einer Subnet-Mask hat, sind die 0-Bits und 1-Bits anders zu interpretieren!

- Ein 0-Bit bedeutet, dass das korrespondierende Bit der zu prüfenden IP-Adresse kontrolliert wird!
- Ein 1-Bit bedeutet, dass das korrespondierende Bit irrelevant ist!
- 0- und 1-Bits können auch gemischt auftreten! Bei einer Subnet-Mask gibt es ja eine Grenze bis zu der nur 1-Bits auftauchen, danach nur noch 0-Bits. Das bedeutet, dass bei Wildcards auch innerhalb eines IP-Subnets erneut einzelne Bereich herausgelöst werden können!

Soll eine ACL für **alle IP-Adressen** gelten, so schreibt man:

```
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
(255.255.255.255 : Wildcard mask → ignore all)
```

Dieses Statement kann man auch wie folgt angeben:

```
Router(config)# access-list 1 permit any
```

Soll hingegen nur **eine IP-Adresse** betroffen sein, so schreibt man:

Router(config)# access-list 1 permit 172.30.26.29 0.0.0.0

(0.0.0.0 : Wildcard mask → check all bits)

Dieses Statement kann man auch wie folgt angeben:

Router(config)# access-list 1 permit host 172.30.26.29

→ wenn alle Bits überprüft werden sollen

Standard ACLs

IP - Nummernbereich 0 - 99

Diese ACLs werden verwendet, um den gesamten Datenverkehr aus einem Netz oder von einem Protokollstapel zu sperren.

Sie überprüfen nur die Source-Adresse der Datensätze

Router(config)# access-list **access-list-number** { deny | permit } source [source wildcard]
[log]

no access-list **access-list-number**

show access-lists [<number|name>]

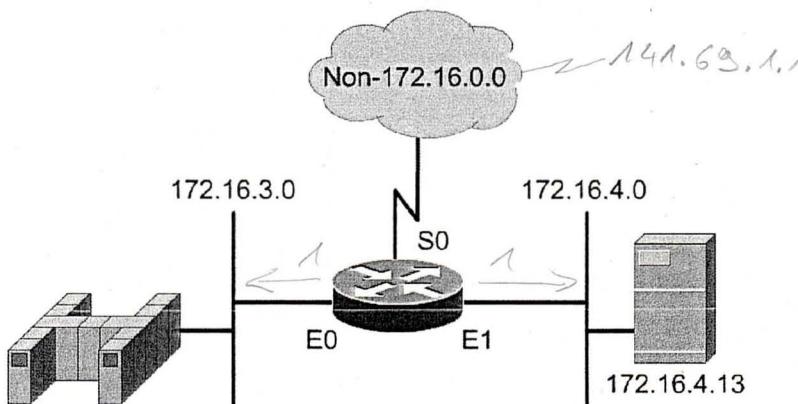
→ Wenn nichts, werden alle, ansonsten entsprechende Nummer

Die wildcard kann weggelassen werden, wenn sie nur aus Nullen besteht.

Router(config-if)# ip access-group **access-list-number** { in | out }

entweder in oder out muß angegeben werden

Standard Access List Example 1



Command Output

```

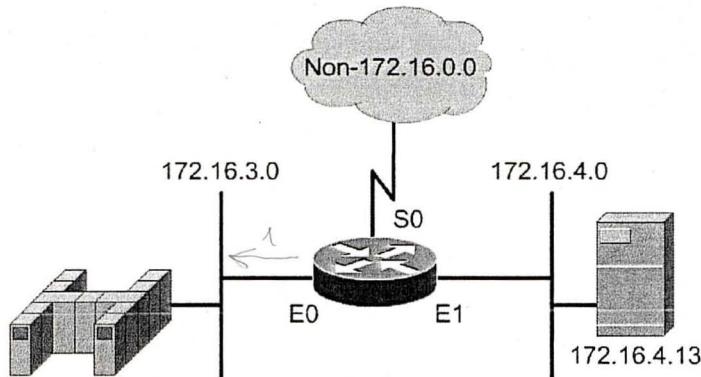
172.16.3.1
  access-list 1 permit 172.16.0.0 0.0.255.255
  (implicit deny any - not visible in the list)
  (access-list 1 deny 0.0.0.0 255.255.255.255) ← deny any
  interface ethernet 0
  ip access-group 1 out
  interface ethernet 1
  ip access-group 1 out

```

Fragen zur ACL:

- 1.) Lässt aus E0 und E1 nur Datenpakete austreten, die folgende Quell adressen aufweisen: 172.16.x.x
- 2.) Werden folgende Datenpakete weitergeleitet?
 - a.) 172.16.4.13 → 172.16.3.1 ✓ wird durchgelassen
 - b.) 172.16.4.13 → 141.69.1.1 ✓ - " -
 - c.) 141.69.1.1 → 172.16.4.1 ✗ nicht weiterleiten,
Quelladresse ist nicht aus dem Bereich 172.16.x.x

Standard Access List Example 2



Command Output

Richterfolg
relevant

```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny any)
(access-list 1 deny 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 1 out
```

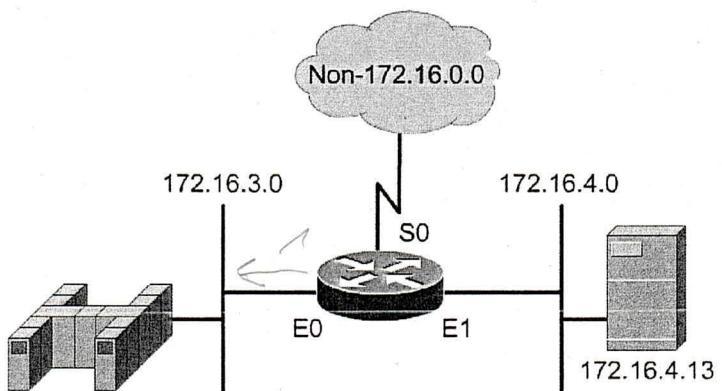
+ = deny host 172.16.4.13
- = permit any

Der Host 172.16.4.13 darf nicht auf 172.16.3.0 zugreifen

Warum an E0 und nicht an E1 binden?

{⇒ Beim Binden an E1 (Richtung in) müßte der gesamte Datenverkehr von 172.16.4.0 geprüft werden.

Standard Access List Example 3



Command Output

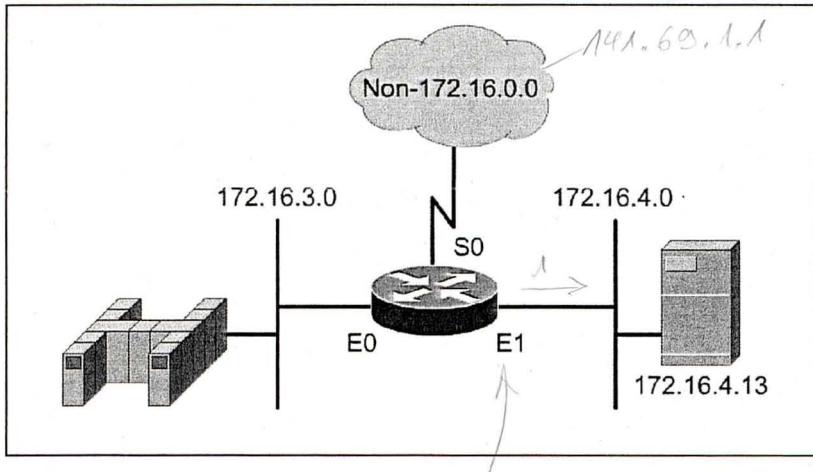
```
access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(implicit deny any)
access-list 1 deny any

interface ethernet 0
ip access-group 1 out
```

Netz 172.16.4.0 darf nicht
auf Netz 172.16.3.0 zugreifen

Aufgabe: Standard- ACL

Realisieren Sie eine Numbered Standard-ACL, die Pakete vom Rechner 141.69.1.1 ins Netz 172.16.4.0 zulässt. Ferner soll der Datenverkehr aus dem Subnetz 172.16.3.0 in das Netz 172.16.4.0 zugelassen werden.



Beschriftung: ethernet 1

Rahmenfolge {accesslist 1 permit host 141.69.1.1
hängt vom accesslist 1 permit 172.16.3.0 0.0.0.255
Datenvorlehr ab
interface ethernet 1
ip access-group 1 out

Extended ACL (IP: 100 - 199)

überprüfen Quell-, Zieladresse und Porte
Eben falls: Protokolle

Inbound ACL-Lists:

Zugelassene Pakete werden weiter bearbeitet (z.B. durch eine outbound ACL)

Outbound ACL

Pakete die zugelassen werden, werden direkt zum Ausgangsinterface gesendet.

```
Router(config)# access-list access-list-number { permit | deny } protocol source
[source-mask destination destination-mask operator operand] [established]
```

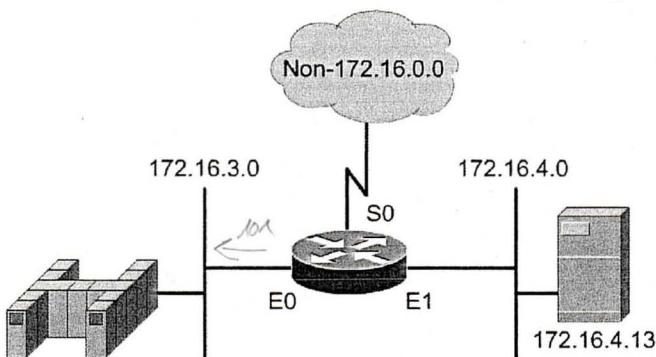
```
Router(config-if)# ip access-group access-list-number { in | out }
```

gleich

access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
 interface ethernet 0 ↗
 ↗ source ↗ destination ↗ Port
 ip access-group 101 out

Zum Bearbeiten einer extended ACL muss zunächst die gesamte ACL gelöscht werden.

Extended Access List Example 1



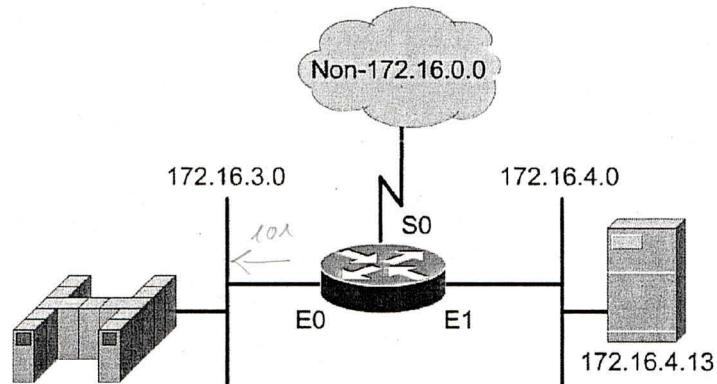
Command Output

```
access-list 101 deny tcp 172.16.4.0
  0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 permit ip 172.16.4.0
  0.0.0.255 0.0.0.255.255.255.255
(implicit deny any)
(access-list 101 deny ip 0.0.0.0
  255.255.255.255 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 101 out
```

Von Netz 172.16.4.0 kein
 FTP ins Netz 172.16.3.0
 alle anderen Dienste zulasse

Extended Access List Example 2



Command Output

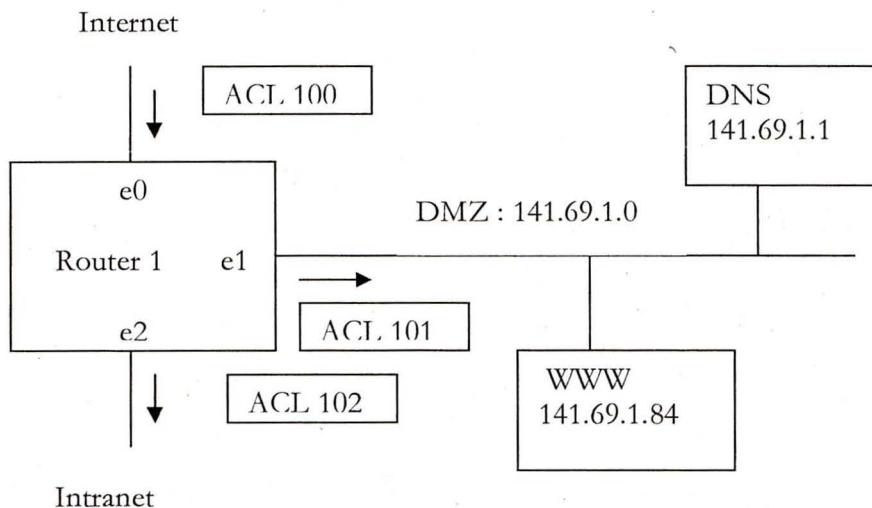
```
access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
access-list 101 permit ip any any
(implicit deny any)
(access-list 101 deny ip 0.0.0.0 255.255.255.255
0.0.0.0 255.255.255.255) telnet
interface ethernet 0
ip access-group 101 out
```

Sperrt Zugriffe
auf Telnet-Server
im Netz 172.16.3.0
aus dem Netz
172.16.4.0

Aufgabe Extended ACL

Gegeben sind die folgende Topologie eines Netzes und die auf dem Router R1 implementierten ACLs für seine Interfaces s0, e0 und e1.

a.) Erläutern Sie die Aufgaben der einzelnen Regeln.



ACL 100 (e0, in)

deny ip 141.69.0.0 0.0.255.255 any log
 permit ip any any

Quelle C match wird geladen
 ↳ Intranet-Addressbereich

Anti-Spoofing

ACL 101 (e1, out)

(DMZ)

permit udp any host 141.69.1.1 eq domain
 permit tcp any host 141.69.1.84 eq 80
 deny ip any any

→ DNS - Port (53)
 → permit top 141.69.0.0 0.0.255.255 host 141.69.1.1 eq 22
 → host 141.69.1.84 eq 22

ACL 102 (e2, out)

permit tcp any 141.69.0.0 0.0.255.255 gt 1023
 permit udp any any gt 1023
 deny ip any any

größer
 ↳ Ziel
 ↳ Antwortpakete von Servern
 ↳ Port 22

b.) Erweitern Sie die geeignete ACL so, dass SSH aus dem Intranet für den WEB-Server und den DNS-Server erlaubt wird.

↳ Port 22

Erlaubte Operatoren für die Festlegung von Ports: lt, gt, eq, neq (less than, greater than, equal, not equal)

Named ACLs

Named ACLs ermöglichen, dass standard oder extended ACLs durch eine Zeichenkette identifiziert werden. Bei diesen ACLs können einzelne Zeilen einer bestimmten ACL gelöscht werden. Die Reihenfolge der ACL-Anweisungen kann jedoch auch bei diesen ACLs nicht geändert werden. Zusätzliche ACL-Regeln können an das Ende der ACL angehängt werden.

Router(config)#ip access-list { standard|extended } name
Router(config-nacl)# { permit|deny }.....

Name der ACL

```
Rt1(config)#ip access-list extended server-access
Rt1(config-ext-nacl)#permit TCP any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit UDP any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#^Z
Applying the named list:
Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

Eigenschaften von named ACLs

- Name kann Aufgabe beschreiben
- Einfache zu editieren
- Mehr ACLs möglich als bei numbered ACLs

Syntax zum Anlegen von named ACLs

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended test
Router(config-ext-nacl)#deny udp any 171.69.0.0 0.0.255.255 lt 1023
Router(config-ext-nacl)#^Z
%SYS-5-CONFIG_I: Configured from console by console
```

Editieren von named ACLs

```
R1# show access-lists
Standard IP access list WEB SERVER
    10 permit 192.168.10.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip access-list standard WEB SERVER
R1(config-std-nacl)# 15 permit host 192.168.11.10
R1(config-std-nacl)# end
R1#
*Nov 1 19:20:57.591: %SYS-5-CONFIG_I: Configured from console by console
R1# sho access-lists
Standard IP access list WEB SERVER
    10 permit 192.168.10.10
    15 permit 192.168.11.10
    20 deny   192.168.10.0, wildcard bits 0.0.0.255
    30 deny   192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Überprüfung von ACLs

Welche ACLs sind an interfaces gebunden?

```
Router#show ip interface
```

Welche Regeln enthalten die ACLs?

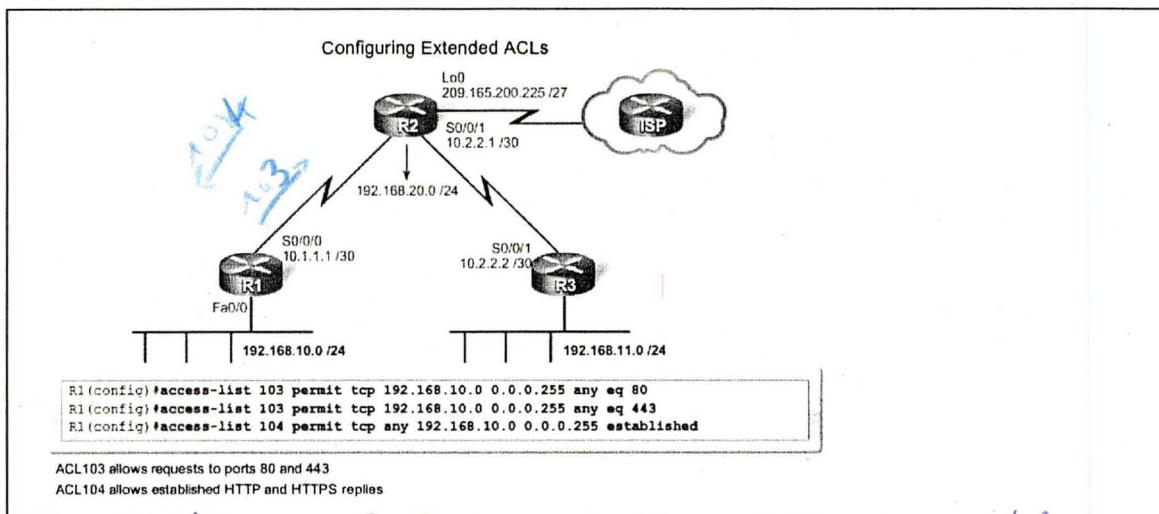
```
Router#show access-lists  
Extended IP access list test  
    deny udp any 171.69.0.0 0.0.255.255 lt 1023  
Router#
```

Brücke, ob ACL geht

```
R1# show access-lists {access-list-number|name}
```

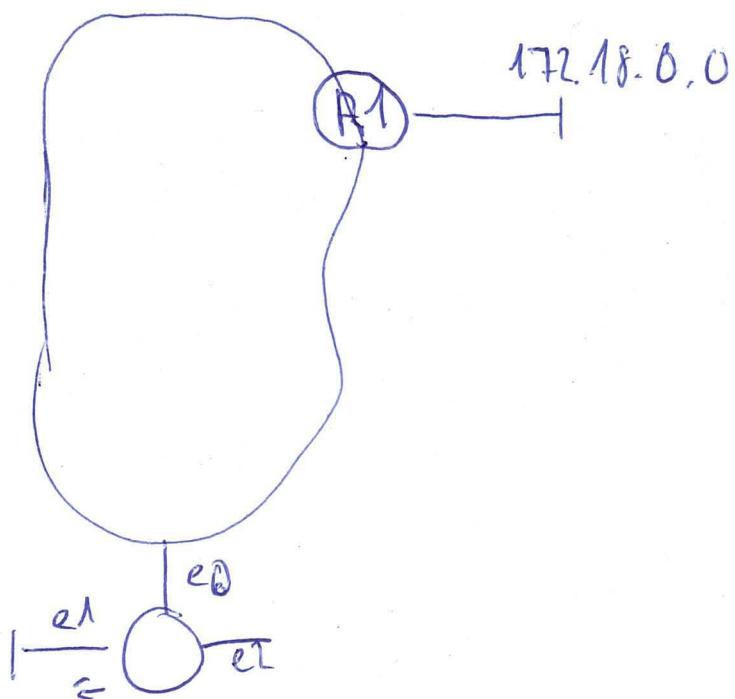
```
R1# show access-lists  
Standard IP access list SALES  
    10 deny   10.1.1.0 0.0.0.255  
    20 permit 10.3.3.1  
    30 permit 10.4.4.1  
    40 permit 10.5.5.1  
Extended IP access list ENG  
    10 permit tcp host 192.168.10.2 any eq telnet (25 matches)  
    20 permit tcp host 192.168.10.2 any eq ftp  
    30 permit tcp host 192.168.10.2 any eq ftp-data
```

ACLs with keyword established



104 Den vom Netz 192.168.10.0/24 mit Webrowsing möglich sein.
Pakete aus dem Internet müssen All-Flag gesetzt haben oder RST-Flag.
ACK, RST-Flag gesetzt- bedeutet nicht zu bestehender Verbindung

Optimale Platzierung von ACLs



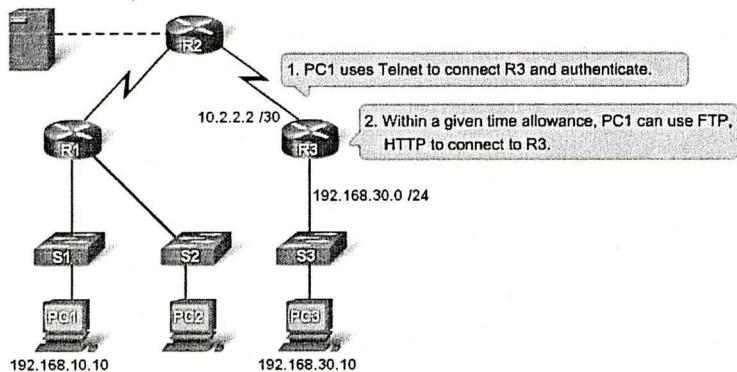
- Standard-ACL: prüft nur Quell-IP
Kein Zugriff auf den Netz
172.18.0.0. auf e1 nicht leg
(möglichst nah am Ziel)
- Extended ACLs: Möglichst nah an der Quellnetz
(prüft Quelle und Ziel)

Complex ACLs

Complex ACL	Description
Dynamic ACLs (lock-and-key)	Users that want to traverse the router are blocked until they use Telnet to connect to the router and are authenticated
Reflexive ACLs	Allows outbound traffic and limits inbound traffic in response to sessions that originate inside the router
Time-based ACLs	Allows for access control based on the time of day and week

Dynamic ACLs

Port - Knob - Daemon



Step 1	R3(config)#username Student password 0 cisco
Step 2	R3(config)# access-list 101 permit tcp any host 10.2.2.2 eq telnet R3(config)#access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Step 3	R3(config)#interface serial 0/0/1 R3(config-if)#ip access-group 101 in
Step 4	R3(config)#line vty 0 4 R3(config-line)#login local R3(config-line) # autocommand access-enable host timeout 5

User auf dem Rechner 192.168.10.10 muss sich zunächst über Telnet auf Router 3 anmelden. Dann wird der Datenverkehr aus dem Netz 192.168.10.0 in das Netz 192.168.30.0 freigegeben.

Reflexive ACLs

nur möglich für extended named IPACLs
Was versteht man unter Reflexive ACLs?

Verbindungen vom Intranet ins Internet werden für bestimmte Dienste zugelassen

Dafür werden ACLs definiert (Datenverkehr ins Internet)
In dieser ACL wird angegeben, dass die Antwortpakete untersucht werden sollen (z.B. reflect TCP Traffic)

In der ACL für die Antwortpakete wird mit evaluate TCP TRAFFIC auf die outgoing ACL Bezug genommen.

Vorteile von "Reflexive ACLs"

Schwieriger für Angriffe zu überwachen (z.B. Rückspiegel) nur von dem Benutzer, zu dem ein Client des Datennets eine Verbindung aufgebaut hat.

<pre>Step 1 R2(config)#ip access-list extended OUTBOUNDFILTERS R2(config-ext-nacl)# permit tcp 192.168.0.0 0.0.255.255 any reflect TCPTRAFFIC R2(config-ext-nacl)# permit icmp 192.168.0.0 0.0.255.255 any reflect ICMPTRAFFIC</pre>	<pre>Step 2 R2(config)#ip access-list extended INBOUNDFILTERS R2(config-ext-nacl)# evaluate TCPTRAFFIC R2(config-ext-nacl)# evaluate ICMPTRAFFIC</pre>
<pre>Step 3 R2(config)#interface S0/1/0 R2(config-if)#ip access-group INBOUNDFILTERS in R2(config-if)#ip access-group OUTBOUNDFILTERS out</pre>	

Time-based ACLs

Step 1

```
R1(config)#time-range EVERYOTHERDAY  
R1(config-time-range)#periodic Monday Wednesday Friday 8:00 to  
17:00
```

Step 2

```
R1(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255  
any eq telnet time-range EVERYOTHERDAY
```

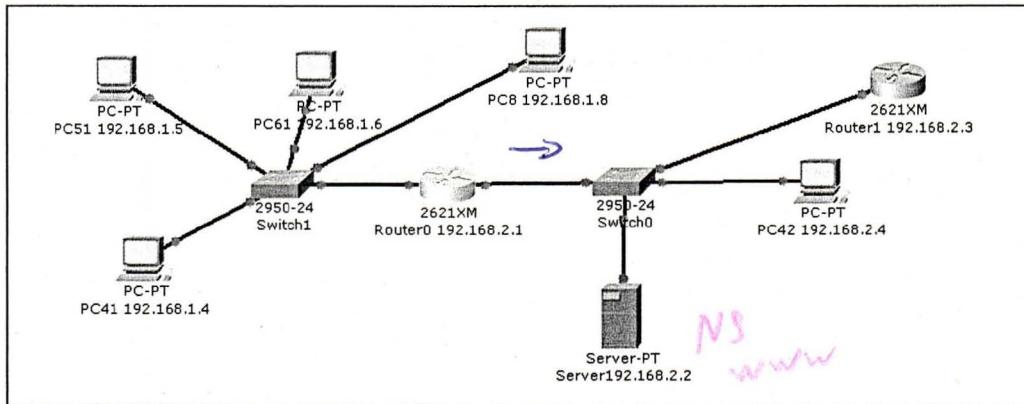
Step 3

```
R1(config)#interface s0/0/0  
R1(config-if)#ip access-group 101 out
```

Aufgaben ACL

Aufgabe 1

Gegeben ist die folgende Topologie. Diese Konfiguration ist als acl1.pkt im Downloadbereich unter www.usadel.de abgelegt.



1.) Realisieren Sie eine extended acl auf Router0 so, dass ausschließlich folgende Zugriffe möglich sind:

Alle Rechner aus dem Netz 192.168.1.0/24 haben Zugriff auf den Nameserver (192.168.2.2).

Rechner mit den Adressen 192.168.1.4 bis 192.168.1.7 haben Zugriff auf den Webserver (192.168.2.2:80). Realisieren Sie diese Vorgabe mit einer ACL-Regel!

PC41 hat Zugriff auf Router1 über Telnet.

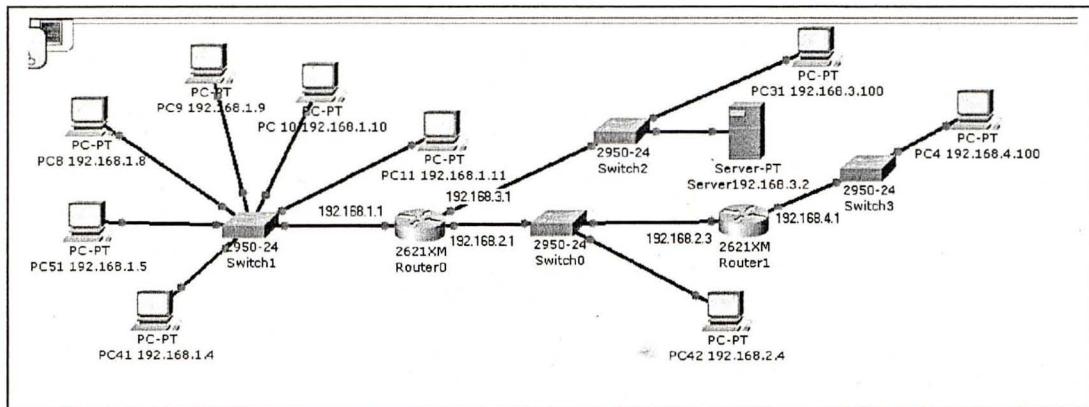
2.) Platzieren Sie im linken Teilnetz einen Web-Server mit der IP- Adresse 192.168.1.100!

a.) Erweitern Sie die ACL aus 1.) soweit, dass ein Ping zwischen den PCs funktioniert.

b.) Erweitern Sie die ACL aus 1.) in der Weise, dass PC42 auf den Webserver im linken Teilnetz zugreifen kann

Aufgabe 2

Gegeben ist die folgende Topologie.

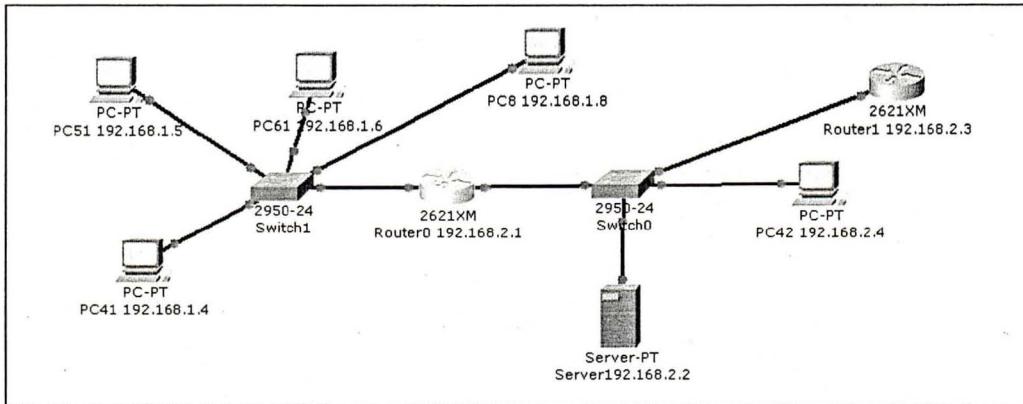


1.) Realisieren Sie extended acls auf den Routern so, dass folgende Zugriffe möglich sind:

- Aus dem Netz 192.168.1.0 darf auf den Server 192.168.3.2 zugegriffen werden und zwar auf folgende Ports: (WWW Port 80 und DNS Port 53). Anderer Datenverkehr soll zunächst blockiert werden. Erstellen Sie hierfür die ACL 100. Gebunden auf Interface 192.168.3.1 von Router0 in Richtung out.
- Ping soll nur vom Rechner 192.168.1.4 auf die Rechner 192.168.1.8 bis 192.168.1.11 möglich sein. Diese Rechner sind durch eine geeignete Wildcard in einer Regel zusammenzufassen. Anderer IP- Datenverkehr soll uneingeschränkt möglich sein. Erstellen Sie dazu die ACL 101. Diese wird auf Interface 192.168.1.1 von Router0 in Richtung out gebunden.
- Erweitern Sie ACL 100 so, dass zusätzlich zum Datenverkehr aus a.) ausschließlich PC31 (192.168.3.100) aus dem Netz 192.168.3.0 auf Router1 über Telnet zuzugreifen kann. Geben Sie an, an welcher Stelle der ACL100 diese Modifikationen vorgenommen werden müssen.

Aufgabe 3 (Reflexive ACL)

Gegeben ist die folgende Topologie.



- 1.) Realisieren Sie eine named extended acl auf Router0 so, dass ausschließlich folgende Zugriffe möglich sind:

Alle Rechner aus dem Netz 192.168.1.0/24 haben Zugriff auf den Nameserver (192.168.2.2).

Rechner mit den Adressen 192.168.1.4 bis 192.168.1.7 haben Zugriff auf den Webserver (192.168.2.2:80). Realisieren Sie diese Vorgabe mit einer ACL-Regel!

Verwenden Sie Reflexive ACLs.

Lösung : Aufgaben ACC S-139 -

Router#sho runn
Building configuration...

Current configuration : 711 bytes
!
version 12.2
no service password-encryption
!
hostname Router
!
!
!
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip access-group 101 out
duplex auto
speed auto
!
ip classless
!
access-list 101 permit udp 192.168.1.0 0.0.0.255 host 192.168.2.2 eq domain
access-list 101 permit tcp 192.168.1.4 0.0.0.3 host 192.168.2.2 eq www
access-list 101 permit tcp host 192.168.1.4 host 192.168.2.3 eq telnet
access-list 101 permit icmp any any echo
access-list 101 permit icmp any any echo-reply
access-list 101 permit tcp host 192.168.1.100 eq www any gt 1023
!
!
!
line con 0
line vty 0 4
login
!
!

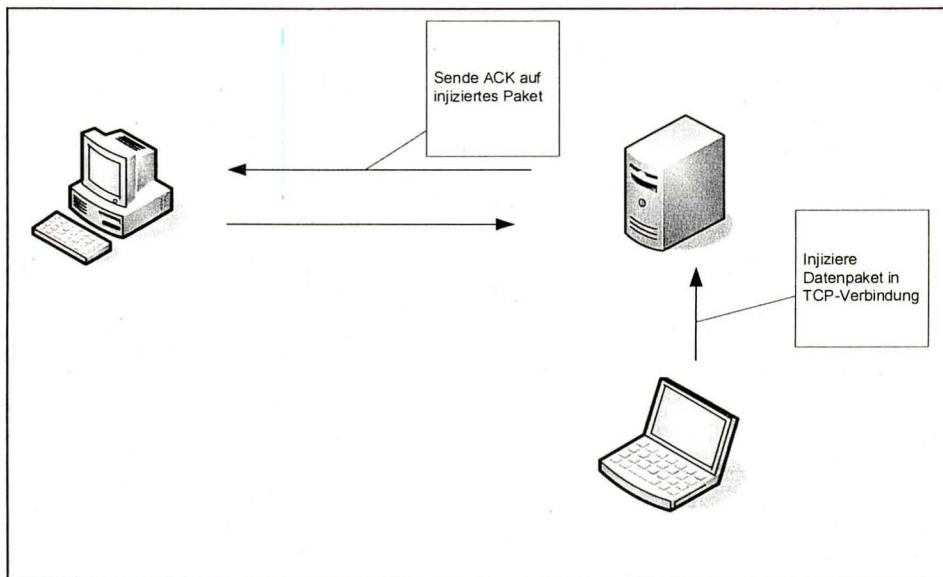
host 192.168.2.4

Aufgabe 1

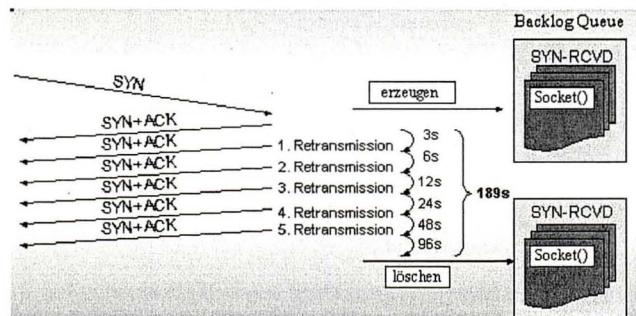
a.) Was versteht man unter den folgenden Begriffen?

- Penetrations-Test
- Enumeration
- OS-Fingerprinting
- Remote Forensic Software
- Keylogger

b.) Beschreiben Sie, wie ein TCP ACK- Storm zustande kommt. Verwenden Sie dazu die Begriffe der folgenden Skizze!



c.) Beschreiben Sie wie ein SYN-Flood Angriff arbeitet. Verwenden Sie dazu die Begriffe der folgenden Skizze.



d.) Welche Maßnahmen gibt es gegen die SYN-Flood Angriffe?

e.) Was ist ein Botnet?

f.) Beschreiben Sie, wie ein Angriff mit "Overlapping IP-Fragments" arbeitet!

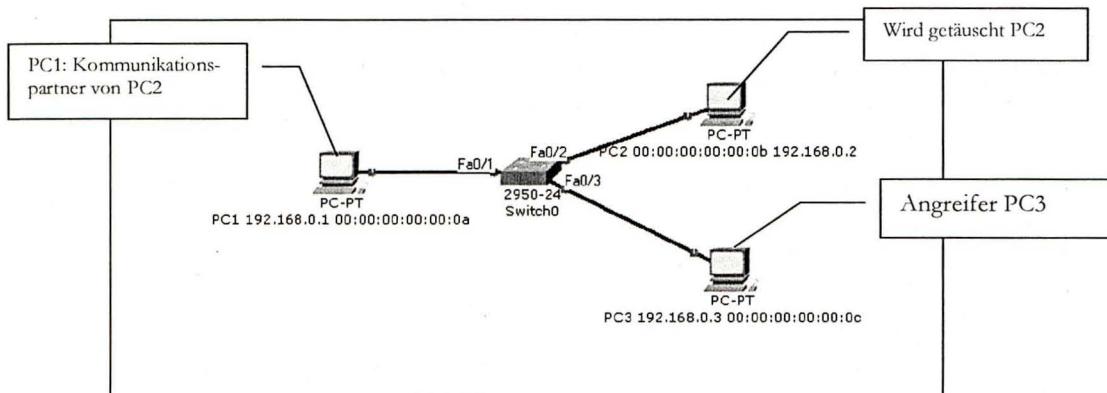
g.) Was versteht man unter dem Begriff IP Spoofing?

h.) Beschreiben Sie einen Oscillation-Data Flood Angriff.

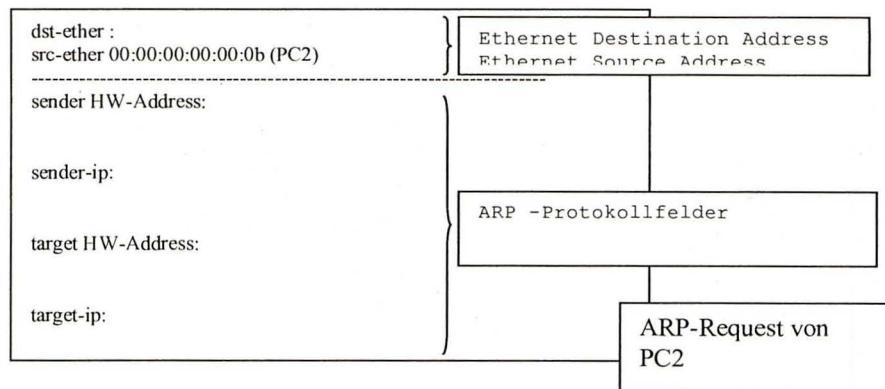
i.) Wozu wird ein TCP-Wrapper eingesetzt?

- j.) Wie arbeitet ein Smurfing-Angriff?
 k.) Erläutern Sie die Arbeitsweise von Tripwire.

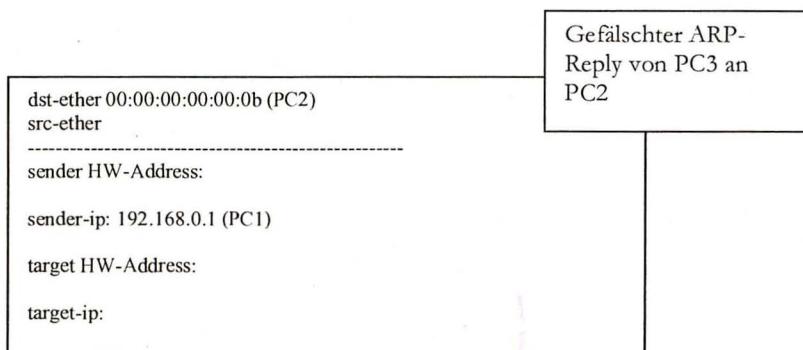
Aufgabe 2



- a.) PC2 sendet einen ARP-Request. PC2 will von PC1 die MAC-Adresse erhalten. Ergänzen Sie die Protokollfelder dieses ARP-Request in dem folgenden Datenrahmen.

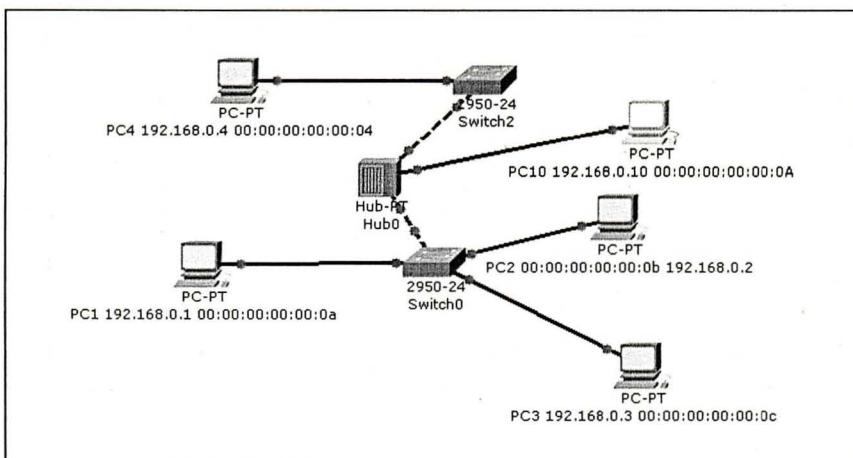


- b.) PC3 will erreichen, dass er die Datenpakete, die PC2 an PC1 sendet, abhören kann. Dazu sendet PC3 einen gefälschten ARP-Reply auf den ARP-Request von PC2. Ergänzen Sie die ARP-Reply-Datenfelder so, dass PC3 sein Ziel (das Abhören) erreichen kann. Erläutern Sie, wie PC3 sein Ziel erreicht.



c.) Was muss PC3 tun, damit PC2 und PC1 nicht merken, dass ihre Kommunikation abgehört wird.

d.) Der Hub in der folgenden Skizze befindet sich in der Tagging-Leitung zwischen Switch2 und Switch0. Alle PCs befinden sich im selben VLAN. Die Netzwerkkarte von PC10 unterstützt das IEEE802.1q-Protokoll.



Füllen Sie die folgende Tabelle aus. "PC1 an PC3" ist in der Tabelle 2-mal aufgeführt. Hier ist eine Fallunterscheidung aufgrund der Zustände nötig, in denen sich die Switches befinden.

Datenverkehr	PC10 kann mit-hören ja/nein	Begründung
PC4 an PC1		
PC1 an PC3 Fall a		
PC1 an PC3 Fall b		
ARP-Request von PC1		

e.) Mit welchem anderen Verfahren (kein arp-Spoofing) könnte PC3 den Datenverkehr von PC2 an PC1 abhören?

- a.) Welche Probleme kann es bei SNMP bezüglich der Community Strings geben?
- b.) Welcher Nachteil ergibt sich bei der Verwendung von aktive FTP für Firewalls?
- c.) Wie arbeiten stateful Firewalls?
- d.) Was versteht man unter einer rekursiven Anfrgae bei einem DNS -Server?
- e.) Was versteht man unter einem "open resolver"?
- f.) Warum sollten TCP-Sequenznummern nicht leicht zu erraten sein?
- g.) Was ist ein IDS?
- h.) Was versteht man unter HIDS bzw. NIDS? Welche Informationen werten sie aus?
- i.) Was versteht man unter Proxy-Arp bei einem Router?
- j.) Wozu wird bei Cisco ACLs eine Wildcard-Mask verwendet?
- k.) Wie kennzeichnet ein NAPT-Router beim ins Internet weitergeleiteten Datenpaketen von welchem Rechner im Intranet die betreffende Datenpakte stammen?
- l.) Wozu werden TCP-Wrapper eingesetzt? In welchen Dateien werden beim tcpd die berchtigten IP-Adressen konfiguriert?
- m.) Was versteht man unter der Source Route Option bei IP? Warum werden Pakete, die diese Option verwenden, in der Regel von Firewalls blockiert?
- n.) Was erleichtert bei Nameservern das Vergiften des Namecache?
- o.) Woran kann man bei einem Antwortpaket eines Nameservers erkennen, dass die darin enthaltenen Informationen aus dem Namecache entnommen wurden?
- p.) Was ist der Grundgedanke eines Angriffs, welcher tiny fragments verwendet?
- q.) Wodurch ergibt sich die "Amplification" bei einer DNS DDoS Amplification Attack? Welche Eigenschaft weisen die bei dieser Attacke missbrauchten DNS-Server auf?