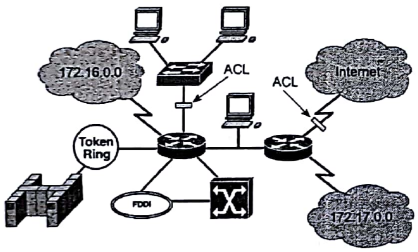
Name: Klasse: Datum:

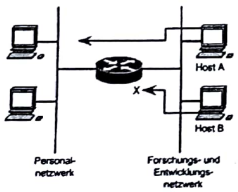
Zugangssteuerungslisten (Access Control Lists, ACLs, Filter)

ACLs sind Anweisungslisten, die auf eine Router-Schnittstelle angewendet werden. Mit diesen Listen wird dem Router mitgeteilt, welche Datenpakete zugelassen und welche abgewiesen werden sollen. Das Zulassen bzw. Abweisen kann auf bestimmten Spezifikationen basieren, etwa der Absenderadresse, der Zieladresse oder der Port-Nummer. Wenn Sie ACLs auf eine Router-Schnittstelle anwenden, können Sie den Verkehr verwalten und bestimmte Datenpakete verfolgen. Der gesamte Datenverkehr, der eine Schnittstelle durchläuft, wird im Hinblick auf bestimmte Bedingungen überprüft, die Teil der ACL sind.



ACLs können für alle gerouteten Netzprotokolle erstellt werden, beispielsweise Internet Protocol (IP) und Internetwork Packet Exchange (IPX). Damit werden Datenpakete beim Durchlaufen des Routers ausgefiltert.

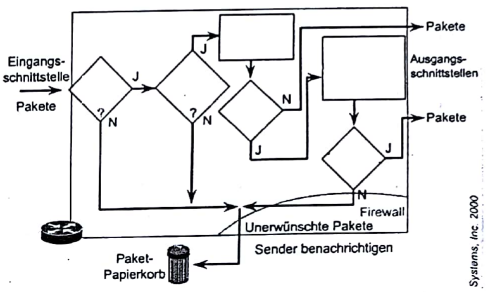
Reduzieren des Netzverkehrs



Heinz-Nixdorf-Berufskolleg
für Elektrotechnik, Informations- und Telekommunikationstechnik der Stadt Essen

Name: Klasse: Datum:

Das Prinzip von ACLs



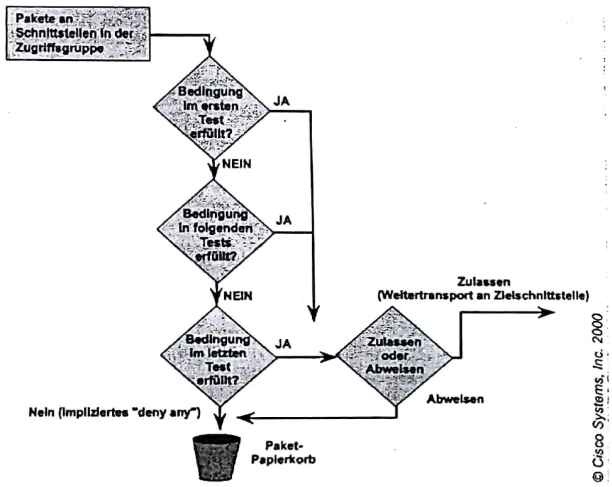
Der Beginn des Kommunikationsprozesses ist immer gleich, unabhängig davon, ob ACLs verwendet werden oder nicht. Wenn ein Paket an einer Schnittstelle ankommt, überprüft der Router, ob das Paket geroutet oder gebridget werden soll. Anschließend überprüft der Router, ob für die Eingangsschnittstelle eine ACL definiert wurde. Ist eine ACL vorhanden, so wird das Paket im Hinblick auf die in der Liste festgelegten Bedingungen überprüft. Wenn das Paket zugelassen wird, wird es mit den Einträgen in der Routing-Tabelle verglichen. Auf diese Weise wird die Zielschnittstelle ermittelt.

Anschließend überprüft der Router, ob für die Zielschnittstelle eine ACL definiert wurde. Ist dies nicht der Fall, kann das Paket direkt an die Zielschnittstelle gesendet werden.
Liegt an der Ausgangsschnittstelle eine ACL vor, muß diese abgearbeitet werden.
ACL-Anweisungen unterliegen einer aufeinander folgenden, logischen Reihenfolge. Wird eine Bedingung erfüllt, so wird das Paket zugelassen oder abgewiesen, und die restlichen ACL-Anweisungen werden nicht mehr überprüft. Wenn keine der ACL-Anweisungen erfüllt wird, wird als letzte Anweisung ein implizites "deny any" ausgeführt. Sie können dieses "deny any" in der letzten Zeile der ACL zwar nicht sehen, die ACL arbeitet aber so als ob dieses „deny any" eingetragen wäre.

1. Erstellen sie einen PAP, ähnlich der Vorgabe aber detailgetreuer!

Name: Klasse: Datum:

Das Prinzip von ACLs



Name: Klasse: Datum:

Das folgende Beispiel veranschaulicht, wie eine ACL aufgebaut sein muss, damit der Datenverkehr einer bestimmten Adresse, 172.16.4.13, abgewiesen und gleichzeitig der gesamte andere Datenverkehr auf Schnittstelle Ethernet 0 weitergeleitet wird. Der erste Befehl access-list verwendet den "deny"-Parameter, um den Datenverkehr des angegebenen Hosts abzuweisen. Die Adressmaske 0.0.0.0 in dieser Zeile gibt an, dass alle Bits die Testbedingungen erfüllen müssen.

Im zweiten Befehl access-list wird mit der Kombination aus IP-Adresse und Wildcard-Maske 172.16.4.0 0.0.0.255 der Verkehr von jeder beliebigen Quelle des Netzes abgedeckt. Diese Kombination kann auch durch den Begriff any wiedergegeben werden. Ausschließlich Nullen in der Adresse stehen für einen Platzhalter, während ausschließlich Einsen in der Wildcard-Maske angeben, dass die 32 Bits der Absenderadresse nicht geprüft werden. Alle Pakete, die die erste Zeile der ACL nicht erfüllen, erfüllen die zweite Zeile und werden weitergeleitet.

Abweisen eines bestimmten Hosts:

Gluecksburg (config) # access-list 1 deny 172.16.4.13 0.0.0.0
Gluecksburg (config) # access-list 1 permit 172.16.4.0 0.0.0.255

("deny any" implizit)
(access-list 1 deny 0.0.0.0 255.255.255.255)

Gluecksburg (config) # interface ethernet 1/0
Gluecksburg (config-if) # ip access-group 1 out