Konfigurieren häufig verwendeter IP-ACLs

Inhalt

Einleitung

In diesem Dokument werden Beispielkonfigurationen für häufig verwendete IP-Zugriffskontrolllisten (ACLs) beschrieben, die IP-Pakete filtern.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgende Anforderung erfüllen, bevor Sie diese Konfiguration ausprobieren:

- Grundlegendes Verständnis der IP-Adressierung

Weitere Informationen finden Sie unter IP Addressing and Subnetting for New Users.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

IP-Zugriffskontrolllisten filtern Pakete basierend auf:

- Quelladresse
- Zieladresse
- Pakettyp
- Eine beliebige Kombination dieser Elemente

Um den Netzwerkverkehr zu filtern, steuern ACLs, ob geroutete Pakete an der Router-Schnittstelle weitergeleitet oder blockiert werden. Ihr Router untersucht jedes Paket, um anhand der Kriterien, die Sie innerhalb der ACL angeben, zu bestimmen, ob das Paket weitergeleitet oder verworfen werden soll. Zu den ACL-Kriterien gehören:

- Quelladresse des Datenverkehrs
- Zieladresse des Datenverkehrs
- Protokoll der oberen Schicht

Gehen Sie folgendermaßen vor, um eine ACL zu erstellen, wie die Beispiele in diesem Dokument zeigen:

1. Erstellen Sie eine ACL.
2. Wenden Sie die ACL auf eine Schnittstelle an.

Die IP-ACL ist eine sequenzielle Sammlung von Zulassungs- und Verweigerungsbedingungen, die für ein IP-Paket gelten. Der Router testet die Pakete einzeln anhand der Bedingungen in der ACL.

Die erste Übereinstimmung bestimmt, ob die Cisco IOS®-Software das Paket akzeptiert oder ablehnt. Da die Cisco IOS-Software den Zustandstest nach der ersten Übereinstimmung beendet, ist die Reihenfolge der Bedingungen entscheidend. Wenn keine Bedingungen zutreffen, lehnt der Router das Paket aufgrund einer impliziten „deny all“-Klausel (Alle ablehnen) ab.

In der Cisco IOS-Software können beispielsweise folgende IP-ACLs konfiguriert werden:

- Standardzugriffskontrolllisten
- Erweiterte Zugriffskontrolllisten
- Dynamische ACLs (Lock and Key)
- IP-benannte ACLs
- Reflexive Zugriffskontrolllisten
- Zeitbasierte ACLs, die Zeitbereiche verwenden
- Kommentierte Einträge in IP-Zugriffskontrolllisten
- Kontextbasierte ACLs
- Authentifizierungs-Proxy
- Turbozugriffskontrolllisten
- Verteilte zeitbasierte Zugriffskontrolllisten

Dieses Dokument behandelt einige häufig verwendete Standard- und erweiterte ACLs. Unter Configuring IP Access Lists finden Sie weitere Informationen zu den verschiedenen Arten von ACLs, die von der Cisco IOS-Software unterstützt werden, sowie zum Konfigurieren und Bearbeiten von ACLs.

Das Befehlssyntaxformat einer Standard-ACL lautet **access-list access-list-number {permit|deny} {host|source-wildcard|any}**.

Standard-ACLs steuern den Datenverkehr durch Abgleich der Quelladresse von IP-Paketen mit den in der ACL konfigurierten Adressen.

Erweiterte ACLs steuern den Datenverkehr durch Abgleich der Quelladresse und der Zieladresse von IP-Paketen mit den in der ACL konfigurierten Adressen. Sie können erweiterte ACLs auch granularer gestalten und so konfigurieren, dass der Datenverkehr nach folgenden Kriterien gefiltert wird:

- Protokolle
- Port-Nummern
- Wert des Differentiated Services Code Point (DSCP)
- Präzedenz-Wert
- Status des SYN-Bit (Synchronize Sequence Number)

Die Befehlssyntaxformate der erweiterten ACLs sind

IP

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} protocol source source-wildcard destination destination-wildcard
 [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

Internet Control Message Protocol (ICMP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} icmp source source-wildcard destination destination-wildcard
[[icmp-type] [icmp-code] | [icmp-message]] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

Transmission Control Protocol (TCP)

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[established] [precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

User Datagram Protocol (UDP)

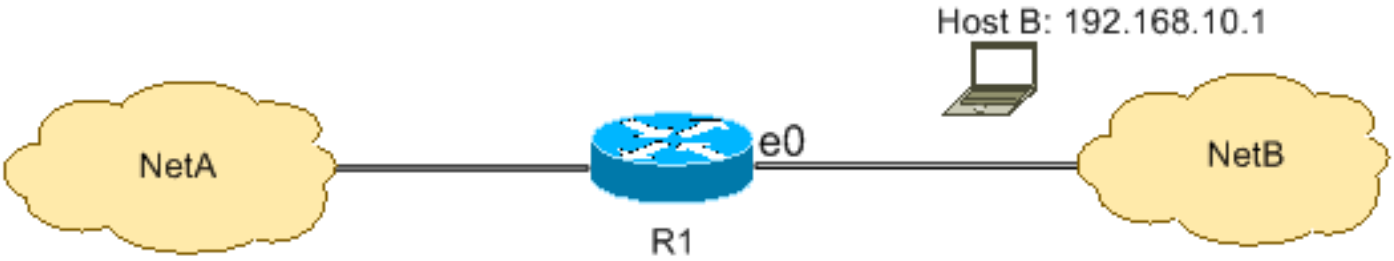
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name][fragments]
```

Konfigurieren

Diese Konfigurationsbeispiele verwenden die gängigsten IP-ACLs.

Einem ausgewählten Host den Zugriff auf das Netzwerk erlauben

Diese Abbildung zeigt, dass einem ausgewählten Host die Berechtigung für den Zugriff auf das Netzwerk erteilt wird. Der gesamte Datenverkehr von Host B an NetA ist zulässig, und sämtlicher anderer Datenverkehr von NetB an NetA wird abgelehnt.



Die Ausgabe in Tabelle R1 zeigt, wie das Netzwerk dem Host Zugriff gewährt. Diese Ausgabe zeigt Folgendes:

- Die Konfiguration lässt nur den Host mit der IP-Adresse 192.168.10.1 über die Ethernet 0-Schnittstelle auf R1 zu.
- Dieser Host hat Zugriff auf die IP-Services von NetA.
- Kein anderer Host in NetB hat Zugriff auf NetA.
- In der ACL ist keine Deny-Anweisung konfiguriert.

Standardmäßig befindet sich am Ende jeder ACL eine implizite „deny all“-Klausel. Alles, was nicht ausdrücklich erlaubt ist, wird verweigert.

R1

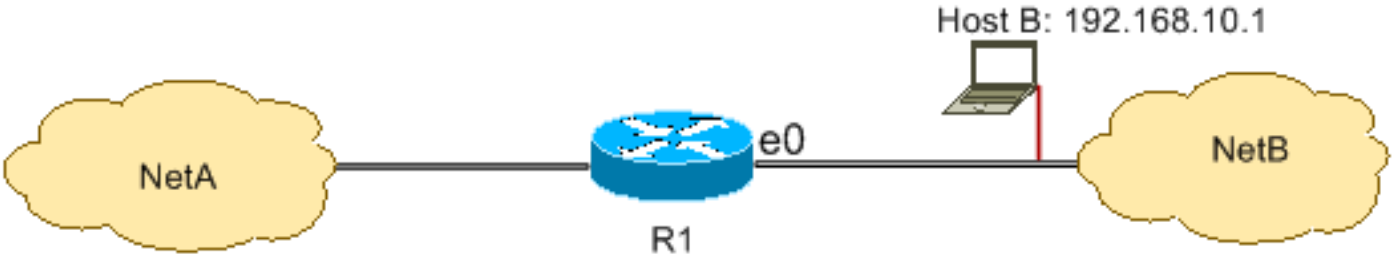
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Hinweis**: Die ACL filtert IP-Pakete von NetB nach NetA, mit Ausnahme von Paketen, die von Host B stammen. Pakete, die von Host B nach NetA stammen, sind weiterhin zulässig.

> **Anmerkung:** Die ACL **access-list 1 permit 192.168.10.1 0.0.0.0 ist eine weitere Möglichkeit, dieselbe Regel zu konfigurieren.**

Einem ausgewählten Host den Zugriff auf das Netzwerk verweigern

Diese Abbildung zeigt, dass Datenverkehr von Host B an NetA abgelehnt wird, während der gesamte andere Datenverkehr von NetB zum Zugriff auf NetA erlaubt ist.



Diese Konfiguration lehnt alle Pakete vom Host 192.168.10.1/32 über Ethernet 0 auf R1 ab und erlaubt alles andere. Sie müssen den Befehl **access list 1 permit any verwenden, um alles andere explizit zuzulassen, da jede ACL eine implizite „deny all“-Klausel enthält.**

R1

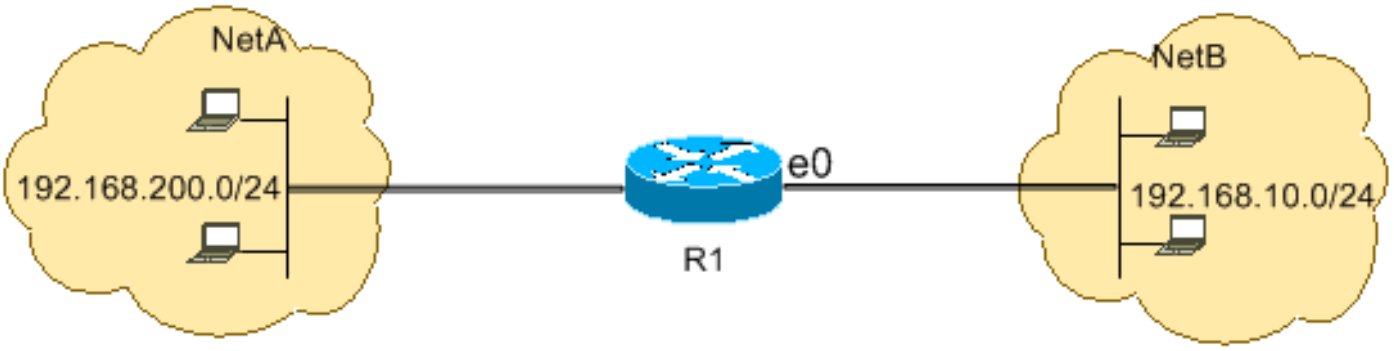
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Anmerkung:** Die Reihenfolge der Anweisungen ist entscheidend für das Funktionieren einer ACL. Wenn die Reihenfolge der Einträge umgekehrt ist, wie dieser Befehl zeigt, stimmt die erste Zeile mit jeder Paket-Quelladresse überein. Daher blockiert die ACL den Zugriff von Host 192.168.10.1/32 auf NetA nicht.

```
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

Zugriff auf einen Bereich zusammenhängender IP-Adressen zulassen

Diese Abbildung zeigt, dass alle Hosts in NetB mit der Netzwerkadresse 192.168.10.0/24 auf das Netzwerk 192.168.200.0/24 in NetA zugreifen können.



Diese Konfiguration ermöglicht den IP-Paketen mit einem IP-Header, dessen Quelladresse sich im Netzwerk 192.168.10.0/24 und dessen Zieladresse sich im Netzwerk 192.168.200.0/24 befindet, Zugriff auf NetA. Am Ende der ACL befindet sich die implizite „deny all“-Klausel, die jeglichen anderen Datenverkehr über eingehendes Ethernet 0 auf R1 verbietet.

R1

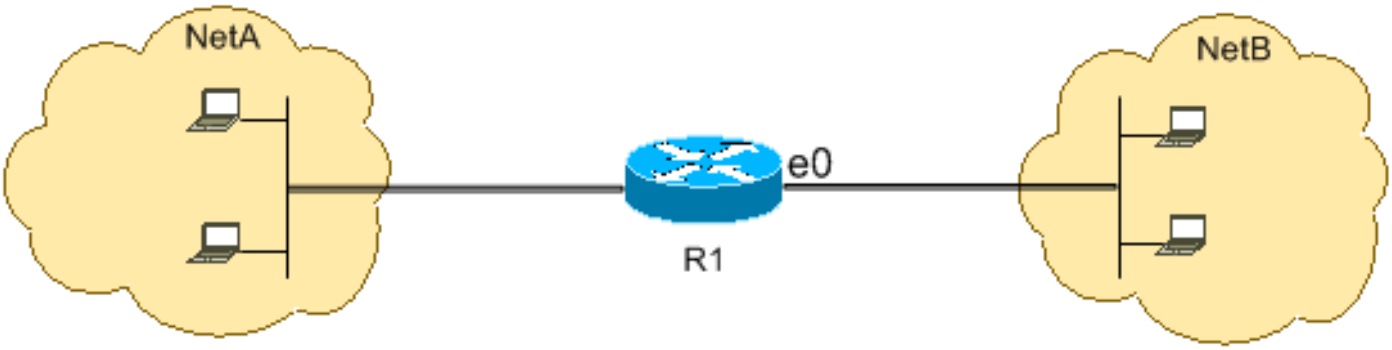
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

> **Anmerkung:** Im Befehl **access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255** ist "0.0.0.255" die invertierte Maske des Netzwerks 192.168.10.0 mit Maske 255.255.255.0. ACLs verwenden die invertierte Maske, um zu ermitteln, wie viele Bits in der Netzwerkadresse übereinstimmen müssen. In der Tabelle erlaubt die ACL alle Hosts mit Quelladressen im Netzwerk 192.168.10.0/24 und Zieladressen im Netzwerk 192.168.200.0/24.

Weitere Informationen zur Maske einer Netzwerkadresse und zur Berechnung der für ACLs erforderlichen umgekehrten Maske finden Sie im Abschnitt Masks (Masken) in Configuring IP Access Lists.

Telnet-Datenverkehr verweigern (TCP, Port 23)

Um höhere Sicherheitsbedenken auszuräumen, können Sie den Telnet-Zugriff auf Ihr privates Netzwerk über das öffentliche Netzwerk deaktivieren. Diese Abbildung zeigt, wie Telnet-Datenverkehr von NetB (öffentlich) zu NetA (privat) abgelehnt wird. Dadurch kann NetA eine Telnet-Sitzung mit NetB initiieren und einrichten, während der gesamte andere IP-Datenverkehr zugelassen wird.



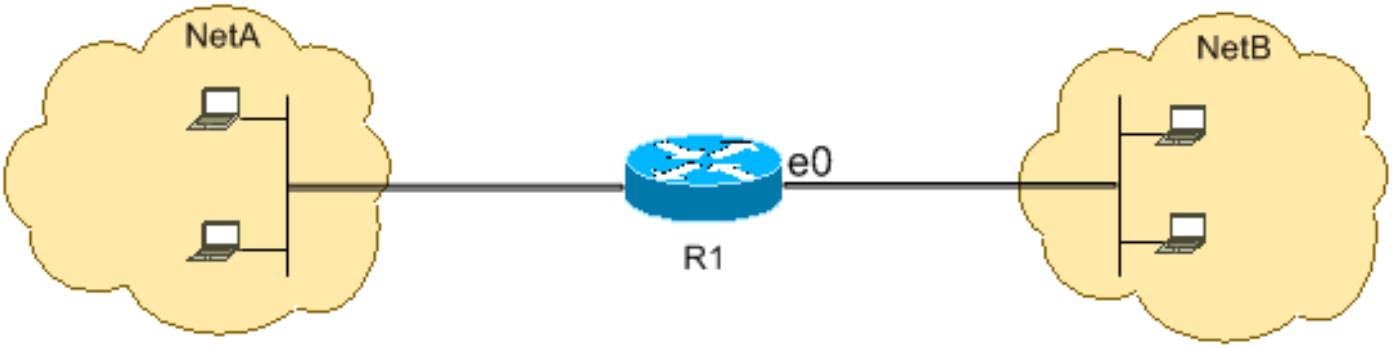
Telnet verwendet TCP, Port 23. Diese Konfiguration zeigt, dass der gesamte TCP-Datenverkehr, der für Port 23 an NetA gerichtet ist, blockiert ist und der gesamte andere IP-Datenverkehr zulässig ist.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq 23
access-list 102 permit ip any any
```

Nur internen Netzwerken erlauben, eine TCP-Sitzung zu initiieren

Diese Abbildung zeigt, dass TCP-Datenverkehr von NetA an NetB erlaubt ist, während TCP-Datenverkehr von NetB an NetA abgelehnt wird.



Der Zweck der ACL in diesem Beispiel ist:

- Hosts in NetA zu erlauben, eine TCP-Sitzung mit Hosts in NetB zu initiieren und einzurichten.
- Hosts in NetB zu verweigern, eine TCP-Sitzung mit Hosts in NetA zu initiieren und einzurichten.

Diese Konfiguration ermöglicht es einem Datagramm, die eingehende Schnittstelle Ethernet 0 auf R1 zu passieren, wenn:

- Aktivierte (ACK) oder zurückgesetzte (RST) Bits festgelegt (zeigt eine hergestellte TCP-Sitzung an)
- Sein Zielport-Wert größer als 1023 ist

R1

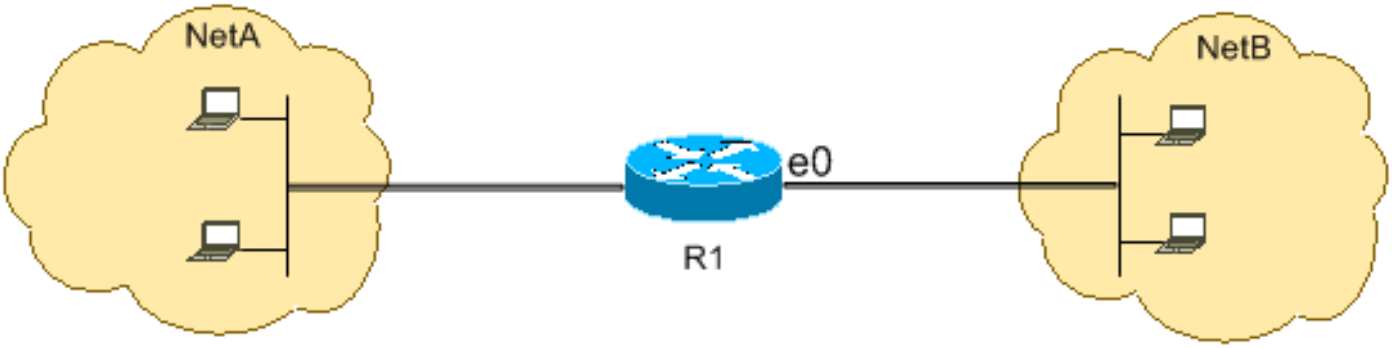
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Da die meisten bekannten Ports für IP-Dienste Werte von weniger als 1023 verwenden, wird jedes Datagramm mit einem Zielport von weniger als 1023 oder einem nicht gesetzten ACK/RST-Bit durch ACL 102 abgelehnt. Daher, wenn ein Host von NetB eine TCP-Verbindung initiiert und das erste TCP-Paket (ohne Synchronize/Start-Paket (SYN/RST)-Bit-Set) für einen Portnummer kleiner als 1023, wird sie abgelehnt und die TCP-Sitzung schlägt fehl. Die TCP-Sitzungen, die von NetA initiiert wurden und an NetB gerichtet sind, sind zulässig, da ihre ACK / RST-Bits für die Rücksendung von Paketen gesetzt sind und Port-Werte größer als 1023 verwendet werden.

Eine vollständige Liste der Ports finden Sie unter RFC 1700.

FTP-Datenverkehr verweigern (TCP, Port 21)

Diese Abbildung zeigt, dass FTP-Datenverkehr (TCP, Port 21) und FTP-Datenverkehr (Port 20) von NetB an NetA abgelehnt werden, während der gesamte andere IP-Datenverkehr zugelassen wird.



FTP verwendet Port 21 und Port 20. TCP-Datenverkehr, der an Port 21 und Port 20 gerichtet ist, wird abgelehnt, und alle anderen Vorgänge sind explizit zulässig.

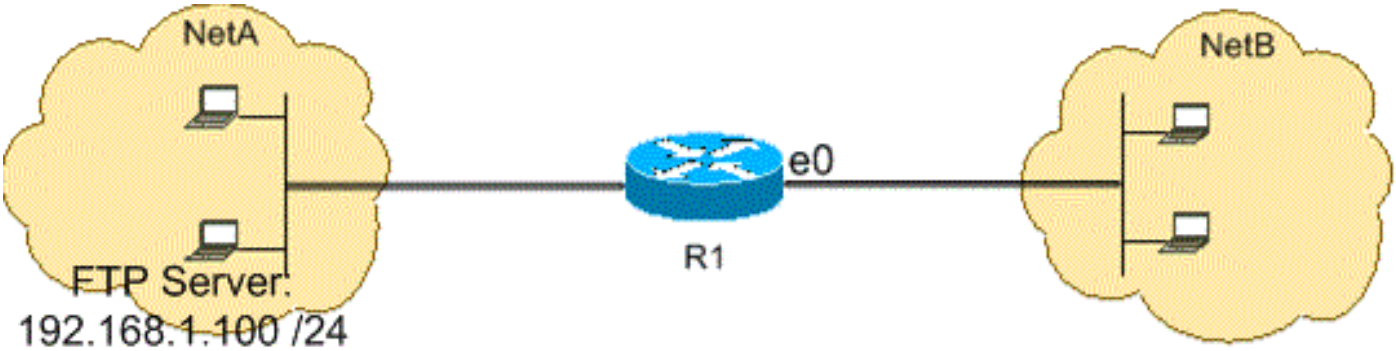
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any
```

FTP-Datenverkehr zulassen (aktives FTP)

FTP kann in zwei verschiedenen Modi betrieben werden: aktiv und passiv.

Wenn FTP im aktiven Modus ausgeführt wird, verwendet der FTP-Server Port 21 für die Steuerung und Port 20 für Daten. Der FTP-Server (192.168.1.100) befindet sich in NetA. Diese Abbildung zeigt, dass FTP-Datenverkehr (TCP, Port 21) und FTP-Datenverkehr (Port 20) von NetB an den FTP-Server (192.168.1.100) zugelassen werden, während der gesamte andere IP-Datenverkehr abgelehnt wird.



R1

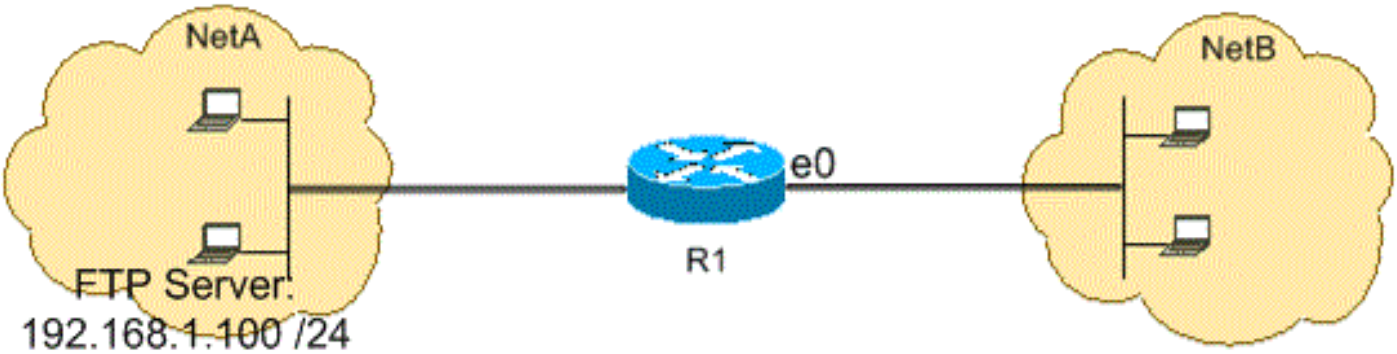
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
```

```
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 eq ftp-data any
```

FTP-Datenverkehr zulassen (Passives FTP)

FTP kann in zwei verschiedenen Modi betrieben werden: aktiv und passiv.

Wenn FTP im passiven Modus ausgeführt wird, verwendet der FTP-Server Port 21 für die Steuerung und die dynamischen Ports größer oder gleich 1024 für Daten. Der FTP-Server (192.168.1.100) befindet sich in NetA. Diese Abbildung zeigt, dass FTP-Datenverkehr (TCP, Port 21) und FTP-Datenverkehr (Ports größer oder gleich 1024) von NetB an den FTP-Server (192.168.1.100) zugelassen werden, während der gesamte andere IP-Datenverkehr abgelehnt wird.

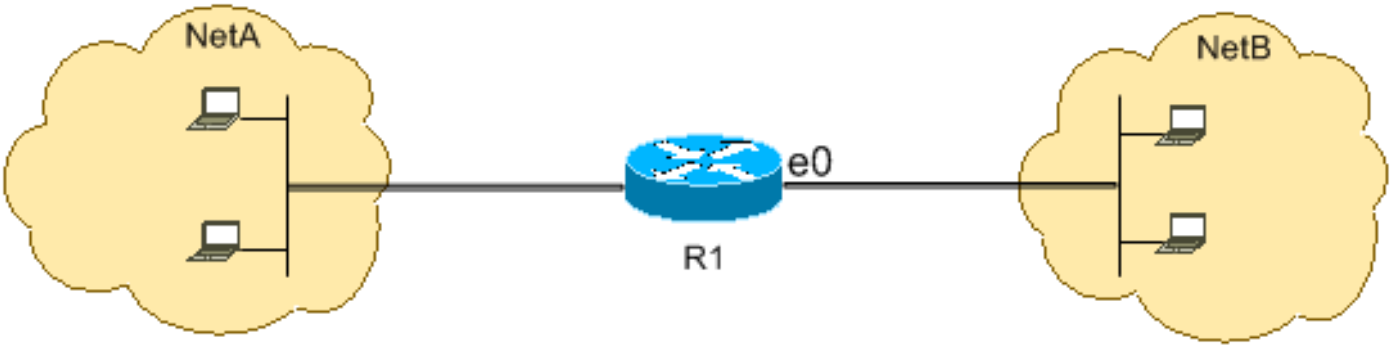


R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 gt 1023
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established
access-list 110 permit host 192.168.1.100 gt 1023 any established
```

Pings zulassen (ICMP)

Diese Abbildung zeigt, dass ICMP von NetA an NetB zulässig ist und Pings von NetB an NetA abgelehnt werden.



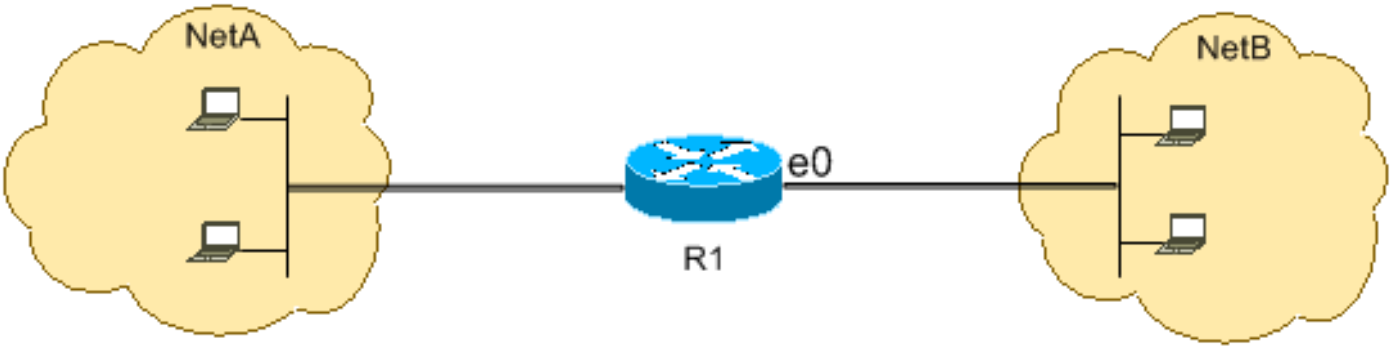
Diese Konfiguration erlaubt nur Echo-Reply (Ping-Antwort)-Pakete auf der Schnittstelle Ethernet 0 von NetB zu NetA. Die Konfiguration blockiert jedoch alle ICMP-Pakete mit Echo-Anforderung, wenn Pings von NetB an NetA gesendet werden. Daher können Hosts in NetA Hosts in NetB anpingen, aber Hosts in NetB können keine Hosts in NetA anpingen.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit icmp any any echo-reply
```

HTTP, Telnet, Mail, POP3 und FTP zulassen

Diese Abbildung zeigt, dass nur HTTP-, Telnet-, Simple Mail Transfer Protocol (SMTP)-, POP3- und FTP-Datenverkehr zulässig sind und der restliche Datenverkehr von NetB an NetA abgelehnt wird.



Diese Konfiguration ermöglicht TCP-Datenverkehr mit Zielportwerten, die mit WWW (Port 80), Telnet (Port 23), SMTP (Port 25), POP3 (Port 110), FTP (Port 21) oder FTP-Daten (Port 20) übereinstimmen. Beachten Sie, dass eine implizite „deny all“-Klausel am Ende einer ACL sämtlichen anderen Datenverkehr ablehnt, der nicht mit den „permit“-Klauseln übereinstimmt.

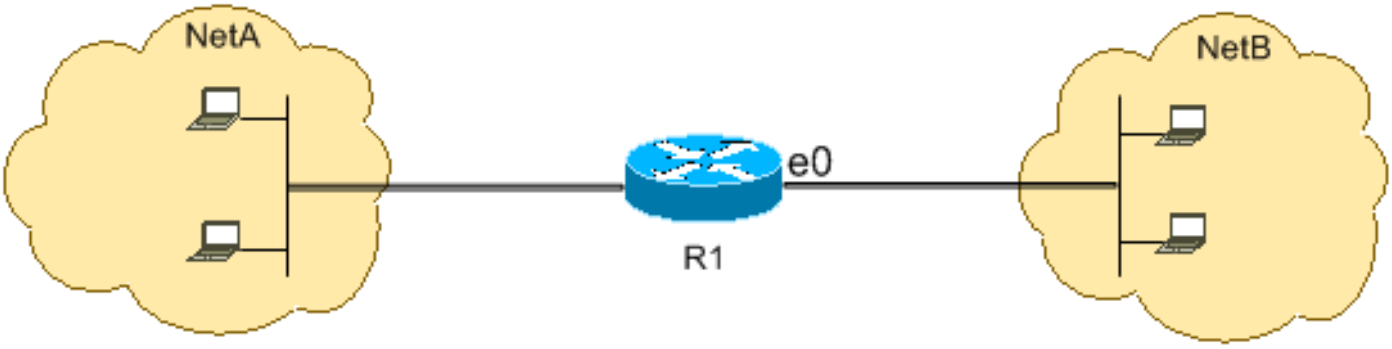
R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any eq www
access-list 102 permit tcp any any eq telnet
```

```
access-list 102 permit tcp any any eq smtp
access-list 102 permit tcp any any eq pop3
access-list 102 permit tcp any any eq 21
access-list 102 permit tcp any any eq 20
```

DNS zulassen

Diese Abbildung zeigt, dass nur DNS-Datenverkehr (Domain Name System) zulässig ist und der restliche Datenverkehr von NetB an NetA abgelehnt wird.



Diese Konfiguration lässt TCP-Datenverkehr mit dem Zielport-Wert 53 zu. Die implizite deny all-Klausel am Ende einer ACL verweigert den gesamten anderen Datenverkehr, der nicht mit den permit-Klauseln übereinstimmt.

R1

```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit udp any any eq domain
access-list 102 permit udp any eq domain any
access-list 102 permit tcp any any eq domain
access-list 102 permit tcp any eq domain any
```

Routing-Updates zulassen

Wenn Sie eine ACL für eingehende Datenverkehr auf eine Schnittstelle anwenden, stellen Sie sicher, dass Routing-Updates nicht herausgefiltert werden. Verwenden Sie die entsprechende ACL aus dieser Liste, um Routing-Protokoll-Pakete zuzulassen:

Geben Sie den folgenden Befehl ein, um Routing Information Protocol (RIP) zuzulassen:

```
access-list 102 permit udp any any eq rip
```

Geben Sie den folgenden Befehl ein, um das Interior Gateway Routing Protocol (IGRP) zuzulassen:

```
access-list 102 permit igrp any any
```

Geben Sie den folgenden Befehl ein, um Enhanced IGRP (EIGRP) zuzulassen:

```
access-list 102 permit eigrp any any
```

Geben Sie den folgenden Befehl ein, um Open Shortest Path First (OSPF) zuzulassen:

```
access-list 102 permit ospf any any
```

Geben Sie diesen Befehl ein, um Border Gateway Protocol (BGP) zuzulassen:

```
access-list 102 permit tcp any any eq 179
access-list 102 permit tcp any eq 179 any
```

Debuggen von Datenverkehr basierend auf ACL

Die Verwendung von **debug-Befehlen erfordert die Zuweisung von Systemressourcen wie Arbeitsspeicher und Rechenleistung und kann in extremen Situationen dazu führen, dass ein stark ausgelastetes System zum Erliegen kommt.** Verwenden Sie **Debug-Befehle mit Bedacht.** Verwenden Sie eine ACL, um den zu untersuchenden Datenverkehr selektiv zu definieren, um die Auswirkungen des **debug-**Befehls zu reduzieren. Eine solche Konfiguration filtert keine Pakete.

Diese Konfiguration aktiviert den Befehl **debug ip packet nur für Pakete zwischen den Hosts 10.1.1.1 und 172.16.1.1.**

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
R1(config)#end
R1#debug ip packet 199 detail IP packet debugging is on (detailed) for access list 199
```

Weitere Informationen zu den Auswirkungen von Debug-Befehlen finden Sie unter Important Information on Debug Commands.

Weitere Informationen zur Verwendung von ACLs mit **debug-Befehlen finden Sie unter** Understanding the Ping and Traceroute Commands im Abschnitt Use the Debug Command.

MAC-Adressfilterung

Sie können Frames mit einer bestimmten Quell- oder Zieladresse auf der MAC-Schicht filtern. Es kann eine beliebige Anzahl von Adressen im System ohne Leistungseinbußen konfiguriert werden. Um nach MAC-Adresse zu filtern, verwenden Sie im globalen Konfigurationsmodus den folgenden Befehl:

```
Router#config terminal
Router(config)#bridge irb
Router(config)#bridge 1 protocol ieee
Router(config)#bridge 1 route ip
```

Wenden Sie das Bridge-Protokoll auf eine Schnittstelle an, die Sie zusammen mit der mit dem Befehl **bridge-group <Gruppennummer> {input-address-list <ACL-Nummer> erstellten** Zugriffsliste filtern müssen. **| Ausgabe-Adressliste <ACL-Nummer>}**:

```
Router#config terminal
Router(config-if)#interface fastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#bridge-group 1 input-address-list 700
Router(config-if)#exit
```

Erstellen Sie eine virtuelle Bridge-Schnittstelle, und wenden Sie die der physischen Ethernet-

Schnittstelle zugewiesene IP-Adresse an:

```
Router#config terminal
Router(config-if)#int bvi1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#access-list 700 deny aaaa.bbbb.cccc 0000.0000.0000
Router(config)#access-list 700 permit 0000.0000.0000 ffff.ffff.ffff
```

Mit dieser Konfiguration lässt der Router nur die in Zugriffsliste 700 konfigurierten MAC-Adressen zu. Mit dem Zugriffslistenbefehl **access-list <ACL-Nummer> deny <MAC-Adresse> 0000.0000.000** die MAC-Adresse, auf die kein Zugriff möglich ist, verweigern und den Rest zulassen (in diesem Beispiel aaaaaaa.bb) bbb.cccc).

> **Anmerkung:** Erstellen Sie jede Zeile der Zugriffsliste für jede MAC-Adresse.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- Konfigurieren von IP-Zugriffslisten
- Support-Seite zum Thema Zugriffslisten
- IP Routing-Support-Seite
- Support-Seite für IP-Routed-Protokolle
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.