Veelgebruikte IP ACL's configureren

Inhoud

Inleiding

Dit document beschrijft voorbeeldconfiguraties voor veelgebruikte IP-toegangscontrolelijsten (ACL's) die IP-pakketten filteren.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereiste worden voldaan:

- Basisbegrip van IP-adressering

Raadpleeg IP Addressing and Subnetting for New Users (IP-adressering en subnets voor nieuwe gebruikers) voor meer informatie.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

IP-toegangscontrolelijsten voor filterpakketten op basis van:

- Bronadres
- Bestemmingsadres
- Type pakket
- Elke combinatie hiervan

Om netwerkverkeer te filteren, bepalen ACL's of gerouteerde pakketten worden doorgestuurd of geblokkeerd bij de routerinterface. De router onderzoekt elk pakket om te bepalen of het moet worden doorgestuurd of geweigerd op basis van de criteria die u in de ACL opgeeft. ACL-criteria omvatten:

- Bronadres van het verkeer
- Bestemmingsadres van het verkeer
- Upper Layer Protocol

Voer de volgende stappen uit om een ACL te maken zoals getoond in de voorbeelden in dit document:

1. Maak een ACL.
2. Pas de ACL toe op een interface.

IP ACL is een opeenvolgende reeks van voorwaarden voor toestaan/weigeren die van toepassing zijn op een IP pakket. De router toetst pakketten een voor aan de voorwaarden in de ACL.

De eerste overeenkomst bepaalt of de Cisco IOS®-software het pakket accepteert of afwijst. Omdat de Cisco IOS-software de test van voorwaarden na de eerste overeenkomst stopt, is de volgorde van de voorwaarden kritiek. Als aan geen van de voorwaarden wordt voldaan, wordt het pakket door de router afgewezen op basis van een impliciete clausule met deny all.

Dit zijn voorbeelden van IP ACL's die in Cisco IOS-software kunnen worden geconfigureerd:

- Standaard ACL's
- Uitgebreide ACL's
- Dynamische (lock and key) ACL's
- ACL's met benoemde IP's
- Reflexieve ACL's
- Tijdgebaseerde ACL's met tijdbereiken
- Vermeldingen in IP ACL's met opmerking
- Contextgebaseerde ACL's
- Verificatieproxy
- Turbo ACL's
- Gedistribueerde tijdgebaseerde ACL's

In dit document worden enkele veelgebruikte standaard en uitgebreide ACL's beschreven. Raadpleeg Configuring IP Access Lists (IP-toegangslijsten configureren) voor meer informatie over verschillende typen ACL's die worden ondersteund in Cisco IOS-software en hoe ACL's kunnen worden geconfigureerd en bewerkt.

Het formaat van de opdrachtsyntaxis van een standaard ACL is een **toegangslijst met toegangslijsten en toegangslijsten met {license|deny} {host|source-wildcard|any}**.

Standaard ACL's beheren verkeer door het bronadres van de IP-pakketten te vergelijken met de adressen die in de ACL zijn geconfigureerd.

Uitgebreide ACL's beheren verkeer door de bron- en bestemmingsadressen van de IP-pakketten te vergelijken met de adressen die in de ACL zijn geconfigureerd. U kunt uitgebreide ACL's ook gedetailleerder maken en deze configureren om verkeer te filteren op basis van criteria zoals:

- Protocol
- Poortnummers
- Waarde van Differentiated Services Code Point (DSCP)
- Prioriteitswaarde
- Status van het SYN-bit (synchronisatie van sequentienummers)

De opdrachtsyntaxissen van uitgebreide ACL's zijn:

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]
```

Transport 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)

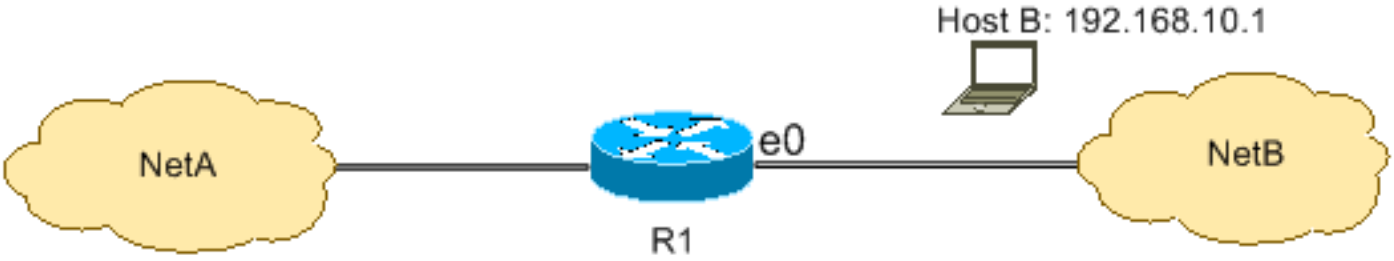
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]]
[precedence precedence] [tos tos] [log | log-input] [time-range time-range-name][fragments]
```

Configureren

In deze configuratievoorbeelden worden de meestgebruikte IP ACL's gebruikt.

Een bepaalde host toegang tot het netwerk toestaan

Dit cijfer toont dat een geselecteerde host toestemming krijgt om het netwerk te gebruiken. Al het verkeer afkomstig van Host B met bestemming NetA wordt toegestaan; al het andere verkeer afkomstig van NetB met bestemming NetA wordt geweigerd.



De output in de R1-tabel toont hoe het netwerk toegang tot de host verleent. Deze output geeft aan dat:

- De configuratie alleen de host met het IP-adres 192.168.10.1 toestaat via de Ethernet 0-interface op R1.
- Deze host toegang heeft tot de IP-services van NetA.
- Geen andere host in NetB toegang heeft tot NetA.
- In de ACL geen instructie met deny is geconfigureerd.

Standaard is een impliciete clausule met deny all opgenomen aan het eind van elke ACL. Alles wat niet uitdrukkelijk wordt toegestaan, wordt geweigerd.

R1

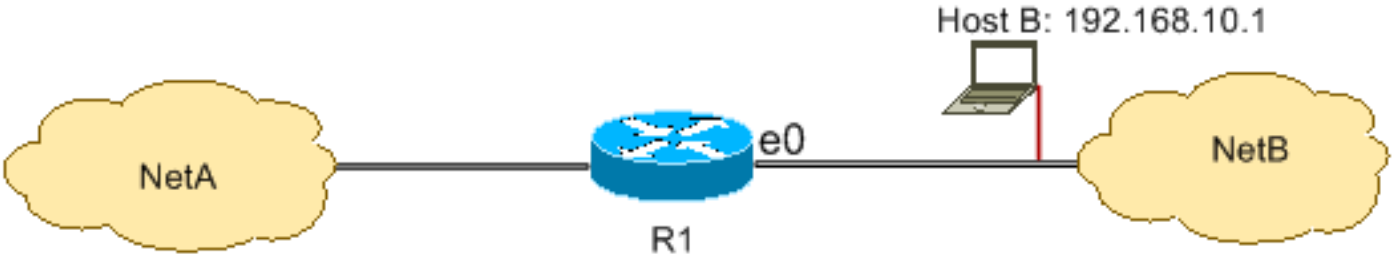
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 permit host 192.168.10.1
```

> **Opmerking**: de ACL-filters voor IP-pakketten van NetB naar NetA, behalve pakketten die van Host B. afkomstig zijn. Pakketten die van Host B naar NetA zijn afkomstig, zijn nog steeds toegestaan.

> **Opmerking:** De ACL **access-list 1 permit 192.168.10.1 0.0.0.0 is een andere manier om dezelfde regel te configureren.**

Een bepaalde host toegang tot het netwerk weigeren

In deze afbeelding wordt getoond dat verkeer afkomstig van Host B met bestemming NetA wordt geweigerd, terwijl al het andere verkeer van NetB toegang wordt verleend tot NetA.



Deze configuratie weigert alle pakketten van host 192.168.10.1/32 via Ethernet 0 op R1 en laat alle andere pakketten toe. U moet de opdracht **access list 1 permit any gebruiken om al het andere verkeer expliciet toe te laten, omdat elke ACL een impliciete clausule met deny all bevat.**

R1

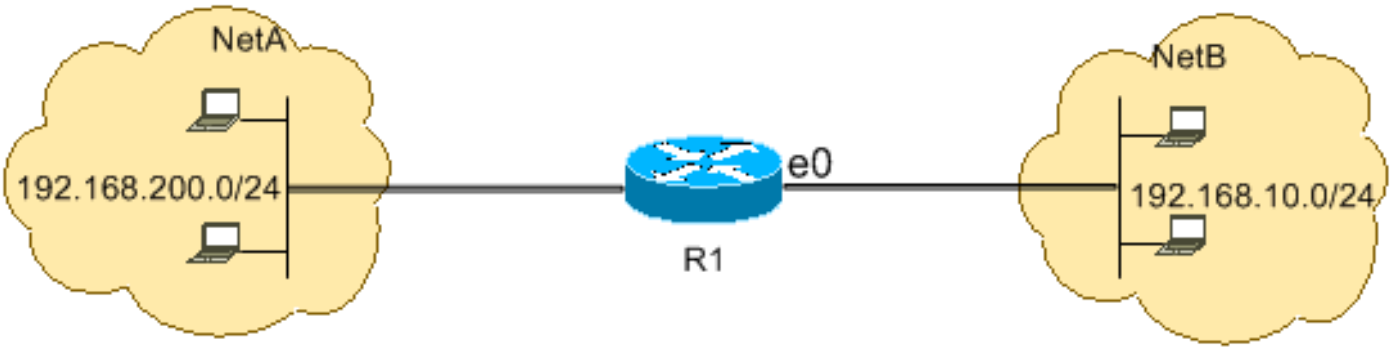
```
hostname R1
!
interface ethernet0
 ip access-group 1 in
!
access-list 1 deny host 192.168.10.1
access-list 1 permit any
```

> **Opmerking:** De volgorde van de instructies is essentieel voor de werking van een ACL. Als de volgorde van de vermeldingen wordt omgedraaid, zoals deze opdracht toont, komt de eerste regel overeen met het bronadres van elk pakket. De ACL blokkeert dan niet de toegang tot NetA voor host 192.168.10.1/32.

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

Toegang verlenen tot een reeks aaneengesloten IP-adressen

In deze afbeelding wordt getoond dat alle hosts in NetB met het netwerkadres 192.168.10.0/24 toegang krijgen tot netwerk 192.168.200.0/24 in NetA.



In deze configuratie worden de IP-pakketten met een IP-header met een bronadres in het netwerk 192.168.10.0/24 en een bestemmingsadres in het netwerk 192.168.200.0/24 toegang verleend tot NetA. Er is een impliciete clausule met deny all opgenomen aan het eind van de ACL om toegang voor al het andere inkomende verkeer via Ethernet 0 op R1 te weigeren.

R1

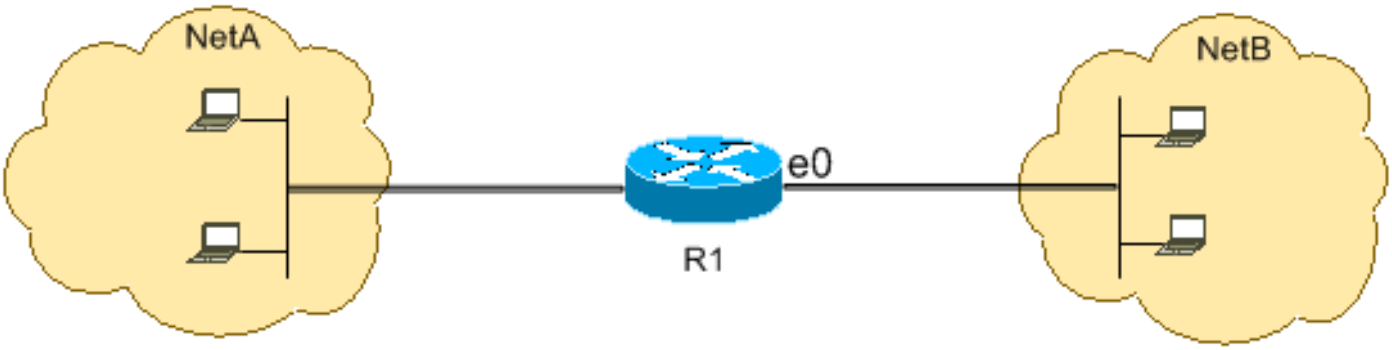
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

> **Opmerking:** In de commando **toegangslijst 101 vergunning ip 192.168.10.0 0.0.255 192.168.200.0 0.0.0.255**, de "0.0.0.255" is het inverse masker van netwerk 192.168.10.0 met masker 255.255.255.0. ACLs gebruiken het inverse masker om te weten bits in het netwerkadres moeten overeenkomen. In de tabel laat de ACL alle hosts toe met bronadressen in netwerk 192.168.10.0/24 en bestemmingsadressen in netwerk 192.168.200.0/24.

Raadpleeg de sectie Masks (Maskers) bij Configuring IP Access Lists (IP-toegangslijsten configureren) voor meer informatie over het masker van een netwerkadres en het berekenen van het voor de ACL's benodigde inverse masker.

Telnet-verkeer weigeren (TCP, poort 23)

Om aan hogere veiligheidszorgen te voldoen, kunt u de toegang van Telnet tot uw privé netwerk van het openbare netwerk onbruikbaar maken. In deze afbeelding wordt getoond hoe Telnet-verkeer van NetB (openbaar) naar NetA (privaat) wordt geweigerd, waarbij NetA een Telnet-sessie kan starten en tot stand brengen met NetB terwijl al het andere IP-verkeer wordt toegelaten.



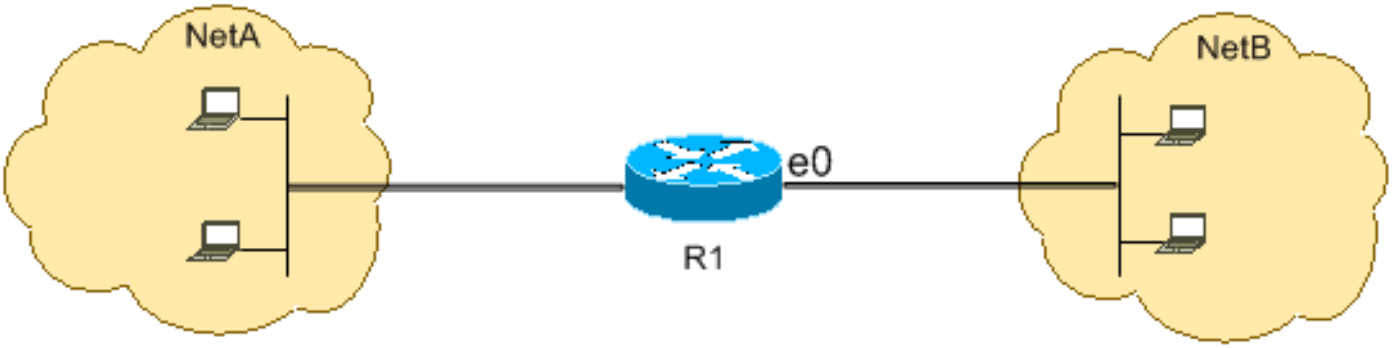
Telnet gebruikt TCP, poort 23. Deze configuratie toont aan dat al het TCP-verkeer dat is bestemd voor NetA voor poort 23 is geblokkeerd en dat al het andere IP-verkeer is toegestaan.

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
```

Alleen interne netwerken toestaan een TCP-sessie te starten

In deze afbeelding wordt getoond dat TCP-verkeer afkomstig van NetA met bestemming NetB wordt toegelaten, terwijl TCP-verkeer afkomstig van NetB met bestemming NetA wordt geweigerd.



Het doel van de ACL in dit voorbeeld is als volgt:

- Hosts in NetA toestaan om een TCP-sessie te starten en tot stand te brengen met hosts in NetB.
- Hosts in NetB niet toestaan een TCP-sessie te starten en tot stand te brengen met hosts in NetA.

Met deze configuratie kan een datagram interface Ethernet 0 inkomend op R1 passeren wanneer het datagram:

- Erkende (ACK) of reset (RST)-bits ingesteld (geeft een ingestelde TCP-sessie aan)
- Een waarde van de bestemmingspoort groter dan 1023 heeft

R1

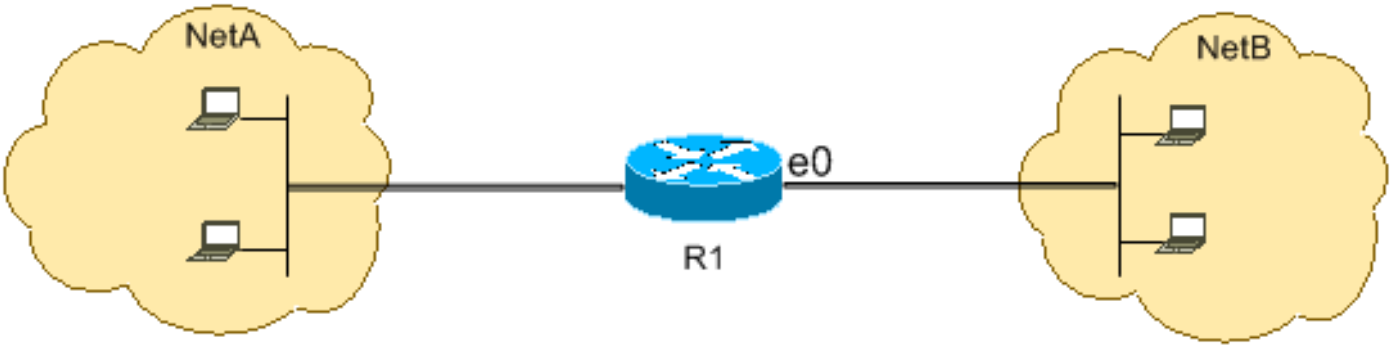
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any any gt 1023 established
```

Aangezien de meeste bekende poorten voor IP-services waarden van minder dan 1023 gebruiken, wordt elk datagram met een bestemmingshaven van minder dan 1023 of een ACK/RST bit niet-set ontkend door ACL 102. Daarom wordt een host van NetB die een TCP-verbinding start en het eerste TCP-pakket verstuurt (zonder synchronize/start packet (SYN/RST) bit set) voor een poortnummer minder dan 1023, ontkend en mislukt de TCP-sessie. De TCP-sessies die vanaf NetA naar NetB worden gestart worden toegestaan, omdat daar de ACK/RST-bit is ingesteld voor het retourneren van pakketten en poortwaarden hoger dan 1023 worden gebruikt.

Raadpleeg RFC 1700 voor een volledige lijst met poorten.

FTP-verkeer weigeren (TCP, poort 21)

In deze afbeelding wordt getoond dat FTP-verkeer (TCP, poort 21) en FTP-dataverkeer (poort 20) afkomstig van NetB met bestemming NetA wordt geweigerd, terwijl al het andere IP-verkeer wordt toegelaten.



FTP gebruikt poort 21 en poort 20. TCP-verkeer bestemd voor poort 21 en poort 20 wordt geweigerd en al het andere is expliciet toegestaan.

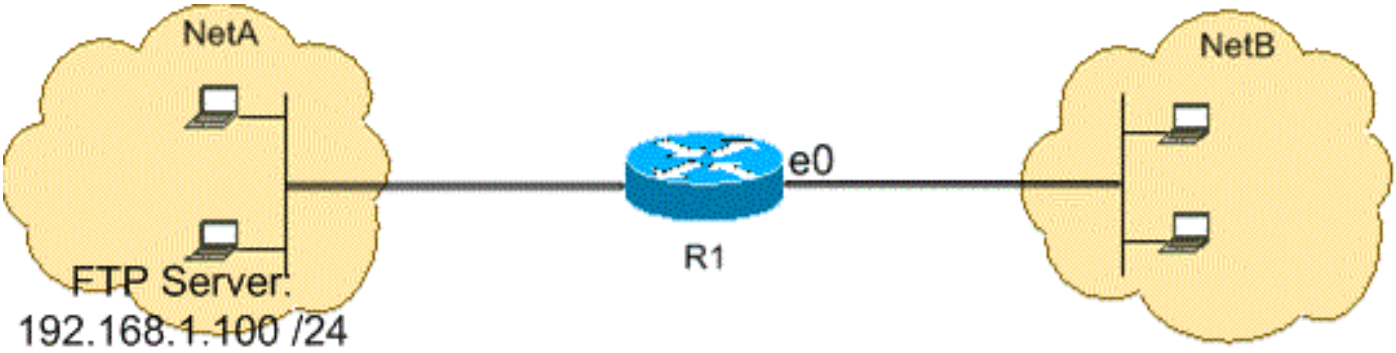
R1

```
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-verkeer toestaan (actieve FTP)

FTP kan in twee verschillende modi werken: actief en passief.

Wanneer FTP in actieve modus werkt, gebruikt de FTP-server poort 21 voor beheer en poort 20 voor data. De FTP-server (192.168.1.100) bevindt zich in NetA. In deze afbeelding wordt getoond dat FTP-verkeer (TCP, poort 21) en FTP-dataverkeer (poort 20) afkomstig van NetB met bestemming FTP-server (192.168.1.100) wordt toegelaten, terwijl al het andere IP-verkeer wordt geweigerd.



R1

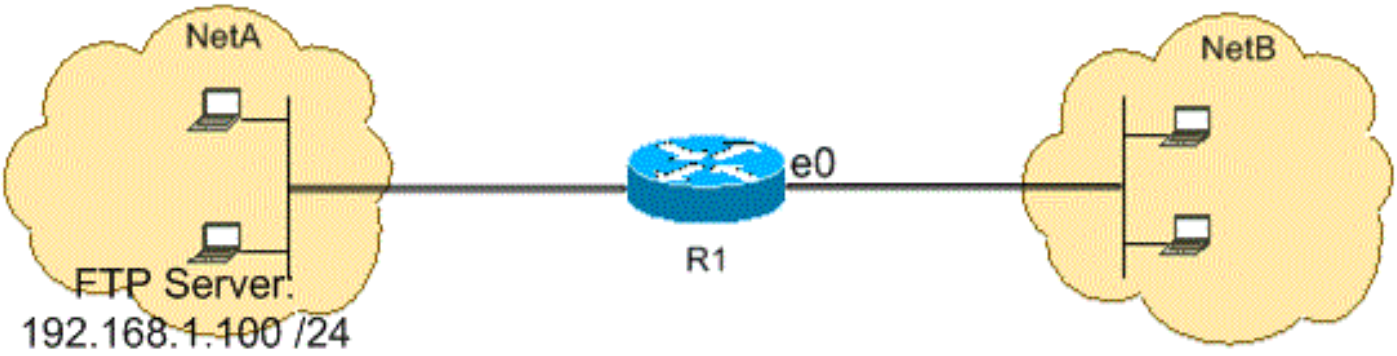
```
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
```

```
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-verkeer toestaan (passieve FTP)

FTP kan in twee verschillende modi werken: actief en passief.

Wanneer FTP in passieve modus werkt, gebruikt de FTP-server poort 21 voor beheer en de dynamische poorten 1024 en hoger voor data. De FTP-server (192.168.1.100) bevindt zich in NetA. In deze afbeelding wordt getoond dat FTP-verkeer (TCP, poort 21) en FTP-dataverkeer (poorten hoger of gelijk aan 1024) afkomstig van NetB met bestemming FTP-server (192.168.1.100) wordt toegelaten, terwijl al het andere IP-verkeer wordt geweigerd.

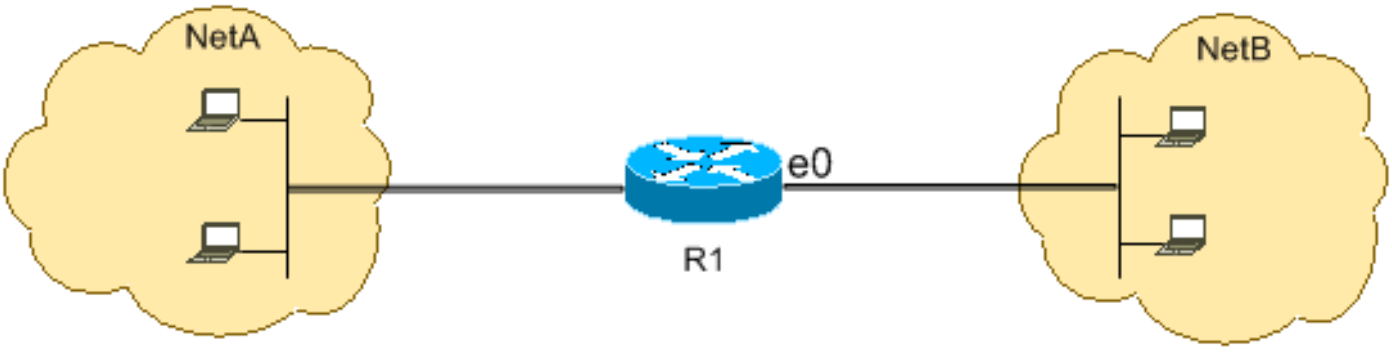


R1

```
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 (ICMP) toestaan

In deze afbeelding wordt getoond dat ICMP afkomstig van NetA met bestemming NetB wordt toegestaan, en pings afkomstig van NetB met bestemming NetA worden geweigerd.



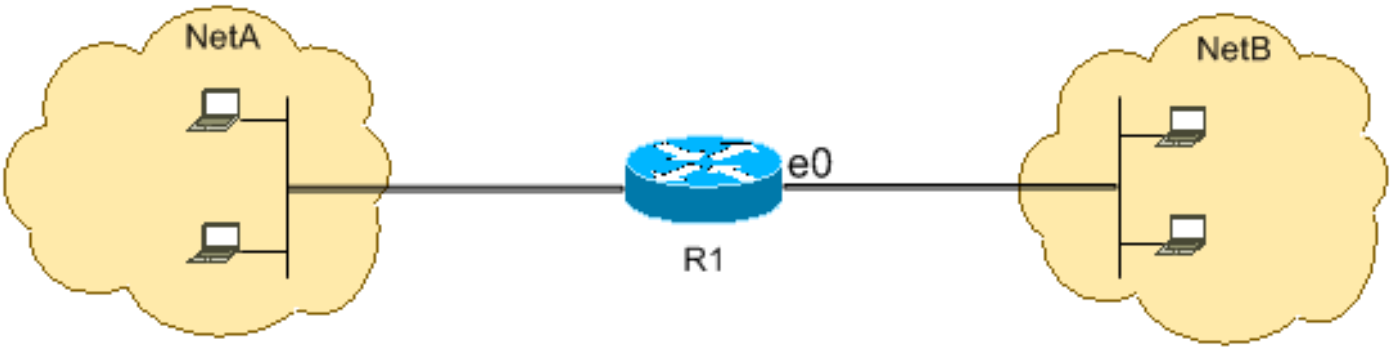
Deze configuratie laat alleen echo-reply (pingrespons) pakketten toe op interface Ethernet 0 vanaf NetB naar NetA. De configuratie blokkeert echter alle echo-request ICMP-pakketten bij pings afkomstig van NetB met als bestemming NetA. Hosts in NetA kunnen dus hosts in NetB pingen, maar hosts in NetB kunnen geen hosts in NetA pingen.

R1

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

HTTP, Telnet, Mail, POP3, FTP toestaan

In deze afbeelding wordt getoond dat alleen HTTP-, Telnet-, SMTP- (Simple Mail Transfer Protocol), POP3- en FTP-verkeer wordt toegelaten en de rest van het verkeer afkomstig van NetB met als bestemming NetA wordt geweigerd.



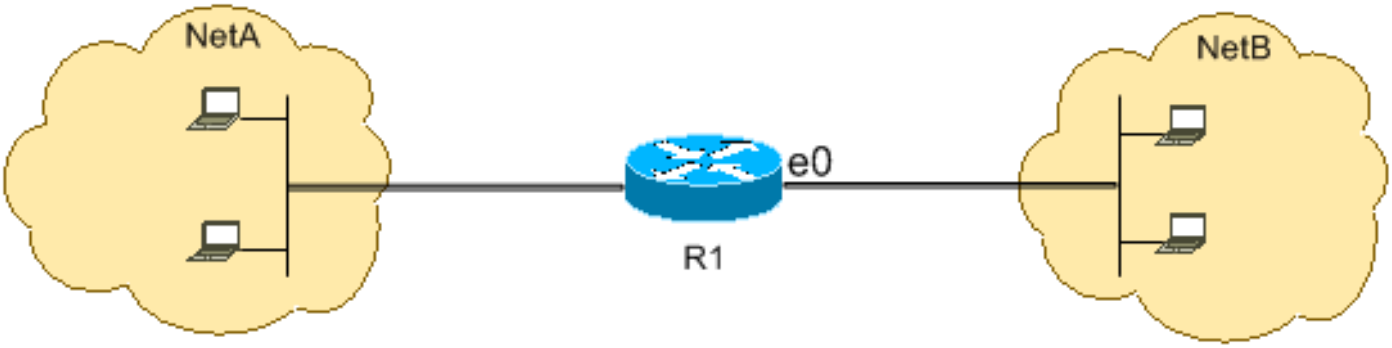
Deze configuratie laat TCP-verkeer met de bestemmingspoortwaarden die overeenkomen met WWW (poort 80), Telnet (poort 23), SMTP (poort 25), POP3 (poort 110), FTP (poort 21) of FTP-data (poort 20) toe. De impliciete clausule met deny all aan het eind van de ACL weigert al het andere verkeer dat niet overeenkomt met de clausules met permit.

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 toestaan

In deze afbeelding wordt getoond dat alleen DNS-verkeer (Domain Name System) wordt toegelaten, en de rest van het verkeer afkomstig van NetB met als bestemming NetA wordt geweigerd.



Deze configuratie maakt TCP-verkeer met bestemmingspoortwaarde 53 mogelijk. De impliciete ontkennen alle clausule aan het eind van een ACL ontkent al het andere verkeer, dat niet overeenkomt met de vergunningsclausules.

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
```

Routingupdates toestaan

Wanneer u een inkomende ACL toepast op een interface, moeten routingupdates niet worden uitgefilterd. Gebruik de relevante ACL uit deze lijst om routingprotocolpakketten toe te staan:

Voer deze opdracht in om Routing Information Protocol (RIP) toe te staan:

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

Voer deze opdracht in om Interior Gateway Routing Protocol (IGRP) toe te staan:

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

Voer deze opdracht in om Enhanced IGRP (EIGRP) toe te staan:

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

Voer deze opdracht in om Open Shortest Path First (OSPF) toe te staan:

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

Voer deze opdracht in om Border Gateway Protocol (BGP) toe te staan:

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

Fouten in verkeer gebaseerd op ACL opsporen

Het gebruik van opdrachten met **debug vereist de toewijzing van systeembronnen, zoals geheugen en verwerkingskracht, en kan in extreme situaties ertoe leiden dat een zwaar belast systeem vertraagt.** Ga zorgvuldig om met opdrachten met **debug.** Gebruik een ACL om selectief het verkeer te definiëren dat moet worden onderzocht om de impact van de **debug-**opdracht te verminderen. Een dergelijke configuratie filtert geen pakketten.

Deze configuratie schakelt de opdracht **debug ip packet alleen in voor pakketten tussen de hosts 10.1.1.1 en 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
```

Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voor meer informatie over de impact van opdrachten met debug.

Raadpleeg de sectie Use the Debug Command (De opdracht debug gebruiken) bij Understanding the Ping and Traceroute Commands (Begrip van de opdrachten ping en Traceroute) voor meer informatie over het gebruik van ACL's met opdrachten met **debug.**

MAC-adresfiltering

U kunt frames met een bepaald bron- of bestemmingsadres op de MAC-laag filteren. Elk gewenst aantal adressen kan in het systeem worden geconfigureerd zonder concessies aan de prestaties. Om te filteren op adres op de MAC-laag gebruikt u de volgende opdracht in de modus Global Configuration:

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

Pas het brugprotocol op een interface toe die u nodig hebt om verkeer samen met de toegangslijst te filteren die met de bevel **bridge-group <group number> {input-address-list <ACL number> wordt** gemaakt **| Uitvoer-adreslijst <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
```

Maak een overbrugde virtuele interface en pas het IP-adres toe dat aan de fysieke Ethernet-interface is toegewezen:

```
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
```

Met deze configuratie, staat de router slechts de adressen van MAC toe die op de toegang-lijst 700 worden gevormd. Met de van het toegangslijst bevel **toegangslijst <ACL-nummer> ontkennen**

<mac-adres> 000.000.000, ontkennen het adres van MAC dat geen toegang kan hebben en dan de rest (dit bijvoorbeeld, aaaa.bbbb.ccc) toelaten.

> **Opmerking:** Maak elke regel van de toegangslijst voor elk MAC-adres.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke informatie beschikbaar om deze configuratie problemen op te lossen.

Gerelateerde informatie

- IP-toegangslijsten configureren
- Ondersteuningspagina voor ACL's
- Ondersteuningspagina voor IP-routing
- Ondersteuningspagina voor IP-routeringsprotocollen
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.