

Configurazione degli ACL di indirizzi IP più utilizzati

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Consentire a un host selezionato di accedere alla rete](#)

[Rifiutare l'accesso alla rete di un host](#)

[Consentire l'accesso a un intervallo di indirizzi IP contigui](#)

[Rifiutare il traffico Telnet \(TCP, porta 23\)](#)

[Consentire solo alle reti interne di avviare una sessione TCP](#)

[Rifiutare il traffico FTP \(TCP, porta 21\)](#)

[Consentire il traffico FTP \(FTP attivo\)](#)

[Consentire il traffico FTP \(FTP passivo\)](#)

[Consentire i ping \(ICMP\)](#)

[Consentire HTTP, Telnet, Mail, POP3, FTP](#)

[Consentire il traffico DNS](#)

[Consentire gli aggiornamenti routing](#)

[Debug del traffico basato su ACL](#)

[Filtro degli indirizzi MAC](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte configurazioni di esempio per gli Access Control List (ACL) IP di uso comune, che filtrano i pacchetti IP.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Nozioni di base sull'indirizzamento IP.

Per ulteriori informazioni, consultare [Indirizzamento IP e subnetting per nuovi utenti](#).

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Gli elenchi di controllo di accesso IP filtrano i pacchetti in base a:

- Source address
- Indirizzo di destinazione
- Tipo di pacchetto
- Una combinazione dei due

Per filtrare il traffico di rete, gli ACL controllano se i pacchetti indirizzati sono inoltrati o bloccati sull'interfaccia del router. Il router esamina ogni pacchetto per stabilire se inoltrarlo o eliminarlo in base ai criteri specificati nell'ACL. I criteri dell'ACL includono:

- Indirizzo di origine del traffico
- Indirizzo di destinazione del traffico
- Protocollo di livello superiore

Per creare un ACL come quello degli esempi di questo documento completare questi passaggi:

1. Creare un ACL.
2. Applicare l'ACL a un'interfaccia.

L'ACL di indirizzi IP è una raccolta sequenziale di condizioni di autorizzazione e rifiuto che si applicano a un pacchetto IP. Il router confronta i pacchetti con le condizioni dell'ACL uno alla volta.

La prima corrispondenza determina se il software Cisco IOS® accetta o rifiuta il pacchetto. Poiché il software Cisco IOS interrompe il test delle condizioni dopo la prima corrispondenza, l'ordine delle condizioni è critico. Se nessuna condizione corrisponde, il router rifiuta il pacchetto in base alla clausola implicit deny all.

Questi sono esempi di ACL di indirizzi IP che è possibile configurare nel software Cisco IOS:

- ACL standard
- ACL estesi
- ACL dinamici (lock and key)
- ACL con nome IP
- ACL riflessivi

- ACL con limiti di tempo e uso di intervalli
- Voci ACL IP con commento
- ACL basati sul contesto
- Proxy di autenticazione
- ACL turbo
- ACL con limiti di tempo distribuiti

Questo documento descrive alcuni ACL standard ed estesi di uso comune. Consultare [Configurazione degli elenchi di accesso IP](#) per ulteriori informazioni sui diversi tipi di ACL supportati nel software Cisco IOS e su come configurare e modificare gli ACL.

Il formato della sintassi dei comandi di un ACL standard è `access-list access-list-number {permit|deny} {host|source source-wildcard|any}`.

Gli ACL standard controllano il traffico confrontando l'indirizzo di origine dei pacchetti IP con gli indirizzi configurati nell'ACL.

Gli ACL estesi controllano il traffico confrontando gli indirizzi di origine e di destinazione dei pacchetti IP con gli indirizzi configurati nell'ACL. È inoltre possibile rendere gli ACL estesi più granulari e configurarli per filtrare il traffico in base a criteri quali:

- Protocollo
- Numeri di porta
- Valore DSCP (Differentiated Services Code Point)
- Valore di precedenza
- Stato del bit del numero di sequenza sincronizzazione (SYN)

I formati di sintassi del comando degli ACL estesi sono:

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]
```

Protocollo ICMP (Internet Control Message Protocol)

```
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]
```

Protocollo TCP (Transmission Control Protocol)

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

Protocollo UDP (User Datagram Protocol)

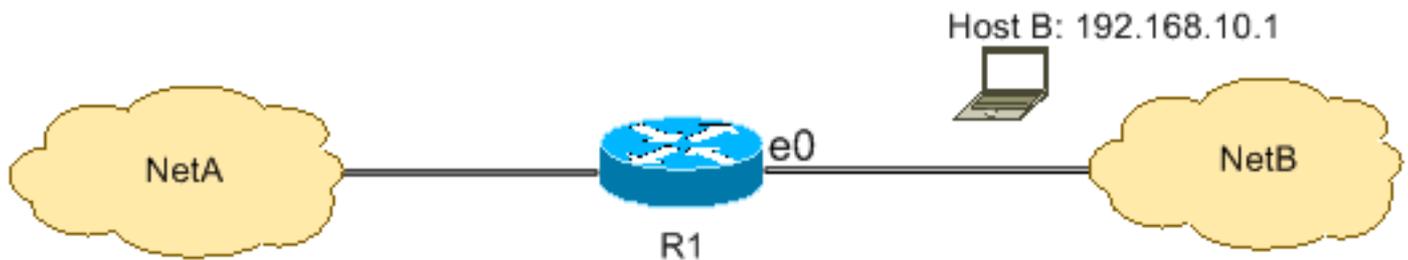
```
access-list access-list-number [dynamic dynamic-name [timeout minutes]]
{deny | permit} udp source source-wildcard [operator [port]] destination destination-wildcard [operator
[precedence precedence] [tos tos] [log | log-input]
[time-range time-range-name][fragments]
```

Configurazione

Questi esempi di configurazione utilizzano gli ACL di indirizzi IP più comuni.

Consentire a un host selezionato di accedere alla rete

Nell'immagine viene mostrato come a un host selezionato sia stata concessa l'autorizzazione di accesso alla rete. Tutto il traffico originato dall'Host B e destinato a NetA è autorizzato, mentre tutto il traffico originato da NetB e destinato a NetA è rifiutato.



La tabella R1 mostra il modo in cui la rete concede l'accesso all'host. La tabella mostra che:

- La configurazione consente di accedere solo all'host con indirizzo IP 192.168.10.1 tramite l'interfaccia Ethernet 0 su R1.
- Questo host può accedere ai servizi IP di NetA.
- Nessun altro host in NetB può accedere a NetA.
- Nell'ACL non è stata configurata alcuna istruzione deny.

Per impostazione predefinita, è presente una clausola implicit deny all alla fine di ogni ACL. Tutti i pacchetti non consentiti esplicitamente vengono rifiutati.

R1

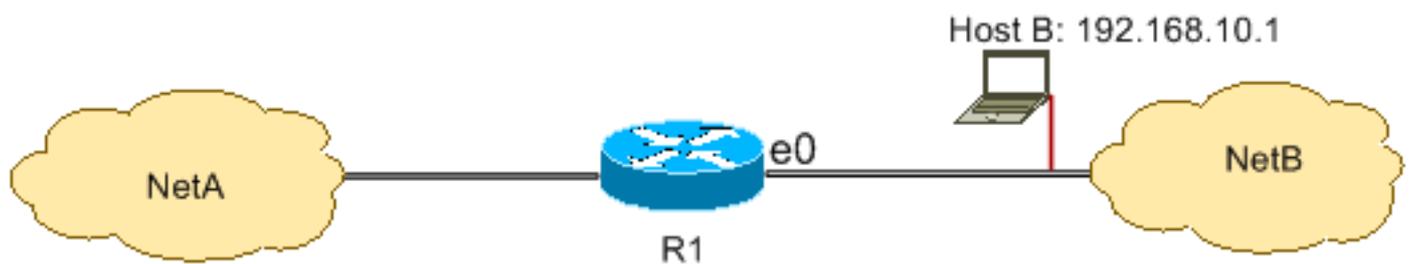
```
hostname R1
!  
interface ethernet0
 ip access-group 1 in
!  
access-list 1 permit host 192.168.10.1
```

 Nota: l'ACL filtra i pacchetti IP da NetB a NetA, ad eccezione dei pacchetti provenienti dall'host B. I pacchetti provenienti dall'host B a NetA sono ancora consentiti.

 Nota: l'ACL access-list 1 allow 192.168.10.1 0.0.0.0 è un altro modo per configurare la stessa regola.

Rifiutare l'accesso alla rete di un host

Nell'immagine viene mostrato che il traffico proveniente dall'host B e destinato a NetA viene rifiutato, mentre tutto il resto del traffico proveniente da NetB e diretto ad accedere a NetA viene autorizzato.



Questa configurazione rifiuta tutti i pacchetti dall'host 192.168.10.1/32 a Ethernet 0 su R1 e consente tutto il resto. È necessario utilizzare il comando access list 1 permit any per consentire esplicitamente il traffico restante, perché in ogni ACL è presente una clausola implicit deny all.

R1

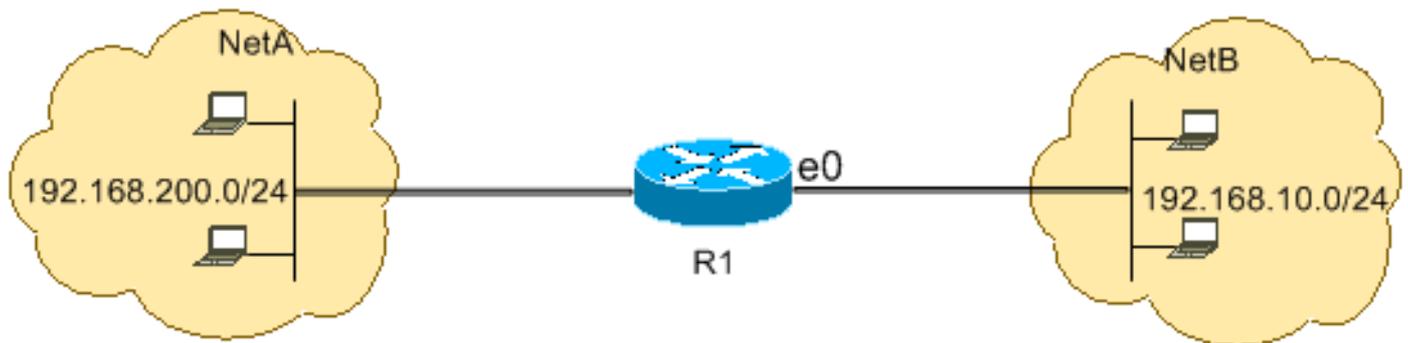
```
hostname R1
!  
interface ethernet0
 ip access-group 1 in
!  
access-list 1 deny host 192.168.10.1  
access-list 1 permit any
```

 Nota: l'ordine delle istruzioni è fondamentale per il funzionamento di un ACL. Se l'ordine delle voci è invertito, come mostrato in questo comando, la prima riga trova l'indirizzo di origine di ogni pacchetto. Pertanto, l'ACL non riesce a impedire all'host 192.168.10.1/32 di accedere a NetA.

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

Consentire l'accesso a un intervallo di indirizzi IP contigui

Nell'immagine viene mostrato come tutti gli host in NetB con indirizzo di rete 192.168.10.0/24 possano accedere alla rete 192.168.200.0/24 in NetA.



Questa configurazione consente ai pacchetti IP la cui intestazione IP ha indirizzo di origine nella rete 192.168.10.0/24 e indirizzo di destinazione nella rete 192.168.200.0/24 di accedere a NetA. Alla fine dell'ACL è presente la clausola implicit deny all, che rifiuta tutto il resto del traffico in entrata su R1 attraverso Ethernet 0.

R1

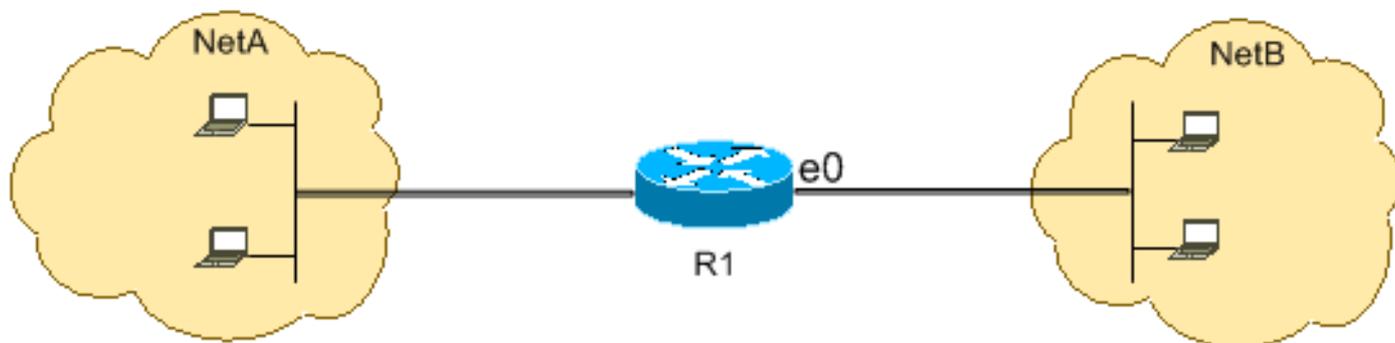
```
hostname R1
!
interface ethernet0
 ip access-group 101 in
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255
```

 Nota: nel comando access-list 101 allow ip 192.168.10.0 0.0.0.255.192.168.200.0.0.0.255, la maschera 0.0.0.255 è la maschera inversa della rete 192.168.10.0 con maschera 255.255.255.0. Gli ACL usano la maschera inversa per sapere quanti bit dell'indirizzo di rete devono corrispondere. Nella tabella, l'ACL autorizza tutti gli host con indirizzi di origine nella rete 192.168.10.0/24 e indirizzi di destinazione nella rete 192.168.200.0/24.

Consultare la sezione [Maschere](#) in [Configurazione degli ACL di indirizzi IP](#) per ulteriori informazioni sulla maschera di un indirizzo di rete e su come calcolare la maschera inversa necessaria per gli ACL.

Rifiutare il traffico Telnet (TCP, porta 23)

Per risolvere problemi di protezione più elevati, è possibile disabilitare l'accesso Telnet alla rete privata dalla rete pubblica. Nell'immagine viene mostrato come il traffico Telnet da NetB (pubblico) destinato a NetA (privato) viene rifiutato, il che consente a NetA di avviare e stabilire una sessione Telnet con NetB, mentre tutto il resto del traffico IP viene autorizzato.



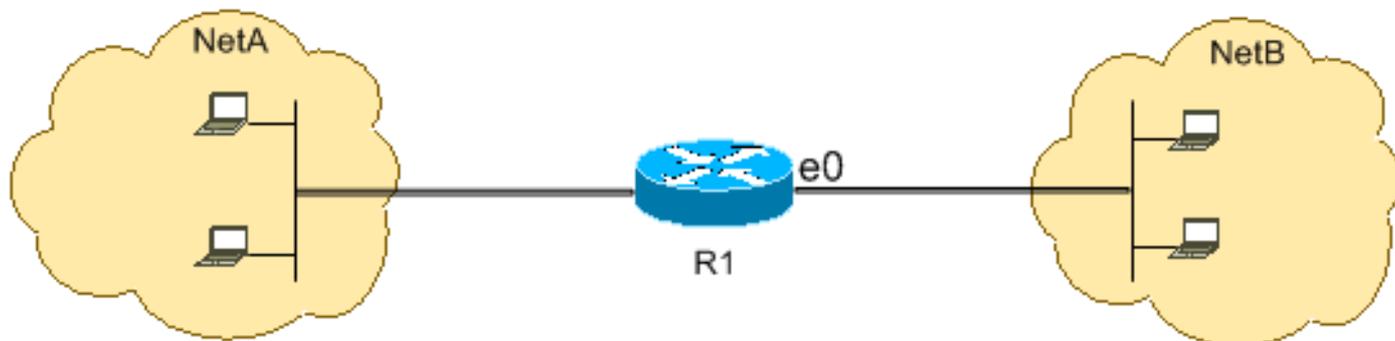
Telnet usa TCP, porta 23. Questa configurazione mostra che tutto il traffico TCP destinato a NetA per la porta 23 è bloccato e tutto il resto del traffico IP è autorizzato.

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
```

Consentire solo alle reti interne di avviare una sessione TCP

Questa figura mostra che il traffico TCP originato proveniente da NetA e destinato a NetB è autorizzato, mentre il traffico TCP proveniente da NetB e destinato a NetA è rifiutato.



Lo scopo dell'ACL in questo esempio è:

- Consentire agli host in NetA di avviare e stabilire una sessione TCP per gli host in NetB.
- Impedire agli host in NetB di avviare e stabilire una sessione TCP destinata agli host in

NetA.

Questa configurazione consente a un datagramma di passare attraverso l'interfaccia Ethernet 0 in entrata su R1 quando sono presenti:

- Bit riconosciuti (ACK) o reimpostati (RST) (indica una sessione TCP stabilita)
- Una porta di destinazione maggiore di 1023

R1

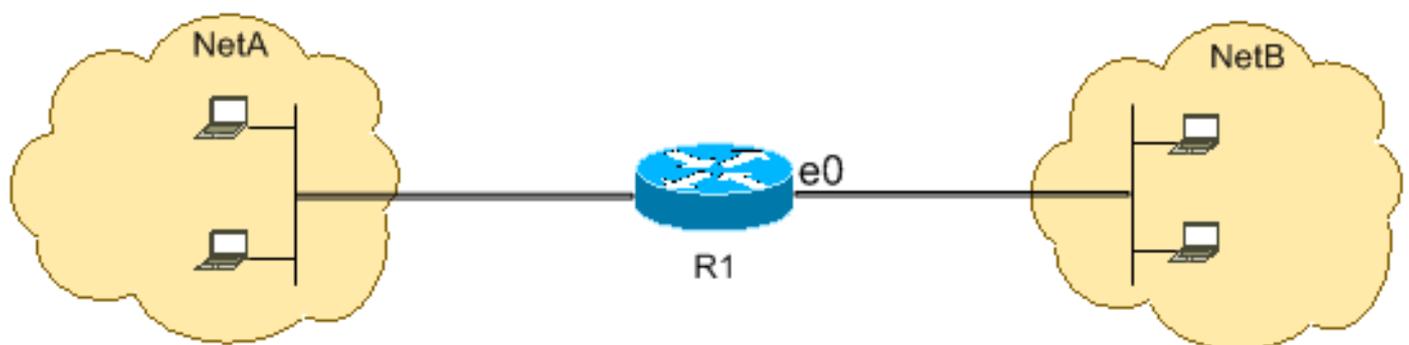
```
hostname R1
!  
interface ethernet0  
 ip access-group 102 in  
!  
access-list 102 permit tcp any any gt 1023 established
```

Poiché la maggior parte delle porte conosciute per i servizi IP utilizza valori inferiori a 1023, qualsiasi datagramma con una porta di destinazione inferiore a 1023 o con un bit ACK/RST non impostato viene rifiutato da ACL 102. Pertanto, quando un host di NetB avvia una connessione TCP e invia il primo pacchetto TCP (senza bit di sincronizzazione/avvio del pacchetto (SYN/RST) impostato) per un numero di porta inferiore a 1023, il pacchetto viene rifiutato e la sessione TCP non riesce. Le sessioni TCP avviate da NetA e destinate a NetB sono consentite perché hanno bit ACK/RST impostati per i pacchetti di ritorno e usano le porte maggiori di 1023.

Consultare la richiesta [RFC 1700](#) per un elenco completo delle porte.

Rifiutare il traffico FTP (TCP, porta 21)

Nell'immagine viene mostrato come il traffico FTP (TCP, porta 21) e i dati FTP (porta 20) provenienti da NetB e destinati a NetA vengano rifiutati, mentre tutto il resto del traffico IP è autorizzato.



L'FTP utilizza la porta 21 e la porta 20. Il traffico TCP destinato alla porta 21 e alla porta 20 viene rifiutato e tutto il resto viene esplicitamente autorizzato.

R1

```

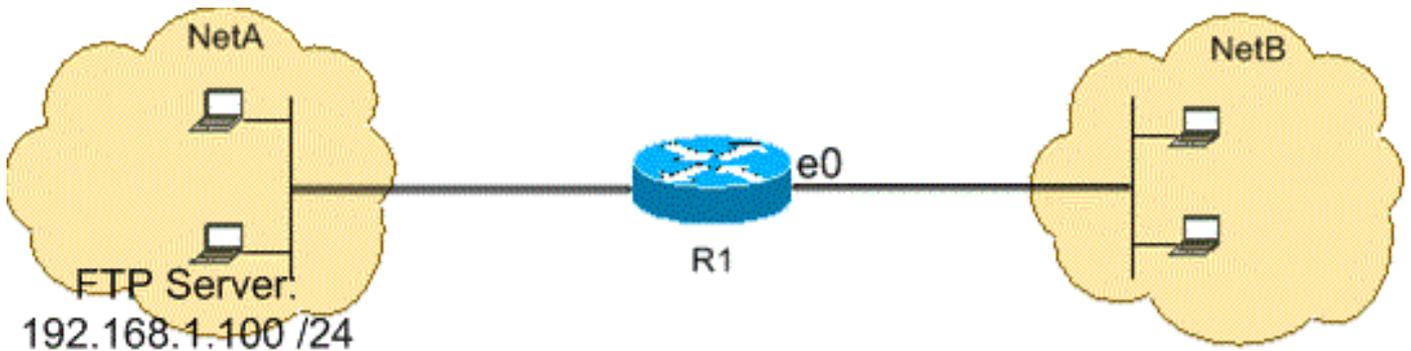
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 deny tcp any any eq ftp
access-list 102 deny tcp any any eq ftp-data
access-list 102 permit ip any any

```

Consentire il traffico FTP (FTP attivo)

FTP può operare in due diverse modalità, dette attiva e passiva.

Quando l'FTP funziona in modalità attiva, il server FTP utilizza la porta 21 per il controllo e la porta 20 per i dati. Il server FTP (192.168.1.100) si trova in NetA. Nell'immagine viene mostrato come il traffico FTP (TCP, porta 21) e i dati FTP (porta 20) provenienti da NetB e destinati al server FTP (192.168.1.100) siano autorizzati, mentre tutto il resto del traffico IP è rifiutato.



R1

```

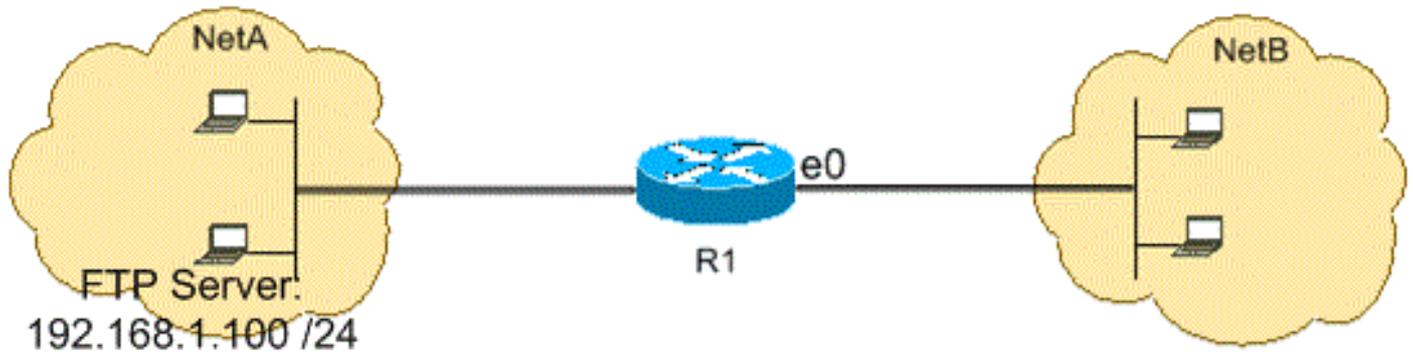
hostname R1
!
interface ethernet0
 ip access-group 102 in
!
access-list 102 permit tcp any host 192.168.1.100 eq ftp
access-list 102 permit tcp any host 192.168.1.100 eq ftp-data established
!
interface ethernet1
 ip access-group 110 in
!
access-list 110 permit host 192.168.1.100 eq ftp any established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

```

Consentire il traffico FTP (FTP passivo)

FTP può operare in due diverse modalità, dette attiva e passiva.

Quando l'FTP funziona in modalità passiva, il server FTP utilizza la porta 21 per il controllo e le porte dinamiche a partire dalla 1024 per i dati. Il server FTP (192.168.1.100) si trova in NetA. Nell'immagine viene mostrato come il traffico FTP (TCP, porta 21) e i dati FTP (porte maggiori o uguali a 1024) provenienti da NetB e destinati al server FTP (192.168.1.100) siano autorizzati, mentre tutto il resto del traffico IP è rifiutato.

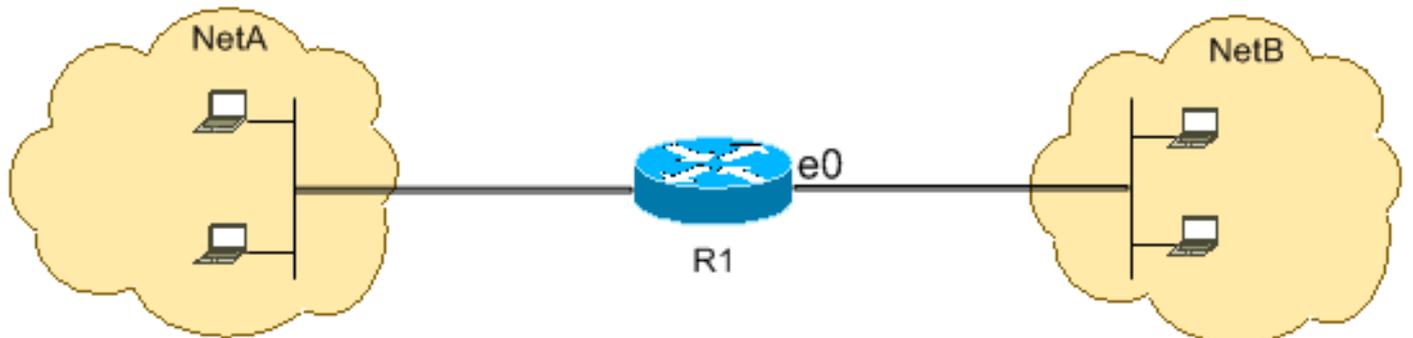


R1

```
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
```

Consentire i ping (ICMP)

Nell'immagine viene mostrato come l'ICMP proveniente da NetA e destinato a NetB sia autorizzato e i ping provenienti da NetB e destinati a NetA siano rifiutati.



Questa configurazione consente solo i pacchetti echo-reply (risposta ping) in ingresso sull'interfaccia Ethernet 0 da NetB verso NetA. Tuttavia, la configurazione blocca tutti i pacchetti

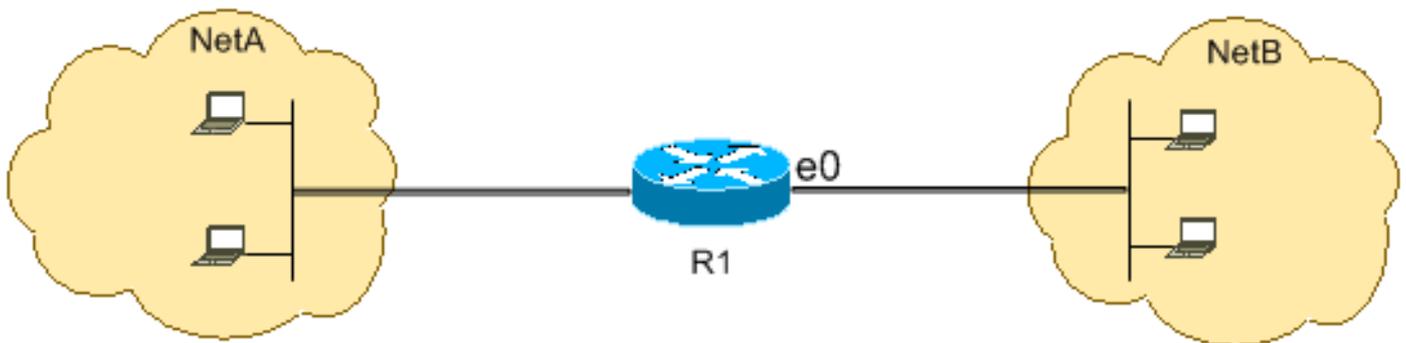
ICMP echo-request quando i ping sono originati in NetB e destinati a NetA. Pertanto, gli host in NetA possono eseguire il ping degli host in NetB, ma gli host in NetB non possono eseguire il ping degli host in NetA.

R1

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

Consentire HTTP, Telnet, Mail, POP3, FTP

Nell'immagine viene mostrato che è consentito solo il traffico HTTP, Telnet, SMTP (Simple Mail Transfer Protocol), POP3 e FTP e il resto del traffico proveniente da NetB e destinato a NetA viene rifiutato.



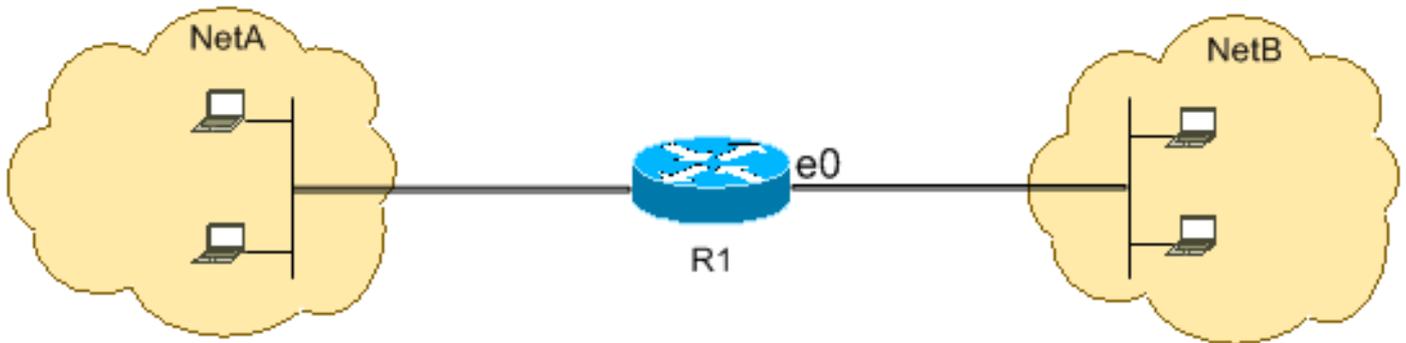
Questa configurazione consente il traffico TCP con porte di destinazione che corrispondono ai dati WWW (porta 80), Telnet (porta 23), SMTP (porta 25), POP3 (porta 110), FTP (porta 21) o dati FTP (porta 20). Ricordiamo che una clausola implicita deny all alla fine di un ACL rifiuta tutto il traffico rimanente che non corrisponde alle clausole di autorizzazione.

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
```

Consentire il traffico DNS

Nell'immagine viene mostrato che è consentito solo il traffico DNS (Domain Name System) e il resto del traffico proveniente da NetB e destinato a NetA viene rifiutato.



Questa configurazione consente il traffico TCP con valore della porta di destinazione 53. La clausola implicita deny all situata alla fine di un ACL nega tutto il resto del traffico, che non corrisponde alle clausole di autorizzazione.

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
```

Consentire gli aggiornamenti routing

Quando si applica un ACL in ingresso a un'interfaccia, assicurarsi che gli aggiornamenti di routing non vengano filtrati. Utilizzare l'ACL pertinente di questo elenco per autorizzare i pacchetti del protocollo di routing:

Immettere questo comando per autorizzare il protocollo RIP (Routing Information Protocol):

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

Immettere questo comando per autorizzare il protocollo IGRP (Interior Gateway Routing Protocol):

```
access-list 102 permit igmp any any
```

Immettere questo comando per autorizzare il protocollo EIGRP (Enhanced IGRP):

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

Immettere questo comando per autorizzare il protocollo OSPF (Open Shortest Path First):

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

Immettere questo comando per autorizzare il protocollo BGP (Border Gateway Protocol):

```
<#root>
```

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

```
179
```

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

```
179
```

```
any
```

Debug del traffico basato su ACL

L'uso di comandi di debug richiede l'allocazione di risorse di sistema come la memoria e la potenza di elaborazione, e in situazioni estreme può causare l'arresto di un sistema sovraccarico. Utilizzare i comandi di debug con cautela. Per definire in modo selettivo il traffico da esaminare e ridurre l'impatto del comando debug, usare un ACL. Una configurazione di questo tipo non filtra i pacchetti.

Questa configurazione attiva il comando debug ip packet solo per i pacchetti tra gli host 10.1.1.1 e 172.16.1.1.

```
<#root>
```

```
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
```

Per ulteriori informazioni sull'effetto dei comandi di debug, fare riferimento a [Informazioni importanti sui comandi di debug](#).

Consultare la sezione [Uso dei comandi di debug](#) in [Informazioni sui comandi Ping e Traceroute](#) per ulteriori informazioni sull'uso degli ACL con i comandi di debug.

Filtro degli indirizzi MAC

È possibile filtrare i frame con un indirizzo di origine o destinazione di una stazione di livello MAC specifica. Il sistema consente di configurare qualsiasi numero di indirizzi senza compromettere le prestazioni. Per filtrare i pacchetti in base all'indirizzo di livello MAC, utilizzare questo comando in modalità di configurazione globale:

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

Applicare il protocollo bridge a un'interfaccia necessaria per filtrare il traffico insieme all'elenco degli accessi creato con il comando `bridge-group <numero gruppo> {input-address-list <numero ACL> | output-address-list <numero ACL>}`:

```
<#root>
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
```

Creare un'interfaccia virtuale con bridging e applicare l'indirizzo IP assegnato all'interfaccia Ethernet fisica:

```
<#root>
```

```
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
```

Con questa configurazione, il router consente solo gli indirizzi MAC configurati sull'elenco degli accessi 700. Con il comando `access-list access-list <numero ACL> deny <indirizzo mac> 0000.0000.0000`, negare l'indirizzo MAC a cui non è possibile accedere, quindi autorizzare il resto (ad esempio, `aaaa.bbbb.ccc`).



Nota: creare ogni riga dell'elenco degli accessi per ogni indirizzo MAC.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- [Configurazione degli elenchi di accesso IP](#)
- [Pagina di supporto sugli elenchi degli accessi](#)
- [Pagina di supporto per il routing IP](#)
- [Pagina di supporto per i protocolli di routing IP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).