Configurazione e filtro degli elenchi di accesso IP

Sommario

Introduzione

In questo documento vengono descritti vari tipi di Access Control List (ACL) IP e le relative modalità di filtro del traffico di rete.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento. Quanto qui illustrato si basa sul software Cisco IOS® versione 8.3 o successive. La versione viene menzionata per ciascuna funzionalità ACL.

Componenti usati

In questo documento vengono illustrati vari tipi di ACL. Alcuni di essi sono presenti già nel software Cisco IOS versione 8.3 mentre altri sono stati introdotti in versioni più recenti. Per ciascun tipo menzionato, vengono indicate le versioni che lo usano.

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

In questo documento viene illustrato come usare gli Access Control List (ACL) di indirizzi IP per filtrare il traffico della rete. Inoltre, vengono fornite brevi descrizioni sui tipi di ACL IP, le funzionalità disponibili e un esempio di uso in rete.

> **Nota:** RFC 1700 contiene i numeri assegnati alle porte conosciute. RFC 1918 contiene l'allocazione degli indirizzi di Internet private, ossia indirizzi IP che normalmente non devono essere visualizzati su Internet.

> **Nota:** Solo gli utenti Cisco registrati possono accedere alle informazioni interne.

> **Nota:** Gli ACL possono essere usati anche per definire il traffico diretto al Network Address Translate (NAT), per criptare o filtrare i protocolli non IP, ad esempio AppleTalk o IPX. La trattazione di questi argomenti esula tuttavia dalle finalità del presente documento.

Nozioni base sugli ACL

Maschere

Le maschere vengono usate negli elenchi ACL IP per specificare quali indirizzi IP devono essere autorizzati e quali devono essere rifiutati. Le maschere usate per configurare gli indirizzi IP sulle interfacce iniziano tutte con 255, con i valori più alti posizionati a sinistra; ad esempio la maschera dell'indirizzo IP 10.165.202.129 è 255.255.255.224. Le maschere degli ACL IP sono invertite, ad esempio la maschera è 0.0.0.255. Una maschera di questo tipo viene chiamata a volte maschera inversa o wildcard mask. Quando il valore della maschera è espresso in formato binario (0 e 1), il risultato determina i bit dell'indirizzo da prendere in considerazione per elaborare il traffico. Se il valore del bit nella maschera è 0, il bit dell'indirizzo deve essere preso in considerazione (corrispondenza esatta); se il valore nella maschera è 1, il bit dell'indirizzo *può essere ignorato*. Per un esempio concreto, vedere la tabella sotto.

Esempio di maschera	
indirizzo di rete (traffico da elaborare)	*10.1.1.0*
maschera	*0.0.0.255*
indirizzo di rete (formato binario)	*00001010.00000001.00000001.00000000*
maschera (formato binario)	*00000000.00000000.00000000.11111111*

Osservando la maschera in formato binario, se ne deduce che i primi tre gruppi di bit (ottetti) devono corrispondere esattamente all'indirizzo di rete in formato binario specificato (00001010.00000001.00000001). L'ultima serie di numeri *può essere ignorata* (.1111111). Pertanto, tutto il traffico che inizia con 10.1.1. corrisponde poiché l'ultimo ottetto è *quello* che *non importa*. Con questa maschera, vengono elaborati gli indirizzi di rete da 10.1.1.1 a 10.1.1.255 (10.1.1.x).

Per determinare la maschera inversa dell'ACL, occorre sottrarre la maschera normale da 255.255.255.255. Nell'esempio, viene calcolata la maschera inversa dell'indirizzo di rete 172.16.1.0 con una maschera normale di 255.255.255.0.

- 255.255.255.255 - 255.255.255.0 (maschera normale) = 0.0.0.255 (maschera inversa)

Notare gli equivalenti ACL.

- Il valore 0.0.0.0/255.255.255.255 per source/source-wildcard equivale a **any (qualsiasi).**
- Il valore 10.1.1.2/0.0.0.0 per source/source-wildcard equivale a **host 10.1.1.2**.

Riepilogo di ACL

> **Nota:** le subnet mask possono essere rappresentate anche come notazioni a lunghezza fissa. Ad esempio, 192.168.10.0/24 sta per 192.168.10.0 255.255.255.0.

Di seguito viene spiegato come riepilogare un intervallo di reti in una singola rete per ottimizzare il funzionamento degli ACL. Prendiamo in considerazione le reti seguenti.

```
192.168.32.0/24
192.168.33.0/24
192.168.34.0/24
192.168.35.0/24
192.168.36.0/24
192.168.37.0/24
192.168.38.0/24
```

```
192.168.39.0/24
```

I primi due ottetti e l'ultimo ottetto sono uguali su tutte le reti. Nella tabella viene mostrato come riepilogare tutti questi indirizzi in un'unica rete.

Il terzo ottetto può essere scritto come mostrato nella tabella, corrispondente alla posizione dei bit dell'ottetto e al valore dell'indirizzo di ciascuno di essi.

Decimale	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

Poiché i primi cinque bit corrispondono, le otto reti precedenti possono essere riepilogate in un'unica rete (192.168.32.0/21 o 192.168.32.0 255.255.248.0). Le otto possibili combinazioni degli ultimi tre bit sono significative per i nostri intervalli di rete. Questo comando definisce un ACL che autorizza questa rete. Se si sottrae 255.255.248.0 (maschera normale) da 255.255.255.255, si ottiene 0.0.7.255.

```
access-list acl_permit permit ip 192.168.32.0 0.0.7.255
```

Per la prossima spiegazione, prendiamo in considerazione questo gruppo di reti.

```
192.168.146.0/24
192.168.147.0/24
192.168.148.0/24
192.168.149.0/24
```

I primi due ottetti e l'ultimo ottetto sono uguali su tutte le reti. La tabella spiega come riepilogarli.

Il terzo ottetto può essere scritto come mostrato nella tabella, corrispondente alla posizione dei bit dell'ottetto e al valore dell'indirizzo di ciascuno di essi.

Decimale	128	64	32	16	8	4	2	1
146	1	0	0	1	0	0	1	0
147	1	0	0	1	0	0	1	1
148	1	0	0	1	0	1	0	0
149	1	0	0	1	0	1	0	1
	M	M	M	M	M	?	?	?

A differenza dell'esempio precedente, queste reti non possono essere riepilogate in un'unica rete. Se lo fossero, la rete diventerebbe 192.168.144.0/21, a causa dei cinque bit simili presenti nel terzo ottetto. La rete 192.168.144.0/21 include una serie di reti da 192.168.144.0 a 192.168.151.0. Tra queste, le reti 192.168.144.0, 192.168.145.0, 192.168.150.0 e 192.168.151.0, che non sono nell'elenco di quattro reti fornito . Per includere le reti specifiche dell'esempio, occorre usare almeno due reti di riepilogo. Le quattro reti fornite possono essere riepilogate in queste due reti:

- Nelle reti 192.168.146.x e 192.168.147.x, tutti i bit corrispondono eccetto l'ultimo, che può essere *ignorato*. La rete può essere scritta come 192.168.146.0/23 (o 192.168.146.0

255.255.254.0).
- Nelle reti 192.168.148.x e 192.168.149.x, tutti i bit corrispondono eccetto l'ultimo, che può essere *ignorato*. La rete può essere scritta come 192.168.148.0/23 (o 192.168.148.0 255.255.254.0).

L'output mostrato di seguito definisce un ACL di riepilogo per le reti precedenti.

```
!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.146.0 to 192.168.147.254. access-list 10 permit
192.168.146.0 0.0.1.255
```

```
!--- This command is used to allow access access for devices with IP
!--- addresses in the range from 192.168.148.0 to 192.168.149.254 access-list 10 permit
192.168.148.0 0.0.1.255
```

Elaborazione degli ACL

Il traffico che entra nel router viene analizzato sulla base delle voci ACL, nell'ordine con cui le voci si presentano nel router. Le istruzioni nuove sono aggiunte alla fine dell'elenco. Il router continua a cercare finché non trova una corrispondenza. Se il router raggiunge la fine dell'elenco senza trovare una corrispondenza, il traffico viene rifiutato. Per questo motivo, le voci con più probabilità di avere una corrispondenza devono essere posizionate in cima all'elenco. Tutto il traffico che non è esplicitamente autorizzato viene rifiutato. Un ACL con un'unica voce e una sola voce di rifiuto può bloccare tutto il traffico. Ecco perché occorre avere nell'ACL almeno un'istruzione di autorizzazione, pena il blocco di tutto il traffico. I due ACL (101 e 102) riportati di seguito hanno lo stesso effetto.

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
```

```
!--- This command is used to permit IP traffic from 10.1.1.0
!--- network to 172.16.1.0 network. All packets with a source
!--- address not in this range will be rejected. access-list 102 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
access-list 102 deny ip any any
```

Nell'esempio successivo è sufficiente l'ultima voce. Le prime tre voci non sono necessarie, in quanto l'indirizzo IP include il protocollo TCP, il protocollo User Datagram Protocol (UDP) e il protocollo Internet Control Message Protocol (ICMP).

```
!--- This command is used to permit Telnet traffic
!--- from machine 10.1.1.2 to machine 172.16.1.1. access-list 101 permit tcp host 10.1.1.2 host
172.16.1.1 eq telnet
```

```
!--- This command is used to permit tcp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit tcp host 10.1.1.2
host 172.16.1.1
```

```
!--- This command is used to permit udp traffic from
!--- 10.1.1.2 host machine to 172.16.1.1 host machine. access-list 101 permit udp host 10.1.1.2
host 172.16.1.1


!--- This command is used to permit ip traffic from
!--- 10.1.1.0 network to 172.16.1.10 network. access-list 101 permit ip 10.1.1.0 0.0.0.255
172.16.1.0 0.0.0.255
```

Definizione delle porte e dei tipi di messaggio

Non solo è possibile definire l'origine e la destinazione degli ACL, ma anche le porte, i tipi di messaggi ICMP e altri parametri. Per ulteriori informazioni sulle porte conosciute, una valida fonte da consultare è la RFC 1700 . I tipi di messaggi ICMP sono spiegati nella RFC 792 .

Il router può visualizzare testo descrittivo su alcune delle porte conosciute. Per la Guida, utilizzare il punto interrogativo **?**.

```
access-list 102 permit tcp host 10.1.1.1 host 172.16.1.1 eq ?
  bgp          Border Gateway Protocol (179)
  chargen      Character generator (19)
  cmd          Remote commands (rcmd, 514)
```

Durante la configurazione, il router trasforma i valori numerici in testo più comprensibile per l'utente. In questo esempio viene digitato il numero del tipo di messaggio ICMP e il router converte il numero in un nome.

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 14
```

diventa

```
access-list 102 permit icmp host 10.1.1.1 host 172.16.1.1 timestamp-reply
```

Applicazione degli ACL

Gli ACL possono essere definiti e non applicati. Tuttavia, non possono avere alcun effetto finché non vengono applicati all'interfaccia del router. È buona norma applicare l'ACL all'interfaccia più vicina alla sorgente del traffico. Come mostrato nell'esempio, quando si cerca di bloccare il traffico da origine a destinazione, è possibile applicare un ACL in entrata su E0 sul router A anziché un elenco in uscita su E1 sul router C. Un elenco degli accessi contiene **adeny ip any** in modo implicito alla fine di un elenco degli accessi. Se il traffico è associato a una richiesta DHCP e non è autorizzato esplicitamente, viene interrotto in quanto, verificando la richiesta DHCP nell'indirizzo IP, l'indirizzo di origine risulta essere s=0.0.0.0 (Ethernet1/0), d=255.255.255.255, len 604, rcvd 2 UDP src=68, dst=67. Si noti che l'indirizzo IP di origine è 0.0.0.0 e l'indirizzo di destinazione è 255.255.25. è 68, la destinazione è 67. È quindi necessario autorizzare questo tipo di traffico nell'ACL, o il traffico verrà negato a causa del rifiuto implicito presente nell'istruzione.

> **Nota:** per consentirne la trasmissione, il traffico UDP deve essere autorizzato esplicitamente anche dall'ACL.

Definizione di entrata, uscita, in entrata, in uscita, origine e destinazione

Sui router vengono usati i termini entrata, uscita, origine e destinazione. Il traffico su un router può essere paragonato al traffico di una autostrada. Se foste un ufficiale di polizia in Pennsylvania e voleste fermare un camion che va dal Maryland a New York, l'origine del camion sarebbe il Maryland, e la destinazione del camion sarebbe New York. Potremmo creare un blocco stradale al confine tra la Pennsylvania e New York (uscita) o al confine tra il Maryland e la Pennsylvania (entrata).

Su un router, questi termini assumono i seguenti significati.

- **Uscita: il traffico che ha già attraversato il router e sta lasciando l'interfaccia.** In questo caso, l'origine è il luogo dove il traffico è già passato, ossia il lato opposto del router, la destinazione il luogo a cui è diretto.
- **Entrata: il traffico che arriva all'interfaccia per passare poi attraverso il router.** In questo caso, l'origine è il luogo dove il traffico è già passato, la destinazione il luogo a cui è diretto, ossia il lato opposto del router.
- **In entrata : se l'elenco degli accessi filtra il traffico in entrata, quando il router riceve un pacchetto, il software Cisco IOS controlla i criteri dell'elenco alla ricerca di una corrispondenza.** Se il pacchetto è autorizzato, il software continua a trasmetterlo. Se il pacchetto non è autorizzato, il software lo elimina.
- **In uscita: se l'elenco degli accessi filtra il traffico in uscita, quando il software riceve e instrada un pacchetto verso l'interfaccia di uscita, controlla i criteri dell'elenco alla ricerca di una corrispondenza.** Se il pacchetto è autorizzato, il software continua a trasmetterlo. Se il pacchetto non è autorizzato, il software lo elimina.

Nell'ACL di entrata, l'origine si trova su un segmento dell'interfaccia a cui deve essere applicato, la destinazione è esterna a tutte le altre interfacce. Nell'ACL di uscita, l'origine si trova su un segmento di un'interfaccia diversa da quella a cui verrà applicato, la destinazione è esterna all'interfaccia a cui deve essere applicato.

Modifica di ACL

Per modificare un ACL, occorre procedere con molta cautela. Ad esempio, se si intende eliminare una determinata riga da un ACL esistente con numero, come mostrato di seguito, sarà l'intero ACL a essere eliminato.

```
!--- The access-list 101 denies icmp from any to any network
!--- but permits IP traffic from any to any network. router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#access-list 101 deny icmp any any
  router(config)#access-list 101 permit ip any any
  router(config)#^Z

  router#show access-list
  Extended IP access list 101
```

```
      deny icmp any any
      permit ip any any
  router#
  *Mar  9 00:43:12.784: %SYS-5-CONFIG_I: Configured from console by console

  router#configure terminal
  Enter configuration commands, one per line.  End with CNTL/Z.
  router(config)#no access-list 101 deny icmp any any
  router(config)#^Z

  router#show access-list
  router#
  *Mar  9 00:43:29.832: %SYS-5-CONFIG_I: Configured from console by console
```

Per modificare gli ACL con numero, copiare la configurazione del router su un server TFTP o in un editor di testo, ad esempio Blocco note. Apportare quindi le modifiche desiderate e copiare nuovamente la configurazione sul router.

In alternativa, eseguire questa operazione.

```
router#configure terminal
  Enter configuration commands, one per line.
  router(config)#ip access-list extended test

!--- Permits IP traffic from 10.2.2.2 host machine to 10.3.3.3 host machine. router(config-ext-
nacl)#permit ip host 10.2.2.2 host 10.3.3.3

!--- Permits www traffic from 10.1.1.1 host machine to 10.5.5.5 host machine. router(config-ext-
nacl)#permit tcp host 10.1.1.1 host 10.5.5.5 eq www

!--- Permits icmp traffic from any to any network. router(config-ext-nacl)#permit icmp any any

!--- Permits dns traffic from 10.6.6.6 host machine to 10.10.10.0 network. router(config-ext-
nacl)#permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
  router(config-ext-nacl)#^Z
  1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

  router#show access-list
  Extended IP access list test
      permit ip host 10.2.2.2 host 10.3.3.3
      permit tcp host 10.1.1.1 host 10.5.5.5 eq www
      permit icmp any any
      permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
```

Ogni elemento eliminato viene rimosso dall'ACL, ogni elemento aggiunto viene inserito alla fine dell'ACL.

```
router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#ip access-list extended test

!--- ACL entry deleted. router(config-ext-nacl)#no permit icmp any any

!--- ACL entry added. router(config-ext-nacl)#permit gre host 10.4.4.4 host 10.8.8.8
   router(config-ext-nacl)#^Z
   1d00h: %SYS-5-CONFIG_I: Configured from console by consoles-l

   router#show access-list
   Extended IP access list test
       permit ip host 10.2.2.2 host 10.3.3.3
       permit tcp host 10.1.1.1 host 10.5.5.5 eq www
```

```
       permit udp host 10.6.6.6 10.10.10.0 0.0.0.255 eq domain
       permit gre host 10.4.4.4 host 10.8.8.8
```

Inoltre, è possibile aggiungere righe agli ACL con numero standard o estesi assegnando un numero di sequenza in Cisco IOS. Ecco un esempio della configurazione.

Configurare l'ACL esteso nel modo seguente:

```
Router(config)#access-list 101 permit tcp any any
Router(config)#access-list 101 permit udp any any
Router(config)#access-list 101 permit icmp any any
Router(config)#exit
Router#
```

Usare il comando show access-listper visualizzare le voci dell'elenco. Verranno visualizzati anche i numeri di sequenza, ad esempio 10, 20 e 30.

```
Router#show access-list
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Aggiungere la voce all'elenco degli accessi 101 con il numero di sequenza 5.

Esempio 1:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended 101
Router(config-ext-nacl)#5 deny tcp any any eq telnet
Router(config-ext-nacl)#exit
Router(config)#exit
Router#
```

Nell'output show access-listcommand, il numero di sequenza 5 è stato aggiunto come prima voce dell'elenco degli accessi 101.

```
Router#show access-list
Extended IP access list 101
    5 deny tcp any any eq telnet
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
Router#
```

Esempio 2:

```
internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any

internetrouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
internetrouter(config)#ip access-list extended 101
internetrouter(config-ext-nacl)#18 per tcp any host 172.16.2.11
```

```
internetrouter(config-ext-nacl)#^Z

internetrouter#show access-lists
Extended IP access list 101
    10 permit tcp any any
    15 permit tcp any host 172.16.2.9
    18 permit tcp any host 172.16.2.11
    20 permit udp host 172.16.1.21 any
    30 permit udp host 172.16.1.22 any
internetrouter#
```

Analogamente, è possibile configurare l'elenco degli accessi standard nel modo seguente:

```
internetrouter(config)#access-list 2 permit 172.16.1.2
internetrouter(config)#access-list 2 permit 172.16.1.10
internetrouter(config)#access-list 2 permit 172.16.1.11

internetrouter#show access-lists
Standard IP access list 2
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    10 permit 172.16.1.2

internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#25 per 172.16.1.7
internetrouter(config-std-nacl)#15 per 172.16.1.16

internetrouter#show access-lists
Standard IP access list 2
    15 permit 172.16.1.16
    30 permit 172.16.1.11
    20 permit 172.16.1.10
    25 permit 172.16.1.7
    10 permit 172.16.1.2
```

La differenza principale con l'elenco degli accessi standard consiste nel fatto che Cisco IOS aggiunge la voce dell'indirizzo IP in ordine discendente e non assegna un numero di sequenza.

Nell'esempio vengono mostrate le diverse voci per autorizzare un indirizzo IP (192.168.100.0) o le reti (10.10.10.0).

```
internetrouter#show access-lists
Standard IP access list 19
    10 permit 192.168.100.0
    15 permit 10.10.10.0, wildcard bits 0.0.0.255
    19 permit 10.101.110.0, wildcard bits 0.0.0.255
    25 deny any
```

Aggiungere la voce all'elenco degli accessi 2 per autorizzare l'indirizzo IP 172.22.1.1:

```
internetrouter(config)#ip access-list standard 2
internetrouter(config-std-nacl)#18 permit 172.22.1.1
```

Questa voce viene aggiunta in cima all'elenco in modo da dare priorità all'indirizzo IP specifico piuttosto che alla rete.

```
internetrouter#show access-lists
Standard IP access list 19
```

```
10 permit 192.168.100.0
18 permit 172.22.1.1
15 permit 10.10.10.0, wildcard bits 0.0.0.255
19 permit 10.101.110.0, wildcard bits 0.0.0.255
25 deny   any
```

Nota: gli ACL precedenti non sono supportati nelle appliance di sicurezza, ad esempio nei firewall ASA/PIX.

Linee guida per modificare gli elenchi degli accessi quando applicati alle mappe crittografiche

- Se si aggiunge la crittografia a una configurazione dell'elenco degli accessi corrente, non è necessario rimuovere la mappa crittografica. L'aggiunta diretta delle voci senza aver prima eliminato la mappa crittografica è una procedura accettabile e supportata.
- Al contrario, se si desidera modificare o eliminare delle voci da un elenco degli accessi corrente, la mappa crittografica deve essere rimossa dall'interfaccia. Dopo aver rimosso la mappa crittografica, apportare le modifiche desiderate, quindi aggiungere nuovamente la mappa crittografica. Se si eliminano voci dall'elenco degli accessi senza aver prima rimosso la mappa crittografica, i risultati sono imprevedibili in quanto questa procedura non è supportata.

Risoluzione dei problemi

Come rimuovere un ACL da un'interfaccia?

Per rimuovere un ACL dall'interfaccia, accedere in modalità configurazione e specificare **no davanti al comando access-group, come mostrato nell'esempio.**

```
interface <interface-name> no ip access-group <acl-number> {in|out}
```

Cosa fare quando viene rifiutato un volume di traffico eccessivo?

Se viene rifiutato un volume troppo elevato di traffico, riesaminare la logica dell'elenco e cercare di definire e applicare un elenco più ampio. Il comando **show ip access-lists restituisce un numero di pacchetto che mostra la voce ACL con cui è stata trovata una corrispondenza.** La parola chiave log situata alla fine di una voce dell'elenco restituisce il numero ACL e se il pacchetto è stato autorizzato o rifiutato, oltre a informazioni specifiche sulla porta.

Nota: la parola chiave log-input viene usata nel software Cisco IOS versione 11.2 e successive e in alcune versioni 11.1 create appositamente per alcuni mercati. Non è supportata sulle versioni software meno recenti. L'uso di questa parola chiave include l'interfaccia di input e l'indirizzo MAC di origine, ove applicabile.

Come eseguire il debug sui pacchetti che usano un router Cisco?

In questa procedura viene illustrato il processo di debug. Prima di iniziare, accertarsi che non vi siano ACL applicati, che un ACL sia stato definito e sia presente e che l'opzione di commutazione veloce non sia disabilitata.

Nota: procedere con estrema cautela quando si esegue il debug su sistemi interessati da traffico elevato. Per eseguire il debug del traffico, usare un ACL. Verificare prima il processo e il flusso del traffico.

1. Per acquisire i dati desiderati, usare **il** comando **access-**list.Nell'esempio, l'acquisizione dei dati è impostata sull'indirizzo di destinazione 10.2.6.6 o sull'indirizzo di origine 10.2.6.6.
   ```
   access-list 101 permit ip any host 10.2.6.6
   access-list 101 permit ip host 10.2.6.6 any
   ```

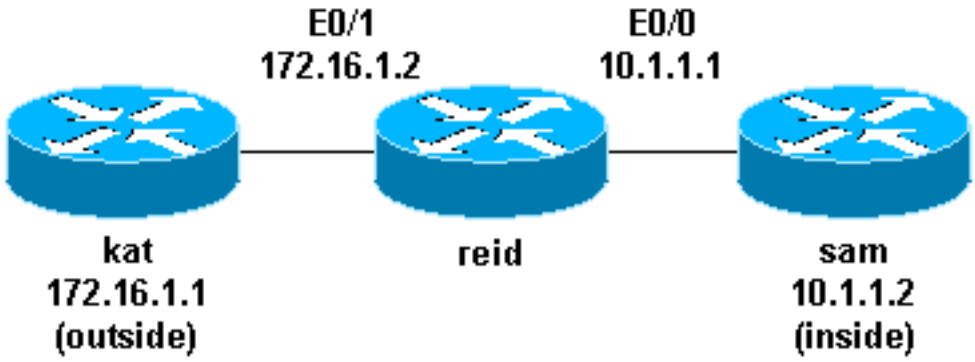
2. Disabilitare l'opzione di commutazione veloce sulle interfacce interessate. È possibile vedere il primo pacchetto solo se l'opzione di commutazione veloce non è stata disabilitata.
   ```
   configure terminal
   interface
   ```

3. Usare il comando **terminal monitor**in modalità abilitazione per visualizzare l'output del comando debug e i messaggi di errore del terminale e della sessione correnti.
4. Usare il comando **debug ip packet 101** o **debug ip packet 101 detail** per avviare il processo di debug.
5. Eseguire il comando **no debug all in modalità abilitazione e il comando interface configuration per interrompere il processo di debug.**
6. Riavviare la memorizzazione nella cache.
   ```
   configure terminal
   interface
   ```

Tipi di ACL IP

In questa sezione del documento vengono descritti i tipi di elenchi degli accessi.

Esempio di rete



ACL standard

Il primo tipo di ACL usati sono chiamati ACL standard. Risalgono al software Cisco IOS versione 8.3. Gli ACL standard controllano il traffico confrontando l'indirizzo di origine dei pacchetti IP con gli indirizzi configurati negli elenchi stessi.

Di seguito viene mostrata la sintassi del comando di un ACL standard.

```
access-list <access-list-number> {permit|deny} {host|source source-wildcard|any}
```

In tutte le versioni software, il valore *access-list-number* può essere un numero compreso tra 1 e 99. Nel software Cisco IOS versione 12.0.1, gli ACL standard hanno iniziato a usare altri numeri (da 1300 a 1999). Gli ACL che usano questi numeri aggiuntivi sono chiamati ACL IP espansi. Dal software Cisco IOS versione 11.2, è possibile usare *testo descrittivo negli ACL standard.*

Si può impostare *s source/source-wildcard* per 0.0.0.0/255.255.255.255 sul valore any (**qualsiasi)**. Se tutti i numeri sono 0, è possibile omettere la wildcard mask. Pertanto, l'host 10.1.1.2 0.0.0.0 è uguale all'host 10.1.1.2.

Dopo aver definito l'ACL, occorre applicarlo all'interfaccia (in entrata o in uscita). Nelle prime versioni del software, se la direzione non era specificata, per impostazione predefinita veniva usata la direzione in uscita (out). Nelle versioni successive, la direzione deve essere specificata dall'utente.

```
interface <interface-name>
 ip access-group number {in|out}
```

Di seguito viene riportato un esempio d'uso di un ACL standard per bloccare tutto il traffico eccetto quello proveniente da indirizzi di tipo 10.1.1.x.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 1 in
!
access-list 1 permit 10.1.1.0 0.0.0.255
```

ACL estesi

Gli ACL estesi sono stati introdotti nel software Cisco IOS versione 8.3. Gli ACL estesi controllano il traffico confrontando gli indirizzi di origine e di destinazione dei pacchetti IP con gli indirizzi configurati negli elenchi stessi.

Di seguito viene mostrata la sintassi del comando degli ACL estesi. Nell'esempio, le righe vanno a capo per motivi di spazio.

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]
```

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]
```

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]
```

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]
```

In tutte le versioni software, il valore *access-list-number* può essere un numero compreso tra 100 e 199. Nel software Cisco IOS versione 12.0.1, gli ACL estesi hanno iniziato a usare altri numeri (da 2000 a 2699). Gli ACL che usano questi numeri aggiuntivi sono chiamati ACL IP espansi. Dal software Cisco IOS versione 11.2, è possibile usare *testo descrittivo negli ACL estesi.*

Il valore di 0.0.0.0/255.255.255.255 può essere impostato su **any (qualsiasi).** Dopo aver definito l'ACL, occorre applicarlo all'interfaccia (in entrata o in uscita). Nelle prime versioni del software, se la direzione non era specificata, per impostazione predefinita veniva usata la direzione in uscita (out). Nelle versioni successive, la direzione deve essere specificata dall'utente.

```
interface <interface-name>
 ip access-group {number|name} {in|out}
```

Questo ACL esteso è usato per autorizzare il traffico sulla rete 10.1.1.x (interna). Inoltre, permette di ricevere risposte ping dall'esterno e di bloccare ping non richiesti da utenti esterni alla rete, autorizzando tutto il resto del traffico.

```
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group 101 in
!
access-list 101 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 101 permit ip any 10.1.1.0
0.0.0.255
```

> **Nota:** in alcune applicazioni, ad esempio la gestione della rete, è necessario poter ricevere i ping per le funzioni keepalive. In questo caso, è possibile limitare i ping in entrata che vengono bloccati o essere più granulari negli IP consentiti/negati.

Lock and Key (ACL dinamici)

La funzionalità Lock and Key, nota anche come ACL dinamici, è stata introdotta nel software Cisco IOS versione 11.1. Questa funzionalità dipende dalla modalità Telnet, dall'autenticazione (locale o remota) e dagli ACL estesi.

La configurazione della funzionalità Lock and Key inizia con l'applicazione di un ACL esteso che blocchi il traffico sul router. Gli utenti che vogliono passare attraverso il router vengono bloccati dall'ACL esteso finché non si collegano in modalità Telnet e non vengono autenticati. La connessione Telnet viene quindi interrotta e un ACL dinamico con un'unica voce viene aggiunto all'ACL esteso esistente. Il traffico viene autorizzato sul router per un determinato periodo di tempo, in cui è possibile avere timeout di inattività e assoluti.

Di seguito viene riportata la sintassi del comando che permette di configurare la funzione Lock and Key con l'autenticazione locale.

```
username <user-name> password <password>
!
interface <interface-name>
 ip access-group {number|name} {in|out}
```

L'ACL con un'unica voce di questo comando viene aggiunto dinamicamente all'ACL esistente dopo l'autenticazione.

```
access-list access-list-number dynamic name {permit|deny} [protocol]
{source source-wildcard|any} {destination destination-wildcard|any}
[precedence precedence][tos tos][established] [log|log-input]
[operator destination-port|destination port]

line vty <line_range>
login local
```

Questo è un esempio semplice della funzionalità Lock and Key.

```
username test password 0 test

!--- Ten (minutes) is the idle timeout. username test autocommand access-enable host timeout 10
!
interface Ethernet0/0
  ip address 10.1.1.1 255.255.255.0
  ip access-group 101 in
!
access-list 101 permit tcp any host 10.1.1.1 eq telnet

!--- 15 (minutes) is the absolute timeout. access-list 101 dynamic testlist timeout 15 permit ip
10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
!
line vty 0 4
 login local
```

L'ACL dinamico viene applicato dopo che l'utente dell'indirizzo 10.1.1.2 effettua una connessione Telnet all'indirizzo 10.1.1.1. La connessione viene quindi interrotta e l'utente può accedere alla rete 172.16.1.x.

ACL IP con nome

Gli ACL IP con nome sono stati introdotti nel software Cisco IOS versione 11.2. È quindi possibile usare ACL standard ed estesi con nome anziché con numero.

Di seguito viene mostrata la sintassi del comando degli ACL IP con nome.

```
ip access-list {extended|standard} name
```

Questo è un esempio di TCP:

```
{permit|deny} tcp source source-wildcard [operator [port]] destination destination-wildcard
[operator [port]] [established] [precedence precedence] [tos tos] [log] [time-range time-range-
name]
```

Questo è un esempio di come usare un ACL con nome per bloccare tutto il traffico eccesso la connessione Telnet tra l'host 10.1.1.2 e l'host 172.16.1.1.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group in_to_out in
!
ip access-list extended in_to_out
 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

ACL riflessivi

Gli ACL riflessivi sono stati introdotti nel software Cisco IOS versione 11.3. Gli ACL riflessivi permettono di filtrare i pacchetti IP in base alle informazioni sulla sessione di livello superiore. In genere vengono utilizzati per autorizzare il traffico in uscita e limitare il traffico in entrata in risposta a sessioni che hanno avuto origine all'interno del router.

Gli ACL riflessivi possono essere definiti solo con ACL IP estesi con nome. Non possono essere definiti con ACL IP con numero o ACL IP standard con nome o con altri tipi di ACL. È possibile usare gli ACL riflessivi insieme ad altri ACL estesi standard e statici.

Questa è la sintassi del comando degli ACL riflessivi.

```
interface <interface-name>
 ip access-group {number|name} {in|out}
!
ip access-list extended <name>
 permit protocol any any reflect name [timeoutseconds]
!
ip access-list extended <name>
 evaluate <name>
```

Nell'esempio, viene mostrato come autorizzare il traffico ICMP in entrata e in uscita, autorizzando solo il traffico TCP che ha avuto origine all'interno; il traffico di altro tipo viene rifiutato.

```
ip reflexive-list timeout 120
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip access-group inboundfilters in
 ip access-group outboundfilters out
!
ip access-list extended inboundfilters
 permit icmp 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 evaluate tcptraffic

!--- This ties the reflexive ACL part of the outboundfilters ACL,
!--- called tcptraffic, to the inboundfilters ACL. ip access-list extended outboundfilters
 permit icmp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 reflect tcptraffic
```

ACL con limiti di tempo e uso degli intervalli

Gli ACL con limiti di tempo sono stati introdotti nel software Cisco IOS versione 12.0.1.T. Sebbene simili agli ACL estesi già in uso, gli ACL con limiti di tempo permettono di controllare gli accessi sulla base di intervalli temporali. Vengono quindi definiti alcuni intervalli di tempo che regolamentano gli orari del giorno e della settimana in cui questi ACL devono essere applicati. L'intervallo di tempo è identificato da un nome e richiamato quindi da una funzione. Le restrizioni temporali vengono applicate alla funzione stessa. L'intervallo di tempo è sincronizzato con l'orologio di sistema del router. Si potrebbe usare anche l'orologio del router, ma la sincronizzazione Network Time Protocol (NTP) offre risultati migliori.

Questi sono comandi di ACL con limiti di tempo.

```
!--- Defines a named time range. time-range time-range-name

!--- Defines the periodic times. periodic days-of-the-week hh:mm to [days-of-the-week] hh:mm

!--- Or, defines the absolute times. absolute [start time date] [end time date]

!--- The time range used in the actual ACL. ip access-list name|number time-rangename_of_time-
range
```

Nell'esempio, una connessione Telnet viene autorizzata dalla rete interna verso l'esterno nei giorni di lunedì, mercoledì e venerdì, durante l'orario di lavoro:

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
EVERYOTHERDAY
!
time-range EVERYOTHERDAY
 periodic Monday Wednesday Friday 8:00 to 17:00
```

Voci ACL IP con commento

Le voci ACL IP con commento sono state introdotte nel software Cisco IOS versione 12.0.2.T. I

commenti semplificano la comprensione degli ACL e possono essere utilizzati per ACL IP standard o estesi.

Questa è la sintassi del comando degli ACL IP con nome e con commento.

```
ip access-list {standard|extended} <access-list-name> remark remark
```

Questa è la sintassi del comando degli ACL IP con numero e con commento.

```
access-list <access-list-number> remark remark
```

Questo è un esempio di commenti all'interno di un ACL con numero.

```
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip access-group 101 in
!
access-list 101 remark permit_telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
```

Controllo degli accessi basato sul contesto

Il controllo degli accessi basato sul contesto (CBAC) è stato introdotto nel software Cisco IOS versione 12.0.5.T e richiede una serie di funzionalità di Cisco IOS Firewall. La funzione CBAC controlla il traffico che attraversa il firewall per individuare e gestire le informazioni sullo stato relative alle sessioni TCP e UDP. Queste informazioni sullo stato vengono usate per creare varchi temporanei negli elenchi degli accessi del firewall. Configurare gli elenchi di controllo IP nella direzione del flusso del traffico iniziale in modo da consentire traffico di ritorno e altre connessioni dati di sessioni autorizzate, ossia sessioni originate nella rete interna protetta.

Questa è la sintassi della funzione CBAC.

```
ip inspect name inspection-name protocol [timeoutseconds]
```

Questo è un esempio di come usare la funzione CBAC per controllare il traffico in uscita. L'ACL esteso 111 in genere blocca il traffico di ritorno diverso dal traffico ICMP senza che la funzione CBAC debba aprire dei varchi per il traffico di ritorno.

```
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw tcp timeout 3600
ip inspect name myfw udp timeout 3600
ip inspect name myfw tftp timeout 3600
! interface Ethernet0/1 ip address 172.16.1.2 255.255.255.0 ip access-group 111 in ip inspect
myfw out !
access-list 111 deny icmp any 10.1.1.0 0.0.0.255 echo access-list 111 permit icmp any 10.1.1.0
0.0.0.255
```

Proxy di autenticazione

Il proxy di autenticazione è stato introdotto nel software Cisco IOS versione 12.0.5.T. È quindi necessario disporre del gruppo di funzionalità di Cisco IOS Firewall. Il proxy di autenticazione viene usato per autenticare gli utenti in entrata o in uscita, o entrambi. Gli utenti che normalmente sono bloccati da un ACL possono configurare il browser in modo che ignori il firewall e venga autenticato su un server TACACS+ o RADIUS. Il server comunica al router altre voci ACL in modo da permettere il passaggio del traffico dopo l'autenticazione.

Il proxy di autenticazione ha una logica simile alla funzione Lock and Key (ACL dinamici). Queste sono le differenze:

- La funzione Lock and Key viene attivata da una connessione Telnet al router. Il proxy di autenticazione viene attivato dal protocollo HTTP tramite il router.
- Il proxy di autenticazione deve utilizzare un server esterno.
- Il proxy di autenticazione può gestire l'aggiunta di più elenchi dinamici. La funzione Lock and Key può aggiungere un solo elenco.
- Il proxy di autenticazione ha un timeout assoluto ma non ha timeout di inattività. La funzione Lock and Key ha entrambi.

Per esempi sul proxy di autenticazione, consultare la guida alla configurazione di Cisco Secure Integrated Software.

ACL turbo

Gli ACL turbo sono stati introdotti nel software Cisco IOS versione 12.1.5.T e si trovano solo sui router 7200, 7500 e altre piattaforme avanzate. La funzionalità turbo è stata progettata per eseguire gli ACL in modo più efficiente e migliorare le prestazioni del router.

Usare il comando **access-list compiled per gli ACL turbo.** Di seguito viene riportato un esempio di ACL compilato.

```
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq telnet
access-list 101 permit tcp host 10.1.1.2 host 172.16.1.1 eq ftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq syslog
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq tftp
access-list 101 permit udp host 10.1.1.2 host 172.16.1.1 eq ntp
```

Dopo aver definito l'ACL standard o esteso, usare il comando di **configurazione globaleper compilarlo.**

```
!--- Tells the router to compile. access-list compiled
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0

!--- Applies to the interface.  ip access-group 101 in
```

Il comando **show access-list compiled mostra le statistiche sull'ACL.**

ACL con limiti di tempo distribuiti

Gli ACL con limiti di tempo distribuiti sono stati introdotti nel software Cisco IOS versione 12.2.2.T per implementare gli ACL con limiti di tempo sui router serie 7500 con abilitazione VPN. Prima dell'introduzione degli ACL con limiti di tempo distribuiti, gli ACL con limiti di tempo non erano

supportati sulle schede di linea dei router Cisco serie 7500. Se gli ACL con limiti di tempo sono stati configurati, si comportano come ACL normali. Se l'interfaccia di una scheda di linea è stata configurata con ACL con limiti di tempo, i pacchetti commutati nell'interfaccia non vengono distribuiti sulla scheda di linea come commutati ma vengono inoltrati al processore di routing per essere elaborati.

La sintassi degli ACL con limiti di tempo distribuiti è simile a quella degli ACL con limiti di tempo, l'unica differenza riguarda i comandi sullo stato dei messaggi Inter Processor Communication (ICP) scambiati tra il processore di routing e la scheda di linea.

```
debug time-range ipc
show time-range ipc
clear time-range ipc
```

Receive ACL

I receive ACL vengono usati per aumentare la sicurezza sui router Cisco 12000 usando la protezione del Gigabit Route Processor (GRP) del router per bloccare il traffico non necessario o potenzialmente dannoso. I receive ACL sono stati aggiunti come funzionalità speciale nel software Cisco IOS versione 12.0.21S2 e sono stati integrati nella versione 12.0(22)S. Per ulteriori informazioni, fare riferimento al documento GSR: receive Access Control List.

ACL di protezione infrastruttura

Questi ACL di protezione vengono usati per ridurre al minimo i rischi e l'efficacia di attacchi diretti all'infrastruttura permettendo esplicitamente solo il traffico autorizzato ai dispositivi dell'infrastruttura e tutto il resto del traffico di transito. Per ulteriori informazioni, fare riferimento al documento sulla protezione del core: Access Control List di protezione dell'infrastruttura.

ACL transit

Gli ACL transit vengono usati per aumentare la sicurezza della rete in quanto autorizzano esplicitamente solo il traffico necessario per la rete o le reti interessate. Per ulteriori informazioni, fare riferimento al documento Access Control List transit: filtraggio sul perimetro della rete.

Informazioni correlate

- Configurazione degli ACL di indirizzi IP più utilizzati
- RFC 1700
- RFC 1918
- Pagina di supporto sugli elenchi degli accessi
- Cisco IOS Firewall
- 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).