Access Control List Tutorial

L'Access control list (ACL) fornisce un metodo per filtrare pacchetti. Consente ad un amministratore di rete di autorizzare o impedire il passaggio dei pacchetti IP attraverso una specificata interfaccia del router. Le ACL si comportano come un guardiano che controlla i biglietti: fa passare solo le persone in possesso del biglietto.

L'Access Control list filtra il traffico di rete controllando se i pacchetti che giungono alle interfacce del router rispettano i requisiti specificati.

Per usare le ACL, l'amministratore di sistema deve:

1) configurare le ACL
2) applicarle a specifiche interfacce.

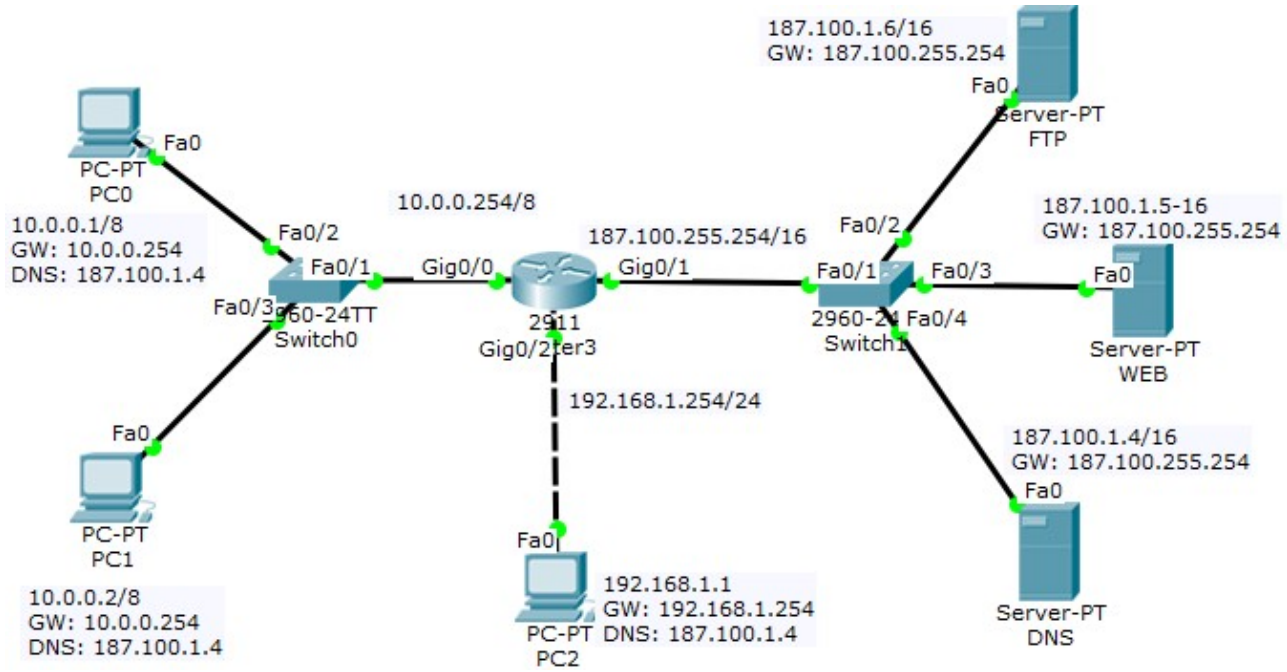
Esistono tre tipi di ACL: Standard, Extended e Named ACL.

Standard IP Access List

Le Standard IP list (1-99) controllano solo gli indirizzi sorgenti di tutti i pacchetti IP.

Configurazione	**access-list** *access-list-number* {permit | deny} *source* {source-mask}
Applicare l'ACL ad una interfaccia	**ip access-group** *access-list-number* {in | out}

Esempio di Standard IP Access List



Dopo aver realizzato la rete e configurato i dispositivi, verificare la connettività tra i PC delle due sottoreti con i server.

Configurazione:

in questo esempio si definirà una standard access list che autorizza solo la rete 10.0.0.0/8 ad accedere al server (situato sull'interfaccia Gig0/1)

Definire quale sorgente è autorizzata a passare:

```
Router(config)# access-list 1 permit 10.0.0.0 0.255.255.255
```

(alla fine di qualsiasi ACL, c'è sempre una negazione implicita per tutto il traffico restante, quindi non è necessario definire il traffico vietato)

Applicare questa ACL ad una interfaccia:

```
Router(config)# interface Giga0/1
Router(config-if)# ip access-group 1 out
```

L'ACL 1 viene applicata per consentire solo ai pacchetti provenienti da 10.0.0.0/8 di attraversare l'interfaccia Giga0/1 e nega tutto il restante traffico. Si può applicare questa ACL ad altre interfacce?, ad esempio a Giga0/0. Si può, ma è sconsigliato, perché gli utenti potrebbero accedere al server da altre interfacce. Per questo motivo una ACL standard deve essere applicata all'interfaccia vicina alla destinazione.

Nota: "0.255.255.255" è la wildcard mask che appartiene alla rete "10.0.0.0". Verrà descritta in seguito.

Verificare nuovamente la connettività tra i PC delle due sottoreti, verso il server. Questa volta il router blocca i pacchetti ping uscenti verso il server e provenienti dalla sottorete diversa da 10.0.0.0/8.

Eliminare l'ACL:

```
Router(config-if)# no access-list 1
```

Extended IP Access List

Le Extended IP list (100-199) controllano entrambi gli indirizzi, sorgente e destinazione, specificati nei protocolli UDP, TCP o IP e le porte di destinazione.

Sintassi di Configurazione

```
access-list access-list-number {permit | deny} protocol source {source-mask}
destination {destination-mask} [eq destination-port]
```

Esempio di Extended IP Access List

In questo esempio si crea una extended ACL che blocca il traffico FTP proveniente dalla rete 10.0.0.0/8 ma autorizza il passaggio del traffico restante.

Nota: FTP si appoggia su TCP ed usa le porte 20 e 21.

Definire i protocolli, la sorgente, la destinazione e la porta da negare:

```
Router(config)# access-list 101 deny tcp 10.0.0.0 0.255.255.255
187.100.1.6 0.0.0.0 eq 21
Router(config)# access-list 101 deny tcp 10.0.0.0 0.255.255.255
187.100.1.6 0.0.0.0 eq 20
Router(config)# access-list 101 permit ip any any
```

Applicare questa ACL ad una interfaccia:

```
Router(config)# interface Giga0/1
Router(config-if)# ip access-group 101 out
```

Notare che, con la riga `access-list 101 permit ip any any`, si autorizza esplicitamente il restante traffico perché alla fine di ogni ACL c'è un comando "`deny all`".

Per leggere le regole inserite, usare il comando

```
Router# show access-lists
```

La destinazione della access list è "`187.100.1.6 0.0.0.0`" che specifica un host. Si potrebbe usare anche "`host 187.100.1.6`", senza aggiungere la wildcard mask.

Abilitare il servizio ftp sul server, specificando un account utente, oppure accettare quello di default: username: `cisco`, password: `cisco`.

Aprire la scheda desktop su un client della rete 10.0.0.0/8 e verificare che la connessione viene rifiutata.

Aprire il prompt dei comandi nella scheda desktop su un client della rete 192.168.1.0/24 e verificare che la connessione viene accettata. Il prompt cambia in `ftp>`. Leggere il contenuto della cartella corrente digitando `dir`.

Aprire la scheda Desktop del PC della sottorete 192.168.1.0/24. Aprire il Text Editor e creare un file con un testo generico. Salvarlo con nome "esempio.txt". Chiudere il text editor ed aprire la scheda "Prompt dei comandi". Collegarsi al server ftp: `ftp 187.100.1.6`. Trasferire il file: `ftp> put esempio.txt` (il nome del file è case sensitive).

Da un altro computer della stessa sottorete scaricare il file: `ftp> get esempio.txt`.

Rimuovere il file: **`ftp> delete esempio.txt`**.

Come riepilogo, il range delle access list standard ed extended è:

Access list type	Range
Standard	1-99, 1300-1999
Extended	100-199, 2000-2699

Dove specificare le access list?

Le Standard IP access list devono essere memorizzate sull'interfaccia vicina alla destinazione.

Le Extended IP access list devono essere memorizzate sull'interfaccia vicina alla sorgente..

Quante access list servono?

Si deve specificare una access-list per protocollo, per direzione e per interfaccia. Ad esempio, non si possono specificare due access list in entrata sull'interfaccia Fa0/0. Si può specificare una Access List in entrata ed una in uscita, applicate alla stessa interfaccia Fa0/0.

Uso della wildcard mask

Le Wildcard mask sono usate con le ACL per specificare un host, una sottorete o parte di una rete.

Gli zero e gli uno in una wildcard determinano se i bit corrispondenti nell'indirizzo IP devono essere considerati o ignorati dalla ACL. Ad esempio, se si vuole creare una standard ACL che autorizza il passaggio dei soli pacchetti della rete 172.23.16.0/20, si deve scrivere l'ACL come la seguente:

```
access-list 1 permit 172.23.16.0 255.255.240.0
```

In una ACL non si può scrivere la subnet mask, si devono complementare tutti i bit.

255 = 1111 1111 -> si converte in 0000 0000

240 = 1111 0000 -> si converte in 0000 1111

0 = 0000 0000 -> si converte in 1111 1111

Quindi 255.255.240.0 può essere scritto nella wildcard mask come 00000000.00000000.00001111.11111111 = 0.0.15.255

In pratica, nella wildcard mask, i bit **1 significano NON IMPORTA, e i bit 0 significa IMPORTA**. Con questa precisazione, la wildcard mask può essere interpretata come segue:

I bit dei primi due byte sono tutti 0, quindi i corrispondenti bit dell'indirizzo IP da considerare sono **172.23**.x.x. I bit del terzo byte (15) hanno i valori 0000 1111, per intendere che si devono considerare i primi 4 bit e ignorare gli altri 4. Quindi il terzo byte dell'indirizzo IP, in binario, ha la forma: 0001xxxx (minimo:0001**0000** = 16; massimo: 0001**1111** = 31).

Esempio 2.

L'indirizzo del server Web è 187.100.1.5. Per sapere quale interfaccia del router è collegata al server web dare il comando:

```
Router> ena
Router# show running-config
```

Si ottiene un output su più pagine. Per avanzare da una pagina alla successiva premere il tasto spazio, fino a quando si trova la sezione:

```
interface GigabitEthernet0/1
      ip address 187.100.255.254 255.255.0.0
      ip access-group 101 out
      duplex auto
      speed auto
```

questo output conferma che la sottorete 187.100.0.0/16 è collegata all'interfaccia Giga0/1.

Verificare che esiste connettività tra tutti i PC verso il server web. Aprire la scheda desktop di un PC nella sottorete 10.0.0.0/8 e cliccare sull'icona del browser. Nella barra dell'indirizzo scrivere 187.100.1.5 per accertarsi che il server web risponde.

Ripetere la verifica con un PC della sottorete 192.168.1.0/24.

Si deve creare una access-list ed applicarla all'interfaccia connessa al Server perché può filtrare il traffico.

```
Router# conf terminal
```

L'access-list deve consentire all'host 192.168.1.1 di accedere al server Web 187.100.1.5 (port 80).

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 100 permit tcp host 192.168.1.1 host
187.100.1.5 eq 80
```

Negare a tutti gli altri host di accedere al server Web.

```
Router(config)# access-list 100 deny tcp any host 187.100.1.5 eq 80
```

Tutto il restante traffico è permesso

```
Router(config)# access-list 100 permit ip any any
```

Applicare questa access-list all'interfaccia Fa0/1 (per i pacchetti uscenti)

```
Router(config)# interface gig0/1
Router(config-if)# ip access-group 100 out
Router(config-if)#
```

Notare: l'access-list si applica all'interfaccia Giga0/1 (non alle interfacce Giga0/0 e Giga0/2) in modo che l'access-list possa filtrare il traffico entrante dalle ret1 10.0.0.0/8 e 192.168.1.0/24. Se l'access list viene applicata in entrata ad una delle altre interfacce si può solo filtrare il traffico di una rete LAN.

Aprire il browser dell'host 192.168.1.1. Nella barra dell'indirizzo scrivere **http://187.100.1.5** per verificare se è consentito o no l'accesso al ServerWeb. Se la configurazione è corretta si riesce ad accedere.

Ripetere la stessa operazione per gli altri host ed accertarsi che non è possibile accedere al Server Web.

Infine, salvare la configurazione

```
Router (config-if)# end
Router # copy running-config startup-config
```

Questa configurazione impedisce solo agli host di accedere al Server Web ma, se questo server è abilitato anche per altro traffico, FTP, SMTP ecc. allora gli altri host possono accedere).

Per esercizio, provare a consentire ad uno degli altri host di accedere al Server Web.

Alcune modifiche:

Modifica 1 (Mod 1):

permettere all'host di accedere al server web	`access-list 100 permit ip host 192.168.1.1 host 187.100.1.1`
negare all'host l'accesso ad altri server (non l'intera rete)	`access-list 100 deny ip host 192.168.1.1 187.100.1.16 0.0.0.15`
Altrimenti permettere qualsiasi altra operazione	`access-list 100 permit ip any any`

Modifica 2 (Mod 2):

Permettere solo ad un altro Host di accedere al financial server	`access-list 100 permit ip host 10.0.1.2 host 187.100.1.5`
Non permettere a nessuno di comunicare con il server web	`access-list 100 deny ip any host 187.100.1.5`
Permettere il restante traffico	`access-list 100 permit ip any any`

Nota: non dimenticare di applicare questa access list all'interfaccia corretta

```
interface giga0/1
ip access-group 100 out
```

Nota: dopo aver scritto tutti i comandi precedentemente elencati, inviando un "ping" da uno degli host PC0, PC1, PC3 il Server web può rispondere perché è stato filtrato solo il traffico HTTP, non il traffico ICMP. Per generare traffico HTTP, selezionare "Web Browser" nella scheda "Desktop" dei PC. Quando si apre il browser, scrivere l'indirizzo IP del Server web per vedere il traffico in Simulation Mode.

Notare anche che, nella configurazione iniziale, le sottoreti possono inviare pacchetti ping al Server web. Creare una ACL per filtrare anche questo traffico.