Introduzione alle Access Control List

I Router CISCO sono in grado di svolgere funzioni proprie di un firewall, in particolare possono filtrare il traffico dei pacchetti in transito applicando le cosiddette ACL = Access Control List.

Si tratta di liste di regole che permettono e/o negano il transito dei pacchetti sulla base degli indirizzi IP e dei port number di origine e di destinazione dei pacchetti stessi.

C'è una sintassi STANDARD che prevede solo la specificazione dell'indirizzo IP del mittente del pacchetto e una sintassi EXTENDED che prevede la specificazione dell'indirizzo IP e del port number sia del mittente che del destinatario. Data la loro maggiore versatilità conviene solitamente utilizzare le ACL EXTENDED.

Le ACL vengono dichiarate a livello di configurazione globale del router con il comando **access-list**. Esse sono identificate da un numero che per quelle standard va da 1 a 99 e per quelle estese da 100 a 199.

La sintassi delle ACL EXTENDED è sostanzialmente la seguente:

Router(config)# access-list *numero* permit/deny *protocollo mittente destinatario*

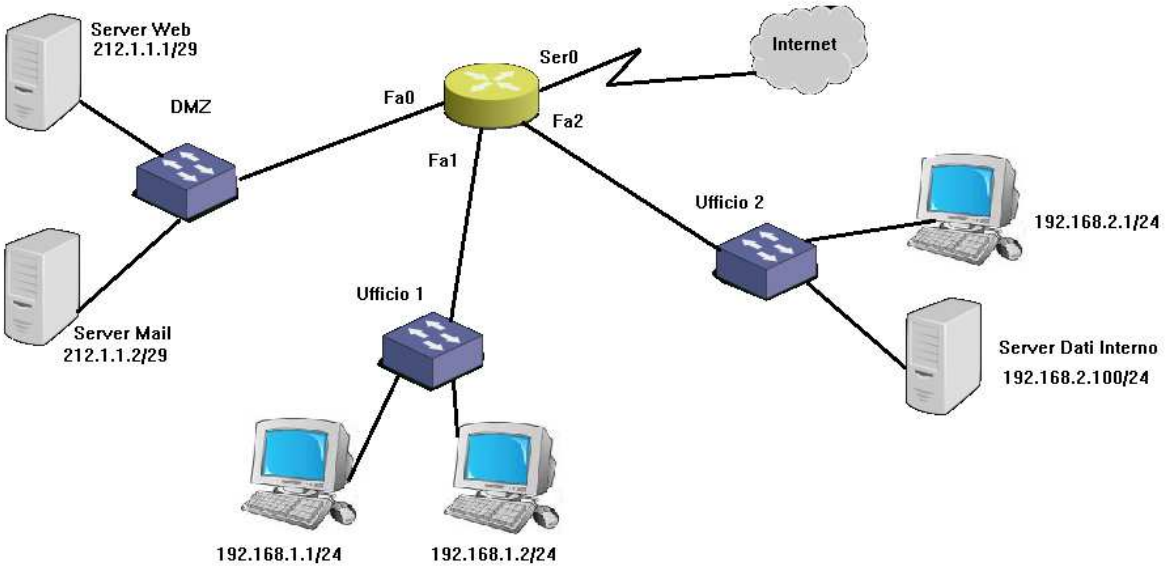
dove il protocollo può essere: ip, icmp (per filtrare ping e traceroute), tcp, udp

Dopo avere dichiarato le regole che costituiscono una ACL, la si deve associare ad una interfaccia del router specificando se essa va a filtrare il traffico in ingresso (in) o in uscita (out) rispetto al router stesso.

Per esempio con i seguenti comandi si applica la ACL di numero 101 in ingresso all'interfaccia Fa0:

Router(config)# interface Fa0
Router(config-if)# ip access-group 101 in

Per comprendere il funzionamento delle ACL conviene applicarle ad una situazione tipica come la seguente:



Una tipica rete aziendale

Vengono ora proposte alcune esigenze di filtraggio del traffico da soddisfare con opportune ACL.

Un Filtro per il server dati interno

Si vuole limitare l'accesso al server dati interno consentendone l'accesso solo ai pc dei due uffici.

La prima difficoltà è quella di ***interpretare correttamente il significato della richiesta*** e le sue implicazioni: se nessun altro al di fuori dei pc dei due uffici può entrare nel server, allora neanche le richieste di aggiornamento software inviate in Internet dal server possono ricevere risposta!

Poi si deve decidere se sia più opportuno applicare una logica del tipo "black list" = elencare gli accessi non desiderati e poi consentire tutti gli altri oppure "white list" = elencare gli accessi desiderati e poi impedire tutti gli altri.

Si propone la seguente **ACL STANDARD** che assegna il permesso di passare a tutto il traffico proveniente dai pc della rete 192.168.1.0

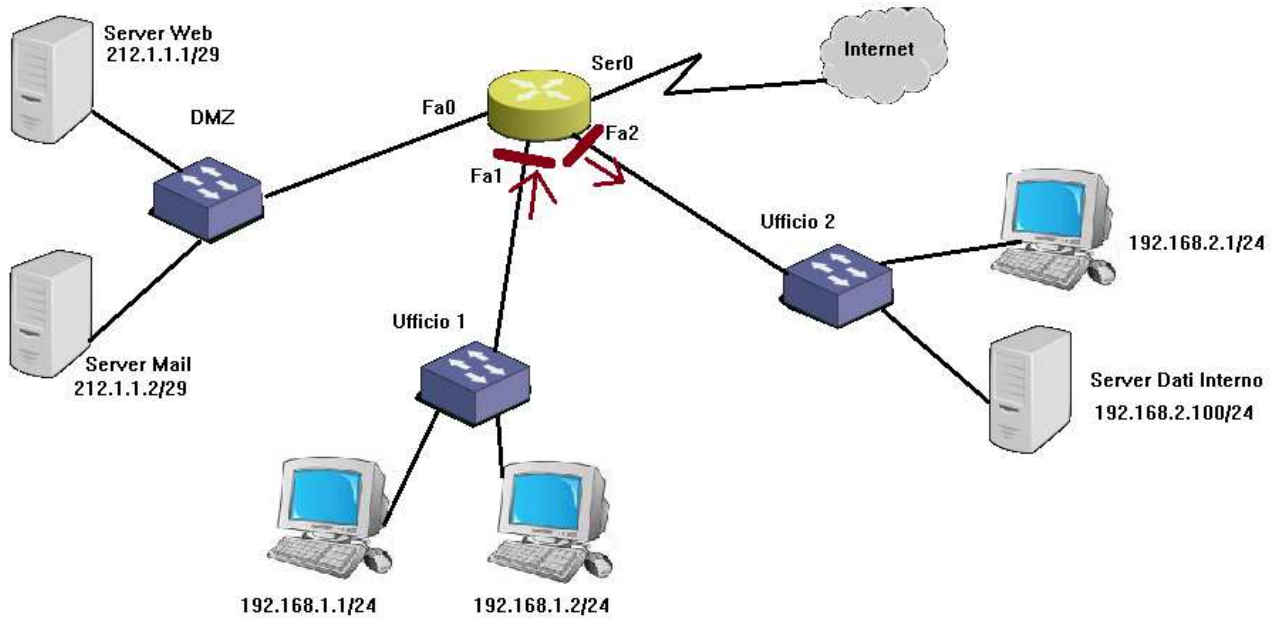
```
R(config)# access-list  1  permit  192.168.1.0  0.0.0.255
R(config)# access-list  1  deny  any
```

Si noti l'uso della wildcard mask 0.0.0.255 per specificare che la regola richiede una corrispondenza (matching) dei primi 3 valori dell'indirizzo IP specificato ➔ la maschera prevede 0 per richiedere la corrispondenza di valore e 255 per lasciare indeterminato il corrispondente valore (la maschera funziona al contrario di una subnetmask).

La seconda regola nega l'accesso a tutti gli altri pacchetti. Questa regola di negazione viene aggiunta automaticamente in maniera implicita a tutte le ACL, tuttavia per questioni di maggiore chiarezza conviene sempre scriverla in modo esplicito per evitare fraintendimenti e considerazioni errate.

La validità di tale ACL è essenzialmente determinata dalla sua collocazione:

1) Se la ACL 1 viene messa in ingresso (in) nell'interfaccia Fa1 allora viene permesso a tutto il traffico proveniente dall'ufficio 1 di andare ovunque, anche nel server dati ma non solo ➔ non c'è nessun impedimento di traffico verso il server dati!
2) Se la ACL 1 viene messa in uscita (out) dall'interfaccia Fa2 allora viene consentito l'accesso alla rete dell'ufficio 2 solo ai pc dell'ufficio 1 ➔ non si riesce a distinguere tra le diverse destinazioni all'interno dell'ufficio 2 e quindi anche l'accesso al pc viene interdetto allo stesso modo del server dati!



Dopo aver constato che in questo caso con una ACL STANDARD non risulta possibile filtrare il traffico secondo le esigenze, si propone una **ACL EXTENDED**, la quale consente di specificare anche il destinatario del pacchetto:

```
R(config)# access-list  101  remark   accesso al server dati interno

R(config)# access-list  101  permit  ip  192.168.1.0  0.0.0.255    host  192.168.2.100
R(config)# access-list  101  deny    ip   any    host 192.168.2.100
R(config)# access-list  101  permit  ip  any    any
```

Si noti che si devono attentamente alternare il permesso di accesso al server dati da parte dei pc dell'ufficio 1 e la negazione dell'accesso a tale server da parte di chiunque altro ed infine il permesso di accesso da parte di chiunque a qualunque altro pc ➔ l'ordine di scrittura delle regole di una ACL è molto importante perché ne determina l'ordine di applicazione!

Conviene solitamente iniziare una access list con un commento descrittivo (remark) per ricordarne il significato!

Scritture equivalenti (ma più facili da leggere!)

La scrittura **host** 192.168.2.100 equivale a 192.168.2.100 0.0.0.0
mentre la scrittura **any** equivale a 0.0.0.0 255.255.255.255

La suddetta ACL viene collocata opportunamente in uscita dall'interfaccia Fa2 del router:

```
R(config)# interface Fa2
R(config-if)# ip  access-group 101 out
R(config-if)# exit
```

Un filtro per la DMZ

Il traffico proveniente da Internet può entrare liberamente nella DMZ (DeMilitarized Zone) ma solo nelle porte 80 e 443 del server web (per i protocolli http e https) e 25 e 110 del server mail (per i protocolli smtp e pop3).

Devono poter passare anche le risposte provenienti dai server DNS interrogati per risolvere i nomi dei siti da visitare (protocollo udp oppure tcp con porta numero 53).

Si deve anche consentire il passaggio dei pacchetti provenienti da Internet in risposta a richieste inviate dai pc della rete aziendale ➔ si tratta di pacchetti tcp facenti parte di una connessione logica con un qualche server di Internet.

A tale scopo si propone la seguente ACL EXTENDED:


```
R(config)# access-list  102  remark  accesso alla DMZ

R(config)# access-list  102  permit  tcp  any  host  212.1.1.1 eq 80
R(config)# access-list  102  permit  tcp  any  host  212.1.1.1 eq 443
R(config)# access-list  102  permit  tcp  any  host  212.1.1.2 eq 25
R(config)# access-list  102  permit  tcp  any  host  212.1.1.2 eq 110
R(config)# access-list  102  permit  udp  any  eq 53  any
R(config)# access-list  102  permit  tcp   any  eq 53  any
R(config)# access-list  102  permit  tcp  any   any  established
R(config)# access-list  102  deny  ip  any  any
```

Si noti l'uso della parola chiave "established" per indicare che sono ammessi solo pacchetti tcp facenti parte di una connessione già stabilita!

Ovviamente tale ACL deve agire sul traffico in ingresso all'interfaccia Ser0, ovvero sul traffico proveniente da Internet:

```
R(config)# interface Ser0
R(config-if)# ip  access-group 102  in
R(config-if)# exit
```

Si noti che se si tenta dall'esterno di effettuare un ping verso uno dei server della rete aziendale, non verrà data alcuna risposta, e parimenti un tentativo di ping o traceroute verso un dispositivo in Internet non riceverà risposta!

Se si vuole poter ricevere le risposte ai ping effettuati verso Internet allora si deve inserire questa regola prima dell'ultima riga:

```
R(config)# access-list 102 permit icmp any any echo-reply
```

Correggere una access list

Se ci si accorge di aver sbagliato qualcosa in una access list allora la si deve cancellare e poi riscrivere integralmente.

Il comando per rimuovere la access list 102 è:

```
R(config)# no access-list 102
```

Il comando per rimuovere l'assegnazione della access list 102 all'interfaccia Ser0 in ingresso è:

```
R(config)# int Ser0
R(config-if)# no ip access-group 102 in
```

Visualizzare le ACL di un router

Con il comando

```
R# show access-lists
```

si possono vedere tutte le access list definite in un router

In alternativa si può usare il solito comando **show running-config** che mostra tutta la configurazione effettuata!