LE ACCESS CONTROL LIST

Una lista di controllo degli accessi, spesso chiamata con il nome inglese di Access Control List (ACL), è un meccanismo usato per esprimere regole complesse che determinano l'accesso ad alcune risorse di un sistema informatico. Tra le sue applicazioni principali si ha la configurazione di firewall e router e dei diritti di accesso a file e directory da parte del sistema operativo sui propri utenti.
Le ACL vengono realizzate per:

- limitare il traffico in rete;
- fornire controllo del flusso di traffico (per esempio le ACL possono restringere la consegna degli update di routing);
- offrire un livello base di sicurezza per l'accesso alla rete;
- decidere che tipi di traffico debbano essere instradati o bloccati alle interfacce del router;
- permettere a un amministratore di controllare che un client possa accedere a una rete;
- schermare alcuni host per permettere o negare accesso a parte della rete.

Le ACL si basano o su indirizzo sorgente o destinazione o sui protocolli e sui numeri di porta dei livelli superiori e le filosofie alla loro base sono due, tra loro opposte:
open security policy: tutto è permesso per default e nella lista ACL è presente l'elenco dei divieti;
closed security policy: tutto è vietato per default e nella lista ACL sono elencati i pochi accessi che vengono permessi,

Le ACL vengono elaborate dal router in **maniera sequenziale** in base all'ordine in cui sono state inserite le varie clausole. Appena un pacchetto soddisfa una delle condizioni la valutazione si interrompe ed il resto delle ACL non viene preso in considerazione. Il pacchetto viene quindi inoltrato o eliminato secondo l'istruzione eseguita (figura 1). Se il pacchetto non soddisfa nessuna delle condizioni viene scartato (si considera cha alla fine di un ACL non vuota ci sia l'istruzione deny any ovvero nega tutto). **L'ordine con cui sono scritte, quindi, è fondamentale**: è necessario scrivere le condizioni più restrittive prima, altrimenti potrebbero essere accettati pacchetti che non dovrebbero.

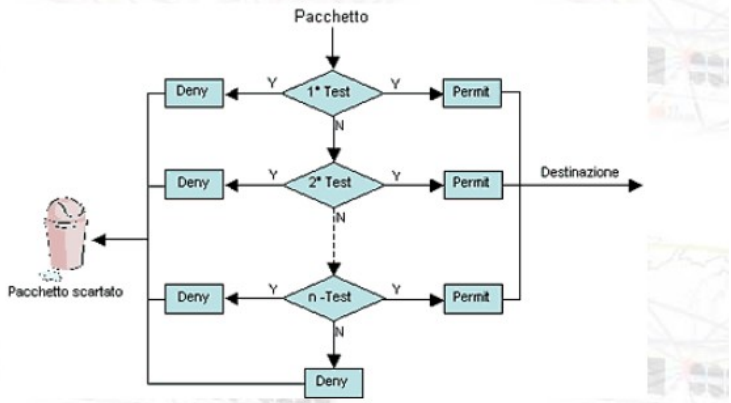

Figura 1

Nelle ACL vengono quindi elencate in ordine le regole che indicano quali utenti o processi di sistema possono accedere a degli oggetti e quali operazioni sono possibili su particolari oggetti. Ciascuna regola, definita Access Control Entry (ACE), esprime una o più proprietà dell'oggetto da valutare (sempre in riferimento all'esperienza, l'indirizzo sorgente di un pacchetto IP) e se queste proprietà sono verificate indica quale decisione prendere (per esempio far passare il pacchetto oppure rifiutarlo). La valutazione inizia dalla prima regola e continua fino a quando le condizioni di una regola non sono verificate. Se le condizioni sono verificate, la valutazione finisce e viene applicata la decisione presa; altrimenti, la valutazione prosegue alla regola successiva. Se nessuna regola viene soddisfatta, viene applicata una decisione di default, chiamata policy dell'ACL.

Uno degli aspetti fondamentali da ricordare è il **posizionamento delle ACL**. Questo è di non secondaria importanza, in quanto un cattivo posizionamento delle ACL può aver un impatto negativo sulla rete:
- maggiori risorse utilizzate dal router nel processare i pacchetti;

- decadimento delle prestazioni della rete;

- collasso della rete stessa.

Due sono gli aspetti fondamentali da tenere in considerazione nel posizionamento di un' ACL:

1.I pacchetti scartati non andranno a utilizzare risorse della rete;

2.Processare le ACL richiede risorse aggiuntive per il router (questo è anche uno dei motivi per cui non bisogna abusare delle ACL, specie in presenza di processori poco potenti).

Cisco consiglia, a riguardo, di posizionare le **ACL standard più vicino alla destinazione** e le **ACL Estese più vicino alla sorgente**.

Le ACL possono essere usate per controllare il traffico ai livelli 2, 3, 4 e 7: in passato venivano usate le ACL numeriche per filtrare il traffico in base al campo Ethernet Type delle Trame oppure in base agli indirizzi MAC mentre oggi le ACL sono più spesso basate sugli indirizzi IPv4 o IPv6 e sulle porte TCP e/o UDP. Le ACL utilizzano un nuovo tipo di maschera, la WildCard Mask.

WildCard Mask

La WildCard Mask è un numero di 32 bit diviso in 4 ottetti. Quest'ultimo conserva la stessa divisione (8 bit per ottetto) della notazione decimale puntata degli indirizzi IPv4. Questa, solitamente, viene abbinata a un indirizzo IP, in modo simile alla SubNet Mask e i bit assumono valori 1 o 0 per stabilire come elaborare i corrispondenti bit dell'indirizzo IP. Il termine stesso indica il procedimento di checking su una qualsiasi Access List, tramite una maschera.
L'analogia nasce dal Jolly (WildCard), usato nel gioco del poker, che permette l'abbinamento, a tale carta, di una qualsiasi altra pari, presente nel mazzo.
Più precisamente, gli 0 e 1 nella WildCard Mask stabiliscono se i bit, corrispondenti nell'indirizzo IP, debbano essere controllati o ignorati. Ogni bit a 0, della WildCard Mask, indica che il bit corrisposto dev'essere incluso nel processo di controllo dell'uguaglianza, mentre il valore 1 tralascia ogni vincolo di confronto.

ESEMPIO

Vediamo un esempio per comprendere l'utilizzo della WildCard mask: si supponga di voler effettuare un controllo dell'indirizzo IP: 169.12.5.0/24, che appartiene a una LAN di classe B 169.12.0.0 dove possono essere create 255 reti che contengono 253 host ognuna.
Si desidera bloccare il traffico in arrivo dai seguenti indirizzi IP: da 169.12.5.4 a 169.12.5.7.
169.12.5.0 in binario, è tradotto in
10101010.00001100.00000101.00000000
e la subnet mask è 11111111.11111111.11111111.00000000 (un /24, come già visto, è un 255.255.255.0).
Guardando gli indirizzi da bloccare in formato binario si osserva che c'è una parte di indirizzo che non cambia mai:

```
169.12.5.4 - 10101010.00001100.00000101.000001 00
169.12.5.5 - 10101010.00001100.00000101.000001 01
169.12.5.6 - 10101010.00001100.00000101.000001 10
169.12.5.7 - 10101010.00001100.00000101.000001 11
```

Tramite la WildCard Mask, è possibile raggruppare gli indirizzi IP interessati in un'unica dicitura e ridurre il numero di ACL da impostare per bloccare il traffico. In questo caso è possibile impostare una sola ACL per fermare i dati in arrivo dal range che va dal 169.12.5.4 al 169.12.5.7: è sufficiente individuare l'indirizzo di inizio sequenza che corrisponde all'insieme dei bit non mutevoli.
In tutti e quattro gli indirizzi la parte che non cambia è 169.12.5.4 e sarà l'inizio sequenza che ci permette di individuare la WildCard Mask esatta, composta dal valore 1 nella posizione dei bit che mutano, cioè solo gli ultimi due: la WildCard Mask, in forma binaria, sarà 00000000.00000000.00000000.00000011. In forma decimale puntata 0.0.0.3.

Prima di scrivere le ACL è necessario capire se il gruppo di dispositivi/servizi relativo all'ACL sia da riferirsi alle richieste in entrata (in e inbound) oppure in uscita (out e outbound).
Vediamo le differenze tra le diverse situazioni:

- out: si riferisce al traffico che ha attraversato il router e lascia l'interfaccia;
- in: è il traffico che arriva sulla interfaccia e poi passa attraverso il router;
- inbound: se la lista di accesso è in entrata, quando il router riceve un pacchetto, il software Cisco IOS controlla i criteri della ACL e se al pacchetto è consentito l'accesso continua a elaborarlo altrimenti lo scarta;
- outbound: se la lista di accesso è in uscita, quando il software riceve l'indirizzo dell'interfaccia d'uscita, controlla i criteri della ACL e se è consentito a quel pacchetto di raggiungere l'interfaccia, lo trasmette, altrimenti lo scarta.

ROUTER e ACL

Descriviamo la sequenza delle operazioni che vengono eseguite da un router nell'analisi di un pacchetto:

non appena una PDU di livello 2 entra in un'interfaccia, il router verifica se l'indirizzo di strato 2 corrisponde al suo indirizzo o se sia un indirizzo di broadcast;

- se il check è positivo, il router estrae allora il pacchetto ed esamina la ACL associata all'interfaccia di ingresso, sempre che ne sia definita una;
- il router esegue ogni comando della ACL;
- se si riscontra una corrispondenza sulla condizione corrispondente a un comando, il router compie l'azione collegata a quel comando;
- se il pacchetto è accettato il router eseguirà la funzione di instradamento;
- se è definita una ACL sull'interfaccia di uscita, il pacchetto sarà di nuovo testato in base ai comandi contenuti in questa ACL;
- se tutti i test autorizzano il pacchetto a proseguire il suo cammino, questo viene incapsulato nel protocollo di strato 2 definito sull'interfaccia d'uscita.

ACL STANDARD

Le ACL Standard specificano delle limitazioni ai pacchetti guardando esclusivamente l'indirizzo della sorgente e vanno posizionate sull'interfaccia del router più vicino alla destinazione.
Per creare una ACL su un router Cisco occorre seguire i seguenti passi in configuration mode:

1. Definire la ACL con il seguente comando:

Router(config)# **access-list** access-list number {**permit**|**deny**} {test-conditions}

- access-list number è il numero univoco che identifica ogni ACL e che ne definisce il tipo. Dalla versione 11.2 del Cisco IOS si può utilizzare un nome al posto del numero.
- Permit e deny definiscono le condizioni (permetti e nega) su come devono essere maneggiati i pacchetti: Permit indica che il pacchetto ha il permesso di utilizzare una o più interfacce specificate di seguito; deny indica che il pacchetto deve essere droppato.
- Il termine finale specifica la condizione da soddisfare.

Protocollo	Range
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

Access-list Number

2. si deve applicare la ACL a una o più interfacce:

Router(config-if)# **access-group** access-list number

Per eliminare una ACL bisogna utilizzare il comando
Router(config)# **no access-list** access-list number

ESEMPIO APPLICATIVO:
Router(config)#access-list 10 deny 192.168.1.0 0.0.0.31
Router(config)#access-list 10 permit **any // questa è la regola di default che verrà applicata a tutti i pacchetti**

ACL ESTESE

Le ACL estese forniscono una maggiore flessibilità e controllo se paragonate a quelle standard. Le ACL estese, infatti, possono effettuare il controllo non solo sull'indirizzo del mittente, ma anche su quello del destinatario, su uno specifico protocollo, sul numero di porta o su altri parametri.

Il controllo effettuato sul protocollo merita una precisazione; infatti, sebbene le ACL standard permettano di negare o no un'intera suite di protocolli (es. IP, …) (eseguendo il controllo su un'intera rete come fanno le ACL standard, si effettua di conseguenza anche il controllo sul protocollo di comunicazione utilizzato), non permettono di gestirne singolarmente le varie componenti. Al contrario le ACL estese possono effettuare controlli sui singoli protocolli che compongono la suite (es. ICMP, …).

Per definire un'ACL Estesa sui router Cisco entrare in configuration mode ed eseguire i seguenti passi:

1. Definire l'ACL secondo la sintassi:

Router(config)# **access-list** access-list-number {**deny** | **permit**} protocol source source-wildcard **destination** destination-wildcard [**operator** operand] [established] [**precedence** precedence] [log]

Parametri	**Descrizione**
Access-list-number	Numero dell'ACL. Ne indica il nome e il tipo (es. da 100 a 199 e da 2000 a 2699 per le ACL IP Estese). E' importante ricordare che le ACL estese utilizzano *access-list number* differenti da quelli utilizzati dalle standard, anche se riferiti allo stesso protocollo.
Permit	Permette l'accesso se le condizioni sono soddisfatte
Deny	Nega l'accesso se le condizioni sono soddisfatte
Protocol	Il protocollo di comunicazione; es. IP, TCP, UDP, ICMP, IGRP, …
Source e Destination	Indirizzo del mittente e del destinatario.
Souce-wildcard e Destination-wildcard	La wildcard mask che deve essere applicata all'indirizzo sorgente e a quello di destinazione.
Operator *operand*	Un operatore logico: lt, gt, eq, neq, range (less than, greater than, equal, not equal, range) e il numero o il nome della porta TCP o UDP (vedi Tabella n.1). Nel caso dell'operatore *range* occorre inserire due valori *operand* (es. range 21 25)
Established	(Optional) Si utilizza solo con il protocollo TCP: indica una "estabilished connection". Il controllo viene effettuato solo se il datagramma ha settato il bit di ACK o RST, mentre non ci sono controlli sul pacchetto iniziale per stabilire la connessione.
Precedence	(Optional) Indica un numero da 0 a 7, che specifica la precedenza del pacchetto rispetto a un altro (Queuing).
Log	(Optional) Attiva i messaggi di log. Questi comprendono l'indirizzo sorgente, il numero di pacchetti e l'esito del controllo (permit o deny). I log vengono generati a intervalli di 5 minuti.

Applicare l'ACL a una o più interfacce:
Router(config-if)# **ip access-group** *access-list number* {**in**|**out**}

Per cancellare un ACL o rimuoverla da un'interfaccia del Router occorre utilizzare rispettivamente i seguenti comandi:

Router(config)# **no access-list** *access-list number*

Router(config-if)# **no ip access-group** *access-list number*

Per visualizzare le informazioni sulle ACL si possono utilizzare i seguenti comandi:
– Router> **show access-list** [*access-list number*]: mostra il contenuto di tutte le ACL caricate sul router (utilizzando l'opzione *access-list number* vengono elencate solo le condizioni di una determinata ACL);

– Router> **show ip interface** [*interface-type number*] : mostra le informazioni sulle interfacce IP e quindi anche la presenza di un'eventuale ACL collegata all'interfaccia (le opzioni *interface-type* e *number* permettono di indicare una determinata interfaccia).