ACCESS CONTROL LIST (ACL)

Introduzione ACL

Le ACL (Access Control List) sono una lista di istruzioni da applicare alle interfacce di un router allo scopo di gestire il traffico, filtrando i pacchetti in entrata e in uscita.

USO DEGLI ACL

Esistono svariati motivi per cui utilizziamo gli ACL. Il motivo principale è fornire un livello base di sicurezza per la rete. Gli ACL non sono così complessi e di protezione come firewall , ma forniscono protezione su interfacce ad alta velocità in cui la velocità della linea è importante, ed i firewall possono essere restrittivi. Gli ACL vengono anche utilizzati per limitare gli aggiornamenti per il routing dai peer di rete, e possono essere determinanti nella definizione del controllo di flusso per il traffico di rete.

DESCRIZIONE ACL

Gli ACL sono un filtro di rete utilizzato dai router e alcuni switch,per consentire e limitare i flussi di dati in entrata e in uscita dalle interfacce di rete. Quando un ACL è configurato su un'interfaccia, il dispositivo di rete analizza i dati che passano attraverso l'interfaccia, li confronta con i criteri descritti nell'ACL e consente ai dati di scorrere o vietarli.

Esistono due tipi di ACL:

- ACL Standard
- ACL Estese

DIFFERENZE

La differenze tra ACL Standard e Estese sono:

- Un ACL standard può consentire o negare il traffico basato solo sugli indirizzi di origine.
- Un ACL esteso può consentire o negare il traffico in base agli indirizzi di origine e di destinazione, nonché ai tipi di traffico tcp (Affidabiltá comunicazione tra mittente e destinatario)/ udp(Piú veloce ma neno affidabile / icmp (avverte se ci sono malfunzionamenti nella trasmissione).

TIPI DI ACL NEL DETTAGLIO

Protocollo	Range
IP Indica il Numero ed il nome delle ACL.	1-99
Extended IP Indica il numero e il nome delle ACL IP Estese.	100-199
AppleTalk AppleTalk era un protocollo molto usato nelle reti Macintosh. Il suo principale scopo era quello di condividere stampanti e/o file, e quindi metterli a disposizioni degli utenti che facevano parte della rete.	600-699
IPX Protocollo variante delle IP usate nello scambio di pacchetti nelle reti netware.	800-899
Extended IPX Protocollo variante delle Extended IP usate nello scambio di pacchetti nelle reti netware.	900-999
IPX Service Advertising Protocol Aggiunge o rimuove servizi in una intrarete IPX.	1000-1099

Differenza tra ACL e Firewall

Gli ACL eseguono ispezioni senza stato, il che significa che l'elenco di accesso esamina un pacchetto e non ha alcuna conoscenza di ciò che è venuto prima. Se un ACL esamina un pacchetto che utilizza TCP con il set di bit ACK, l'ACL può solo capire che si tratta di un pacchetto di riconoscimento. Tuttavia, non è a conoscenza se esiste realmente una conversazione a cui appartiene questo pacchetto.

Un firewall ha un uso e uno scopo principali ed è quello di esaminare il traffico che passa attraverso una parte della rete e prendere decisioni su cosa lasciare e cosa bloccare. Di solito un firewall esegue un'ispezione di stato, il che significa che il firewall non vede solo il pacchetto TCP con il bit ACK impostato, ma il firewall è in grado di sapere se c'è stato un inizio corretto per questa conversazione TCP.

ESEMPIO DI COME APPLICARLE LE ACL

Standard

Extended