Access List

Una Access List è una serie di comandi che vengono configurati nel router o switch e che consentono di controllare il traffico dei dati in ingresso ed uscita sulla base di regole inserite all'interno del router sui pacchetti e quindi si può stabilire di consentire o bloccare del traffico, limitare alcuni pacchetti in arrivo da determinati sorgenti o verso determinate destinazioni.

Come si configura una Access List?

I comandi sono una serie di Control Access Entries, quindi una serie di permit and denied statment inseriti all'interno dello stesso router.

Quando il traffico arriva all'interfaccia del router ed è presente una Access List, il router compara le informazioni che sono nel pacchetto rispetto ad ognuna delle entries che stanno dell'access list del router in ordine sequenziale e si verifica se una di questa viene soddisfatta o meno.

L'ultimo statment di una access list è sempre un denied implict, ovvero se non c'è nessun'altra riga in precedenza soddisfatta allora ci sarà un implicit denied alla fine, ovvero il traffico verrà comunque bloccato, invece per consentire il traffico bisogna inserire un permit come ultimo statment se bloccare un traffico specifico ma consentire tutto il resto.

Le Access List (ACL) sono regole utilizzate nei dispositivi di rete, come router e switch, per controllare il traffico che può entrare o uscire da una rete.

Concetti chiave:

1. **Scopo**:
    - Filtrare il traffico basandosi su criteri come indirizzo IP, porta, protocollo.
    - Migliorare la sicurezza bloccando traffico indesiderato.
2. **Tipologie**:
    - **ACL standard**: Filtrano solo basandosi sull'indirizzo IP sorgente.
    - **ACL estese**: Filtrano basandosi su indirizzo IP sorgente/destinazione, porte e protocolli.
3. **Posizionamento**:
    - ACL standard: Vicino alla **destinazione**.
    - ACL estese: Vicino alla **sorgente**.
4. **Regole**:
    - Elencate in ordine sequenziale.
    - Il primo match determina l'azione (allow/deny).
    - **Implicit deny**: Tutto il traffico non esplicitamente permesso è bloccato.

Ecco un esempio pratico di configurazione di una ACL su un router Cisco:

Scenario:

Supponiamo di avere una rete:

- **Rete interna**: 192.168.1.0/24
- **Rete esterna**: 192.168.2.0/24
- Obiettivo: Consentire il traffico HTTP (porta 80) dalla rete interna verso l'esterno, bloccando tutto il resto.

Configurazione passo per passo:

1. **Creazione di un'ACL estesa**:

   ```
   bash
   Copia codice
   Router(config)# access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
   Router(config)# access-list 100 deny ip any any
   ```

2. **Applicazione dell'ACL sull'interfaccia**: Supponiamo che l'interfaccia verso l'esterno sia **FastEthernet 0/1**.

   ```
   bash
   Copia codice
   Router(config)# interface FastEthernet 0/1
   Router(config-if)# ip access-group 100 out
   ```

Spiegazione:

1. **Regola 1**:
   - Consente solo il traffico TCP proveniente dalla rete interna (192.168.1.0/24) verso qualsiasi destinazione sulla porta 80 (HTTP).
   - `192.168.1.0 0.0.0.255`: Specifica la rete interna (wildcard mask).
2. **Regola 2**:
   - Blocca tutto il traffico non corrispondente alla regola precedente (implicit deny aggiunto esplicitamente).
3. **Applicazione**:
   - L'ACL è applicata in uscita sull'interfaccia che porta alla rete esterna.

Verifica:

Usa il comando:

```
bash
Copia codice
Router# show access-lists
```

Per verificare i contatori delle regole e se l'ACL sta funzionando come previsto.