Informazioni sugli Access Control List dei punti di accesso al servizio

Sommario

Introduzione

Questo documento spiega come leggere e creare Access Control List (ACL) di punti di accesso (SAP) nei router Cisco. Sebbene esistano diversi tipi di ACL, nel presente documento vengono illustrati quelli che filtrano in base ai valori SAP. L'intervallo numerico per questo tipo di ACL è compreso tra 200 e 299. Questi ACL possono essere applicati alle interfacce Token Ring per filtrare il traffico Source Route Bridge (SRB), alle interfacce Ethernet per filtrare il traffico Transparent Bridge (TB) o ai router peer Data Link Switching (DLSw).

La sfida principale degli ACL SAP è sapere esattamente quali SAP sono autorizzati o rifiutati da una determinata voce dell'elenco. Verranno analizzati quattro diversi scenari in cui un particolare protocollo viene filtrato.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Architettura di rete dei sistemi di filtraggio

Il traffico SNA (Systems Network Architecture) di IBM utilizza SAP con dimensioni comprese tra 0x00 e 0xFF. Virtual Telecommunications Access Method (VTAM) V3R4 e versioni successive supportano un intervallo di valori SAP compreso tra 4 e 252 (o da 0x04 a 0xFC in rappresentazione esadecimale), dove 0xF0 è riservato al traffico NetBIOS. Gli SAP devono essere multipli di 0x04, a partire da 0x04. Il seguente ACL consente gli SAP SNA più comuni e nega il resto (considerato che esiste un **rifiuto** implicito **tutto** alla fine di ciascun ACL):

```
access-list 200 permit 0x0000 0x0D0D
```

Esadecimale	Binario
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

Utilizzare i bit nella maschera con caratteri jolly per determinare gli SAP consentiti da questa voce ACL specifica. Per interpretare i bit della maschera con caratteri jolly, attenersi alle seguenti regole:

- 0 = Corrispondenza esatta richiesta. Ciò significa che l'SAP consentito deve avere lo stesso valore dell'SAP configurato nell'ACL. Fare riferimento alla tabella seguente per ulteriori dettagli.
- 1 = L'indirizzo SAP consentito può avere 0 o 1 in questa posizione di bit, la posizione "non importa".

Sap consentiti da ACL, dove X=0 o X=1	Maschera con caratteri jolly	SAP configurato nell'ACL
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

Utilizzando i risultati riportati nella tabella precedente, di seguito è riportato l'elenco degli SAP che soddisfano il modello indicato.

Sap consentiti (formato binario)	Sap consentiti

								(esadecimale)
0	0	0	0	0	0	0	0	0x00
0	0	0	0	0	0	0	1	0x01
0	0	0	0	0	1	0	0	0x04
0	0	0	0	0	1	0	1	0x05
0	0	0	0	1	0	0	0	0x08
0	0	0	0	1	0	0	1	0x09
0	0	0	0	1	1	0	0	0x0C
0	0	0	0	1	1	0	1	0x0D

Come mostrato dalla tabella, non tutti i possibili SAP SNA sono inclusi in questo ACL. Questi SAP, tuttavia, coprono i casi più comuni.

Un altro fattore da considerare quando si progetta l'ACL è che i valori SAP cambiano a seconda che si tratti di comandi o risposte. Il punto di accesso al servizio di origine (SSAP) include il bit di comando/risposta (C/R) per distinguerli. Il valore di C/R è impostato su 0 per i comandi e su 1 per le risposte. Pertanto, l'ACL deve consentire o bloccare sia i comandi che le risposte. Ad esempio, SAP 0x05 (utilizzato per le risposte) è SAP 0x04 con C/R impostato su 1. Lo stesso vale per SAP 0x09 (SAP 0x08 con C/R impostato su 1), 0x0D e 0x01.

Filtraggio NetBIOS

Il traffico NetBIOS utilizza i valori SAP 0xF0 (per i comandi) e 0xF1 (per le risposte). In genere, gli amministratori di rete utilizzano questi valori SAP per filtrare il protocollo. La voce dell'elenco degli accessi riportata di seguito consente il traffico NetBIOS e nega tutto il resto (ricordare la voce implicita **deny all** alla fine di ciascun ACL):

```
access-list 200 permit 0xF0F0 0x0101
```

Utilizzando la stessa procedura descritta nella sezione precedente, è possibile verificare che l'ACL sopra riportato consenta gli ACL SAP 0xF0 e 0xF1.

Al contrario, se il requisito è bloccare NetBIOS e consentire il resto del traffico, usare il seguente ACL:

```
access-list 200 deny 0xF0F0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

Filtraggio IPX

Per impostazione predefinita, i router Cisco collegano il traffico IPX. Per modificare questo comportamento, usare il comando **ipx routing** sul router. IPX, utilizzando l'incapsulamento 802.2, utilizza SAP 0xE0 come DSAP (Destination Service Access Point) e SAP. Pertanto, se un router Cisco sta effettuando il bridging IPX e il requisito è quello di autorizzare solo questo tipo di traffico, utilizzare il seguente ACL:

```
access-list 200 permit 0xE0E0 0x0101
```

Al contrario, il seguente ACL blocca l'IPX e consente il resto del traffico:

```
access-list 200 deny 0xE0E0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

Autorizza o nega tutto il traffico

Ogni ACL include una clausola **deny all** implicita. È necessario tenere presente questa voce quando si analizza il comportamento di un ACL configurato. L'ultima voce ACL mostrata di seguito nega tutto il traffico.

```
access-list 200 permit ....
access-list 200 permit ....
access-list 200 deny 0x0000 0xFFFF
```

Tenere presente che quando si legge la maschera con caratteri jolly (in formato binario), 1 è considerato una posizione di bit "ignora". Una maschera con caratteri jolly all 1s in rappresentazione binaria viene convertita in 0xFFFF in rappresentazione esadecimale.

Informazioni correlate

- Pagina di supporto DLSw
- Access Control Lists: Panoramica e linee guida
- Tecniche di filtro DLSw+ SAP/MAC
- Supporto tecnico – Cisco Systems