Cómo funcionan las listas de control de acceso a los puntos de acceso al servicio

Contenido

Introducción

Este documento explica cómo leer y crear Listas de control de acceso (ACL) al punto de acceso al servicio (SAP) en los routers Cisco. Si bien existen diversos tipos de ACL, este documento se enfoca en aquellas que filtran sobre base de los valores SAP. El rango numérico para este tipo de ACL es de 200 a 299. Estas ACL se pueden aplicar a las interfaces Token Ring para filtrar el tráfico del puente de ruta de origen (SRB), a las interfaces Ethernet para filtrar el tráfico del puente transparente (TB) o a los routers de peer Data Link Switching (DLSw).

El desafío principal en el caso de los SAP ACL es saber específicamente cuáles son los SAP que están siendo permitidos o denegados por una entrada ACL en particular. Analizaremos cuatro escenarios diferentes en los que se filtra un protocolo determinado.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Filtrado de System Network Architecture

El tráfico de la arquitectura de red de sistemas (SNA) de IBM utiliza SAP que oscilan entre 0x00 y 0xFF. El método de acceso virtual de telecomunicación (VTAM) V3R4 y posteriores admiten un rango de valor de SAP de 4 a 252 (o 0x04 a 0xFC en una representación hexadecimal), donde 0xF0 se reserva para el tráfico de NetBIOS. Los SAP deben ser múltiplos de 0x04, comenzando con 0x04. La siguiente ACL permite los SAP de SNA más comunes y rechaza el resto (considerando que existe una negación implícita de todos ellos al final de cada ACL):

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

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

Utilice los bits en la máscara de comodín para determinar qué SAP están permitidos por esta entrada ACL determinada. Para interpretar los bits de máscara de comodín utilice las reglas siguientes:

- 0 = Se requiere coincidencia exacta. Esto significa que el SAP permitido debe tener el mismo valor que el SAP configurado en la ACL. Para obtener más detalles, consulte la siguiente tabla.
- 1 = El SAP puede tener un 0 o un 1 en esta posición de bit, la posición "sin importancia".

Saps permitidos por ACL, donde X=0 o X=1	Máscara comodín	SAP configurado en 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

Utilizando los resultados de la tabla anterior, a continuación se muestra la lista de los SAP que coinciden con el patrón anterior.

Saps permitidos (binario)	SAP permitidos

								(hexadecimal)
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

Como puede ver en la tabla anterior, no todos los SAP SNA posibles se incluyen en esta ACL. Estos SAP, sin embargo, cubren la mayoría de los casos comunes.

Otro punto a considerar al diseñar la ACL es que los valores de SAP cambian dependiendo de si son comandos o respuestas. El punto de acceso del servicio de origen (SAP) incluye el bit de comando/respuesta (C/R) para diferenciarlos. El C/R está configurado en 0 para los comandos y en 1 para las respuestas. Por lo tanto, el ACL debe permitir o bloquear comandos y también respuestas. Por ejemplo, SAP 0x05 (utilizado para las respuestas) es SAP 0x04 con el C/R configurado en 1. Lo mismo se aplica a SAP 0x09 (SAP 0x08 con C/R configurado en 1), 0x0D y 0x01.

Filtro de NetBIOS

El tráfico de NetBIOS usa valores SAP 0xF0 (para comandos) y 0xF1 (para respuestas). Normalmente, los administradores de red utilizan estos valores SAP para filtrar este protocolo. La entrada de la lista de acceso que se muestra a continuación permite el tráfico de NetBIOS y lo niega todo (recuerde el **rechazo implícito** de **todo** al final de cada ACL):

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

Mediante el mismo procedimiento que se muestra en la sección anterior, puede determinar que la ACL mencionada permite los SAP 0xF0 y 0xF1.

Por el contrario, si el requisito es bloquear NetBIOS y permitir el resto del tráfico, utilice la siguiente ACL:

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

Filtrado de IPX

De manera predeterminada, los routers Cisco establecen un puente para el tráfico IPX. Para modificar este comportamiento debe emitir un comando de ruteo ipx en el router. IPX mediante la encapsulación 802.2 utiliza SAP 0xE0 como el Punto de acceso del servicio de destino (DSAP) y SSAP. Por lo tanto, si un router Cisco está conectando en puente IPX y el requisito es permitir

solamente este tipo de tráfico, utilice la siguiente ACL:

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

Por el contrario, la siguiente ACL bloquea los IPX y permite el resto del tráfico:

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

Permitir o denegar todo el tráfico

Cada ACL incluye una negación implícita de todo. Debe tener en cuenta esta entrada al analizar el comportamiento de una ACL configurada. La última entrada ACL que se muestra a continuación niega todo el tráfico.

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

Recuerde al leer la máscara comodín (binaria) que 1 se considera como una posición de bit "sin importancia". Una máscara de comodín toda de 1 en una representación binaria se traduce a 0xFFFF en una representación hexadecimal.

Información Relacionada

- Página de soporte de DLSw
- Listas de control de acceso: Información General y Pautas
- Técnicas de filtrado DLSw+ SAP/MAC
- Soporte Técnico - Cisco Systems