Entendendo as listas de controle de acesso ao ponto de acesso de serviço

Contents

Introduction
Antes de Começar
Conventions
Prerequisites
Componentes Utilizados
Filtrando a arquitetura de rede do sistema
Filtrando o NetBIOS
Filtrando IPX
Permitir ou negar todo o tráfego
Informações Relacionadas

Introduction

Este documento explica como ler e criar Service Access Point (SAP) Access Control Lists (ACLs) em Cisco routers. Embora existam vários tipos de ACLs, este documento concentra-se nos tipos que são filtrados com base nos valores SAP. O intervalo numérico para esse tipo de ACL é de 200 a 299. Essas ACLs podem ser aplicadas às interfaces Token Ring para filtrar o tráfego da Source Route Bridge (SRB), às interfaces Ethernet para filtrar o tráfego da Transparent Bridge (TB) ou aos roteadores de peer DLSw (Data Link Switching).

O maior desafio com as ACLs do SAP é saber exatamente o que uma determinada entrada ACL permite ou recusa para os SAPs. Serão analisados quatro cenários diferentes nos quais um determinado protocolo está sendo filtrado.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Filtrando a arquitetura de rede do sistema

O tráfego da IBM Systems Network Architecture (SNA) usa SAPs que variam de 0x00 a 0xFF. O Virtual Telecommunications Access Method (VTAM) V3R4 e posterior suporta um alcance de valor de SAP de 4 a 252 (ou 0x04 a 0xFC em representação hexadecimal), em que 0xF0 é reservado para o tráfego NetBIOS. SAPs devem ser múltiplos de 0x04, começando com 0x04. O seguinte ACL permite os SNA SAPs mais comuns e recusa os demais (considerando que há uma recusa implícita no final de cada ACL).

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

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

Use os bits da máscara de caractere geral para determinar quais são os SAPs permitidos por essa entrada ACL específica. Utilize as regras a seguir ao interpretar os bits da máscara de caractere geral.

- 0 = correspondência exata necessária. Isso significa que o SAP permitido deve ter o mesmo valor que o SAP configurado na ACL. Consulte a tabela abaixo para obter mais detalhes.
- 1 = O SAP permitido pode ter 0 ou 1 em sua posição de bit, a posição "sem importância".

SAPs Permitidos por ACL, Onde X=0 ou X=1	Máscara de Caracteres Curinga	SAP configurado na 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

Usando os resultados da tabela anterior, a lista de SAPs que atendem ao padrão acima é mostrada abaixo.

Saps permitidos (binário)								Saps permitidos (hexadecimais)
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 você pode ver na tabela acima, nem todos os SAPs SNA possíveis estão incluídos nesta ACL. Esses SAPs, entretanto, abrangem a maioria dos casos.

Outro ponto a ser considerado ao projetar a ACL é que os valores SAP mudam dependendo se são comandos ou respostas. O ponto de acesso de serviço de origem (SSAP) inclui o bit de comando/resposta (C/R) para diferenciá-los. O C/R está configurado para 0 quanto aos comandos e para 1 quanto às respostas. Portanto, a ACL deve permitir ou bloquear comandos e respostas. Por exemplo, SAP 0x05 (usado para respostas) é SAP 0x04 com C/R definido como 1. O mesmo se aplica ao SAP 0x09 (SAP 0x08 com C/R definido como 1), 0x0D e 0x01.

Filtrando o NetBIOS

O tráfego de NetBIOS utiliza os valores de SAP 0xF0 (para comandos) e 0xF1 (para respostas). Normalmente, os administradores de rede usam esses valores de SAP para filtrar esse protocolo. A entrada da lista de acesso mostrada abaixo permite o tráfego NetBIOS e nega todo o resto (lembre-se do implícito **deny all** no final de cada ACL):

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

Usando o mesmo procedimento mostrado na seção anterior, você pode determinar se a ACL anterior permite SAPs 0xF0 e 0xF1.

Por outro lado, se o requisito for bloquear o NetBIOS e permitir o restante do tráfego, use o ACL a seguir:

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

Filtrando IPX

Por padrão, os Cisco routers fazem a ponte do tráfego de IPX. Para alterar esse comportamento, você deve emitir o comando ipx routing no roteador. O IPX, usando encapsulamento 802.2, usa SAP 0xE0 como Destination Service Access Point (DSAP) e SSAP. Portanto, se um roteador Cisco estiver fazendo a ponte IPX e o requisito for permitir apenas esse tipo de tráfego, use a seguinte ACL:

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

Caso contrário, a ACL a seguir bloqueará o IPX e autorizará o resto do tráfego:

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

Permitir ou negar todo o tráfego

Todo ACL inclui uma negação total implícita. Você deve estar ciente dessa entrada ao analisar o comportamento de uma ACL configurada. A última entrada da ACL mostrada abaixo nega todo o tráfego.

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

Lembre-se de que, ao ler a máscara curinga (em binários), 1 é considerado um bit de posição do tipo “desconsiderar". Uma máscara curinga toda 1s em representação binária equivale a 0xFFFF em representação hexadecimal.

Informações Relacionadas

- Página de suporte de DLSw
- Listas de controle de acesso: Visão geral e diretrizes
- Técnicas de filtragem DLSw+ SAP/MAC
- Suporte Técnico - Cisco Systems