Contenu

Introduction

Ce document explique comment lire et créer le Listes de contrôle d'accès (ACL) de point d'accès services (SAP) dans des Routeurs de Cisco. Bien qu'il y ait plusieurs types d'ACLs, les foyers de ce document sur ceux que le filtre a basés sur SAP évalue. La plage numérique pour ce type d'ACL est de 200 à 299. Ces ACLs peut être appliqué aux interfaces Token Ring pour filtrer le trafic du Source Route Bridge (SRB), aux interfaces Ethernet pour filtrer le trafic transparent de la passerelle (TB), ou aux Routeurs de pair de Data-Link Switching (DLSw).

Le défi principal avec SAP ACLs est de connaître qu'exactement ce qui sape sont autorisés ou refusés par une entrée d'ACL particulier. Nous analyserons quatre scénarios différents où un protocole particulier est filtré.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Systems Network Architecture de filtrage

Le trafic du Systems Network Architecture d'IBM (SNA) utilise des sèves s'étendant de 0x00 à

0xFF. Virtual Telecommunications Access Method (vtam) V3R4 et support postérieur une plage de valeurs pour SAP de 4 à de 252 (ou de 0x04 à 0xFC dans la représentation hexadécimale), où 0xF0 est réservé pour le trafic de Netbios. Les sèves doivent être des multiples de 0x04, commençant par 0x04. L'ACL suivant permet les sèves SNA les plus communes, et refuse le repos (considérer là est un implicite **refusent tous à la** fin de chaque ACL) :

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

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

Employez les bits dans le masque de masque pour déterminer quelles sèves sont permises par cette entrée d'ACL particulier. Utilisez les règles suivantes en interprétant les bits de masque générique :

- 0 = précis - correspondance requise. Ceci signifie que SAP permis doit avoir la même valeur que SAP configuré dans l'ACL. Référez-vous à la table ci-dessous pour plus de détails.
- 1 = SAP permis peut avoir un 0 ou 1 à cette position binaire, « ne s'inquiètent pas » la position.

Sèves permises par ACL, où X=0 ou X=1	Masque de masque	SAP a configuré dans l'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

Utilisant les résultats dans la table précédente, la liste de sèves qui se réunissent le modèle ci-dessus est affichée ci-dessous.

Sèves permises (binaire)								Sèves permises (hexadécimales)
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

Comme vous pouvez voir de la table ci-dessus, non toutes les sèves possibles SNA sont incluses dans cet ACL. Ces sèves, cependant, couvrent les cas les plus communs.

Un autre point à considérer quand concevoir l'ACL est que les valeurs de SAP changent selon si elles sont des commandes ou des réponses. Le point d'accès de source de service (SSAP) inclut la commande/réponse (C/R) bit à différencier entre elles. Le C/R est placé à 0 pour des commandes et aux réponses de 1par. Par conséquent, l'ACL doit permettre ou bloquer des commandes aussi bien que des réponses. Par exemple, le sap 0x05 (utilisé pour des réponses) est sap 0x04 avec l'ensemble de référence c à 1. Le même s'applique au sap 0x09 (SAP 0x08 avec l'ensemble de référence c à 1), à 0x0D, et à 0x01.

Netbios de filtrage

Le trafic de Netbios utilise les valeurs de SAP 0xF0 (pour des commandes) et 0xF1 (pour des réponses). Typiquement, les administrateurs réseau emploient ces valeurs de SAP pour filtrer ce protocole. L'entrée de liste d'accès affichée ci-dessous le trafic de Netbios d'autorisations et refuse tout autrement (souvenez-vous l'implicite **refusent tous à la** fin de chaque ACL) :

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

Suivant la même procédure affichée dans la section précédente, vous pouvez déterminer que l'ACL ci-dessus permet les sèves 0xF0 et 0xF1.

Au contraire, si la condition requise est de bloquer Netbios et de permettre le reste du trafic, utilisez l'ACL suivant :

```
access-list 200 deny 0xF0F0 0x0101access-list 200 permit 0x0000 0xFFFF
```

IPX de filtrage

Par défaut, le trafic IPX de pont en Routeurs de Cisco. Pour changer ce comportement, vous devez émettre la commande de **routage ipx** sur le routeur. L'IPX, utilisant l'encapsulation 802.2, utilise SAP 0xE0 en tant que le point d'accès de destination de service (DSAP) et SSAP. Par conséquent, si un routeur de Cisco pont l'IPX et la condition requise est de permettre seulement ce type de trafic, utilisez l'ACL suivant :

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

Au contraire, l'ACL suivant bloque l'IPX et permet le reste du trafic :

```
access-list 200 deny 0xE0E0 0x0101access-list 200 permit 0x0000 0xFFFF
```

Permettez ou refusez tout le trafic

Chaque ACL inclut un implicite **refusent tous**. Vous devez se rendre compte de cette entrée en analysant le comportement d'un ACL configuré. Le dernier rubrique de liste ACL affiché ci-dessous refuse tout le trafic.

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

Souvenez-vous en lisant le masque de masque (dans la binaire), 1 est considéré « ne s'inquiètent pas » la position binaire. Un tout le masque du masque 1s dans la représentation binaire se traduit à 0xFFFF dans la représentation hexadécimale.

Informations connexes

- Page de support de DLSw

- Listes de contrôle d'accès : Aperçu et instructions
- Techniques de filtrage SAP/MAC avec DLSw+
- Support technique - Cisco Systems