Présentation des listes de contrôle d'accès SAP (Service Access Point)

Contenu

Introduction

Ce document explique comment lire et créer des listes de contrôle d'accès SAP (Service Access Point) dans les routeurs Cisco. Bien qu'il existe plusieurs types de listes de contrôle d'accès, ce document se concentre sur celles qui filtrent en fonction des valeurs SAP. La plage numérique de ce type de liste de contrôle d'accès est comprise entre 200 et 299. Ces listes de contrôle d'accès peuvent être appliquées aux interfaces Token Ring pour filtrer le trafic SRB (Source Route Bridge), aux interfaces Ethernet pour filtrer le trafic To (Transparent Bridge) ou aux routeurs homologues DLSw (Data Link Switching).

Le principal défi avec les listes de contrôle d'accès SAP est de savoir exactement quels SAP sont autorisés ou refusés par une entrée de liste de contrôle d'accès donnée. 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.

Components Used

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

Architecture réseau des systèmes de filtrage

Le trafic SNA (Systems Network Architecture) d'IBM utilise des SAP allant de 0x00 à 0xFF. Virtual Telecommunications Access Method (VTAM) V3R4 et versions ultérieures prennent en charge une plage de valeurs SAP de 4 à 252 (ou 0x04 à 0xFC dans la représentation hexadécimale), où 0xF0 est réservé au trafic NetBIOS. Les SAP doivent être des multiples de 0x04, commençant par 0x04. La liste de contrôle d'accès suivante autorise les SAP SNA les plus courants et refuse le reste (considérant qu'il existe un **refus** implicite à la fin de chaque liste de contrôle d'accès) :

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

Hexadécimal	Binaire
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

Utilisez les bits du masque générique pour déterminer quels SAP sont autorisés par cette entrée de liste de contrôle d'accès particulière. Utilisez les règles suivantes lors de l'interprétation des bits de masque générique :

- 0 = correspondance exacte requise. Cela signifie que le SAP autorisé doit avoir la même valeur que le SAP configuré dans la liste de contrôle d'accès. Reportez-vous au tableau ci-dessous pour plus de détails.
- 1 = Le SAP autorisé peut avoir 0 ou 1 à cette position de bit, la position « ne vous souciez pas ».

Nombre de sauts autorisés par liste de contrôle d'accès, où X=0 ou X=1	Masque générique	SAP configuré dans 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

En utilisant les résultats du tableau précédent, la liste des SAP qui répondent au modèle ci-dessus est présentée ci-dessous.

Saps autorisés (binaire)	Sauts autorisés

								(hexadécimal)
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 le voir dans le tableau ci-dessus, tous les SAP SNA possibles ne sont pas inclus dans cette liste de contrôle d'accès. Ces SAP couvrent toutefois les cas les plus courants.

Un autre point à prendre en compte lors de la conception de la liste de contrôle d'accès est que les valeurs SAP changent selon qu'il s'agit de commandes ou de réponses. Le SSAP (Source Service Access Point) inclut le bit C/R (Command/Response) pour les différencier. Le C/R est défini sur 0 pour les commandes et sur 1 pour les réponses. Par conséquent, la liste de contrôle d'accès doit autoriser ou bloquer des commandes ainsi que des réponses. Par exemple, SAP 0x05 (utilisé pour les réponses) est SAP 0x04 avec le C/R défini sur 1. Il en va de même pour SAP 0x09 (SAP 0x08 avec C/R défini sur 1), 0x0D et 0x01.

Filtrage NetBIOS

Le trafic NetBIOS utilise les valeurs SAP 0xF0 (pour les commandes) et 0xF1 (pour les réponses). En règle générale, les administrateurs réseau utilisent ces valeurs SAP pour filtrer ce protocole. L'entrée de liste d'accès présentée ci-dessous autorise le trafic NetBIOS et refuse tout le reste (rappelez-vous le **refus** implicite à la fin de chaque liste de contrôle d'accès) :

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

Àl'aide de la même procédure présentée dans la section précédente, vous pouvez déterminer que la liste de contrôle d'accès ci-dessus autorise les SAP 0xF0 et 0xF1.

Au contraire, si la condition requise est de bloquer NetBIOS et d'autoriser le reste du trafic, utilisez la liste de contrôle d'accès suivante :

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

Filtrage IPX

Par défaut, les routeurs Cisco établissent un pont entre le trafic IPX. Pour modifier ce comportement, vous devez émettre la commande **ipx routing** sur le routeur. IPX, utilisant l'encapsulation 802.2, utilise SAP 0xE0 comme point d'accès au service de destination (DSAP) et SSAP. Par conséquent, si un routeur Cisco ponte IPX et que la condition requise est d'autoriser

uniquement ce type de trafic, utilisez la liste de contrôle d'accès suivante :

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

Au contraire, la liste de contrôle d’accès suivante bloque IPX et autorise le reste du trafic :

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

Autoriser ou refuser tout trafic

Chaque liste de contrôle d’accès inclut un **refus** implicite **all**. Vous devez connaître cette entrée lors de l’analyse du comportement d’une liste de contrôle d’accès configurée. La dernière entrée de liste de contrôle d’accès présentée ci-dessous refuse tout trafic.

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

N'oubliez pas que lors de la lecture du masque générique (en binaire), 1 est considéré comme une position de bit « ne vous souciez pas ». Un masque générique composé uniquement de 1 dans la représentation binaire se traduit par 0xFFFF dans la représentation hexadécimale.

Informations connexes

- Page de support DLSw
- Listes de contrôle d'accès : Présentation et directives
- Techniques de filtrage SAP/MAC avec DLSw+
- Support technique - Cisco Systems