了解业务访问点访问控制列表

目录

简介

本文档说明如何在思科路由器中读取和创建服务接入点(SAP)访问控制列表(ACL)。虽然ACL有几种类型，但本文档重点介绍基于SAP值过滤的ACL。此类ACL的数值范围是200到299。这些ACL可应用于令牌环接口以过滤源路由网桥(SRB)流量、以太网接口以过滤透明网桥(TB)流量或数据链路交换(DLSw)对等路由器。

SAP ACL的主要挑战是确切了解特定ACL条目允许或拒绝的SAP。我们将分析过滤特定协议的四种不同场景。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档不限于特定的软件和硬件版本。

过滤系统网络架构

IBM的系统网络架构(SNA)流量使用范围从0x00到0xFF的SAP。虚拟电信接入方法(VTAM)V3R4及

更高版本支持4到252（或0x04到0xFC的十六进制表示）的SAP值范围，其中0xF0保留用于NetBIOS流量。SAP必须是0x04的倍数，从0x04开始。以下ACL允许最常见的SNA SAP，并拒绝其余SAP(考虑到每个ACL的末尾有一个隐式**deny all**):

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

十六进制	二进制
0x0000 0x0D0D	DSAP SSAP Wildcard Mask for DSAP and SSAP respectively |-------| |-------| |-------| |-------| 0000 0000 0000 0000 0000 1101 0000 1101

使用通配符掩码中的位确定此特定ACL条目允许哪些SAP。解释通配符掩码位时，请使用以下规则：

- 0 =需要完全匹配。这意味着允许的SAP必须具有与ACL中配置的SAP相同的值。有关详细信息，请参阅下表。
- 1 =允许的SAP在此位位置可以有0或1，即“不在乎”位置。

ACL允许的SAP，其中X=0或X=1	通配符掩码	在ACL中配置的SAP
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

使用上表中的结果，符合上述模式的SAP列表如下所示。

允许的SAP（二进制）								允许的SAP（十六进制）
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

如上表所示，并非所有可能的SNA SAP都包含在此ACL中。但是，这些SAP涵盖最常见的案例。

设计ACL时需要考虑的另一点是，SAP值会根据它们是命令还是响应而改变。源服务接入点(SSAP)包括命令/响应(C/R)位，以区分它们。命令的C/R设置为0，响应的C/R设置为1。因此，ACL必须允许或阻止命令以及响应。例如，SAP 0x05（用于响应）是SAP 0x04,C/R设置为1。SAP 0x09（C/R设置为1的SAP 0x08）、0x0D和0x01也是如此。

过滤 NetBIOS

NetBIOS流量使用SAP值0xF0（用于命令）和0xF1（用于响应）。 通常，网络管理员使用这些SAP值来过滤此协议。下面显示的访问列表条目允许NetBIOS流量并拒绝其他所有流量(请记住每个ACL末尾的隐式**deny all):**

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

使用上一节中所示的相同步骤，您可以确定上述ACL允许SAP 0xF0和0xF1。

相反，如果要求阻止NetBIOS并允许其余流量，请使用以下ACL:

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

过滤 IPX

默认情况下，Cisco路由器桥接IPX流量。要更改此行为，您必须在路由器**上发**出ipx routing命令。IPX使用802.2封装，使用SAP 0xE0作为目标服务接入点(DSAP)和SSAP。因此，如果Cisco路由器桥接IPX，并且要求仅允许此类流量，请使用以下ACL:

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

相反，以下ACL会阻止IPX并允许其余流量：

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

允许或拒绝所有通信量

每个ACL都包含隐式**deny all**。在分析已配置ACL的行为时，必须了解此条目。下面显示的最后一个ACL条目拒绝所有流量。

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

请记住，读取通配符掩码（二进制）时，1被视为“不关心”位。二进制表示中的全1通配符掩码转换为十六进制表示中的0xFFFF。

相关信息

- DLSw支持页面
- 访问控制列表:概述和指南
- DLSw+ SAP/MAC 过滤技术
- 技术支持 - Cisco Systems