Security Device Manager:在一个使用NBAR的Cisco IOS路由器上阻塞P2P数据流配置示例

目录

简介

本文描述如何配置Cisco IOS路由器阻塞从网络内部的对等(P2P)使用基于网络的应用程序识别(NBAR)，流量到互联网。

NBAR 可识别网络中使用的特定网络协议和网络应用程序。一旦 NBAR 识别某个协议或应用程序，您就可以使用模块化服务质量命令行界面 (MQC) 对那些协议或应用程序的关联数据包进行分类。这些类将根据数据包是否符合某些标准进行划分。

对 NBAR 而言，该标准为数据包是否与 NBAR 已知的特定协议或应用程序相匹配。使用 MQC，与一个网络协议（如 Citrix）匹配的网络流量可以划分到一个流量类，与另一个网络协议（如 gnutella）匹配的流量则可以划分到另一个流量类。然后，可以使用流量策略（策略映射）对每个类中的网络流量进行适当的 QoS 处理。有关 NBAR 的详细信息，请参阅 *Cisco IOS 服务质量解决方案配置指南*的使用 NBAR 对网络流量进行分类部分。

先决条件

要求

在将 NBAR 配置为阻止 P2P 流量之前，必须启用 Cisco Express Forwarding (CEF)。

在全局配置模式下使用 **ip cef** 命令可启用 CEF：

```
Hostname(config)#ip cef
```

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 有Cisco IOS软件版本12.4(15)T的Cisco 2801路由器
- Cisco 安全设备管理器 (SDM) 版本 2.5

注意： 为了允许使用 SDM 配置路由器，请参阅使用 SDM 执行基本路由器配置。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Network Based Application Recognition (NBAR) 概述

Network-Based Application Recognition (NBAR) 是一种分类引擎，能够识别各种协议和应用程序并对其进行分类。当 NBAR 识别协议或应用程序并对其进行分类时，可以将网络配置为对该应用程序或使用该协议的流量应用适当的服务质量 (QoS)。

NBAR 执行以下功能：

- **识别应用程序和协议（第 4 层到第 7 层）** NBAR 能够对使用以下项目的应用程序进行分类：静态分配的传输控制协议 (TCP) 和用户数据报协议 (UDP) 端口号。非 UDP 和非 TCP IP 协议。动态分配的在建立连接期间协商的 TCP 和 UDP 端口号。需要对应用程序和协议的分类进行状态检测。状态检测是指数据连接发现功能。通过在具有分配功能的数据连接端口上传递控制连接，即可对数据连接进行分类。子端口分类：根据发布的应用程序名称对 HTTP（URL、mime 或主机名）和 Citrix 应用程序独立计算架构 (ICA) 流量进行分类。根据深度数据包检测和多种特定于应用程序的属性进行分类。Real-Time Transport Protocol (RTP) 有效载荷分类基于这样一种算法：根据 RTP 报头中的多个属性将数据包分类为 RTP。
- **协议发现**协议发现是一种常用 NBAR 功能，用于在每个接口收集应用程序和协议统计信息（数据包计数、字节数和比特率）。基于 GUI 的管理工具能够通过轮询 NBAR PD 管理信息库 (MIB) 的 SNMP 统计信息，以图形方式显示此信息。不管是何种联网功能，在部署到生产网络之前，都必须了解其性能和可扩展性。在基于软件的平台上，需要考虑的度量包括启用此功能时的 CPU 使用率影响，以及可持续数据速率。要将 NBAR 配置为在特定接口上发现 NBAR 已知的所有协议的流量，请在接口配置模式或 VLAN 配置模式下使用 ip nbar protocol-discovery 命令。要禁用流量发现，请使用 **no ip nbar protocol-discovery** 命令。

配置对等 (P2P) 流量阻塞

本部分提供有关如何配置本文档所述功能的信息。

注意： 某些 P2P 流量因其 P2P 协议特性而无法完全阻止。这些 P2P 协议会动态更改其签名，因而可避开任何尝试完全阻止其流量的 DPI 引擎。因此，Cisco 建议您限制带宽，而不是完全阻止它们。(请限制此流量的带宽。提供非常小的带宽，但需要让连接通过。)

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

路由器配置

用于在 Cisco IOS 路由器上阻止 P2P 流量的配置

```
R1#show run
Building configuration...

Current configuration : 4543 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
logging buffered 4096
enable secret 5 $1$bKq9$AHOxTgk6d3hcMGn6jTGxs/
!
aaa new-model
!
!
!
!
aaa session-id common
!--- IP CEF should be enabled at first to block P2P
traffic. !--- P2P traffic cannot be blocked when IPC CEF
is disabled. ip cef
!
!--- Configure the user name and password with Privilege
level 15 !--- to get full access when using SDM for
configuring the router. username cisco123 privilege 15
password 7 121A0C0411045D5679
secure boot-image
secure boot-config
archive
 log config
  hidekeys
!
!
!
!--- Configure the class map named p2p to match the P2P
protocols !--- to be blocked with this class map p2p.

class-map match-any p2p

!--- Mention the P2P protocols to be blocked in order to
block the !--- P2P traffic flow between the required
networks. edonkey, !--- fasttrack, gnutella, kazaa2,
skype are some of the P2P !--- protocols used for P2P
```

```
traffic flow. This example !--- blocks these protocols.
match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match protocol skype

!--- The access list created is now mapped with the
class map P2P !--- to specify the interesting traffic.
match access-group 102
!
!
!--- Here the policy map named SDM-QoS-Policy-2 is
created, and the !--- configured class map p2p is
attached to this policy map. !--- Drop is the command to
block the P2P traffic.

policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
!
!
!--- Below is the basic interface configuration on the
router. interface FastEthernet0/0 ip address
10.77.241.109 255.255.255.192 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.10.10.2
255.255.255.0 !--- The command ip nbar protocol-
discovery enables NBAR !--- protocol discovery on this
interface where the QoS !--- policy configured is being
used.

 ip nbar protocol-discovery
 duplex auto
 speed auto
!--- Use the service-policy command to attach a policy
map to !--- an input interface so that the interface
uses this policy map.

 service-policy input SDM-QoS-Policy-2
!
ip route 10.77.241.0 255.255.255.0 10.10.10.2
ip route 10.77.0.0 255.255.0.0 10.77.241.65
!
!--- Configure the below commands to enable SDM !---
access to the Cisco routers. ip http server
ip http authentication local
no ip http secure-server
!
!--- Configure the access lists and map them to the
configured class map. !--- Here the access list 102 is
mapped to the class map p2p. The access !--- lists are
created for both Incoming and outgoing traffic through
!--- the inside network interface.

access-list 102 remark SDM_ACL Category=256
access-list 102 remark Outgoing Traffic
access-list 102 permit ip 10.10.10.0 0.0.0.255
10.77.241.0 0.0.0.255
access-list 102 remark Incoming Traffic
access-list 102 permit ip 10.77.241.0 0.0.0.255
10.10.10.0 0.0.0.255
!
```

```
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 02250C520807082E01165E41
line vty 0 4
 exec-timeout 0 0
 password 7 05080F1C22431F5B4A
 transport input all
!
!
webvpn cef
end
```

使用 SDM 配置路由器

路由器 SDM 配置

请完成以下步骤，将 Cisco IOS 路由器配置为阻止 P2P 流量：

注意： 要将 NBAR 配置为在特定接口上发现 NBAR 已知的所有协议的流量，可在接口配置模式或 VLAN 配置模式下使用 ip nbar protocol-discovery 命令启用流量发现。在要使用已配置 QoS 策略的必需接口上配置协议发现后，请继续进行 SDM 配置。

```
Hostname#config t
               Hostname(config)#interface fastEthernet 0/1
               Hostname(config-if)#ip nbar protocol-discovery
               Hostname(config-if)#end
```

1. 打开浏览器，并输入已针对 SDM 访问进行配置的路由器的 IP 地址。例如，**https://<SDM_Router_IP_Address>**请确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空白。路由器显示此窗口，以便用户能够下载 SDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。SDM 下载现在开始。
2. 下载 SDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco SDM 启动程序。
3. 输入用户名和口令（如果已指定），然后单击 **OK**。此示例使用 **cisco123** 作为用户名，并使用 **cisco123** 作为口令。
4. 选择 **Configure > Quality of Service**，然后在 SDM 主页上单击 **Edit QoS Policy** 选项卡。
5. 从 View Policy on interface 下拉列表中选择接口名称，然后从 In Direction 下拉列表中选择数据流的方向（入站或出站）。在本示例中，接口为 *FastEthernet 0/1*，方向为 *inbound*。
6. 单击 **Add**，为接口添加新的 Qos 类。此时将显示 Add a QoS Class 对话框。
7. 如果要创建新类，请单击 **Class Name** 单选按钮并输入类名称。否则，请单击 **Class Default** 单选按钮（如果要使用默认类）。此示例创建了一个名为 *p2p* 的新类。
8. 在 Classification 区域中，单击“匹配”(Match) 选项所对应的 **Any** 单选按钮或 **All** 单选按钮。此示例使用 *Any* 匹配选项，该选项在路由器上运行 class-map match-any p2p 命令。
9. 在 Classifcation 列表中选择 **Protocol**，然后单击 **Edit** 以编辑协议参数。此时将显示 Edit Match Protocol Values 对话框。
10. 从 Available Protocol Values 列表中，选择您要阻止的每个 P2P 协议，然后单击右箭头 (**>>**) 按钮将每个协议移至 Selected Protocol Values 列表。**注意：** 要使用 NBAR 分类 P2P 流量，请转至软件下载页，并下载最新的 P2P 协议描述语言模块 (PDLM) 软件和自述文件。可供下载的 P2P PDLM 包括 WinMX、Bittorrent、Kazaa2、Gnutella、eDonkey、Fasttrack 和 Napster。根据您的 IOS，您可能不需要最新的 PDLM 版本，因为一些 PDLM（如 Fasttrack 和 Napster）可能已集成到您的 IOS 中。下载完成后，请将 PDLM 拷贝到路由器闪存，并通

过配置 **ip nbar pdlm <flash_device>:<filename>.pdlm** 将其加载到 IOS。发出 **show ip nbar pdlm** 命令以确保其加载成功。加载完成后，您就可以在类映射配置下的匹配协议语句中使用它们。

11. 单击 **Ok**。
12. 在 Add a QoS Class 对话框中，从 Classification 列表中选择 **Access Rules**，然后单击 **Edit** 以创建新的访问规则。您也可以将现有访问规则映射到 **p2p** 类映射。此时将显示 Edit Match ACL 对话框。
13. 点击访问规则按钮(...)和请选择适当的选项。本示例将创建新的 ACL。将出现“添加规则”对话框。
14. 在 Add a Rule 对话框中，在 ACL 的 Name/Number 字段中输入要创建的 ACL 名称或编号。
15. 从 Type 下拉列表中选择要创建的 ACL 的类型（*Extended Rule* 或 *Standard Rule*）。
16. 单击 **Add** 将详细信息添加到 ACL 102。将出现Add an Extended Rule条目对话框
17. 在 Add an Extended Rule Entry 对话框中，从 Select an action 下列列表中选择一个操作（*Permit* 或 *Deny*），指示 ACL 规则是应允许还是应拒绝源网络和目的地网络之间的流量。此规则适用于从内部网络到外部网络的传出流量。
18. 分别在 Source Host/Network 和 Destination Host/Network 区域中输入源网络和目的地网络的信息。
19. 在 Protocol and Service 区域单击相应的单选按钮。本示例使用 IP。
20. 如果要根据此 ACL 规则记录匹配的数据包，请选中 **Log Matches against this entry** 复选框。
21. 单击 **Ok**。
22. 在 Add a Rule 对话框中，单击 **OK**。
23. 在 Edit Match ACL 对话框中，单击 **OK**。
24. 在 Add a QoS Class 对话框中，选中 **Drop** 复选框以强制路由器阻止 P2P 流量。
25. 单击 **Ok**。默认情况下将显示以下警告消息，因为没有 QoS 策略映射到该接口。SDM 将自动生成 QoS 策略并将配置的类映射附加到该策略。与此 SDM 配置步骤对应的命令行界面 (CLI) 步骤如下所示：
```
R1(config)#policy-map SDM-QoS-Policy-2
R1(config-pmap)#class p2p
R1(config-pmap-c)#drop
R1(config-pmap-c)#end
R1#
```
26. 在 Edit QoS Policy 选项卡中单击 **Apply Changes**，将配置传送到路由器。

Cisco IOS 版本 12.4(4)T 及更高版本中的应用程序防火墙 - 即时消息流量实施功能

即时消息流量实施

通过应用程序防火墙 - 即时消息流量实施功能，用户可以定义并强制执行某种策略，从而指定哪些即时通讯流量类型可以进入网络。在 **application im** 下的 **appfw policy** 中进行配置时，您可以控制多个即时通讯软件（即 AOL、YAHOO 和 MSN）。因此，您还可以强制执行以下其他功能：

- 配置防火墙检测规则
- 有效负载的深度数据包检测（寻找文本聊天之类的服务）

注意： Cisco IOS 版本 12.4(4)T 及更高版本支持应用程序防火墙 - 即时消息流量实施功能。

即时通讯应用程序策略

应用程序防火墙使用应用程序策略（包括静态签名集合）来检测安全违规。静态签名是一个参数集

合，可用于指定在采取行动前必须满足的协议条件。这些协议条件和回应由终端用户通过 CLI 进行定义，从而形成应用程序策略。

Cisco IOS 应用程序防火墙已经得到增强，可支持即时本地通讯软件应用程序策略。因此，Cisco IOS 防火墙现在能够检测和禁止 AOL Instant Messenger (AIM)、Yahoo! Messenger 和 MSN Messenger 即时消息服务与即时通讯服务器的用户连接。此功能可以控制支持的服务（包括文本、语音、视频和文件传输功能）的所有连接。可以单独拒绝或允许这三个应用程序。每项服务都可以单独进行控制，因此，您可以在允许文本聊天服务的同时，限制语音、文件传输、视频和其他服务。此功能增强了现有的应用程序检测功能，可控制伪装成 HTTP (Web) 流量的即时通讯 (IM) 应用流量。有关详细信息，请参阅应用程序防火墙 - 即时消息流量实施。

注意： 如果 IM 应用程序被阻止，则会重置连接并根据情况生成 syslog 消息。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ip nbar pdlm** - 要显示 NBAR 所使用的 PDLM，请在特权 EXEC 模式下使用 **show ip nbar pdlm** 命令：
```
Router#show ip nbar pdlm
        The following PDLMs have been loaded:
        flash://edonkey.pdlm
        flash://fasttrack.pdlm
        flash://gnutella.pdlm
        flash://kazaa2.pdlm
```
- **show ip nbar version** - 要显示 Cisco IOS 版本中的 NBAR 软件版本或 Cisco IOS 路由器上的 NBAR PDLM 版本的相关信息，请在特权 EXEC 模式下使用 **show ip nbar version** 命令：
```
R1#show ip nbar version

NBAR software version:  6

1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 9
4   static               Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 10
14  fasttrack            Mv: 2
15  gnutella             Mv: 4
16  kazaa2               Mv: 7
17  custom-protocols     Mv: 1
18  rtsp                 Mv: 4
19  rtp                  Mv: 5
20  mgcp                 Mv: 2
21  skinny               Mv: 1
22  h323                 Mv: 1
23  sip                  Mv: 1
24  rtcp                 Mv: 2
```

```
25  edonkey              Mv: 5
26  winmx                Mv: 3
27  bittorrent           Mv: 4
28  directconnect        Mv: 2
29  skype                Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>
}{Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}
```

- show policy-map interface - 要显示为所有服务策略配置的所有类的数据包统计数据，不管是在指定的接口或子接口上配置的，还是在接口的特定永久虚电路 (PVC) 上配置的，均请在特权 EXEC 模式下使用 **show policy-map interface** 命令：`R1#show policy-map interface fastEthernet 0/1`

```
 FastEthernet0/1

  Service-policy input: SDM-QoS-Policy-2

    Class-map: p2p (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: protocol edonkey
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol fasttrack
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol gnutella
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol kazaa2
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol winmx
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: access-group 102
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: protocol skype
        0 packets, 0 bytes
        5 minute rate 0 bps
      drop

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **show running-config policy-map** - 要显示所有策略映射配置以及默认策略映射配置，请使用 **show running-config policy-map** 命令：`R1#show running-config policy-map`

```
Building configuration...

Current configuration : 57 bytes
!
policy-map SDM-QoS-Policy-2
 class p2p
   drop
!
end
```

- **show running-config class-map** - 要显示有关类映射配置的信息，请使用 **show running-config class-map** 命令：`R1#show running-config class-map`

```
Building configuration...
```

```
Current configuration : 178 bytes
!
class-map match-any p2p
 match protocol edonkey
 match protocol fasttrack
 match protocol gnutella
 match protocol kazaa2
 match protocol winmx
 match access-group 102
!
end
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **show access-list** - 要显示在 Cisco IOS 路由器上运行的访问列表配置，请使用 **show access-list** 命令：`R1#show access-lists`

```
Extended IP access list 102
    10 permit ip 10.10.10.0 0.0.0.255 10.77.241.0 0.0.0.255
    20 permit ip 10.77.241.0 0.0.0.255 10.10.10.0 0.0.0.255
```

相关信息

- Cisco IOS 安全配置指南 12.4 版 - 支持
- 基于网络的应用程序识别 (NBAR)
- Cisco 快速转发 (CEF)
- 技术支持和文档 - Cisco Systems