H3C MSR810[2600][3600]路由器

DPI 深度安全配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W304-20190828
产品版本：MSR-CMW710-R0707

前 言

本配置指导主要介绍 IPS、URL 过滤和带宽管理等的配置。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料意见反馈

1.1 读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

1.2 本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
说明	对操作内容的描述进行必要的补充和说明。
窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

1.3 资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 DPI深度安全概述 ····· 1-1
1.1 DPI深度安全简介 ····· 1-1
1.1.1 DPI深度安全的功能 ····· 1-1
1.1.2 DPI特征库 ····· 1-1
1.1.3 DPI业务 ····· 1-1
1.1.4 DPI深度安全的处理流程 ····· 1-2
1.2 DPI深度安全概述与硬件适配关系 ····· 1-3
1.3 DPI深度安全配置流程 ····· 1-4

1 DPI深度安全概述

1.1 DPI深度安全简介

DPI（Deep Packet Inspection，深度报文检测）深度安全是一种基于应用层信息对经过设备的网络流量进行检测和控制的安全机制。在日益复杂的网络安全威胁中，很多恶意行为（比如，蠕虫病毒、垃圾邮件、漏洞等）都是隐藏在数据报文的应用层载荷中。传统防火墙技术仅仅依靠网络层和传输层的安全检测技术已经无法满足网络安全要求。因此，设备必须具备 DPI 功能，实现对网络应用层信息的检测和控制，以保证数据内容的安全，提高网络的安全性。

1.1.1 DPI深度安全的功能

DPI 深度安全提供如下功能：

- 业务识别

  应用层检测引擎模块对报文传输层以上的内容进行分析，并与设备中的特征字符串进行匹配来识别业务流的类型。应用层检测引擎是实现 DPI 深度安全功能的核心和基础。业务识别的结果可为 DPI 各业务模块对报文的处理提供判断依据。

- 业务控制

  业务识别之后，设备根据各 DPI 业务模块的策略以及规则配置，实现对业务流量的灵活控制。目前，设备支持的控制方法主要包括：放行、丢弃、源阻断、重置、捕获和生成日志。

- 业务统计

  业务统计是指对业务流量的类型、协议解析的结果、特征报文的检测和处理结果等进行统计。业务统计的结果可以直观体现业务流量分布和用户的各种业务使用情况，便于更好的发现促进业务发展和影响网络正常运行的因素，为网络和业务优化提供依据。

1.1.2 DPI特征库

DPI 深度安全功能的业务识别是对报文进行特征字符串匹配，所以设备中必须拥有业务识别所需要的特征项。DPI 特征库就是这些公共的、通用的特征项的集合，可被打包到标准的特征库文件中供设备加载。通常情况下，管理员只需要定期加载最新的特征库文件到设备上即可及时更新本地的特征项。除此之外，管理员还可以根据实际网络需求按照设备支持的语法，自定义特征，作为特殊网络环境下的补充。

目前，设备中支持的 DPI 特征库包括：IPS 特征库、URL 分类特征库和 APR 特征库。

1.1.3 DPI业务

有关设备支持的DPI业务介绍，请参见 表 1-1。

表1-1 DPI 业务详细介绍

DPI 业务	功能
IPS	IPS通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作

DPI 业务	功能
	来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的
URL过滤	URL过滤功能可对用户访问的URL进行控制，即允许或禁止用户访问的Web资源，达到规范用户上网行为的目的
NBAR	NBAR功能通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议，有关NBAR功能的详细介绍请参见“安全配置指导”中的“APR”

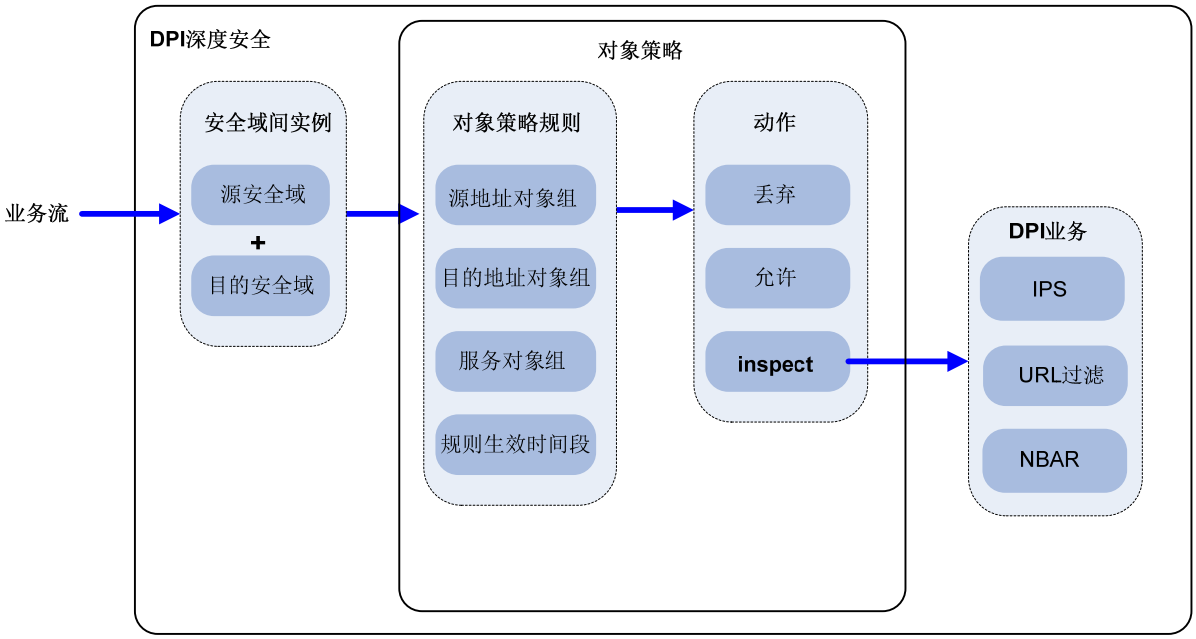
1.1.4 DPI深度安全的处理流程

DPI 深度安全功能基于对象策略实现。

1. 基于对象策略实现DPI深度安全功能

当属于某安全域间实例的报文经过设备时，DPI深度安全处理流程如 图 1-1 所示。

图1-1 DPI 深度安全处理流程图



DPI 深度安全处理流程具体如下：

(1) 进入安全域间实例的报文将与此安全域间实例下的对象策略规则进行匹配。每一个安全域间实例下可以关联多个对象策略规则，且其中定义了匹配报文的源 IP 地址、目的 IP 地址和服务类型等信息。仅当报文与对象策略规则中的所有条件都匹配，才认为成功匹配对象策略规则。有关安全域间实例的详细介绍请参见“安全配置指导”中的“安全域”。

(2) 如果报文未与对象策略规则匹配成功，则此报文将会被拒绝通过。

(3) 如果报文成功匹配对象策略规则，设备将执行此对象策略规则中指定的动作。

- 如果动作为“丢弃”，则设备将阻断此报文；
- 如果动作为“允许”，则设备将允许此报文通过；

- 如果动作为“**inspect**”，且引用的 DPI 业务存在，则设备将对此报文进行 DPI 业务的一体化检测。
- 如果动作为“**inspect**”，且引用的 DPI 业务不存在，则设备将允许此报文通过。

1.2 DPI深度安全概述与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

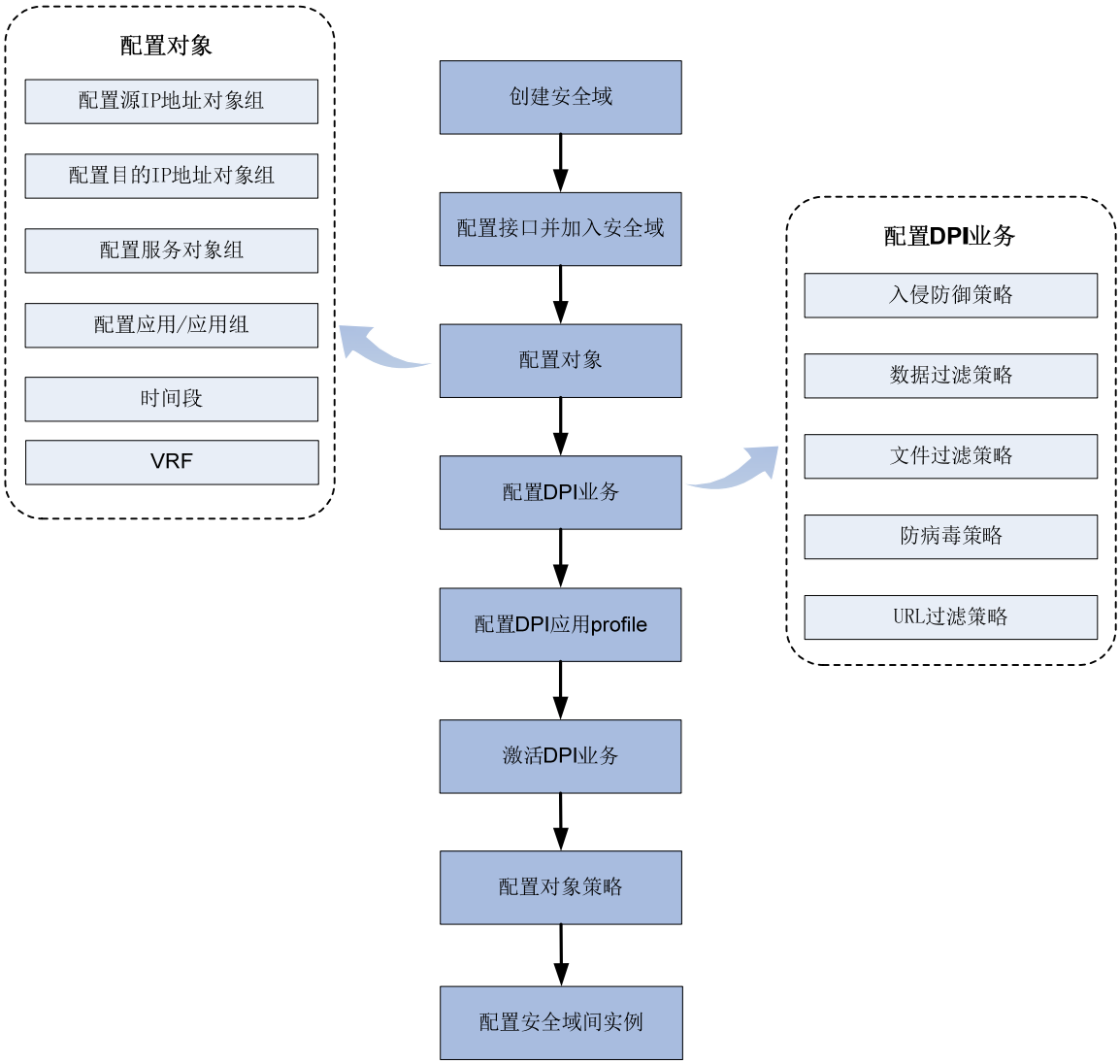
型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.3 DPI深度安全配置流程

DPI深度安全是一种综合的安全机制，是多种安全业务功能的系统组合，有关DPI深度安全的常规配置流程如 图 1-2 所示。

图1-2 DPI 深度安全配置指导图



目 录

1 应用层检测引擎 1-1
1.1 应用层检测引擎简介 1-1
1.1.1 应用层检测引擎的基本功能 1-1
1.1.2 检测规则 1-1
1.1.3 应用层检测引擎工作机制 1-1
1.2 应用层检测引擎与硬件适配关系 1-3
1.3 应用层检测引擎配置任务简介 1-4
1.4 配置DPI应用Profile 1-4
1.5 激活DPI业务模块的策略和规则配置 1-5
1.6 配置应用层检测引擎动作参数 1-5
1.6.1 配置源阻断动作参数 1-5
1.6.2 配置捕获动作参数 1-6
1.6.3 配置日志动作参数 1-6
1.6.4 配置重定向动作参数 1-7
1.6.5 配置邮件动作参数 1-7
1.7 优化应用层检测引擎性能 1-8
1.8 配置应用层检测引擎CPU门限响应功能 1-9
1.9 配置应用层检测引擎检测固定长度数据流功能 1-9
1.10 配置DPI业务特征库在线升级所使用的代理服务器 1-10
1.11 配置DPI业务云端服务器 1-10
1.12 关闭应用层检测引擎功能 1-11
1.13 应用层检测引擎显示和维护 1-11

1 应用层检测引擎

1.1 应用层检测引擎简介

应用层检测引擎服务于 DPI 业务模块，用于对报文的应用层信息（应用层协议以及应用行为）进行统一识别。DPI 业务模块使用应用层检测引擎提供的识别结果，对报文进行相应的业务处理。

1.1.1 应用层检测引擎的基本功能

应用层检测引擎提供以下基本功能：

- 协议解析：识别并分析报文应用层字段，区分应用层协议，并对部分字段进行正规化和解压缩。
- 关键字匹配：根据检测规则对报文载荷内容进行关键字匹配，是应用层检测引擎的核心。
- 选项匹配：关键字匹配成功后，对其所属检测规则中的选项做进一步匹配。该过程与关键字匹配相比，匹配速度比较缓慢。

1.1.2 检测规则

应用层检测引擎使用检测规则对报文进行匹配，检测规则由各 DPI 业务的规则或特征转换而成，包含关键字和选项两种匹配项。

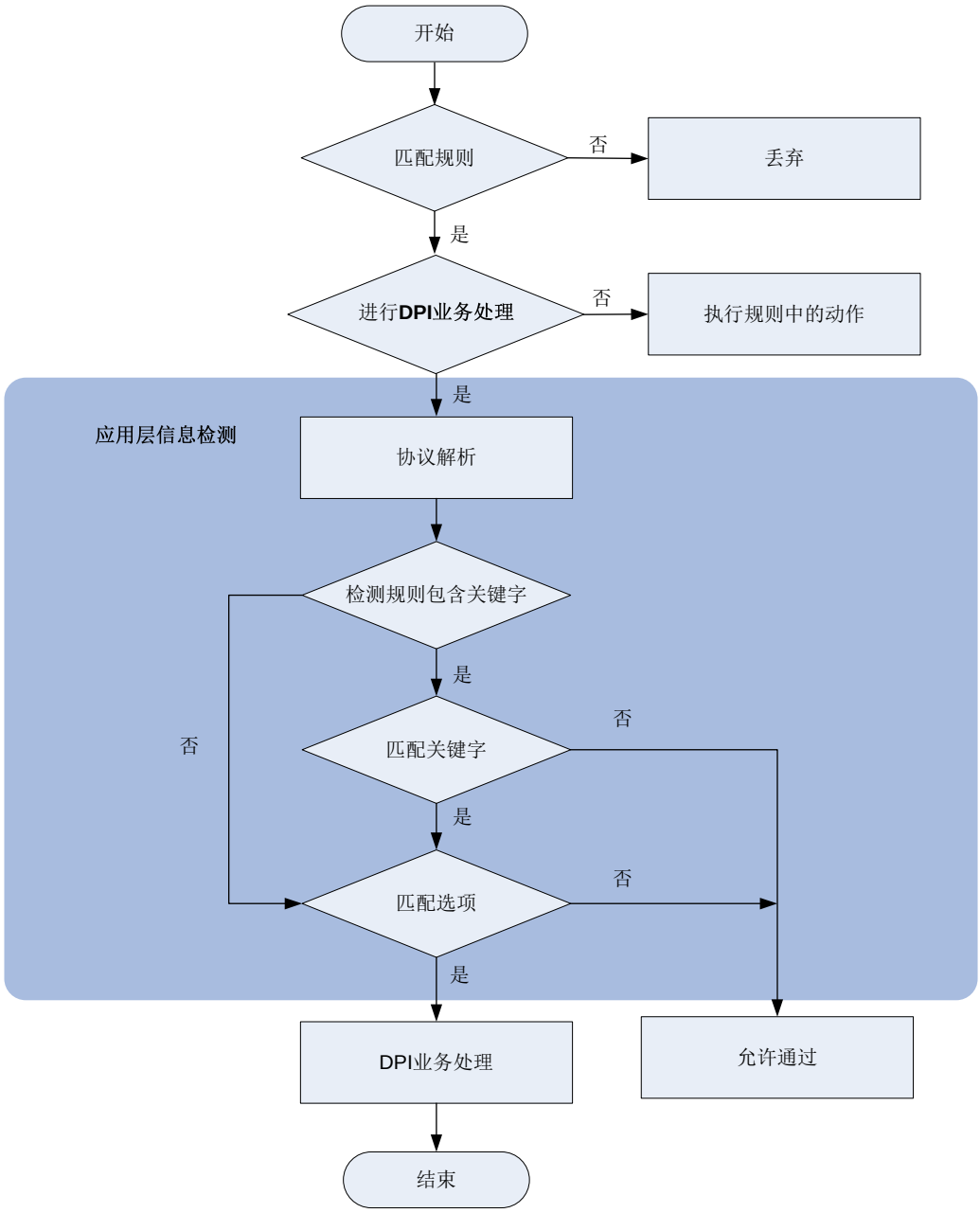
- 关键字：标识报文特征的不少于 3 个字节的字符串，也称作“AC 关键字”。
- 选项：非关键字的辅助匹配项，例如报文的端口号、协议类型等。

检测规则中可以同时包含关键字和选项，或者仅包含选项。如果检测规则中同时包含关键字和选项，则两者都被匹配上才算是与该检测规则匹配成功；如果检测规则中仅包含选项，则只要匹配选项就算与该检测规则匹配成功。

1.1.3 应用层检测引擎工作机制

如 图 1-1 所示，应用层检测引擎的具体工作机制如下：

图1-1 应用层检测引擎工作机制示意图



应用层检测引擎的处理机制如下：

(2) 设备收到报文后，首先对报文进行规则（即对象策略规则）匹配：

- 如果规则匹配成功，且规则中需要进行 DPI 业务处理，则此报文进入应用层检测引擎处理；如果规则中不需要进行 DPI 业务处理，则根据规则中的动作对此报文进行处理。
- 如果规则匹配失败，则直接丢弃此报文。

有关对象策略规则的详细介绍请参见“安全配置指导”中的“对象策略”。

(3) 报文进入应用层检测引擎后，应用层检测引擎首先对报文进行协议解析，根据分析结果查找相应的检测规则。

(4) 应用层检测引擎判断检测规则中是否包含关键字，如果包含关键字，则首先进行关键字匹配，否则直接进行选项匹配。

(5) 如果报文匹配上关键字，则继续进行选项匹配（该选项是匹配上的关键字所属检测规则中的选项）；如果报文未匹配上关键字，则直接允许报文通过。

(6) 如果报文与选项匹配成功，则表示此报文与该检测规则匹配成功。

(7) 应用层检测引擎通知相应的 DPI 业务模块对此报文做进一步的处理；如果报文与选项匹配失败，则直接允许报文通过。

1.2 应用层检测引擎与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持

型号	描述
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.3 应用层检测引擎配置任务简介

应用层检测引擎配置任务如下：

(1) 配置DPI应用Profile

(2) 激活DPI业务模块的策略和规则配置

(3) 配置应用层检测引擎动作参数

(4) （可选）优化应用层检测引擎性能

(5) （可选）配置应用层检测引擎CPU门限响应功能

(6) （可选）配置应用层检测引擎检测固定长度数据流功能

(7) （可选）配置DPI业务特征库在线升级所使用的代理服务器

(8) （可选）配置DPI业务云端服务器

(9) （可选）关闭应用层检测引擎功能

1.4 配置DPI应用Profile

1. 功能简介

DPI 应用 profile 是 DPI 业务的配置模板，用于关联各 DPI 业务的策略（例如 URL 过滤业务）。DPI 应用 profile 被对象策略规则引用后，各 DPI 业务策略才能生效。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 DPI 应用 profile 视图，并进入 DPI 应用 profile 视图。

app-profile *profile-name*

(3) 关联各 DPI 业务策略。

- 在 DPI 应用 profile 中引用 IPS 策略。

  ips apply policy *policy-name* **mode** { **protect** | **alert** }

  关于该命令的详细介绍请参见“DPI 深度安全命令参考”中的“IPS”。
- 在 DPI 应用 profile 中引用 URL 过滤策略。

  url-filter apply policy *policy-name*

  关于该命令的详细介绍请参见“DPI 深度安全命令参考”中的“URL 过滤”。

缺省情况下，未关联 DPI 业务策略。

1.5 激活DPI业务模块的策略和规则配置

1. 功能简介

当 DPI 业务模块（比如 URL 过滤业务）的策略和规则被创建、修改和删除后，有以下方式可以使得这些策略和规则的配置生效：

- 保存配置后重启设备
- 执行 **inspect activate** 命令

2. 配置限制和指导

执行 **inspect activate** 命令会暂时中断 DPI 业务的处理，为了避免重复执行此命令对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一执行此命令。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 激活 DPI 业务模块的策略和规则配置。

inspect activate

缺省情况下，DPI 业务模块的策略和规则被创建、修改和删除时不生效。

1.6 配置应用层检测引擎动作参数

1.6.1 配置源阻断动作参数

1. 功能简介

源阻断动作参数 profile 用来为 DPI 业务模块的源阻断动作提供动作参数，在此 profile 中可以配置报文被阻断的时长。

2. 配置限制和指导

本功能仅在开启黑名单过滤功能后生效。如果设备上开启了黑名单过滤功能，则在源阻断动作参数 profile 中配置的阻断时长内，来自该源 IP 地址的报文将被直接丢弃，不再进入应用层检测引擎中检测。

有关黑名单过滤功能的详细介绍，请参见“安全配置指导”中的“攻击检测与防范”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建应用层检测引擎的源阻断动作参数 profile，并进入该源阻断动作参数 profile 视图。

inspect block-source parameter-profile *parameter-name*

(3) 配置报文源 IP 地址被阻断的时长。

block-period *period*

缺省情况下，报文源 IP 地址被阻断的时长为 1800 秒。

1.6.2 配置捕获动作参数

1. 功能简介

捕获动作参数 profile 用来为 DPI 业务模块的捕获动作提供动作参数，在此 profile 中可以配置捕获报文的最大字节数、捕获报文的上传时间和 URL 地址参数。

捕获到的报文将被缓存到设备本地，并在以下任意条件满足的情况下被上传到指定的 URL 上：

- 缓存的报文字节数达到指定上限值时；
- 当天指定的上传时间到达时

上传到指定的 URL 之后，系统将清空本地缓存，然后重新开始捕获报文。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建应用层检测引擎的捕获动作参数 profile 视图，并进入该捕获动作参数 profile 视图。

inspect capture parameter-profile *parameter-name*

(3) 配置捕获报文的最大字节数。

capture-limit *kilobytes*

缺省情况下，捕获报文的最大字节数为 512 千字节。

(4) 配置每天定时上传捕获报文的时间。

export repeating-at *time*

缺省情况下，每天凌晨 1 点定时上传捕获报文。

(5) 配置上传捕获报文的 URL 地址。

export url *url-string*

缺省情况下，未配置上传捕获报文的 URL 地址。

1.6.3 配置日志动作参数

1. 功能简介

日志动作参数 profile 用来为 DPI 业务模块的日志动作提供动作参数，此 profile 中可以配置日志的输出方式。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建应用层检测引擎的日志动作参数 profile 视图，并进入该日志动作参数 profile 视图。

inspect logging parameter-profile *parameter-name*

(3) 配置记录报文日志的方式。

log { email | syslog }

缺省情况下，报文日志被输出到信息中心。

1.6.4 配置重定向动作参数

1. 功能简介

重定向动作参数 profile 用来为 DPI 业务模块的重定向动作提供动作参数，在此 profile 中可以配置重定向报文的 URL。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建应用层检测引擎的重定向动作参数 profile，并进入重定向动作参数 profile 视图。

inspect redirect parameter-profile *parameter-name*

(3) 配置重定向 URL。

redirect-url *url-string*

缺省情况下，未配置重定向 URL。

1.6.5 配置邮件动作参数

1. 功能简介

邮件动作参数 profile 用来为 DPI 业务模块的邮件动作提供动作参数，在此 profile 中可以配置邮件服务器地址、收件人与发件人地址和登录邮件服务器的用户名和密码等。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建应用层检测引擎的邮件动作参数 profile 视图，并进入邮件动作参数 profile 视图。

inspect email parameter-profile *parameter-name*

(3) 配置邮件服务器的地址。

email-server *addr-string*

缺省情况下，未配置邮件服务器的地址。

(4) 配置域名解析服务器的地址。

dns-server *ip-address*

缺省情况下，未配置域名解析服务器的地址。

(5) 配置发件人地址。

sender *addr-string*

缺省情况下，未配置发件人地址。

(6) 配置收件人地址。

receiver *addr-string*

缺省情况下，未配置收件人地址。

(7) （可选）配置客户端身份验证功能。

a. 开启发送邮件的认证功能。

authentication enable

缺省情况下，发送邮件的认证功能处于开启状态。

b. 配置登录邮件服务器的用户名。

username *name-string*

缺省情况下，未配置登录邮件服务器的用户名。

c. 配置登录邮件服务器的密码。

password { **cipher** | **simple** } *string*

缺省情况下，未配置登录邮件服务器的密码。

d. （可选）开启安全传输登录邮件服务器密码功能。

secure-authentication enable

缺省情况下，安全传输登录邮件服务器密码功能处于关闭状态。

1.7 优化应用层检测引擎性能

1. 功能简介

对经过压缩或编码等处理后的报文应用层信息进行识别时，需要应用层检测引擎先对此类报文进行解压缩或解码等相应处理后才能识别。通过开启应用层检测引擎性能优化功能或调高各项性能参数，可以提高应用层信息的识别能力和准确率，但同时也会消耗一定的系统资源。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置应用层检测引擎可检测有载荷内容的报文的最大数目。

inspect packet maximum *max-number*

缺省情况下，应用层检测引擎可检测有载荷内容的报文的最大数目为 32。

(3) 配置应用层检测引擎缓存待检测选项的最大数目。

inspect cache-option maximum *max-number*

缺省情况下，应用层检测引擎缓存待检测选项的最大数目为 32。

(4) 配置 TCP 数据段重组功能

a. 开启 TCP 数据段重组功能。

inspect tcp-reassemble enable

缺省情况下，TCP 数据段重组功能处于关闭状态。

b. 配置 TCP 数据段重组缓存区可缓存的 TCP 数据段最大数目。

inspect tcp-reassemble max-segment *max-number*

缺省情况下，TCP 数据段重组缓冲区可缓存的 TCP 数据段最大数目为 10。

(5) （可选）关闭指定的应用层检测引擎的优化调试功能。

inspect optimization [chunk | no-acsignature | raw | uncompress | url-normalization] disable

缺省情况下，应用层检测引擎的所有优化调试功能处于开启状态。

如果设备的吞吐量较差，不能满足基本的通信需求，可关闭相关优化调试功能提高设备的性能。

1.8 配置应用层检测引擎CPU门限响应功能

1. 功能简介

应用层检测引擎对报文的检测是一个比较复杂且会占用一定系统资源的过程。当设备的 CPU 利用率较高时，应用层检测引擎 CPU 门限响应功能会启动如下机制来缓解系统资源紧张的问题。

- 当 CPU 利用率达到设备上配置的 CPU 利用率阈值时：
  - 若固定长度数据流检测功能处于关闭状态，则系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。
  - 若固定长度数据流检测功能处于开启状态，则应用层检测引擎只对一条数据流首包后固定长度内的数据进行检测，超出固定长度后的数据不再进行检测。
- 当设备的 CPU 利用率恢复到或低于设备上配置的 CPU 利用率恢复阈值时，系统会对整条数据流的内容进行检测。

有关 CPU 利用率的详细配置请参见“基础配置指导”中的“设备管理”。

2. 配置限制和指导

在系统 CPU 占用率较高的情况下，建议保持应用层检测引擎 CPU 门限响应功能处于开启状态；在系统 CPU 占用率较低的情况下，可以考虑关闭本功能。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启应用层检测引擎 CPU 门限响应功能。

undo inspect cpu-threshold disable

缺省情况下，应用层检测引擎 CPU 门限响应功能处于开启状态。

1.9 配置应用层检测引擎检测固定长度数据流功能

1. 功能简介

应用层检测引擎检测固定长度数据流功能，是指当设备的 CPU 利用率达到设备上配置的 CPU 利用率阈值时，应用层检测引擎只检测每条数据流首包后固定长度内的数据，不再检测超出固定长度后的数据。当设备的 CPU 利用率恢复到设备上配置的 CPU 利用率恢复阈值时，系统会对整条数据流的内容进行检测。有关 CPU 利用率的详细配置请参见“基础配置指导”中的“设备管理”。

2. 配置限制和指导

开启应用层检测引擎 CPU 门限响应功能，此功能才会生效。

当设备的 CPU 利用率较高的情况下，建议关闭此功能，此时应用层检测引擎 CPU 门限响应功能开启的情况下，系统会自动关闭应用层检测引擎的检测功能来保证设备的正常运行。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启应用层检测引擎检测固定长度数据流功能。

undo inspect stream-fixed-length disable

缺省情况下，应用层检测引擎检测固定长度数据流功能处于开启状态。

(3) 配置应用层检测引擎检测数据流的固定长度。

inspect stream-fixed-length { **email** | **ftp** | **http** } * *length*

缺省情况下，应用层检测引擎对 FTP 协议、HTTP 协议和与 E-mail 相关协议数据流的固定检测长度均为 32 千字节。

调高此参数后，设备的吞吐量性能会下降，但是应用层信息识别的成功率会提高；同理调低参数后，设备的吞吐量会增加，但是应用层信息识别的成功率会降低。

1.10 配置DPI业务特征库在线升级所使用的代理服务器

1. 功能简介

当 DPI 业务模块（例如 URL 过滤）的特征库进行在线升级时，若设备不能连接到官方网站，则可配置一个代理服务器使设备连接到官方网站上的特征库服务专区，进行特性库在线升级。有关特征库在线升级功能的详细介绍，请参见各 DPI 业务配置指导手册中的“特征库升级与回滚”。

2. 配置限制和指导

代理服务器可以通过 IP 地址或者域名的方式进行访问。如果使用域名方式，请确保设备能通过静态或动态域名解析方式获得代理服务器的 IP 地址，并与之路由可达。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DPI 业务特征库在线升级所使用的代理服务器。

inspect signature auto-update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* **password** { **cipher** | **simple** } *string*]

缺省情况下，未配置 DPI 业务特征库在线升级所使用的代理服务器。

1.11 配置DPI业务云端服务器

1. 功能简介

DPI 云端服务器为各 DPI 业务提供云端查询功能，目前支持 URL 过滤分类查询。

2. 配置限制和指导

配置 DPI 云端查询功能时，需要确保设备能通过静态或动态域名解析方式获得 DPI 云端服务器的 IP 地址，并与之路由可达，否则进行云端查询会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 DPI 业务云端服务器。

inspect cloud-server *host-name*

缺省情况下，DPI 云端服务器主机名为 sec.h3c.com。

1.12 关闭应用层检测引擎功能

1. 功能简介

应用层检测引擎对报文的检测是一个复杂且会占用一定系统资源的过程。开启应用层检测引擎功能后，如果出现系统 CPU 使用率过高等情况时，可通过关闭此功能来降低对设备转发性能的影响。

关闭应层检测引擎功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 关闭应用层检测引擎功能。

inspect bypass

缺省情况下，应用层检测引擎功能处于开启状态。

1.13 应用层检测引擎显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后应用层检测引擎的运行情况。

表1-1 应用层检测引擎显示和维护

操作	命令
显示应用层检测引擎的运行状态	**display inspect status**

目 录

1 IPS ····· 1-1
1.1 IPS简介 ····· 1-1
1.1.1 IPS的功能 ····· 1-1
1.1.2 IPS策略 ····· 1-1
1.1.3 IPS实现流程 ····· 1-2
1.1.4 IPS特征库升级与回滚 ····· 1-3
1.2 IPS与硬件适配关系 ····· 1-3
1.3 IPS的License要求 ····· 1-5
1.4 IPS配置任务简介 ····· 1-5
1.5 IPS配置准备 ····· 1-5
1.6 创建IPS策略 ····· 1-5
1.7 配置筛选IPS特征的属性 ····· 1-6
1.8 配置IPS动作 ····· 1-6
1.9 配置IPS引用的应用层检测引擎动作参数profile ····· 1-7
1.10 在DPI应用profile中引用IPS策略 ····· 1-7
1.11 激活IPS策略配置 ····· 1-8
1.12 在对象策略中引用IPS业务 ····· 1-8
1.13 配置IPS特征库升级和回滚 ····· 1-9
1.13.1 配置限制和指导 ····· 1-9
1.13.2 配置定期自动在线升级IPS特征库 ····· 1-9
1.13.3 立即自动在线升级IPS特征库 ····· 1-9
1.13.4 手动离线升级IPS特征库 ····· 1-10
1.13.5 回滚IPS特征库 ····· 1-10
1.14 导入和删除自定义IPS特征 ····· 1-10
1.14.1 导入自定义IPS特征 ····· 1-10
1.14.2 删除所有导入的自定义IPS特征 ····· 1-11
1.15 IPS显示和维护 ····· 1-11
1.16 IPS典型配置举例 ····· 1-11
1.16.1 在对象策略中引用缺省IPS策略配置举例 ····· 1-11
1.16.2 在对象策略中引用自定义IPS策略配置举例 ····· 1-13
1.16.3 手动离线升级IPS特征库配置举例 ····· 1-15
1.16.4 定时自动升级IPS特征库配置举例 ····· 1-16

1 IPS

1.1 IPS简介

IPS（Intrusion Prevention System，入侵防御系统）是一种可以对应用层攻击进行检测并防御的安全防御技术。IPS 通过分析流经设备的网络流量来实时检测入侵行为，并通过一定的响应动作来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的。

1.1.1 IPS的功能

IPS 具有以下功能：

- 深度防护：可以检测报文应用层的内容，以及对网络数据流进行协议分析和重组，并根据检测结果来对报文做出相应的处理。
- 实时防护：实时检测流经设备的网络流量，并对入侵活动和攻击性网络流量进行实时拦截。
- 全方位防护：可以对多种攻击类型提供防护措施，例如蠕虫、病毒、木马、僵尸网络、间谍软件、广告软件、CGI（Common Gateway Interface）攻击、跨站脚本攻击、注入攻击、目录遍历、信息泄露、远程文件包含攻击、溢出攻击、代码执行、拒绝服务、扫描工具、后门等。
- 内外兼防：对经过设备的流量都可以进行检测，不仅可以防止来自企业外部的攻击，还可以防止发自企业内部的攻击。

1.1.2 IPS策略

设备基于 IPS 策略对报文进行 IPS 处理。IPS 策略中定义了匹配报文的 IPS 特征和处理报文的 IPS 动作。

1. IPS特征

IPS 特征用来描述网络中的攻击行为的特征，设备通过将报文与 IPS 特征进行比较来检测和防御攻击。IPS 特征包含多种属性，例如攻击分类、动作、保护对象、严重级别和方向。这些属性可作为过滤条件来筛选 IPS 特征。

设备支持以下两种类型的 IPS 特征：

- 预定义 IPS 特征：系统中的 IPS 特征库自动生成。设备不支持对预定义 IPS 特征的内容进行创建、修改和删除。
- 自定义 IPS 特征：管理员在设备上手工创建。通常新的网络攻击出现后，与其对应的攻击特征会出现的比较晚一些。如果管理员已经掌握了新网络攻击行为的特点，可以通过自定义方式创建 IPS 特征，及时阻止网络攻击，否则，不建议用户自定义 IPS 特征。

2. IPS动作

IPS 动作是指设备对匹配上 IPS 特征的报文做出的处理。IPS 处理动作包括如下几种类型：

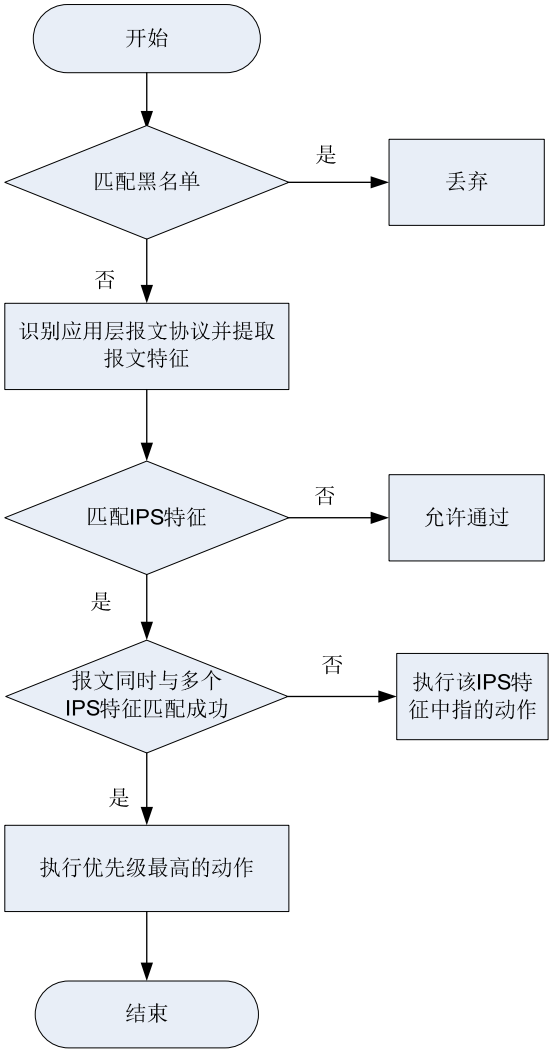
- 重置：通过发送 TCP 的 reset 报文断开 TCP 连接。
- 重定向：把符合特征的报文重定向到指定的 Web 页面上。

- 源阻断：阻断符合特征的报文，并会将该报文的源 IP 地址加入 IP 黑名单。如果设备上同时开启了 IP 黑名单过滤功能（由 **blacklist global enable** 开启），则一定时间内（由 **block-period** 命令指定）来自此 IP 地址的所有报文将被直接丢弃；否则，此 IP 黑名单不生效。有关 IP 黑名单过滤功能的详细介绍请参见“安全配置指导”中的“攻击检测与防范”，有关 **block-period** 命令的详细介绍请参见“DPI 深度安全”中的“应用层检测引擎”。
- 丢弃：丢弃符合特征的报文。
- 放行：允许符合特征的报文通过。
- 捕获：捕获符合特征的报文。
- 生成日志：对符合特征的报文生成日志信息。

1.1.3 IPS实现流程

IPS处理流程如 图 1-1 所示：

图1-1 IPS 数据处理流程图



IPS 功能是通过在 DPI 应用 profile 中引用 IPS 策略，并在对象策略中引用 DPI 应用 profile 来实现的，IPS 处理的具体实现流程如下：

(1) 设备收到报文后，首先与 IP 黑名单匹配：

- 如果匹配成功，则直接丢弃报文。
- 如果匹配失败，则进入步骤 2。

(2) 设备对报文进行规则（即对象策略规则）匹配：

如果规则引用了 IPS 业务，设备将对匹配了规则的报文进行深度内容检测：首先，识别报文的协议，然后根据协议分析方案进行更精细的分析，并深入提取报文特征。

有关对象策略规则的详细介绍请参见“安全配置指导”中的“对象策略”。

(3) 设备将提取的报文特征与 IPS 特征进行匹配，并进行如下处理：

- 如果报文未与任何 IPS 特征匹配成功，则设备对报文执行允许动作。
- 如果报文只与一个 IPS 特征匹配成功，则根据此特征中指定的动作进行处理。
- 如果报文同时与多个 IPS 特征匹配成功，则根据这些动作中优先级最高的动作进行处理。动作优先级从高到低的顺序为：重置 > 重定向 >丢弃 > 允许。但是，对于源阻断、生成日志和捕获三个动作只要匹配成功的特征中存在就会执行。

1.1.4 IPS特征库升级与回滚

IPS 特征库是用来对经过设备的应用层流量进行病毒检测和防御的资源库。随着网络攻击不断的变化和发展，需要及时升级设备中的 IPS 特征库，同时设备也支持 IPS 特征库回滚功能。

1. IPS特征库升级

IPS 特征库的升级包括如下几种方式：

- 定期自动在线升级：设备根据管理员设置的时间定期自动更新本地的 IPS 特征库。
- 立即自动在线升级：管理员手工触发设备立即更新本地的 IPS 特征库。
- 手动离线升级：当设备无法自动获取 IPS 特征库时，需要管理员先手动获取最新的 IPS 特征库，再更新设备本地的 IPS 特征库。

2. IPS特征库回滚

如果管理员发现设备当前 IPS 特征库对报文进行检测和防御网络攻击时，误报率较高或出现异常情况，则可以将其进行回滚到出厂版本和上一版本。

1.2 IPS与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持

型号	说明
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.3 IPS的License要求

IPS 功能需要安装 License 才能使用。License 过期后，IPS 功能可以采用设备中已有的 IPS 特征库正常工作，但无法升级到比当前版本高的特征库。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.4 IPS配置任务简介

IPS 配置任务如下：

(1) 创建IPS策略

(2) 配置筛选IPS特征的属性

(3) 配置IPS动作

(4) 配置IPS引用的应用层检测引擎动作参数profile

(5) 在DPI应用profile中引用IPS策略

(6) 激活IPS策略配置

(7) 在对象策略中引用IPS业务

(8) 配置IPS特征库升级和回滚

(9) （可选）导入和删除自定义IPS特征

1.5 IPS配置准备

在多 MDC 应用场景中，配置非缺省 MDC 的 IPS 业务前，必须先激活缺省 MDC 的应用层检测引擎。激活缺省 MDC 的应用层检测引擎方法有如下几种：

- 在缺省 MDC 的系统视图下执行 **inspect activate** 命令。
- 在缺省 MDC 中进行 IPS 业务的相关配置。

有关 MDC 的详细介绍请参见“虚拟化技术配置指导”中的“MDC”。

1.6 创建IPS策略

1. 功能简介

缺省情况下，IPS 策略将使用当前设备上所有处于生效状态的 IPS 特征与报文进行匹配，并对匹配成功的报文执行 IPS 特征属性中的动作。管理员可根据实际需求，在新建的 IPS 策略中，将 IPS 特征的属性作为过滤条件，筛选出需要与报文进行匹配的 IPS 特征，并配置 IPS 特征动作。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 IPS 策略，并进入 IPS 策略视图。

ips policy *policy-name*

缺省情况下，存在一个缺省 IPS 策略，名称为 default，且不能被修改或删除。

1.7 配置筛选IPS特征的属性

1. 功能简介

IPS 策略将筛选出匹配所有已配置属性的特征，如果属性中配置了多个参数，则 IPS 特征至少需要匹配上其中一个参数，才表示匹配上该属性。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IPS 策略视图。

ips policy *policy-name*

(3) 配置筛选 IPS 特征的属性。

- 配置筛选 IPS 特征的保护对象属性。

  protect-target { *target* [*subtarget* | **all**] }

  缺省情况下，IPS 策略匹配所有保护对象的特征。

- 配置筛选 IPS 特征的攻击分类属性。

  attack-category { *category* [*subcategory*] | **all** }

  缺省情况下，IPS 策略匹配所有攻击分类的特征。

- 配置筛选 IPS 特征的动作属性。

  action { **block-source** | **drop** | **permit** | **reset** } *

  缺省情况下，IPS 策略匹配所有动作的特征。

- 配置筛选 IPS 特征的方向属性。

  object-dir { **client** | **server** } *

  缺省情况下，IPS 策略匹配所有方向的特征。

- 配置筛选 IPS 特征的严重级别属性。

  severity-level { **critical** | **high** | **low** | **medium** } *

  缺省情况下，IPS 策略匹配所有严重级别的特征。

1.8 配置IPS动作

1. 功能简介

缺省情况下，新建 IPS 策略执行特征属性中的动作。管理员也可以根据实际网络需求，为 IPS 策略中所有特征配置统一的动作，或者为指定的特征配置动作。

设备对以上动作执行的优先级为：IPS 策略中为指定特征配置的动作 > IPS 策略为所有特征配置的统一动作 > IPS 特征自身属性的动作。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 IPS 策略视图。

ips policy *policy-name*

(3) 配置 IPS 策略中所有特征的统一动作。

signature override all { { **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging** } *

缺省情况下，IPS 策略执行特征属性中的动作。

(4) （可选）修改 IPS 策略中指定特征的动作和生效状态。

signature override { **pre-defined** | **user-defined** } *signature-id* { { **disable** | **enable** } [{ **block-source** | **drop** | **permit** | **redirect** | **reset** } | **capture** | **logging**] * }

缺省情况下，预定义 IPS 特征使用系统预定义的状态和动作，自定义 IPS 特征的动作和状态在管理员导入的特征库文件中定义。

缺省 IPS 策略中的 IPS 特征的动作属性和生效状态属性不能被修改。

1.9 配置IPS引用的应用层检测引擎动作参数profile

1. 功能简介

每类 IPS 动作的具体执行参数由应用层检测引擎动作参数 profile 来定义，该 profile 的具体配置请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

如果 IPS 引用的应用层检测引擎动作参数 profile 不存在或没有引用，则使用系统各类动作参数的缺省值。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置 IPS 引用的应用层检测引擎动作参数 profile。

ips { **block-source** | **capture** | **email** | **logging** | **redirect** } **parameter-profile** *parameter-name*

缺省情况下，IPS 未引用应用层检测引擎动作参数 profile。

1.10 在DPI应用profile中引用IPS策略

1. 功能简介

DPI 应用 profile 是一个安全业务的配置模板，为实现 IPS 功能，必须在 DPI 应用 profile 中引用指定的 IPS 策略。

2. 配置限制和指导

一个 DPI 应用 profile 中只能引用一个 IPS 策略，如果重复配置，则新的配置会覆盖已有配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DPI 应用 profile 视图。

app-profile *profile-name*

关于该命令的详细介绍请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

(3) 在 DPI 应用 profile 中引用 IPS 策略。

ips apply policy *policy-name* **mode** { **protect** | **alert** }

缺省情况下，DPI 应用 profile 中未引用 IPS 策略。

1.11 激活IPS策略配置

1. 功能简介

当 IPS 的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

2. 配置限制和指导

配置此功能会暂时中断所有 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略后统一配置此功能。

有关此功能的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 激活 IPS 策略配置。

inspect activate

缺省情况下，IPS 策略被创建、修改和删除时不生效。

1.12 在对象策略中引用IPS业务

(1) 进入系统视图。

system-view

(2) 进入对象策略视图。

object-policy { **ip** | **ipv6** } *object-policy-name*

(3) 在对象策略规则中引用 DPI 应用 profile。

rule [*rule-id*] **inspect** *app-profile-name*

缺省情况下，在对象策略规则中未引用 DPI 应用 profile。

(4) 退回系统视图。

quit

(5) 创建安全域间实例，并进入安全域间实例视图。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*

有关安全域间实例的详细介绍请参见“安全配置指导”中的“安全域”。

(6) 应用对象策略。

object-policy apply { **ip** | **ipv6** } *object-policy-name*

缺省情况下，安全域间实例内不应用对象策略。

1.13 配置IPS特征库升级和回滚

1.13.1 配置限制和指导

- 请勿删除设备存储介质根目录下的/dpi/文件夹，否则设备升级或回滚特征库会失败。
- 当系统内存使用状态处于告警门限状态时，请勿进行特征库升级或回滚，否则易造成设备特征库升级或回滚失败，进而影响 IPS 业务的正常运行。有关内存告警门限状态的详细介绍请参见“基础配置指导”中的“设备管理”。
- 自动在线升级（包括定期自动在线升级和立即自动在线升级）IPS 特征库时，需要确保设备能通过静态或动态域名解析方式获得官方网站的 IP 地址，并与之路由可达，否则设备升级 IPS 特征库会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

1.13.2 配置定期自动在线升级IPS特征库

1. 功能简介

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 IPS 特征库进行升级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启定期自动在线升级 IPS 特征库功能，并进入自动在线升级配置视图。

ips signature auto-update

缺省情况下，定期自动在线升级 IPS 特征库功能处于关闭状态。

(3) 配置定期自动在线升级 IPS 特征库的时间。

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

缺省情况下，设备在每天 01:00:00 至 03:00:00 之间自动升级 IPS 特征库。

(4) （可选）开启 IPS 特征文件自动覆盖功能。

override-current

缺省情况下，设备定期自动在线升级 IPS 特征库时会将当前的特征库文件备份为上一版本。

1.13.3 立即自动在线升级IPS特征库

1. 功能简介

当管理员发现官方网站上的特征库服务专区中的 IPS 特征库有更新时，可以选择立即自动在线升级方式来及时升级 IPS 特征库版本。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 立即自动在线升级 IPS 特征库。

ips signature auto-update-now

1.13.4 手动离线升级IPS特征库

1. 功能简介

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 IPS 特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 IPS 特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 IPS 特征库版本。

使用本地升级方式离线升级特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。（IRF 模式）

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 手动离线升级 IPS 特征库。

ips signature update [**override-current**] *file-path*

1.13.5 回滚IPS特征库

1. 功能简介

IPS 特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 IPS 特征库版本是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 回滚 IPS 特征库。

ips signature rollback { **factory** | **last** }

1.14 导入和删除自定义IPS特征

1.14.1 导入自定义IPS特征

1. 功能简介

当需要的 IPS 特征在设备当前 IPS 特征库中不存在时，可通过编辑 Snort 格式的 IPS 特征文件，并将其导入设备中来生成所需的 IPS 特征。导入的 IPS 特征文件内容会自动覆盖系统中所有的自定义 IPS 特征。

2. 配置限制和指导

目前仅支持以 Snort 文件导入的方式生成自定义 IPS 特征，Snort 文件需要遵循 Snort 公司的语法。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 导入自定义 IPS 特征。

ips signature import snort *file-path*

1.14.2 删除所有导入的自定义IPS特征

(1) 进入系统视图。

system-view

(2) 删除导入的所有导入的自定义 IPS 特征。

ips signature remove snort

1.15 IPS显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 IPS 的运行情况，通过查看显示信息验证配置的效果。

表1-1 IPS 显示和维护

操作	命令
显示IPS策略信息	**display ips policy** *policy-name*
显示IPS特征库版本信息	**display ips signature information**
显示IPS特征属性列表	**display ips signature** [**pre-defined** | **user-defined**] [**direction** { **any** | **to-client** | **to-server** }] [**category** *category-name* | **fidelity** { **high** | **low** | **medium** } | **protocol** { **icmp** | **ip** | **tcp** | **udp** } | **severity** { **critical** | **high** | **low** | **medium** }] *
显示指定IPS特征的详细属性	**display ips signature** { **pre-defined** | **user-defined** } *signature-id*
显示IPS自定义特征解析失败的信息	**display ips signature user-defined parse-failed**

1.16 IPS典型配置举例

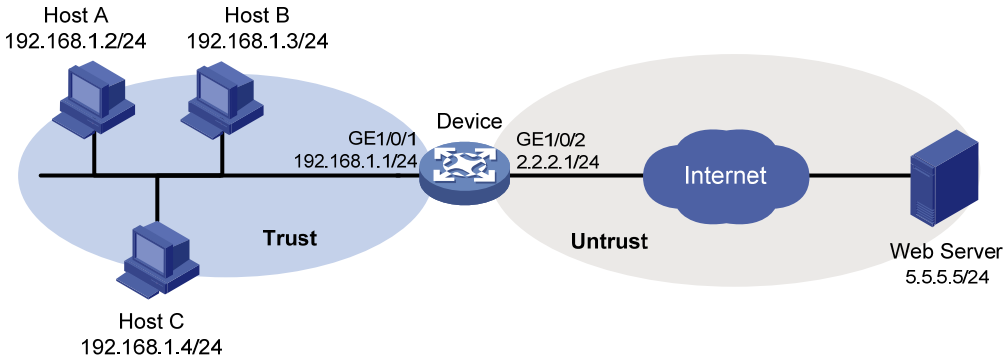
1.16.1 在对象策略中引用缺省IPS策略配置举例

1. 组网需求

如 图 1-2 所示，Device分别通过Trust安全域和Untrust安全域与局域网和Internet相连。现要求使用设备上的缺省IPS策略对用户数据报文进行IPS防御。

2. 组网图

图1-2 在对象策略中引用缺省 IPS 策略的配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域

向安全域 Trust 中添加接口 GigabitEthernet1/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
```

向安全域 Untrust 中添加接口 GigabitEthernet1/0/2。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置对象组

创建名为 ipsfilter 的 IP 地址对象组，并定义其子网地址为 192.168.1.0/24。

```
[Device] object-group ip address ipsfilter
[Device-obj-grp-ip-ipsfilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-ipsfilter] quit
```

(4) 配置 DPI 应用 profile

创建名为 sec 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile sec
```

在 DPI 应用 profile sec 中应用缺省 IPS 策略 default，并指定该 IPS 策略的模式为 protect。

```
[Device-app-profile-sec] ips apply policy default mode protect
[Device-app-profile-sec] quit
```

激活 IPS 策略配置。

```
[Device] inspect activate
```

(5) 配置对象策略引用 IPS 业务

创建名为 ipsfilter 的 IPv4 对象策略，并进入对象策略视图。

```
[Device] object-policy ip ipsfilter
```

对源 IP 地址对象组 ipsfilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 sec。

```
[Device-object-policy-ip-ipsfilter] rule inspect sec source-ip ipsfilter
destination-ip any
[Device-object-policy-ip-ipsfilter] quit
```

配置安全域间实例并应用对象策略，创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例，并应用对源 IP 地址对象组 ipsfilter 对应的报文进行深度检测的对象策略 ipsfilter。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-Trust-Untrust] object-policy apply ip ipsfilter
[Device-zone-pair-security-Trust-Untrust] quit
```

4. 验证配置

以上配置生效后，使用缺省 IPS 策略可以对已知攻击类型的网络攻击进行防御。比如 GNU_Bash_Local_Memory_Corruption_Vulnerability(CVE-2014-718)类型的攻击报文经过 Device 设备时，Device 会匹配该报文，并对报文按照匹配成功的 IPS 特征的动作（reset 和 logging）进行处理。

1.16.2 在对象策略中引用自定义IPS策略配置举例

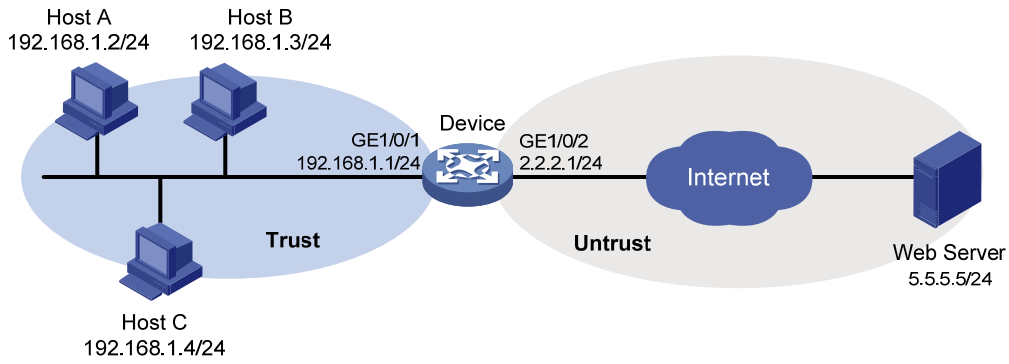
1. 组网需求

如 图 1-3 所示，Device分别通过Trust安全域和Untrust安全域与局域网和Internet相连。现有组网需求如下：

- 将编号为 2 的预定义 IPS 特征的动作改为丢弃并进行报文捕获和生成日志。
- 禁用编号为 4 的预定义 IPS 特征。
- 使编号为 6 的预定义 IPS 特征生效。

2. 组网图

图1-3 在对象策略中引用自定义 IPS 策略配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域

向安全域 Trust 中添加接口 GigabitEthernet1/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
```

向安全域 Untrust 中添加接口 GigabitEthernet1/0/2。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置对象组

创建名为 ipsfilter 的 IP 地址对象组，并定义其子网地址为 192.168.1.0/24。

```
[Device] object-group ip address ipsfilter
[Device-obj-grp-ip-ipsfilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-ipsfilter] quit
```

(4) 配置 IPS 策略

创建一个名称为 ips1 的 IPS 策略，并进入 IPS 策略视图。

```
[Device] ips policy ips1
```

配置 IPS 策略保护所有对象。

```
[Device-ips-policy-ips1] protect-target all
```

将编号为 2 的预定义 IPS 特征的状态为开启，动作为丢弃和捕获报文，并生成日志信息。

```
[Device-ips-policy-ips1] signature override pre-defined 2 enable drop capture logging
```

禁用编号为 4 的预定义 IPS 特征。

```
[Device-ips-policy-ips1] signature override pre-defined 4 disable
```

使编号为 6 的预定义 IPS 特征生效。

```
[Device-ips-policy-ips1] signature override pre-defined 6 enable
[Device-ips-policy-ips1] quit
```

(5) 配置 DPI 应用 profile

创建名为 sec 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile sec
```

在 DPI 应用 profile sec 中应用 IPS 策略 ips1，并指定该 IPS 策略的模式为 protect。

```
[Device-app-profile-sec] ips apply policy ips1 mode protect
[Device-app-profile-sec] quit
```

激活 IPS 策略配置。

```
[Device] inspect activate
```

(6) 配置对象策略引用 IPS 业务

创建名为 ipsfilter 的 IPv4 对象策略，并进入对象策略视图。

```
[Device] object-policy ip ipsfilter
```

对源 IP 地址对象组 ipsfilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 sec。

```
[Device-object-policy-ip-ipsfilter] rule inspect sec source-ip ipsfilter
destination-ip any
[Device-object-policy-ip-ipsfilter] quit
```

(7) 配置安全域间实例并应用对象策略

配置安全域间实例并应用对象策略，创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例，并应用对源 IP 地址对象组 ipsfilter 对应的报文进行深度检测的对象策略 ipsfilter。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-Trust-Untrust] object-policy apply ip ipsfilter
[Device-zone-pair-security-Trust-Untrust] quit
```

4. 验证配置

以上配置生效后，在 IPS 策略 ips1 中可看到以上有关 IPS 策略的配置。

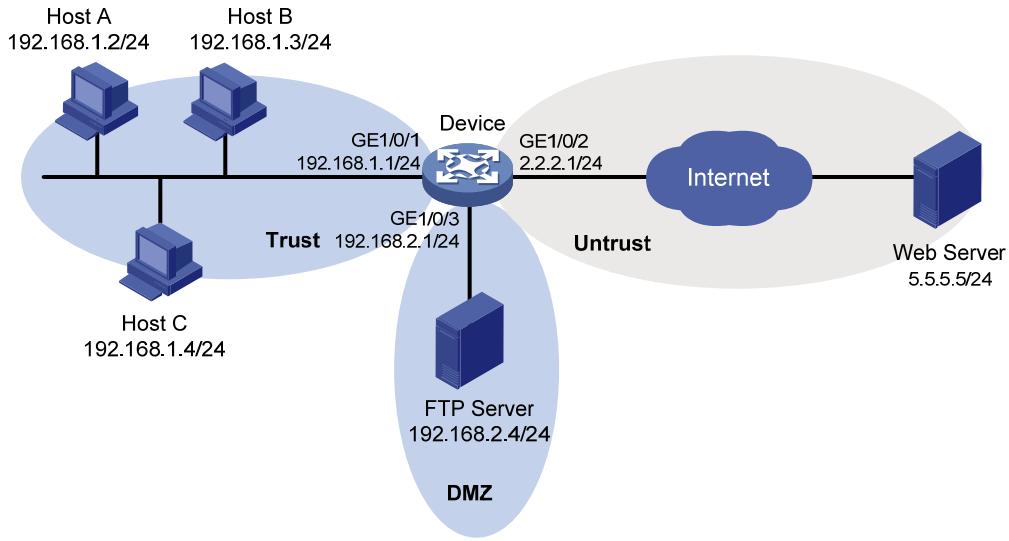
1.16.3 手动离线升级IPS特征库配置举例

1. 组网需求

如 图 1-4 所示，位于Trust安全域的局域网用户通过Device可以访问Untrust安全域的Internet资源，以及DMZ安全域的FTP服务器。FTP服务器根目录下保存了最新的IPS特征库文件ips-1.0.8-encrypt.dat，FTP服务器的登录用户名和密码分别为ips和 123。现需求手动离线升级IPS特征库，加载最新的IPS特征。

2. 组网图

图1-4 手动离线升级 IPS 特征库配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置安全域间实例保证 Device 与 FTP 服务器互通

配置 ACL 2001，定义规则允许所有报文通过。

```
<Device> system-view
[Device] acl basic 2001
[Device-acl-ipv4-basic-2001] rule permit
[Device-acl-ipv4-basic-2001] quit
```

向安全域 DMZ 中添加接口 GigabitEthernet1/0/3。

```
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 1/0/3
[Device-security-zone-DMZ] quit
```

创建源安全域 Local 到目的安全域 DMZ 的安全域间实例，允许 Local 域用户访问 DMZ 域的报文可以通过。

```
[Device] zone-pair security source local destination dmz
[Device-zone-pair-security-Local-DMZ] packet-filter 2001
```

```
[Device-zone-pair-security-Local-DMZ] quit
```

创建源安全域 DMZ 到目的安全域 Local 的安全域间实例，允许 DMZ 域用户访问 Local 域的报文可以通过。

```
[Device] zone-pair security source dmz destination local
[Device-zone-pair-security-DMZ-Local] packet-filter 2001
[Device-zone-pair-security-DMZ-Local] quit
```

(3) 手动升级 IPS 特征库

采用 FTP 方式手动离线升级设备上的 IPS 特征库，且被加载的 IPS 特征库文件名为 ips-1.0.8-encrypt.dat。

```
[Device] ips signature update ftp://ips:123@192.168.2.4/ips-1.0.8-encrypt.dat
```

4. 验证配置

IPS 特征库升级后，可以通过 **display ips signature information** 命令查看当前特征库的版本信息。

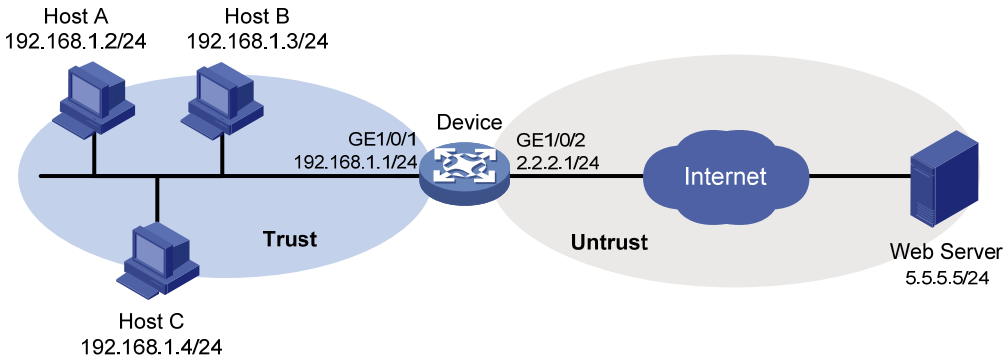
1.16.4 定时自动升级IPS特征库配置举例

1. 组网需求

如 图 1-5 所示，位于Trust安全域的局域网用户通过Device可以访问Untrust安全域的Internet资源。现要求每周六上午九点前后半小时内，定期自动在线升级设备的IPS特征库。

2. 组网图

图1-5 定时自动升级 IPS 特征库配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置设备解析官方网站对应 IP 地址的域名解析功能（略）

(3) 配置对象策略保证 Trust 安全域的局域网用户可以访问 Untrust 安全域的 Internet 资源（略）

(4) 配置定期自动在线升级 IPS 特征库

开启设备自动升级 IPS 特征库功能，并进入自动升级配置视图。

```
<Device> system-view
[Device] ips signature auto-update
[Device-ips-autoupdate]
```

设置定时自动升级 IPS 特征库计划为：每周六上午 9:00:00 自动升级，抖动时间为 60 分钟。

```
[Device-ips-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 60
[Device-ips-autoupdate] quit
```

4. 验证配置

设置的定期自动在线升级 IPS 特征库时间到达后，可以通过 **display ips signature information** 命令查看当前特征库的版本信息。

目 录

1 URL过滤 ····· 1-1
1.1 URL过滤简介 ····· 1-1
1.1.1 URL简介 ····· 1-1
1.1.2 URL过滤规则 ····· 1-1
1.1.3 URL过滤分类 ····· 1-2
1.1.4 URL过滤策略 ····· 1-2
1.1.5 URL过滤黑/白名单规则 ····· 1-2
1.1.6 URL过滤实现流程 ····· 1-3
1.1.7 URL过滤特征库升级与回滚 ····· 1-4
1.2 URL过滤与硬件适配关系 ····· 1-4
1.3 URL过滤的License要求 ····· 1-5
1.4 URL过滤配置任务简介 ····· 1-5
1.5 URL过滤配置准备 ····· 1-6
1.6 配置URL过滤分类 ····· 1-6
1.7 配置URL过滤分类云端查询 ····· 1-7
1.8 配置URL过滤策略 ····· 1-7
1.9 复制URL过滤策略或分类 ····· 1-8
1.9.1 复制URL过滤策略 ····· 1-8
1.9.2 复制URL过滤分类 ····· 1-8
1.10 在DPI应用profile中引用URL过滤策略 ····· 1-9
1.11 激活URL过滤的策略和规则配置 ····· 1-9
1.12 在对象策略中引用URL过滤业务 ····· 1-10
1.13 配置URL过滤特征库升级和回滚 ····· 1-10
1.13.1 配置限制和指导 ····· 1-10
1.13.2 配置定期自动在线升级URL过滤特征库 ····· 1-10
1.13.3 立即自动在线升级URL过滤特征库 ····· 1-11
1.13.4 手动离线升级URL过滤特征库 ····· 1-11
1.13.5 回滚URL过滤特征库 ····· 1-11
1.14 开启应用层检测引擎日志信息功能 ····· 1-12
1.15 配置URL过滤日志信息筛选功能 ····· 1-12
1.15.1 功能简介 ····· 1-12
1.15.2 配置URL过滤仅对网站根目录下资源的访问进行日志记录 ····· 1-12
1.15.3 配置URL过滤对指定类型网页资源的访问不进行日志记录 ····· 1-12

1.16 URL过滤显示和维护 ····· 1-13
1.17 URL过滤典型配置举例 ····· 1-13
1.17.1 在对象策略中引用URL过滤业务配置举例 ····· 1-13
1.17.2 手动离线升级URL过滤特征库配置举例 ····· 1-15
1.17.3 定期自动在线升级URL过滤特征库配置举例 ····· 1-17

1 URL过滤

1.1 URL过滤简介

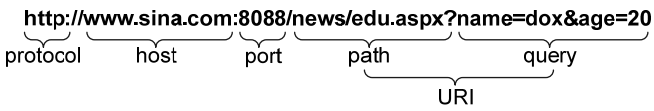
URL 过滤功能是指对用户访问的 URL 进行控制，即允许或禁止用户访问的 Web 资源，达到规范用户上网行为的目的。

目前，仅支持对基于 HTTP 协议的 URL 进行过滤。

1.1.1 URL简介

URL（Uniform Resource Locator，统一资源定位符）是互联网上标准资源的地址。URL用来完整、精确的描述互联网上的网页或者其他共享资源的地址，URL格式为：“protocol://host[:port]/path/[;parameters][?query]#fragment”，格式示意如 图 1-1 所示：

图1-1 URL 格式示意图



URL各字段含义如 表 1-1 所示：

表1-1 URL 各字段含义表

字段	描述
protocol	表示使用的传输协议，例如HTTP
host	表示存放资源的服务器的主机名或IP地址
[:port]	（可选）传输协议的端口号，各种传输协议都有默认的端口号
/path/	是路径，由零或多个“/”符号隔开的字符串，一般用来表示主机上的一个目录或文件地址
[parameters]	（可选）用于指定特殊参数
[?query]	（可选）表示查询用于给动态网页传递参数，可有多个参数，用“&”符号隔开，每个参数的名和值用“=”符号隔开
URI	URI（Uniform Resource Identifier，统一资源标识符）是一个用于标示某一互联网资源名称的字符

1.1.2 URL过滤规则

URL 过滤功能实现的前提条件是对 URL 的识别。可通过使用 URL 过滤规则匹配 URL 中主机名字段和 URI 字段的方法来识别 URL。

1. URL过滤规则类型

URL 过滤规则是指对用户 HTTP 报文中的 URL 进行匹配的原则，且其分为两种规则：

- 预定义规则：根据设备中的 URL 过滤特征库自动生成，包括百万级的主机名或 URI。预定义规则能满足多数情况下的 URL 过滤需求。
- 自定义规则：由管理员手动配置生成，可以通过使用正则表达式或者文本的方式配置规则中主机名或 URI 的内容。

2. URL过滤规则匹配方式

URL 过滤规则支持两种匹配方式：

- 文本匹配：使用指定的字符串对主机名和 URI 字段进行匹配。
  - 匹配主机名字段时，首先判断主机名开头或结尾位置是否含有通配符“*”，若均未出现，则URL中的主机名字段与规则中指定的主机名字符串必须完全一致，才能匹配成功；若“*”出现在开头位置，则该字符串或以该字符串结尾的 URL 会匹配成功；若“*”出现在结尾位置，则该字符串或以该字符串开头的 URL 会匹配成功。若“*”同时出现在开头或结尾位置，则该字符串或含有该字符串的 URL 均会匹配成功。
  - 匹配 URI 字段时，和主机名字段匹配规则一致。
- 正则表达式匹配：使用正则表达式对主机名和 URI 字段进行匹配。例如，规则中配置主机名的正则表达式为 sina.*cn，则主机名为 news.sina.com.cn 的 URL 会匹配成功。

1.1.3 URL过滤分类

为便于管理员对数目众多的URL过滤规则进行统一部署，URL过滤模块提供了URL过滤分类功能，以便对具有相似特征的 URL 过滤规则进行归纳以及为匹配这些规则的 URL 统一指定处理动作。每个 URL 过滤分类具有一个严重级别属性，该属性值表示对属于此过滤分类 URL 的处理优先级。

URL 过滤分类包括两种类型：

- 预定义分类：根据设备中的 URL 过滤特征库自动生成，其名称、内容和严重级别不可被修改。名称以 Pre-开头。设备为预定义 URL 过滤分类保留的严重级别为最低，取值范围为 1～999。URL 过滤支持两级分类，包含父分类和子分类。仅支持预定义父分类，且父分类下仅包含预定义子分类。
- 自定义分类：由管理员手动配置，可修改其严重级别，可添加 URL 过滤规则。自定义分类严重级别的取值范围为 1000～65535。

1.1.4 URL过滤策略

一个 URL 过滤策略中可以配置 URL 过滤分类和处理动作的绑定关系，以及缺省动作（即对未匹配上任何 URL 过滤规则的报文采取的动作）。URL 过滤支持的处理动作包括：丢弃、允许、阻断、重置、重定向和生成日志。

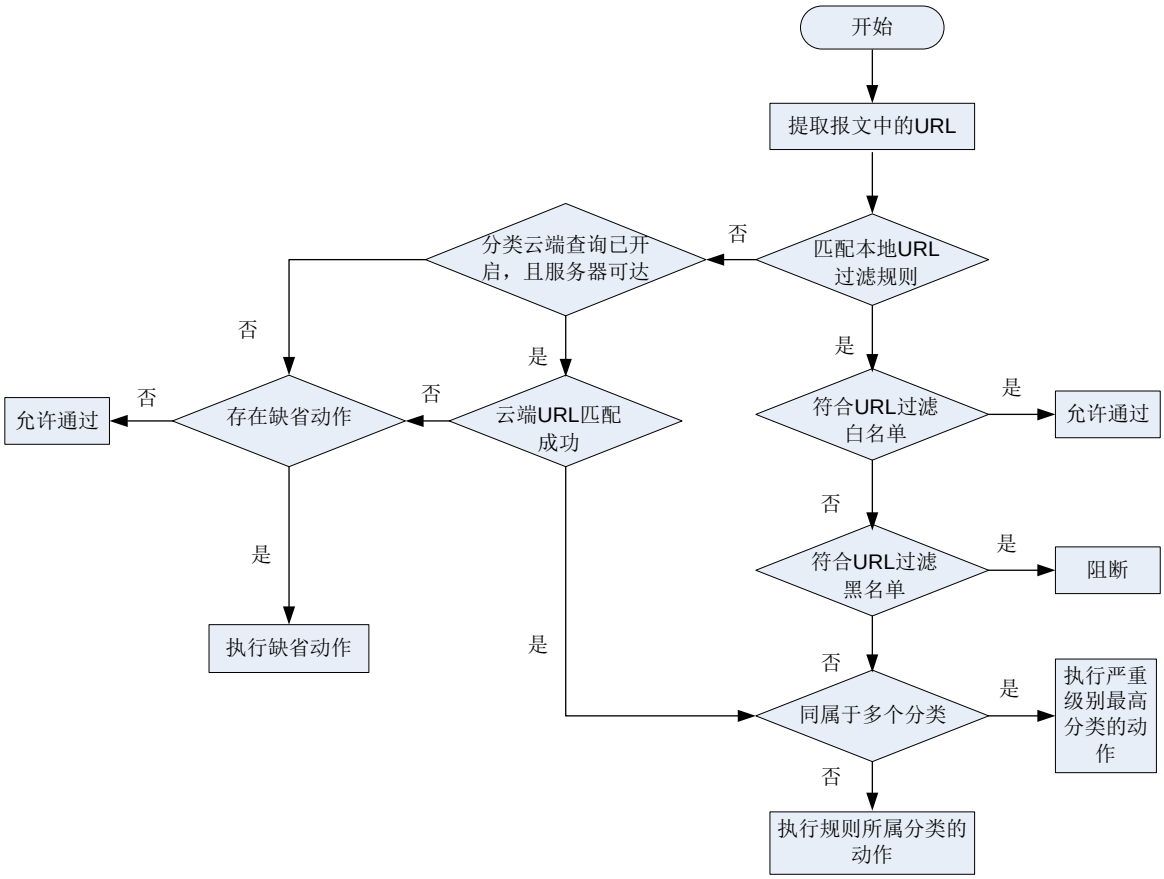
1.1.5 URL过滤黑/白名单规则

可通过 URL 过滤黑/白名单规则快速筛选出不需要进行 URL 过滤的报文。如果用户 HTTP 报文中的 URL 与 URL 过滤策略中的黑名单规则匹配成功，则丢弃此报文；如果与白名单规则匹配成功，则允许此报文通过。

1.1.6 URL过滤实现流程

当用户通过设备使用HTTP访问某个网络资源时，设备将对此HTTP报文进行URL过滤。URL过滤处理流程如 图 1-2 所示：

图1-2 URL 过滤实现流程图



URL 过滤功能是通过在 DPI 应用 profile 中引用 URL 过滤策略，并在对象策略中引用 DPI 应用 profile 来实现的，URL 过滤实现流程如下：

(2) 设备对报文进行规则（即对象策略规则）匹配：

如果规则引用了 URL 过滤业务，设备将对匹配了规则的报文进行 URL 过滤业务处理。设备将提取报文的 URL 字段，并与 URL 过滤规则进行匹配。

有关对象策略的详细介绍请参见“安全配置指导”中的“对象策略”。

(3) 设备将报文与 URL 过滤策略中的过滤规则进行匹配，如果匹配成功，则进行下一步处理；如果匹配失败，则进入步骤（5）的处理。

(4) 首先判断此 URL 过滤规则是否属于 URL 过滤的黑/白名单规则，如果属于 URL 过滤白名单规则则直接允许此报文通过，如果属于 URL 过滤的黑名单规则则直接将此报文阻断。

(5) 如果此 URL 过滤规则既不属于 URL 过滤白名单规则也不属于 URL 过滤黑名单规则，则设备将进一步判断该规则是否同时属于多个 URL 过滤分类。

- 如果此 URL 过滤规则同时属于多个 URL 过滤分类，则根据严重级别最高的 URL 过滤分类的动作对此报文进行处理。

- 如果此 URL 过滤规则只属于一个 URL 过滤分类，则根据该规则所属的 URL 过滤分类的动作对此报文进行处理。

(6) 如果分类云端查询功能已开启，则将报文中的 URL 发向云端服务器进行查询，否则进入步骤（7）的处理。

(7) 如果 URL 云端查询成功，云端服务器将向设备端返回查询结果（该结果中包含了 URL 过滤规则及其所属的分类名称），并进入步骤（4）的处理，否则进入步骤（7）的处理。

(8) 如果设备上配置了 URL 过滤的缺省动作，则根据配置的缺省动作对此报文进行处理；否则直接允许报文通过。

1.1.7 URL过滤特征库升级与回滚

URL 过滤特征库是用来对经过设备的用户访问 Web 请求中的 URL 进行识别的资源库。随着互联网业务的不断变化和发展，需要及时升级设备中的 URL 过滤特征库，同时设备也支持 URL 过滤特征库回滚功能。

1. URL过滤特征库升级

URL 过滤特征库的升级包括如下几种方式：

- 定期自动在线升级：设备根据管理员设置的时间定期自动更新本地的 URL 过滤特征库。
- 立即自动在线升级：管理员手工触发设备立即更新本地的 URL 过滤特征库。
- 手动离线升级：当设备无法自动获取 URL 过滤特征库时，需要管理员先手动获取最新的 URL 过滤特征库，再更新本地的 URL 过滤特征库。

2. URL过滤特征库回滚

如果管理员发现设备当前 URL 过滤特征库对用户访问 Web 的 URL 过滤的误报率较高或出现异常情况，则可以将其回滚到出厂版本和上一版本。

1.2 URL过滤与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持

型号	说明
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.3 URL过滤的License要求

URL 过滤功能需要安装 License 才能使用。License 过期后，URL 过滤功能可以采用设备中已有的 URL 过滤特征库正常工作，但无法升级到比当前版本高的特征库。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.4 URL过滤配置任务简介

URL 过滤配置任务如下：

(1) 配置URL过滤分类

(2) （可选）配置URL过滤分类云端查询

(3) 配置URL过滤策略

(4) （可选）复制URL过滤策略或分类

(5) 在DPI应用profile中引用URL过滤策略

(6) 激活URL过滤的策略和规则配置

(7) 在对象策略中引用URL过滤业务

(8) 配置URL过滤特征库升级和回滚

(9) （可选）开启应用层检测引擎日志信息功能

(10) （可选）配置URL过滤日志信息筛选功能

1.5 URL过滤配置准备

在多 MDC 应用场景中，配置非缺省 MDC 的 URL 过滤业务前，必须先激活缺省 MDC 的应用层检测引擎。激活缺省 MDC 的应用层检测引擎方法有如下几种：

- 在缺省 MDC 的系统视图下执行 **inspect activate** 命令。
- 在缺省 MDC 中进行 URL 过滤业务的相关配置。

有关 MDC 的详细介绍请参见“虚拟化技术配置指导”中的“MDC”。

1.6 配置URL过滤分类

1. 功能简介

当 URL 过滤特征库中预定义的 URL 过滤分类和 URL 过滤规则不能满足对 URL 的控制需求时，可以配置 URL 过滤分类，并在分类中创建 URL 过滤规则。

2. 配置限制和指导

不同 URL 过滤分类的严重级别不能相同，数值越大表示严重级别越高。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 URL 过滤分类，并进入 URL 过滤分类视图。

url-filter category *category-name* [**severity** *severity-level*]

缺省情况下，只存在预定义的 URL 过滤分类，且分类名称以字符串 Pre-开头。

自定义的 URL 过滤分类不能以字符串 Pre-开头。

(3) （可选）配置 URL 过滤分类的描述信息。

description *text*

(4) 配置 URL 过滤规则，请至少选择其中一项进行配置。

- 配置自定义 URL 过滤规则。

  rule *rule-id* **host** { **regex** *regex* | **text** *string* } [**uri** { **regex** *regex* | **text** *string* }]

- 添加预定义 URL 过滤分类中的规则。

include pre-defined *category-name*

缺省情况下，URL 过滤分类中未添加预定义 URL 过滤分类中的规则。

(5) （可选）重命名 URL 过滤分类，并进入新的 URL 过滤分类视图。

rename *new-name*

1.7 配置URL过滤分类云端查询

1. 功能简介

在 URL 过滤策略中开启 URL 过滤分类云端查询功能后，可提高设备识别 HTTP 报文的准确率，实现对报文的准确控制。

从云端服务器学习到的 URL 过滤规则会被缓存在设备的 URL 过滤缓存中进行报文匹配。URL 过滤缓存的记录上限和规则的最短保留时间可以根据实际组网环境进行调整。有关云端服务器的详细介绍，请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 配置云端服务器的主机名。

inspect cloud-server *host-name*

缺省情况下，云端服务器的主机名为 sec.h3c.com。

(3) （可选）配置 URL 过滤缓存区可缓存记录的上限。

url-filter cache size *cache-size*

缺省情况下，URL 过滤缓存区可缓存记录的上限为 16384。

(4) （可选）配置 URL 过滤缓存规则的最短保留时间。

url-filter cache-time *value*

缺省情况下，URL 过滤缓存规则的最短保留时间为 10 分钟。

(5) 进入 URL 过滤策略视图。

url-filter policy *policy-name*

(6) 开启 URL 过滤分类云端查询功能。

cloud-query enable

缺省情况下，URL 过滤分类云端查询功能处于关闭状态。

1.8 配置URL过滤策略

1. 功能简介

URL 过滤策略中包含如下配置：

- URL 过滤分类动作
- URL 过滤分类缺省动作
- 白名单/黑名单规则

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 创建 URL 过滤策略，并进入 URL 过滤策略视图。

url-filter policy *policy-name*

(3) 配置 URL 过滤分类动作。

category *category-name* **action** { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

缺省情况下，未配置 URL 过滤分类动作。

若报文成功匹配的 URL 过滤规则同属于多个 URL 过滤分类，则根据严重级别最高的 URL 过滤分类中指定的动作对此报文进行处理。

(4) （可选）配置 URL 过滤策略的缺省动作。

default-action { **block-source** [**parameter-profile** *parameter-name*] | **drop** | **permit** | **redirect parameter-profile** *parameter-name* | **reset** } [**logging** [**parameter-profile** *parameter-name*]]

(5) （可选）向 URL 过滤策略中添加黑/白名单规则。

add { **blacklist** | **whitelist** } [*id*] **host** { **regex** *host-regex* | **text** *host-name* } [**uri** { **regex** *uri-regex* | **text** *uri-name* }]

(6) （可选）重命名 URL 过滤策略，并进入新的 URL 过滤策略视图。

rename *new-name*

1.9 复制URL过滤策略或分类

1.9.1 复制URL过滤策略

1. 功能简介

此功能用来复制已存在的 URL 过滤策略，可以方便用户快速创建 URL 过滤策略。

2. 配置步骤

(1) 进入系统视图

system-view

(2) 复制 URL 过滤策略

url-filter copy policy *old-name new-name*

1.9.2 复制URL过滤分类

1. 功能简介

此功能用来复制已存在的 URL 过滤分类，可以方便用户快速创建 URL 过滤分类。

2. 配置限制和指导

在复制 URL 过滤分类时，如果指定优先级与已经存在的分类优先级相同，则复制失败。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 复制 URL 过滤分类。

url-filter copy category *old-name new-name* **severity** *severity-level*

1.10 在DPI应用profile中引用URL过滤策略

1. 功能简介

DPI 应用 profile 是一个安全业务的配置模板，为实现 URL 过滤功能，必须在 DPI 应用 porfile 中引用指定的 URL 过滤策略。

2. 配置限制和指导

一个 DPI 应用 profile 中只能引用一个 URL 过滤策略，如果重复配置，则后配置的覆盖已有的。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 DPI 应用 profile 视图。

app-profile *app-profile-name*

关于该命令的详细介绍请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

(3) 在 DPI 应用 profile 中引用 URL 过滤策略。

url-filter apply policy *policy-name*

缺省情况下，DPI 应用 profile 中未引用 URL 过滤策略。

1.11 激活URL过滤的策略和规则配置

1. 功能简介

当 URL 过滤策略和规则被创建、修改和删除后，需要配置此功能使其策略和规则配置生效。

2. 配置限制和指导

配置此功能会暂时中断所有 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请完成部署 DPI 各业务模块的策略和规则后统一配置此功能。

有关此功能的详细介绍请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 激活 URL 过滤策略和规则配置。

inspect activate

缺省情况下，URL 过滤策略和规则被创建、修改和删除时不生效。

1.12 在对象策略中引用URL过滤业务

(1) 进入系统视图。

system-view

(2) 进入对象策略视图。

object-policy { **ip** | **ipv6** } *object-policy-name*

(3) 在对象策略规则中引用 DPI 应用 profile。

rule [*rule-id*] **inspect** *app-profile-name*

缺省情况下，在对象策略规则中未引用 DPI 应用 profile。

(4) 退回系统视图。

quit

(5) 创建安全域间实例，并进入安全域间实例视图。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*

有关安全域间实例的详细介绍请参见“安全配置指导”中的“安全域”。

(6) 应用对象策略。

object-policy apply { **ip** | **ipv6** } *object-policy-name*

缺省情况下，安全域间实例内不应用对象策略。

1.13 配置URL过滤特征库升级和回滚

1.13.1 配置限制和指导

- 请勿删除设备存储介质根目录下的/dpi/文件夹，否则设备升级或回滚特征库会失败。
- 当系统内存使用状态处于告警门限状态时，请勿进行特征库升级或回滚，否则易造成设备特征库升级或回滚失败，进而影响 URL 过滤业务的正常运行。有关内存告警门限状态的详细介绍请参见“基础配置指导”中的“设备管理”。
- 自动在线升级（包括定期自动在线升级和立即自动在线升级）URL 过滤特征库时，需要确保设备能通过静态或动态域名解析方式获得官方网站的 IP 地址，并与之路由可达，否则设备升级 URL 过滤特征库会失败。有关域名解析功能的配置请参见“三层技术-IP 业务配置指导”中的“域名解析”。

1.13.2 配置定期自动在线升级URL过滤特征库

1. 功能简介

如果设备可以访问官方网站上的特征库服务专区，可以采用定期自动在线升级方式来对设备上的 URL 过滤特征库进行升级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启定期自动在线升级 URL 过滤特征库功能，并进入自动在线升级配置视图。

url-filter signature auto-update

缺省情况下，定期自动在线升级 URL 过滤特征库功能处于关闭状态。

(3) 配置定期自动在线升级 URL 过滤特征库的时间。

update schedule { **daily** | **weekly** { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } } **start-time** *time* **tingle** *minutes*

缺省情况下，设备在每天 01:00:00 至 03:00:00 之间自动升级 URL 过滤特征库。

1.13.3 立即自动在线升级URL过滤特征库

1. 功能简介

当管理员发现官方网站上的特征库服务专区中的 URL 过滤特征库有更新时，可以选择立即自动在线升级方式来及时升级 URL 过滤特征库版本。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 立即自动在线升级 URL 过滤特征库。

url-filter signature auto-update-now

1.13.4 手动离线升级URL过滤特征库

1. 功能简介

如果设备不能访问官方网站上的特征库服务专区，管理员可以采用如下几种方式手动离线升级 URL 过滤特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的 URL 过滤特征库版本。
- FTP/TFTP 升级：通过 FTP 或 TFTP 方式下载远程服务器上保存的特征库文件，并升级系统上的 URL 过滤特征库版本。

使用本地升级方式离线升级特征库版本时，特征库文件只能存储在当前主用设备上，否则设备升级特征库会失败。（IRF 模式）

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 手动离线升级 URL 过滤特征库。

url-filter signature update *file-path*

1.13.5 回滚URL过滤特征库

1. 功能简介

URL 过滤特征库版本每次回滚前，设备都会备份当前版本。多次回滚上一版本的操作将会在当前版本和上一版本之间反复切换。例如当前 URL 过滤特征库版本是 V2，上一版本是 V1，第一次执行回滚到上一版本的操作后，特征库替换成 V1 版本，再执行回滚上一版本的操作则特征库重新变为 V2 版本。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 回滚 URL 过滤特征库。

url-filter signature rollback { factory | last }

1.14 开启应用层检测引擎日志信息功能

1. 功能简介

应用层检测引擎日志是为了满足管理员审计需求。设备生成应用层检测引擎日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启应用层检测引擎日志信息功能。

url-filter log enable

缺省情况下，生成应用层检测引擎日志信息功能处于关闭状态。

1.15 配置URL过滤日志信息筛选功能

1.15.1 功能简介

开启 URL 过滤日志功能后（即执行 **category action logging** 或 **default-action logging** 命令）会产生大量的日志信息，不利于查看和分析。管理员可从以下方式中任选其一，对需要进行日志记录的资源进行筛选：

- 仅对网站根目录下资源的访问进行日志记录
- 对指定类型的网页资源的访问不进行日志记录

1.15.2 配置URL过滤仅对网站根目录下资源的访问进行日志记录

(1) 进入系统视图。

system-view

(2) 配置 URL 过滤仅对网站根目录下资源的访问进行日志记录。

url-filter log directory root

缺省情况下，URL 过滤对网站所有路径下资源的访问均进行日志记录。

1.15.3 配置URL过滤对指定类型网页资源的访问不进行日志记录

(1) 进入系统视图。

system-view

(2) 配置 URL 过滤不进行日志记录访问的网页资源类型。

- 配置 URL 过滤对指定预定义类型网页资源的访问不进行日志记录。

  url-filter log except pre-defined { **css** | **gif** | **ico** | **jpg** | **js** | **png** | **swf** | **xml** }
- 配置 URL 过滤对指定自定义类型网页资源的访问不进行日志记录。

  url-filter log except user-defined *text*

缺省情况下，URL 过滤仅对预定义类型（即 css、gif、ico、jpg、js、png、swf 和 xml 类型）网页资源的访问不进行日志记录。

1.16 URL过滤显示和维护

完成上述配置后，在任意视图下执行 **display** 命令可以显示 URL 过滤的配置信息和分类信息等。在用户视图下执行 **reset** 命令可以清除 URL 过滤的统计信息。

表1-2 URL 过滤显示和维护

操作	命令
查看URL过滤缓存中的信息	**display url-filter cache**
显示URL过滤父分类或子分类信息	**display url-filter** { **category** | **parent-category** } [**verbose**]
显示URL过滤特征库信息	**display url-filter signature information**
查看URL过滤的统计信息	**display url-filter statistics**
清除URL过滤的统计信息	**reset url-filter statistics**

1.17 URL过滤典型配置举例

1.17.1 在对象策略中引用URL过滤业务配置举例

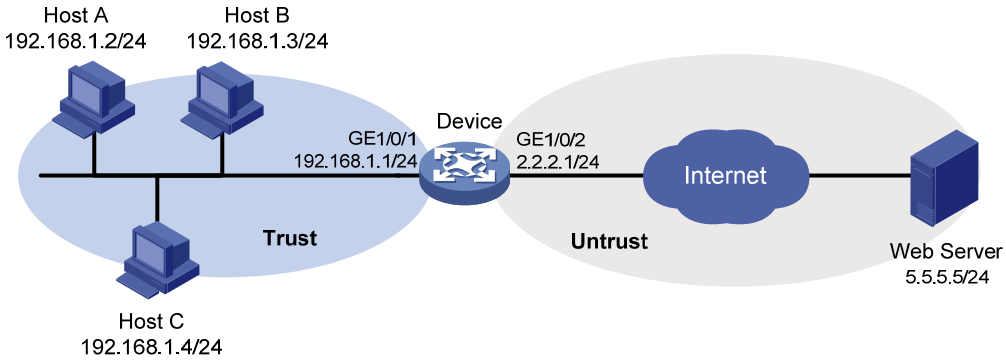
1. 组网需求

如 图 1-3 所示，Device分别通过Trust安全域和Untrust安全域与局域网和Internet相连。现有组网需求如下：

- 配置 URL 过滤功能，允许 Trust 安全域的主机访问 Untrust 安全域的 Web Server 上的 www.sina.com。
- 配置预定义 URL 过滤分类 Pre-Games 的动作为丢弃并生成日志。
- 配置 URL 过滤策略的缺省动作为丢弃和生成日志。

2. 组网图

图1-3 在对象策略中引用 URL 过滤业务配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 创建安全域并将接口加入安全域

向安全域 Trust 中添加接口 GigabitEthernet1/0/1。

```
<Device> system-view
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
```

向安全域 Untrust 中添加接口 GigabitEthernet1/0/2。

```
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
```

(3) 配置对象组

创建名为 urlfilter 的 IP 地址对象组，并定义其子网地址为 192.168.1.0/24。

```
[Device] object-group ip address urlfilter
[Device-obj-grp-ip-urlfilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-urlfilter] quit
```

(4) 配置 URL 过滤功能

创建名 news 的 URL 过滤分类，并进入 URL 过滤分类视图，设置该分类的严重级别为 2000。

```
[Device] url-filter category news severity 2000
```

在 URL 过滤分类 news 中添加一条 URL 过滤规则，并使用字符串 www.sina.com 对主机名字段进行精确匹配。

```
[Device-url-filter-category-news] rule 1 host text www.sina.com
[Device-url-filter-category-news] quit
```

创建名为 urlnews 的 URL 过滤策略，并进入 URL 过滤策略视图。

```
[Device] url-filter policy urlnews
```

在 URL 过滤策略 urlnews 中，配置 URL 过滤分类 news 绑定的动作为允许。

```
[Device-url-filter-policy-urlnews] category news action permit
```

在 URL 过滤策略 urlnews 中，配置预定义 URL 过滤分类 Pre-Games 绑定的动作为丢弃并生成日志。

```
[Device-url-filter-policy-urlnews] category Pre-Games action drop logging
```

在 URL 过滤策略 urlnews 中，配置策略的缺省动作为丢弃和打印日志。

```
[Device-url-filter-policy-urlnews] default-action drop logging
[Device-url-filter-policy-urlnews] quit
```

(5) 配置 DPI 应用 profile

创建名为 sec 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile sec
```

在 DPI 应用 profile sec 中应用 URL 过滤策略 urlnews。

```
[Device-app-profile-sec] url-filter apply policy urlnews
[Device-app-profile-sec] quit
```

激活 URL 过滤策略和规则配置。

```
[Device] inspect activate
```

(6) 配置对象策略

创建名为 urlfilter 的 IPv4 对象策略，并进入对象策略视图。

```
[Device] object-policy ip urlfilter
```

对源 IP 地址对象组 urlfilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 sec。

```
[Device-object-policy-ip-urlfilter] rule inspect sec source-ip urlfilter
destination-ip any
[Device-object-policy-ip-urlfilter] quit
```

(7) 配置安全域间实例并应用对象策略

创建源安全域 Trust 到目的安全域 Untrust 的安全域间实例，并应用对源 IP 地址对象组 urlfilter 对应的报文进行深度检测的对象策略 urlfilter。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-Trust-Untrust] object-policy apply ip urlfilter
[Device-zone-pair-security-Trust-Untrust] quit
```

4. 验证配置

以上配置生效后，Trust 安全域的主机 A、主机 B 和主机 C 都可以访问 Untrust 安全域的 Web Server 上的 www.sina.com，但是都不能访问游戏类的网页。Trust 安全域的主机尝试访问游戏类的 URL 请求将会被 Device 阻断并且打印日志。

1.17.2 手动离线升级URL过滤特征库配置举例

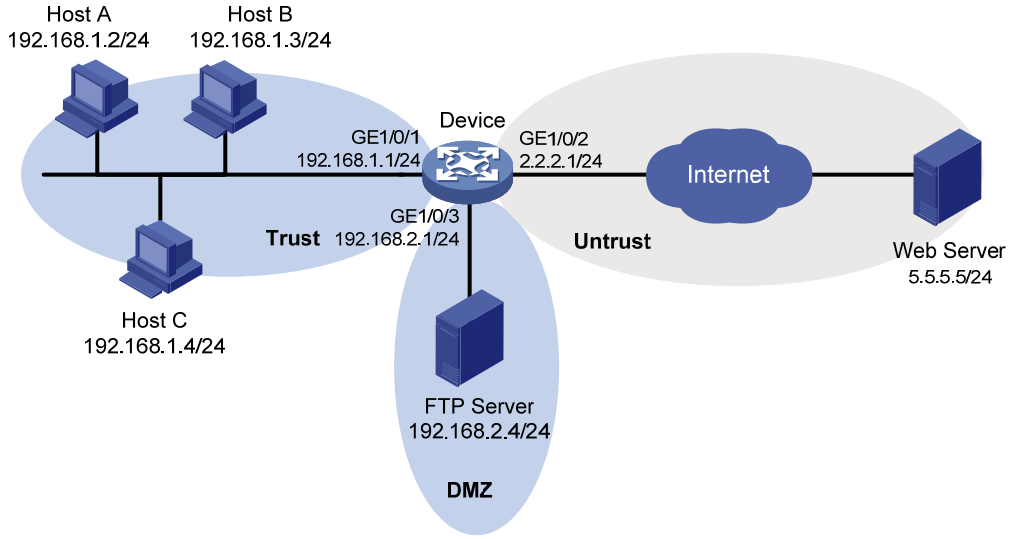
1. 组网需求

如 图 1-4 所示，位于Trust安全域的局域网用户通过Device可以访问Untrust安全域的Internet资源，以及DMZ安全域的FTP服务器。FTP服务器根目录下保存了最新的URL过滤特征库文件url-1.0.2-encrypt.dat，FTP服务器的登录用户名和密码分别为url和 123。现有组网需求如下：

手动离线升级 URL 过滤特征库，加载最新的 URL 过滤分类。

2. 组网图

图1-4 手动离线升级 URL 过滤特征库配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 Device 与 FTP 互通

配置 ACL 2001，定义规则允许所有报文通过。

```
<Device> system-view
[Device] acl basic 2001
[Device-acl-ipv4-basic-2001] rule permit
[Device-acl-ipv4-basic-2001] quit
```

向安全域 DMZ 中添加接口 GigabitEthernet1/0/3。

```
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 1/0/3
[Device-security-zone-DMZ] quit
```

创建源安全域 Local 到目的安全域 DMZ 的安全域间实例，允许 Local 域用户访问 DMZ 域的报文可以通过。

```
[Device] zone-pair security source local destination dmz
[Device-zone-pair-security-Local-DMZ] packet-filter 2001
[Device-zone-pair-security-Local-DMZ] quit
```

创建源安全域 DMZ 到目的安全域 Local 的安全域间实例，允许 DMZ 域用户访问 Local 域的报文可以通过。

```
[Device] zone-pair security source dmz destination local
[Device-zone-pair-security-DMZ-Local] packet-filter 2001
[Device-zone-pair-security-DMZ-Local] quit
```

(3) 升级 URL 过滤特征库

采用 FTP 方式手动离线升级设备上的 URL 过滤特征库，且被加载的 URL 特征库文件名为 url-1.0.2-encrypt.dat。

```
[Device] url-filter signature update ftp://url:123@192.168.2.4/url-1.0.2-encrypt.dat
```

4. 验证配置

URL 过滤特征库升级后，可以通过 **display url-filter signature information** 命令查看当前特征库的版本信息。

1.17.3 定期自动在线升级URL过滤特征库配置举例

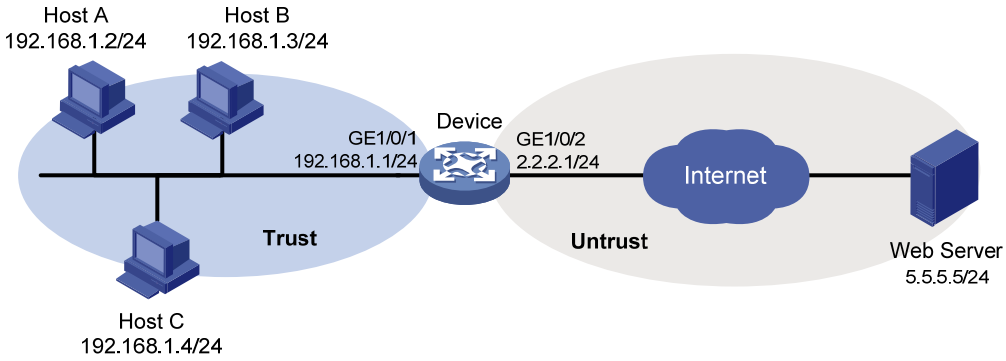
1. 组网需求

如 图 1-5 所示，位于Trust安全域的局域网用户通过Device可以访问Untrust安全域的Internet资源。现有组网需求如下：

配置每周六上午九点前后半小时内，定期自动在线升级设备的 URL 过滤特征库。

2. 组网图

图1-5 定期自动在线升级 URL 过滤特征库配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置设备解析官方网站对应 IP 地址的域名解析功能（略）

(3) 配置对象策略保证 Trust 安全域的局域网用户可以访问 Untrust 安全域的 Internet 资源（略）

(4) 配置定期自动在线升级 URL 过滤特征库

开启自动在线升级 URL 过滤特征库功能，并进入自动在线升级配置视图。

```
<Device> system-view
[Device] url-filter signature auto-update
```

设置定期自动在线升级 URL 过滤特征库计划为：每周六上午 9:00:00 自动在线升级，抖动时间为 60 分钟。

```
[Device-url-filter-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 60
[Device-url-filter-autoupdate] quit
```

4. 验证配置

设置的定期自动在线升级 URL 过滤特征库时间到达后，可以通过 **display url-filter signature information** 命令查看当前特征库的版本信息。

目 录

1 带宽管理 ····· 1-1
1.1 带宽管理简介 ····· 1-1
1.1.1 带宽管理应用场景 ····· 1-1
1.1.2 带宽管理实现流程 ····· 1-1
1.1.3 带宽策略规则 ····· 1-2
1.1.4 带宽通道 ····· 1-2
1.2 带宽管理与硬件适配关系 ····· 1-3
1.3 带宽管理配置限制和指导 ····· 1-4
1.4 带宽管理配置准备 ····· 1-4
1.5 带宽管理配置任务简介 ····· 1-5
1.6 配置带宽通道 ····· 1-5
1.6.1 创建带宽通道 ····· 1-5
1.6.2 配置带宽通道参数 ····· 1-5
1.6.3 配置带宽通道引用方式 ····· 1-7
1.6.4 重命名带宽通道 ····· 1-7
1.7 配置带宽策略规则 ····· 1-7
1.7.1 创建带宽策略规则 ····· 1-7
1.7.2 配置带宽策略规则过滤条件 ····· 1-8
1.7.3 配置带宽策略规则动作 ····· 1-9
1.7.4 配置带宽策略规则生效时间 ····· 1-9
1.8 管理和维护带宽策略规则 ····· 1-10
1.8.1 复制带宽策略规则 ····· 1-10
1.8.2 重命名带宽策略规则 ····· 1-10
1.8.3 移动带宽策略规则 ····· 1-10
1.8.4 禁用带宽策略规则 ····· 1-10
1.9 开启带宽管理统计功能 ····· 1-11
1.10 带宽管理显示和维护 ····· 1-11
1.11 带宽管理典型配置举例 ····· 1-13
1.11.1 单通道模式带宽管理配置举例 ····· 1-13
1.11.2 父子通道模式带宽管理配置举例 ····· 1-15

1 带宽管理

1.1 带宽管理简介

带宽管理对通过设备的流量实现基于 SSID（Service Set Identifier，服务集标识符）、User Profile、源/目的安全域、源/目的 IP 地址、服务、应用、DSCP 优先级和时间段等，实现精细化的管理和控制。

1.1.1 带宽管理应用场景

带宽管理的应用场景如下：

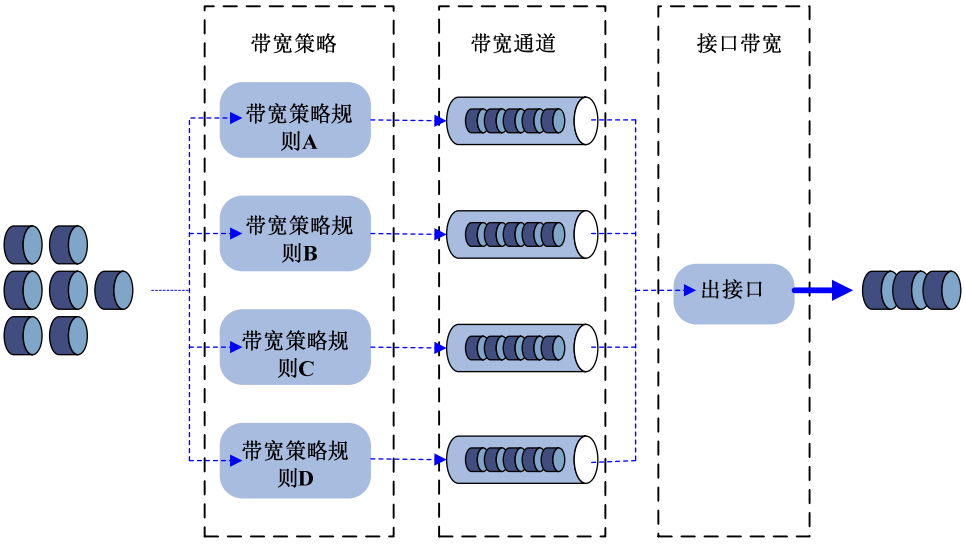
- 企业内网用户所需的带宽远大于从运营商租用的出口带宽，这时网络出口就会存在带宽瓶颈的问题。
- 网络出口中 P2P 业务类型的数据流量消耗了绝大部分的带宽资源，致使企业的关键业务得不到带宽保证。

为了解决以上问题，可以在网络出口设备上部署带宽管理，针对不同的内网业务流量应用不同的带宽策略规则，实现合理分配出口带宽和保证关键业务正常运行的目的。

1.1.2 带宽管理实现流程

带宽策略可以对符合匹配条件的流量应用带宽通道，在带宽通道中可以配置带宽保证和带宽限制功能，进而提高带宽利用率以及在线路拥堵时保证关键业务的正常运行。

图1-1 带宽管理实现流程图



带宽管理实现流程如下：

(1) 将报文的属性信息与带宽策略规则中的过滤条件进行匹配。每种过滤条件的多个匹配项之间是或的关系，即报文与某一个过滤条件中的任意一项匹配成功，则报文与此条过滤条件匹配成功；若报文与某一个过滤条件中的所有项都匹配失败，则报文与此条过滤条件匹配失败。

(2) 若报文与某条带宽策略规则中的所有过滤条件都匹配成功（用户与用户组匹配一项即可），则报文与此条带宽策略规则匹配成功。若有一个过滤条件不匹配，则报文与此条带宽策略规则匹配失败，报文继续匹配下一条带宽策略规则。以此类推，直到最后一条带宽策略规则，若报文还未与规则匹配成功，则不对报文进行带宽管理。

(3) 报文与某条带宽策略规则匹配成功后便结束此匹配过程，如果此规则的动作中引用了带宽通道，则流量继续进入相应的带宽通道进行后续的处理，否则设备不对该流量进行带宽管理。

(4) 流量进入带宽通道后，设备会根据此带宽通道中配置的带宽限制策略对流量进行相应的处理。

(5) 如果出接口出方向上应用了QoS业务，则对流量先进行带宽策略处理，再进行QoS业务处理。

(6) 流量从出接口发送时受该接口带宽的限制。

1.1.3 带宽策略规则

带宽策略中可以配置多个带宽策略规则，这些规则用于定义匹配流量的过滤条件以及流量控制的动作。带宽策略规则支持四级嵌套关系，即一个规则中可以指定一个父规则，最多支持嵌套四级。

1. 带宽策略规则过滤条件

每条带宽策略规则中可以配置多种过滤条件，具体包括：源/目的安全域、源/目的 IP 地址、服务、应用和 DSCP 优先级。每种过滤条件中均可以配置多个匹配项，比如应用过滤条件中可以指定多个应用等。

2. 带宽策略规则动作

在带宽策略规则动作中引用带宽通道后，设备将根据此带宽通道对此流量进行限流。

3. 嵌套规则匹配原则

流量与存在父规则的带宽策略规则进行匹配时，遵守如下原则：

- 首先匹配父规则，如果父规则匹配上了再匹配子规则。如果父规则没有匹配上，也不会进行后续的子规则匹配，该匹配过程失败。
- 如果子规则匹配上了，先执行子规则中指定的动作，再执行父规则中指定的动作，如果父子规则对同一个带宽资源限制参数或流量优先级参数进行限制，则执行最严格的动作。如果子规则没有匹配上但父规则匹配上了，则执行父规则中指定的动作。

1.1.4 带宽通道

带宽通道定义了具体的带宽资源，是进行带宽管理的基础。通过带宽通道，可以将物理的带宽资源从逻辑上划分为多个虚拟的带宽通道，每个带宽通道中都可自定义相应的带宽资源限制参数和流量优先级参数。目前，带宽通道中支持的带宽资源限制参数和流量优先级参数包括以下如下几种：

1. 带宽通道限流方式

带宽通道中对流量的限制方式，包括如下两种：

- 分别设置上下行带宽：对带宽通道中的上下行流量分别限制。
- 设置总带宽：对带宽通道中的上下行流量整体限制。

2. 每规则带宽限制

每规则的保证带宽：保证业务的最小带宽，在线路拥堵时，可以保证公司关键业务所需的带宽，确保此类业务不受影响。

每规则的最大带宽：限制业务的最大带宽，比如限制网络中非关键业务占用的带宽资源，避免该类业务消耗大量的带宽，影响其他关键业务的正常运行。

3. 每IP或每用户带宽限制

每 IP 或每用户的保证带宽：设备除了支持配置每规则的保证带宽之外，还支持基于 IP 地址和用户的保证带宽，实现更加精细化的带宽管理。

每 IP 或每用户的最大带宽：设备除了支持配置每规则的最大带宽之外，还支持基于 IP 地址和用户的最大带宽，实现更加精细化的带宽管理。

4. 连接数限制

每规则、每 IP 或每用户的最大连接数和最大新建连接速率限制：通常在出现以下两类网络问题的组网环境中需要在设备上配置最大连接数和最大新建连接速率限制：某内网用户在短时间内经过设备向外部网络发起大量连接，导致设备系统资源迅速消耗，其它内网用户无法正常使用网络资源；某内部服务器在短时间内接收到大量的连接请求，导致该服务器忙于处理这些连接请求，以至于不能再接受其它客户端的正常连接请求。

5. 流量优先级限制

流量优先级：当多个带宽通道中的流量同时从某个接口发送时，如果此接口发生阻塞，则优先级高的流量优先被发送。优先级相同的流量将会自由竞争出接口的带宽资源。

重标记报文的 DSCP 优先级：修改报文中 DSCP（Differentiated Services Code Point）字段的值，DSCP 优先级是网络设备进行流量分类的依据。位于报文传输路径上的各个网络设备，能够通过 DSCP 优先级来区分流量，因此可以便于上下行设备依据修改后的 DSCP 优先级对流量采取差异化处理。

1.2 带宽管理与硬件适配关系

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK、MSR810-W-LM-HK、MSR810-LM-CNDE-SJK	支持
MSR810-LMS、MSR810-LUS	不支持
MSR810-LMS-EA、MSR810-LME	支持
MSR2600-6-X1、MSR2600-10-X1	支持
MSR 2630	支持
MSR3600-28、MSR3600-51	支持
MSR3600-28-SI、MSR3600-51-SI	不支持
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	支持

型号	说明
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES	支持
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC	支持
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	支持
MSR3610-G、MSR3620-G	支持

型号	描述
MSR810-W-WiNet、MSR810-LM-WiNet	支持
MSR830-4LM-WiNet	支持
MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	支持
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	支持
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	支持
MSR2630-WiNet	支持
MSR3600-28-WiNet	支持
MSR3610-X1-WiNet	支持
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	支持

型号	说明
MSR2630-XS	支持
MSR3600-28-XS	支持
MSR3610-XS	支持
MSR3620-XS	支持
MSR3610-I-XS	支持
MSR3610-IE-XS	支持

1.3 带宽管理配置限制和指导

配置带宽管理策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

1.4 带宽管理配置准备

在配置带宽管理策略之前，需完成以下任务：

- 配置时间段（请参见“ACL 和 QoS 配置指导”中的“时间段”）。

- 配置 IP 地址对象组和服务对象组（请参见“安全配置指导”中的“对象组”）。
- 配置应用（请参见“安全配置指导”中的“APR”）。
- 配置安全域（请参见“安全配置指导”中的“安全域”）。

1.5 带宽管理配置任务简介

带宽管理配置任务如下：

(1) 配置带宽通道
- 创建带宽通道
- 配置带宽通道参数
- 配置带宽通道引用方式
- （可选）重命名带宽通道

(2) 配置带宽策略规则
- 创建带宽策略规则
- 配置带宽策略规则过滤条件
- 配置带宽策略规则动作
- （可选）配置带宽策略规则生效时间

(3) （可选）管理和维护带宽策略规则
- 复制带宽策略规则
- 重命名带宽策略规则
- 移动带宽策略规则
- 禁用带宽策略规则

(4) （可选）开启带宽管理统计功能

1.6 配置带宽通道

1.6.1 创建带宽通道

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 创建带宽通道，并进入带宽通道视图。

profile name *profile-name*

1.6.2 配置带宽通道参数

1. 功能简介

带宽通道定义了实施带宽管理的对象所能够使用的带宽资源，带宽通道将被带宽策略规则引用后生效。

2. 配置限制和指导

每 IP 最大带宽、每用户最大带宽和最大带宽动态均分功能三种控制方式不能同时存在，会相互替换，最后一次配置的控制方式生效。

每 IP 保证带宽与每用户保证带宽两种控制方式不能同时存在，会相互替换，最后一次配置的控制方式生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽通道视图。

profile name *profile-name*

(4) 配置带宽参数。

- 配置每规则的保证带宽和最大带宽。

  bandwidth { **downstream** | **total** | **upstream** } { **guaranteed** | **maximum** } *bandwidth-value*

  缺省情况下，未配置带宽通道的保证带宽和最大带宽。

  请保证最大带宽不小于保证带宽。

  如需开启最大带宽的动态均分功能，则必须配置每规则的最大带宽。

- 配置每 IP 或每用户的保证带宽和最大带宽。

  bandwidth { **downstream** | **total** | **upstream** | } { **guaranteed** | **maximum** } { **per-ip** | **per-user** } *bandwidth-value*

  缺省情况下，未配置每 IP 或每用户的保证带宽和最大带宽。

- 开启最大带宽动态均分功能。

  bandwidth average enable

  缺省情况下，最大带宽动态均分功能处于关闭状态。

(5) 配置连接数限制参数。

- 配置最大连接数。

  connection-limit count { **per-rule** | **per-ip** | **per-user** } *connection-number*

  缺省情况下，未配置最大连接数。

- 配置最大新建连接速率。

  connection-limit rate { **per-rule** | **per-ip** | **per-user** } *connection-rate*

  缺省情况下，未配置最大新建连接速率。

(6) 配置优先级参数。

- 配置流量优先级。

  traffic-priority *priority-value*

  缺省情况下，流量优先级为 1。

- 重标记报文的 DSCP 优先级。

  remark dscp *dscp-value*

  缺省情况下，不修改报文的 DSCP 优先级。

1.6.3 配置带宽通道引用方式

1. 功能简介

多个带宽策略规则引用同一个带宽通道的方式，包括如下两种：

- 策略独占：表示与带宽策略规则匹配成功的流量，独享带宽通道中的带宽限制和连接数限制。
- 策略共享：表示与多条带宽策略规则匹配成功的多条流量，共享带宽通道中的带宽限制和连接数限制。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 并进入带宽通道视图。

profile name *profile-name*

(4) 配置带宽通道的引用方式。

profile reference-mode { **per-rule** | **rule-shared** }

缺省情况下，带宽通道的引用方式为策略独占。

1.6.4 重命名带宽通道

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 重命名带宽通道。

profile rename *old-name new-name*

1.7 配置带宽策略规则

1.7.1 创建带宽策略规则

1. 功能简介

一个带宽策略中可以创建多个带宽策略规则，这些规则可以独立定义，也可以继承其它规则。继承其他带宽策略规则是通过在创建带宽策略规则时为其指定父带宽策略规则实现的。在父带宽策略规则和子带宽策略规则中均可以引用带宽通道。

2. 配置限制和指导

第四级带宽策略规则不能再作为父带宽策略规则。

只能在创建带宽策略规则时指定带宽策略规则的父带宽策略规则，不能为已存在的带宽策略规则添加或修改父带宽策略规则。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 创建带宽策略规则，并进入该带宽策略规则视图。

rule [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

1.7.2 配置带宽策略规则过滤条件

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

- **rule** *rule-id*
- **rule** [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

(4) 配置作为带宽策略规则过滤条件的安全域。

- 配置作为带宽策略规则过滤条件的目的安全域。

  destination-zone *destination-zone-name*

- 配置作为带宽策略规则过滤条件的源安全域。

  source-zone *source-zone-name*

缺省情况下，未配置作为带宽策略规则过滤条件的安全域。

(5) 配置作为带宽策略规则过滤条件的地址对象组。

- 配置作为带宽策略规则过滤条件目的 IP 地址。

  destination-address address-set *object-group-name*

- 配置作为带宽策略规则过滤条件的源 IP 地址。

  source-address address-set *object-group-name*

缺省情况下，未配置作为带宽策略规则过滤条件的地址对象组。

(6) 配置作为带宽策略规则过滤条件的服务。

service *object-group-name*

缺省情况下，未配置作为带宽策略规则过滤条件的服务。

(7) 配置作为带宽策略规则过滤条件的应用。

application { **app** *application-name* | **app-group** *application-group-name* }

缺省情况下，未配置作为带宽策略规则过滤条件的应用。

(8) 配置作为带宽策略规则过滤条件的 DSCP 优先级。

dscp *dscp-value*

缺省情况下，未配置作为带宽策略规则过滤条件的 DSCP 优先级。

1.7.3 配置带宽策略规则动作

1. 功能简介

如果流量成功匹配了某个带宽策略规则，则设备将会根据该带宽策略规则中指定的动作对此流量进行控制和管理，即按照引用的带宽通道对此流量进行限流。

2. 配置限制和指导

子规则引用的带宽通道中的最大带宽不能大于父规则引用的带宽通道中的最大带宽。

父规则引用的带宽通道中的保证带宽不能小于子规则引用的带宽通道中的保证带宽。

子规则与父规则不能引用同一个带宽通道。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

- **rule** *rule-id*
- **rule** [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

(4) 配置带宽策略规则中的动作。

action qos profile *profile-name*

缺省情况下，带宽策略规则中没有配置动作，即对匹配上该规则的流量不进行带宽管理，直接允许通过。

1.7.4 配置带宽策略规则生效时间

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

- **rule** *rule-id*
- **rule** [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

(4) 配置带宽策略规则的生效时间。

time-range *time-range-name*

缺省情况下，带宽策略规则在任何时间下都生效。

1.8 管理和维护带宽策略规则

1.8.1 复制带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 复制带宽策略规则。

rule copy *rule-name new-rule-name*

1.8.2 重命名带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 重命名带宽策略规则。

rule rename *old-rule-name new-rule-name*

1.8.3 移动带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 移动带宽策略规则的排列顺序。

rule move *rule-name1* { **after** | **before** } *rule-name2*

1.8.4 禁用带宽策略规则

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 进入带宽策略规则视图。请选择其中一项进行配置。

- **rule** *rule-id*
- **rule** [*rule-id*] **name** *rule-name* [**parent** *parent-rule-name*]

(4) 禁用带宽策略规则。

disable

缺省情况下，带宽策略规则处于开启状态。

1.9 开启带宽管理统计功能

1. 功能简介

设备支持如下带宽管理统计功能：

- 流量统计功能：带宽管理业务将对匹配带宽策略规则的流量进行统计。
- 连接数限制统计功能：带宽管理业务将对匹配带宽策略规则的连接数限制信息进行统计。
- 规则命中统计功能：带宽管理业务将对带宽策略规则的命中情况进行统计。

2. 配置限制和指导

开启统计功能将对设备处理性能产生影响，建议仅在需要查看统计信息时开启。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入带宽策略视图。

traffic-policy

(3) 开启带宽管理统计功能。

- 开启带宽管理流量统计功能。

  statistics bandwidth enable

  缺省情况下，带宽管理流量统计功能处于关闭状态。

- 开启带宽管理连接数限制统计功能。

  statistics connection-limit enable

  缺省情况下，带宽管理连接数限制统计功能处于关闭状态。

- 开启带宽管理规则命中统计功能。

  statistics rule-hit enable

  缺省情况下，带宽管理规则命中统计功能处于关闭状态。

1.10 带宽管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后带宽管理的运行情况，以及带宽管理处理业务的统计信息。

表1-1 带宽管理显示和维护

操作	命令
显示带宽管理的流量统计信息	（独立运行模式） **display traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } （IRF模式） **display traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]
显示带宽管理的连接数限制统计信息	（独立运行模式） **display traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } （IRF模式） **display traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]
显示带宽策略规则的命中统计信息	（独立运行模式） **display traffic-policy statistics rule-hit** [**rule** *rule-name*] （IRF模式） **display traffic-policy statistics rule-hit** [**rule** *rule-name*] [**slot** *slot-number*]

操作	命令
清除带宽管理的流量统计信息	（独立运行模式） **reset traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } （IRF模式） **reset traffic-policy statistics bandwidth** { **downstream** | **total** | **upstream** } { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } [**slot** *slot-number*]
清除带宽管理的连接数限制统计信息	（独立运行模式） **reset traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } （IRF模式） **reset traffic-policy statistics connection-limit** { **per-ip** { **ipv4** [*ipv4-address*] | **ipv6** [*ipv6-address*] } **rule** *rule-name* | **per-rule** [**name** *rule-name*] | **per-user** [**user** *user-name*] **rule** *rule-name* } } [**slot** *slot-number*]
清除带宽策略规则被命中次数的统计信息	（独立运行模式） **reset traffic-policy statistics rule-hit** [**rule** *rule-name*] （IRF模式） **reset traffic-policy statistics rule-hit** [**rule** *rule-name*] [**slot** *slot-number*]

1.11 带宽管理典型配置举例

1.11.1 单通道模式带宽管理配置举例

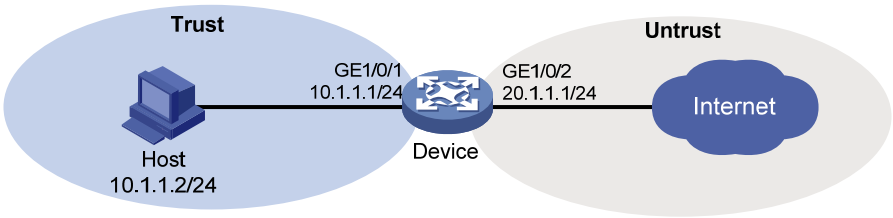
1. 组网需求

内网主机通过 Device 与外网相连，通过在 Device 上配置带宽管理功能，实现当内网流量的出口发生拥塞时优先保证 FTP 业务的需求。具体要求如下：

- 限制内网用户，访问外网爱奇艺（iQiYiPPS）应用流量的上行最大带宽和下行最大带宽均为30720kbps。
- 保证内网用户，访问外网 FTP 应用流量的上行保证带宽和下行保证带宽均为 30720kbps。
- 限制外网出接口的最大带宽为 102400kbps。

2. 组网图

图1-2 单通道模式带宽管理配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间对象策略保证网络可达，具体配置步骤略

(2) 配置带宽通道

创建名为 aiqiyi 的带宽通道，并进入该带宽通道视图。

```
<Device> system-view
[Device] traffic-policy
[Device-traffic-policy] profile name aiqiyi
```

配置上/下行最大带宽均为 30720kbps。

```
[Device-traffic-policy-profile-aiqiyi] bandwidth upstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] bandwidth downstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] quit
```

创建名为 profileFTP 的带宽通道，并进入该带宽通道视图。

```
[Device-traffic-policy] profile name profileFTP
```

配置上/下行保证带宽均为 30720kbps。

```
[Device-traffic-policy-profile-profileFTP] bandwidth upstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] bandwidth downstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] quit
[Device-traffic-policy] quit
```

(3) 配置出接口的最大带宽

配置接口 GigabitEthernet1/0/2 的期望带宽为 102400kbps。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] bandwidth 102400
[Device-GigabitEthernet1/0/2] quit
```

(4) 配置带宽策略规则

进入带宽策略视图。

```
[Device] traffic-policy
```

创建名为 aiqiyi 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name aiqiyi
```

在带宽策略规则 aiqiyi 中引用预定义应用 iQiYiPPS。

```
[Device-traffic-policy-rule-1-aiqiyi] application app iQiYiPPS
```

配置带宽策略规则 aiqiyi 中的动作为限流并应用带宽通道 aiqiyi。

```
[Device-traffic-policy-rule-1-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-1-aiqiyi] quit
```

创建名为 ruleFTP 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name ruleFTP
```

配置带宽策略规则 ruleFTP 中引用预定义的应用 ftp。

```
[Device-traffic-policy-rule-2-ruleFTP] application app ftp
```

配置带宽策略规则 ruleFTP 中的动作为限流并应用带宽通道 profileFTP。

```
[Device-traffic-policy-rule-2-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-2-ruleFTP] quit
[Device-traffic-policy] quit
```

4. 验证配置

配置完成后，当出接口 GigabitEthernet1/0/2 的流量达到 102400kbps 后，爱奇艺应用的流量最大只能达到 30720kbps，FTP 应用的流量能够保证最少达到 30720kbps。

1.11.2 父子通道模式带宽管理配置举例

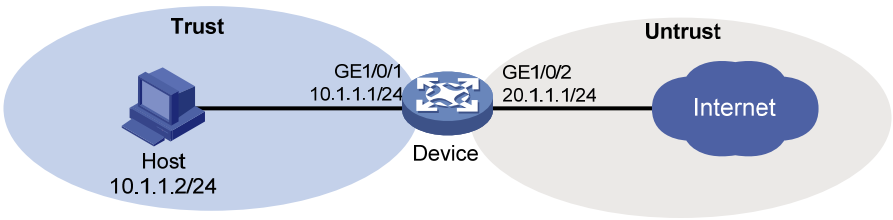
1. 组网需求

内网主机通过 Device 与外网相连，通过在 Device 上配置带宽管理功能，实现当内网流量发生拥塞时优先保证 FTP 业务的需求。具体要求如下：

- 限制内网用户，访问外网爱奇艺（iQiYiPPS）应用流量的上行最大带宽和下行最大带宽均为 30720kbps。
- 保证内网用户，访问外网 FTP 应用流量的上行保证带宽和下行保证带宽均为 30720kbps。
- 限制内网用户的最大带宽为 40960kbps。

2. 组网图

图1-3 父子通道模式带宽管理配置组网图



3. 配置步骤

(1) 配置接口 IP 地址、路由、安全域及域间对象策略保证网络可达，具体配置步骤略

(2) 配置带宽通道

创建名为 profile 的带宽通道，并进入该带宽通道视图。

```
<Device> system-view
[Device] traffic-policy
[Device-traffic-policy] profile name profile
```

配置上/下行最大带宽均为 40960kbps。

```
[Device-traffic-policy-profile-profile] bandwidth upstream maximum 40960
[Device-traffic-policy-profile-profile] bandwidth downstream maximum 40960
[Device-traffic-policy-profile-profile] quit
```

创建名为 aiqiyi 的带宽通道，并进入该带宽通道视图。

```
[Device-traffic-policy] profile name aiqiyi
```

配置上/下行最大带宽均为 30720kbps。

```
[Device-traffic-policy-profile-aiqiyi] bandwidth upstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] bandwidth downstream maximum 30720
[Device-traffic-policy-profile-aiqiyi] quit
```

创建名为 profileFTP 的带宽通道，并进入该带宽通道视图。

```
[Device-traffic-policy] profile name profileFTP
```

配置上/下行保证带宽均为 30720kbps。

```
[Device-traffic-policy-profile-profileFTP] bandwidth upstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] bandwidth downstream guaranteed 30720
[Device-traffic-policy-profile-profileFTP] quit
```

(3) 配置带宽策略

创建名为 rule 的带宽策略规则，并进入该带宽策略规则视图。

```
[Device-traffic-policy] rule name rule
```

配置带宽策略规则 rule 中的动作为限流并应用带宽通道 profile。

```
[Device-traffic-policy-rule-1-rule] action qos profile profile
[Device-traffic-policy-rule-1-rule] quit
```

创建名为 aiqiyi 的带宽策略规则，并进入该带宽策略规则视图，指定带宽策略规则的父规则为 rule。

```
[Device-traffic-policy] rule name aiqiyi parent rule
```

在带宽策略规则 aiqiyi 中引用预定义应用 iQiYiPPS。

```
[Device-traffic-policy-rule-2-aiqiyi] application app iQiYiPPS
```

配置带宽策略规则 aiqiyi 中的动作为限流并应用带宽通道 aiqiyi。

```
[Device-traffic-policy-rule-2-aiqiyi] action qos profile aiqiyi
[Device-traffic-policy-rule-2-aiqiyi] quit
```

创建名为 ruleFTP 的带宽策略规则，并进入该带宽策略规则视图，指定带宽策略规则的父规则为 rule。

```
[Device-traffic-policy] rule name ruleFTP parent rule
```

配置带宽策略规则 ruleFTP 中引用预定义的应用 ftp。

```
[Device-traffic-policy-rule-3-ruleFTP] application app ftp
```

配置带宽策略规则 ruleFTP 中的动作为限流并应用带宽通道 profileFTP。

```
[Device-traffic-policy-rule-3-ruleFTP] action qos profile profileFTP
[Device-traffic-policy-rule-3-ruleFTP] quit
[Device-traffic-policy] quit
```

4. 验证配置

以上配置完成后，内网用户的实际流量会限制在 40960kbps，并且爱奇艺流量被限制在 30720kbps；当网络发生拥塞时，FTP 业务基本不受影响。