UNIS 入侵防御系统产品

DPI 深度安全配置指导

北京紫光恒越网络科技有限公司
http://www.unis-hy.com

资料版本：5PW100-20160929

前 言

UNIS 入侵防御系统产品配置指导介绍了入侵防御系统产品各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《DPI 深度安全配置指导》主要介绍 DPI 深度安全概述、应用层检测引擎、IPS、URL 过滤、数据过滤、文件过滤和防病毒相关的特性。

前言部分包含如下内容：

适用款型

入侵防御系统产品款型较多，形态丰富，本手册所描述的内容适用于如下产品款型：

表1 手册适用的产品款型

款型	形态
UNIS T5000-M06	分布式设备，可以运行在： • 独立运行模式 • IRF 模式
UNIS T5000-G20	集中式IRF设备
UNIS T1000-G20/G50/G60/G80	集中式IRF设备

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

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

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。

技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unis-hy.com

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：zgsm_info@thunis.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 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流经设备的网络流量进行检测和控制的安全机制。

1.1.1 DPI深度安全的应用背景

随着信息技术的日新月异和网络信息系统应用的快速发展，网络技术应用正在从传统、小型业务系统逐渐向大型、关键业务系统扩展，网络所承载的数据应用日益增加，呈现复杂化、多元化趋势。网络在使得我们的工作和生活快捷、方便的同时也带来了许多安全问题，比如，信息泄露和计算机感染病毒等。

虽然防火墙技术在网络中的应用极大提高了网络的安全性。但是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。因此，在网络应用和网络威胁都不断高速增长的今天，仅仅依靠网络层和传输层的安全检测技术，已经无法满足日益增长的网络安全要求。

因此，设备必须具备 DPI 深度安全功能，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。

1.1.2 DPI深度安全的功能

DPI 深度安全提供了一种对数据报文进行一体化检测和多 DPI 业务（如内容过滤、URL 过滤等）处理相结合的安全机制，提高了设备的安全检测以及 DPI 业务处理性能，简化了多 DPI 业务策略配置的复杂度。

具体来说，DPI 深度安全功能可以实现业务识别、业务控制和业务统计。

- 业务识别

业务识别是指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。业务识别功能由应用层检测引擎模块来完成，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、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。

1.1.3 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，设备中的 DPI 特征库包括：IPS 特征库、URL 分类特征库、APR 特征库和防病毒特征库。

1.1.4 DPI业务

目前，设备支持的DPI业务主要包括：IPS（Intrusion Prevention System，入侵防御系统）、URL过滤、数据过滤、文件过滤、防病毒和NBAR（Network Based Application Recognition，基于内容特征的应用层协议识别），有关DPI业务的详细介绍请参见 表 1-1。

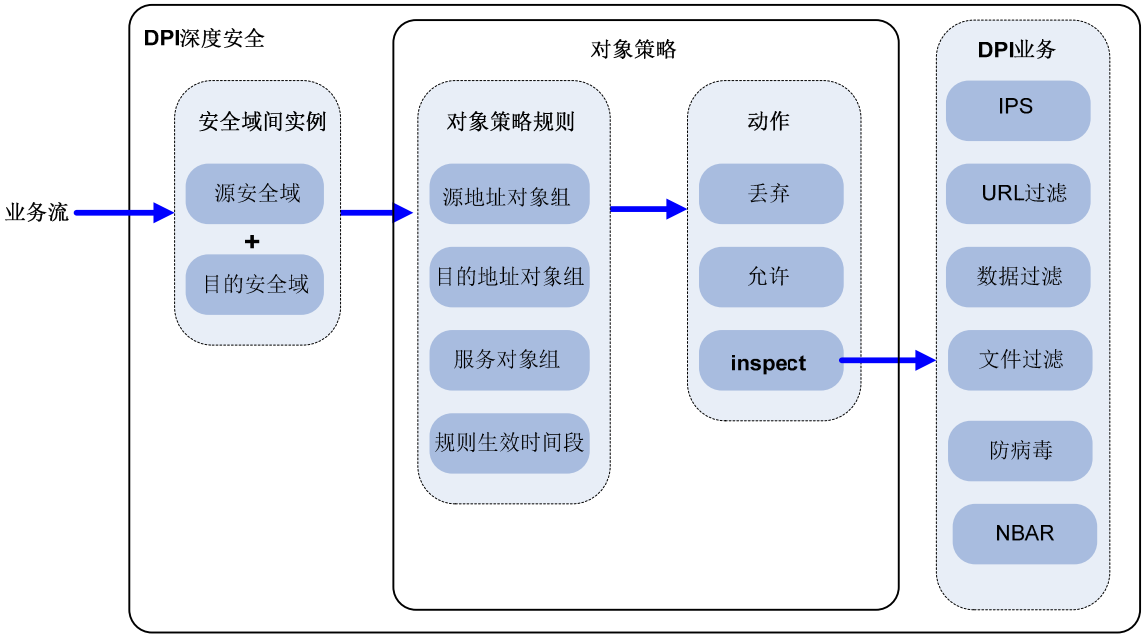
表1-1 DPI 业务详细介绍

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
数据过滤	数据过滤功能可对应用层协议报文中携带的内容进行过滤，阻止企业机密信息泄露和违法、敏感信息的传播
文件过滤	文件过滤功能可根据文件扩展名信息对经设备传输的文件进行过滤
防病毒	防病毒功能可经过设备的文件进行病毒检测和处理，确保内部网络安全
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”

1.1.5 DPI深度安全的处理流程

DPI深度安全功能基于安全域间实例实现。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) 从指定源安全域到指定目的安全域的报文，属于一个安全域间实例。每一个安全域间实例下可以关联多个对象策略规则，且其中定义了报文匹配的源 IP 地址、目的 IP 地址和服务类型等信息。进入安全域间实例的报文将与此安全域实例下的对象策略规则进行匹配。

(2) 如果业务流与对象策略规则中的所有条件都匹配，则此业务流成功匹配对象策略规则。如果业务流未与对象策略规则匹配成功，则此业务流将会被拒绝通过。

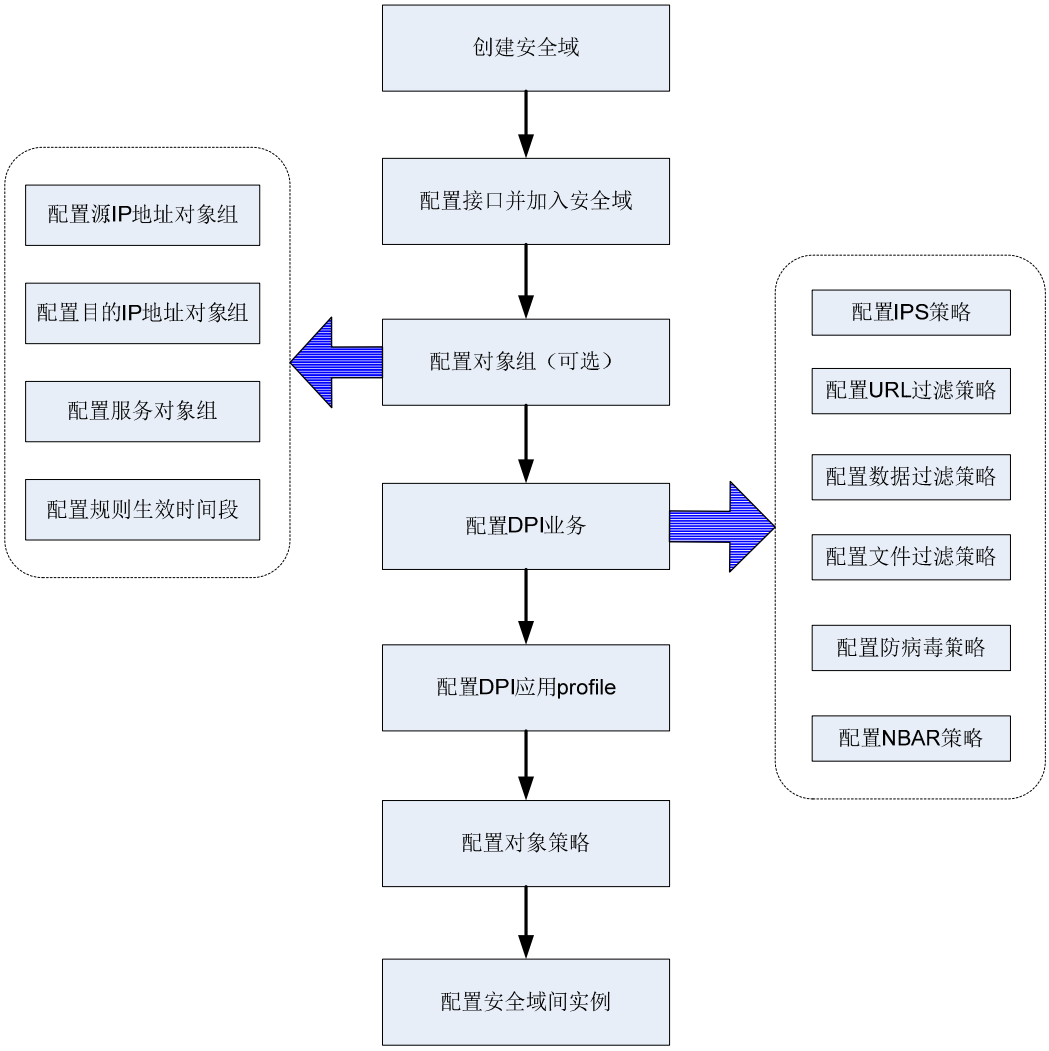
(3) 如果业务流成功匹配对象策略规则，设备将执行此对象策略规则中指定的动作。如果动作为“丢弃”，则设备将阻断此业务流；如果动作为“允许”，则设备将允许此业务流通过；如果动作为“**inspect**”，则继续进行步骤 4 的处理。

(4) 如果对象策略规则中的动作为“**inspect**”且引用的 DPI 业务存在，则设备将对此业务流进行 DPI 业务的一体化检测。如果对象策略规则中引用的 DPI 业务不存在，则设备将允许此业务流通过。

1.2 DPI深度安全配置指导

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

说明

对于本节命令中的 CPU 参数，仅 T5000-M06 产品支持。

1.1 应用层检测引擎简介

1.1.1 应用层检测引擎产生背景

在当前日益复杂和严峻的网络安全威胁中，需要将 IPS（Intrusion Prevention System，入侵防御系统）、URL 过滤、文件过滤、邮件过滤、数据过滤、应用行为控制和防病毒等 DPI（Deep Packet Inspection，深度报文检测）业务集成在一台设备上，且这些业务都需要对报文的应用层信息进行识别，以最终识别出此应用层信息的应用或行为。为了避免因 DPI 业务模块各自进行应用层信息识别，而导致设备性能大幅下降，需要一个公共的检测模块来实现对应用层信息的统一识别，设备会把识别结果反馈给各 DPI 业务模块，各模块再根据自己的策略完成对报文的后续业务处理，这样设备就能对报文实现一次检测，多次处理的效果。应用层检测引擎就是实现这个公共检测功能的模块。

1.1.2 应用层检测引擎简介

应用层检测引擎是 DPI 业务的应用层信息检测模块，提供以下三个基本功能：

- 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，且匹配速度快。
- 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。

1.1.3 检测规则

1. 检测规则

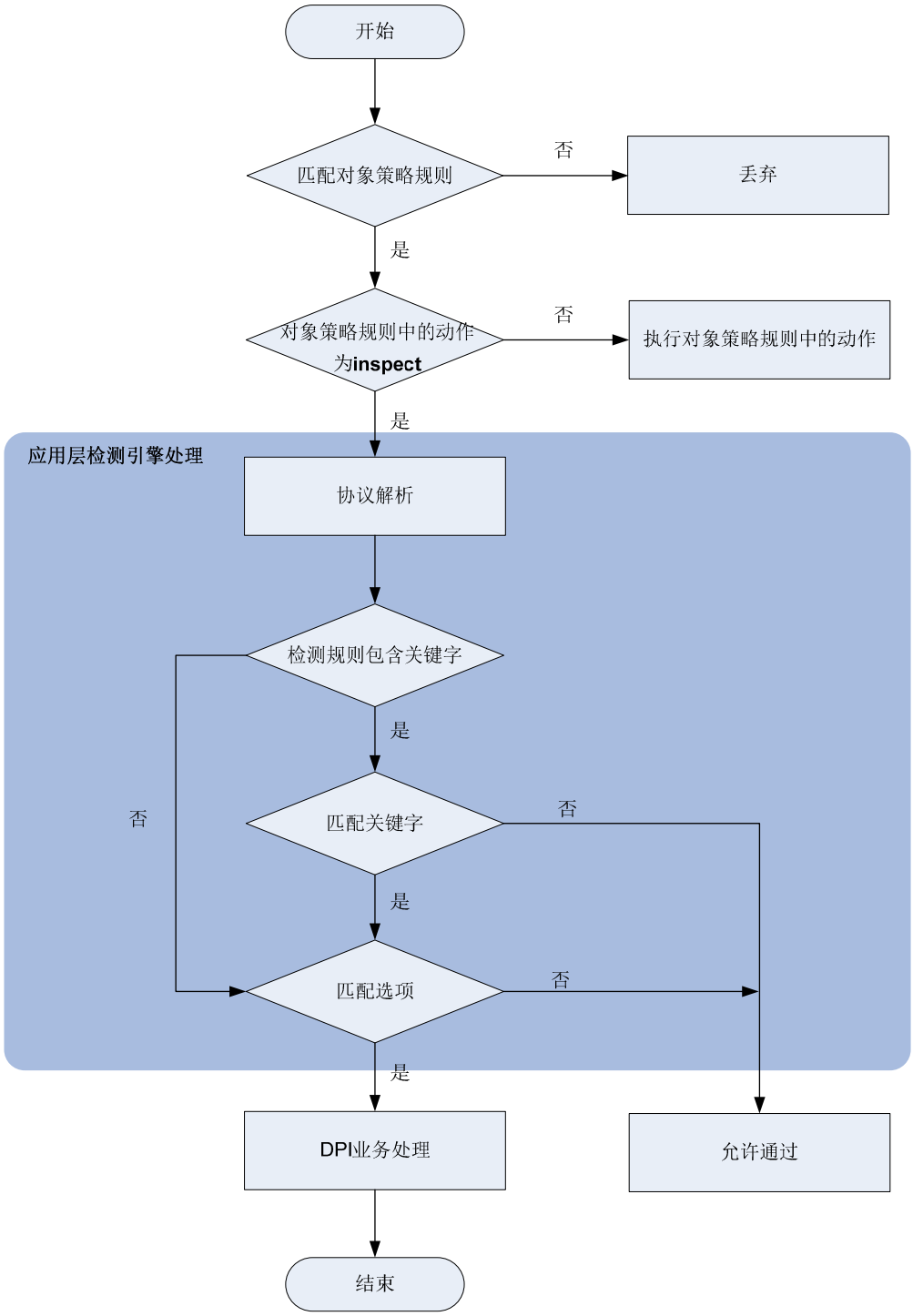
应用层检测引擎使用检测规则对报文进行匹配，检测规则由各 DPI 业务的规则或特征转换而成，包含关键字和选项两种匹配项。

- 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：检测规则中非关键字之外的匹配项，例如报文的端口号、协议类型等。

检测规则中可以包含关键字和选项，也可以不包含关键字。如果检测规则中包含关键字和选项，则两者都被匹配上才算是与该检测规则匹配成功。

1.1.4 应用层检测引擎工作机制

图1-1 应用层检测引擎工作机制示意图



如 图 1-1所示，应用层检测引擎的具体工作机制如下：

(1) 设备收到报文后，首先对报文进行对象策略规则匹配，如果对象策略规则匹配成功，且对象策略规则的动作是 **inspect**，则此报文进入应用层检测引擎处理；如果对象策略规则的动作

不是 **inspect**，则根据对象策略规则中的动作对此报文进行处理。如果报文与对象策略规则匹配失败，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”。

(2) 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，即识别报文的应用层协议和对此报文进行分析，根据分析结果查找相应的检测规则。

(3) 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，则进行关键字匹配，否则直接进行选项匹配。

(4) 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），否则直接允许报文通过。

(5) 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。之后，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 应用层检测引擎配置限制和指导

在多 Context 应用场景中，配置非缺省 Context 的 DPI 业务前，必须先激活缺省 Context 的应用层检测引擎。激活缺省 Context 的应用层检测引擎方法有如下几种：在缺省 Context 的系统视图下执行 **inspect activate** 命令；或在缺省 Context 的对象策略中引用 DPI 应用 profile；或在缺省 Context 上配置带宽管理功能。有关 Context 的详细介绍请参见“虚拟化技术配置指导”中的“Context”。

1.3 应用层检测引擎配置任务简介

表1-1 应用层检测引擎配置任务简介

配置任务	说明	详细配置
配置DPI应用Profile	必选	1.4.1
激活DPI各业务模块的策略配置	必选	1.4.2
配置应用层检测引擎动作参数	可选	1.4.3
优化应用层检测引擎性能	可选	1.4.4
关闭应用层检测引擎功能	可选	1.4.5
关闭应用层检测引擎CPU门限响应功能	可选	1.4.6
配置应用层检测引擎检测固定长度数据流功能	可选	1.4.7

1.4 配置应层检测引擎

1.4.1 配置DPI应用Profile

DPI 应用 Profile 是一个 DPI 业务的配置模板，用于关联各 DPI 业务的策略（例如 IPS 策略、内容过滤策略、URL 过滤策略）。当 DPI 应用 profile 被应用于对象策略之后，应用层检测引擎和 DPI 业务将会对引用该对象策略的安全域间实例上的报文进行检测和控制。

表1-2 配置 DPI 应用 Profile

操作	命令	说明
进入系统视图	**system-view**	-
创建DPI应用profile视图，并进入DPI应用profile视图	**app-profile** *profile-name*	缺省情况下，不存在DPI应用profile
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”
在DPI应用profile下引用数据过滤策略	**data-filter apply policy** *policyname*	关于该命令的详细介绍请参见“DPI深度安全命令参考”中的“数据过滤”
在DPI应用profile下引用文件过滤策略	**file-filter apply policy** *policyname*	关于该命令的详细介绍请参见“DPI深度安全命令参考”中的“文件过滤”
在DPI应用profile下引用防病毒策略	**anti-virus apply policy** *policyname*	关于该命令的详细介绍请参见“DPI深度安全命令参考”中的“防病毒”

1.4.2 激活DPI各业务模块的策略配置

当 DPI 各业务模块（比如 IPS 和 URL 过滤等特性）的策略被创建、修改和删除后，需要执行 **inspect activate** 命令来使其策略配置生效。

当 DPI 各业务模块的策略被创建、修改和删除且保存配置的情况下，设备重启之后，其相关的所有策略配置也会生效。

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 各业务模块的策略后统一执行此命令。

表1-3 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.4.3 配置应用层检测引擎动作参数

1. 配置阻断动作参数

阻断动作参数 profile 用来为 DPI 业务模块的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。

如果设备上同时开启了黑名单功能，则报文的源 IP 地址被添加到 IP 黑名单后的老化时间为阻断动作参数 profile 中配置的阻断时长。报文的源 IP 地址被加入 IP 黑名单后，阻断时长之内，后续来自该源 IP 地址的报文将被丢弃。

如果设备上未开启黑名单功能，报文仅会被阻断，但是报文的源 IP 地址不会被添加到 IP 黑名单。

将报文的源 IP 地址加入 IP 黑名单功能的实现需要执行 **blacklist enable** 或 **blacklist global enable** 命令，有关此命令的详细介绍请参见“安全命令参考”中的“攻击检测与防范”。

表1-4 配置阻断动作参数

操作	命令	说明
进入系统视图	**system-view**	-
创建应用层检测引擎的阻断动作参数profile，并进入该阻断动作参数profile视图	**inspect block-source parameter-profile** *parameter-name*	缺省情况下，不存在应用层检测引擎的阻断动作参数profile
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

2. 配置捕获动作参数

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，当缓存的报文字节数达到指定上限值时，系统会将缓存的报文上传到指定的 URL 上，并清空本地缓存，然后重新开始捕获报文。

每天指定的上传时间到达时，无论本地缓存是否达到最大值，系统都向指定的 URL 上传缓存的捕获报文。

表1-5 配置捕获动作参数

操作	命令	说明
进入系统视图	**system-view**	-
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*	缺省情况下，不存在应用层检测引擎的捕获动作参数profile
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字节
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
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

3. 配置日志动作参数

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 中可以配置日志保存的位置。

表1-6 配置日志动作参数

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
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*	缺省情况下，不存在应用层检测引擎的日志动作参数profile
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

4. 配置重定向动作参数

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。

表1-7 配置重定向动作参数

操作	命令	说明
进入系统视图	**system-view**	-
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*	缺省情况下，不存在应用层检测引擎的重定向动作参数profile
配置重定向URL	**redirect-url** *url-string*	缺省情况下，不存在重定向URL

5. 配置邮件动作参数

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。

表1-8 配置邮件动作参数

操作	命令	说明
进入系统视图	**system-view**	-
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*	缺省情况下，不存在应用层检测引擎的邮件动作参数profile
配置邮件服务器的地址	**email-server** *addr-string*	缺省情况下，不存在邮件服务器的地址
配置域名解析服务器的地址	**dns-server** *ip-address*	缺省情况下，不存在域名解析服务器的地址
配置发件人地址	**sender** *addr-string*	缺省情况下，不存在发件人地址
配置收件人地址	**receiver** *addr-string*	缺省情况下，不存在收件人地址
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。
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
配置登录邮件服务器的用户名	**username** *name-string*	缺省情况下，不存在登录邮件服务器的用户名

操作	命令	说明
配置登录邮件服务器的密码	**password** *pwd-string*	缺省情况下，不存在登录邮件服务器的密码

1.4.4 优化应用层检测引擎性能

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。应用层检测引擎的性能优化功能都开启或参数调高后，其对报文应用层信息的识别能力和准确率都会有所提高，但是也会消耗一定的系统资源。管理员可以根据具体的应用场景定制对报文最优的检测性能。

表1-9 优化应用层检测引擎性能

操作	命令	说明
进入系统视图	**system-view**	-
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
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
开启TCP报文序号排序和分节重组功能	**inspect tcp-reassemble enable**	缺省情况下，TCP报文序号排序和分节重组功能处于关闭状态
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均处于关闭状态

1.4.5 关闭应用层检测引擎功能

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，可通过关闭功能来保证设备的正常运行。

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。

表1-10 关闭应用层检测引擎功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.6 开启应用层检测引擎CPU门限响应功能

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 利用率低于配置的 CPU 利用率阈值或恢复到 CPU 利用率恢复阈值时，系统对整条数据流的内容进行检

测。当 CPU 利用率达到设备上配置的 CPU 利用率阈值时，系统触发 CPU 门限响应功能，系统会根据如下情况对数据流做出不同的处理：

- 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，超出固定长度后的的数据不再进行检测。
- 若应用层检测引擎 CPU 门限响应功能处于关闭状态，则系统仍然对整条数据流的内容进行检测。

在系统 CPU 占用率较高的情况下，不建议用户关闭此功能。

表1-11 开启应用层检测引擎 CPU 门限响应功能

操作	命令	说明
进入系统视图	**system-view**	-
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

1.4.7 配置应用层检测引擎检测固定长度数据流功能

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，超出固定长度后的的数据不再进行检测。当设备的 CPU 利用率未达到设备上配置的 CPU 利用率阈值时，应用层检测引擎检测整条数据流。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”。

开启应用层检测引擎 CPU 门限响应功能，此功能才会生效。

开启此功能后，在设备的 CPU 利用率达到设备上配置的 CPU 利用率阈值的情况下，应用层信息识别的成功率会降低，但设备的吞吐量性能会得到提升。

表1-12 配置应用层检测引擎检测固定长度数据流功能

操作	命令	说明
进入系统视图	**system-view**	-
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
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。

1.5 应用层检测引擎显示维护

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1-13 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

说明

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”。

1.1 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的优势

IPS 具有以下优势：

- 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特征

IPS 特征用来扫描网络中的攻击行为以及对攻击行为采取防御措施，设备通过将数据流与 IPS 特征进行比较来检测和防御攻击。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。预定义IPS特征的内容不能被创建、修改和删除，但是预定义IPS特征的动作属性和生效状态属性可以被修改。有关IPS动作的详细介绍请参见“1.1.3 IPS动作”。
- 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。需要注意的是，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。

1.1.3 IPS动作

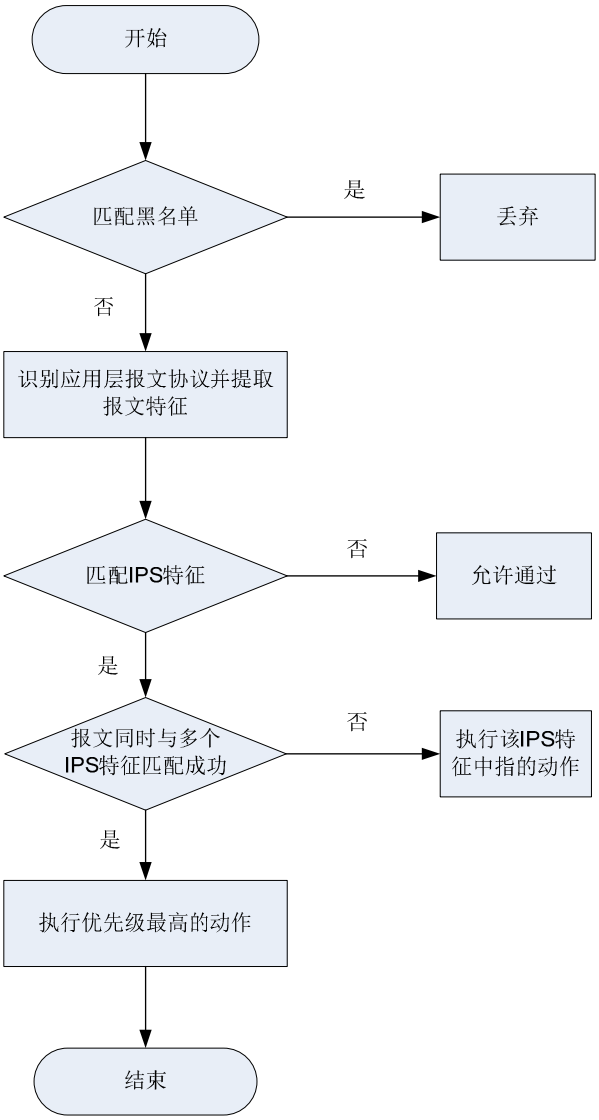
IPS 动作是指设备对匹配上 IPS 特征的报文做出的处理。IPS 处理动作包括如下几种类型：

- 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，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。

1.1.4 IPS实现流程

在设备配置了IPS功能的情况下，当用户的数据流量经过设备时，设备将进行IPS处理。处理流程如图 1-1 所示：

图1-1 IPS 数据处理流程图



IPS 处理的整体流程如下：

(1) 如果报文与 IP 黑名单匹配成功，则直接丢弃该报文。

(2) 如果报文匹配了某对象策略规则，且此对象策略规则的动作是 **inspect**，则设备将对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，并对匹配成功的报文进行如下处理：

- 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。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。动作优先级从高到低的顺序为：重置 > 重定向 > (源阻断/丢弃) > 允许，其中源阻断与丢弃的优先级相同。
- 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。

- 如果报文未与任何 IPS 特征匹配成功，则设备对报文执行允许动作。

1.1.5 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配置任务简介

表1-1 IPS 配置任务简介

配置任务	说明	详细配置
配置IPS策略	必选	1.3.1
指定IPS引用的应用层检测引擎动作参数profile	可选	1.3.2
在DPI应用profile下引用IPS策略	必选	1.3.3
导入自定义IPS特征	可选	1.3.4
在对象策略规则中引用DPI应用profile	必选	1.3.5
在安全域间实例中引用对象策略	必选	1.3.6
配置IPS特征库升级和回滚	可选	1.3.7
激活DPI各业务模块的策略配置	可选	1.3.8

1.3 配置IPS

1.3.1 配置IPS策略

管理员可以根据实际的网络需求，通过配置 IPS 策略修改已有 IPS 特征的动作属性和生效状态属性。设备上的所有 IPS 策略均使用当前系统中的所有 IPS 特征。

表1-2 配置 IPS 策略

操作	命令	说明
进入系统视图	**system-view**	-
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，且不能被修改和删除
修改IPS特征的状态和动作	**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

1.3.2 配置IPS引用的应用层检测引擎动作参数profile

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。

表1-3 配置 IPS 引用的应用层检测引擎动作参数 profile

操作	命令	说明
进入系统视图	**system-view**	-
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

1.3.3 在DPI应用profile中引用IPS策略

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。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。

表1-4 在 DPI 应用 profile 中引用 IPS 策略

操作	命令	说明
进入系统视图	**system-view**	-
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”

操作	命令	说明
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

1.3.4 导入自定义IPS特征

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。

需要注意的是，Snort 文件需要遵循 Snort 公司的语法。

表1-5 导入自定义 IPS 特征

操作	命令	说明
进入系统视图	**system-view**	-
导入自定义IPS特征	**ips signature import snort** *file-path*	缺省情况下，不存在自定义IPS特征

1.3.5 在对象策略规则中引用DPI应用profile

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”。

1. 在IPv4 对象策略中引用DPI应用profile

表1-6 在 IPv4 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv4对象策略	**object-policy ip** *object-policy-name*	-
在IPv4对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass** | **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv4对象策略规则中未引用DPI应用profile

2. 在IPv6 对象策略中引用DPI应用profile

表1-7 在 IPv6 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv6对象策略	**object-policy ipv6** *object-policy-name*	-
在IPv6对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv6对象策略规则中未引用DPI应用profile

1.3.6 在安全域间实例中引用对象策略

有关此功能的详细介绍请参见“安全配置指导”中的“对象策略”。

表1-8 安全域间实例引用对象策略

操作		命令	说明
进入系统视图		**system-view**	-
进入Context系统视图		**switchto context** *context-name*	仅对Context必选
创建源安全域和目的安全域		**security-zone name** *zone-name*	缺省情况下，当首次执行创建安全域的命令时，系统会自动创建以下缺省安全域：Local、Trust、DMZ、Management和Untrust
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*	缺省情况下，不存在安全域间实例
应用对象策略	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用对象策略 二者至少选其一
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

1.3.7 配置IPS特征库升级和回滚

注意

- 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”。

随着网络攻击的不断变化和发展，管理员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. 配置定期自动在线升级IPS特征库

如果设备能访问外网，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。

表1-9 配置定期自动在线升级 IPS 特征库

操作	命令	说明
进入系统视图	**system-view**	-
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
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
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特征库时备份当前的特征库文件

2. 立即自动在线升级IPS特征库

表1-10 立即自动在线升级 IPS 特征库

操作	命令	说明
进入系统视图	**system-view**	-
立即自动在线升级IPS特征库	**ips signature auto-update-now**	-

3. 手动离线升级IPS特征库

如果设备不能访问外网，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。
  - 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。（集中式IRF设备）
  - 特征库文件只能存储在当前主控板上，否则设备升级特征库会失败。（分布式设备-独立运行模式）

- 特征库文件只能存储在当前全局主用主控板上，否则设备升级特征库会失败。（分布式设备-IRF 模式）

- 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。

表1-11 手动离线升级 IPS 特征库

操作	命令	说明
进入系统视图	**system-view**	-
手动离线升级IPS特征库	**ips signature update** [**override-current**] *file-path*	-

4. 回滚IPS特征库

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。

表1-12 回滚 IPS 特征库

操作	命令	说明
进入系统视图	**system-view**	-
回滚IPS特征库	**ips signature rollback** { **factory** | **last** }	-

1.3.8 激活DPI各业务模块的策略配置

当 DPI 各业务模块的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

配置此功能会暂时中断 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”。

表1-13 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.4 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1-14 IPS 显示和维护

操作	命令
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特征库版本信息	**display ips signature information**
显示IPS策略信息	**display ips policy** *policy-name*

1.5 IPS典型配置举例

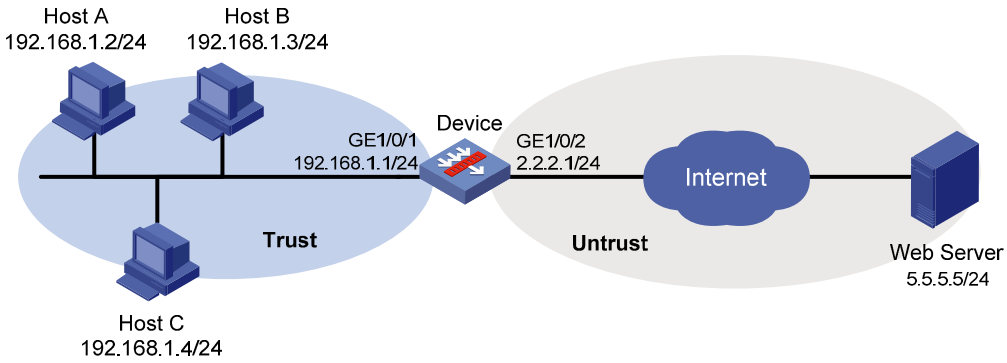
1.5.1 应用缺省IPS策略的典型配置举例

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 应用缺省 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
```

- 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
```

(3) 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
```

(4) 配置对象策略

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
```

(5) 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
```

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

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。

1.5.2 应用自定义IPS策略的典型配置举例

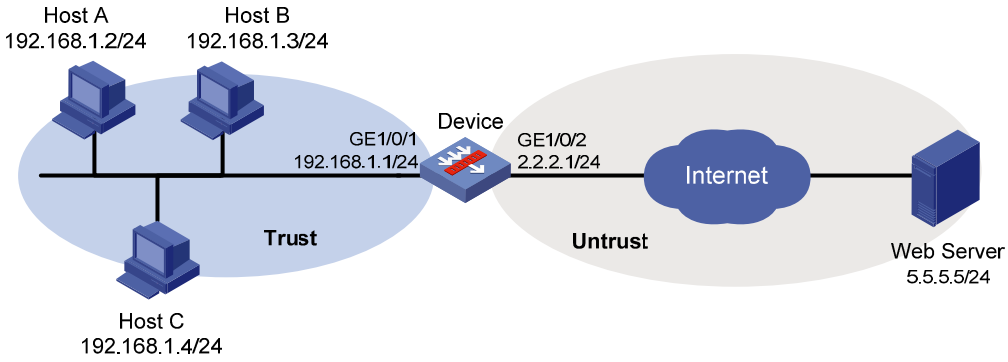
1. 组网需求

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 应用自定义 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 功能

创建一个名称为 ips1 的 IPS 策略，并进入 IPS 策略视图。

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

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
```

(6) 配置对象策略

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

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
```

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

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。

1.5.3 手动离线升级IPS特征库典型配置举例

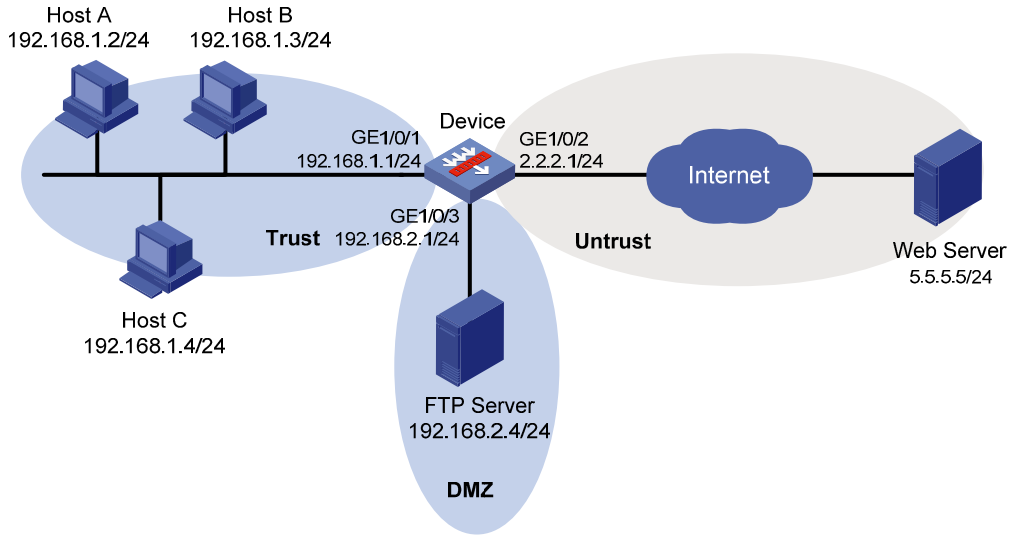
1. 组网需求

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。现有组网需求如下：

- 手动离线升级 IPS 特征库，加载最新的 IPS 特征。
- 使用设备上的缺省 IPS 策略对常见的网络攻击进行防御。

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 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) 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] 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
```

(4) 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
```

(5) 配置 IPS 功能

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
```

(6) 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
```

(7) 配置对象策略

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
```

(8) 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
```

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

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。

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。

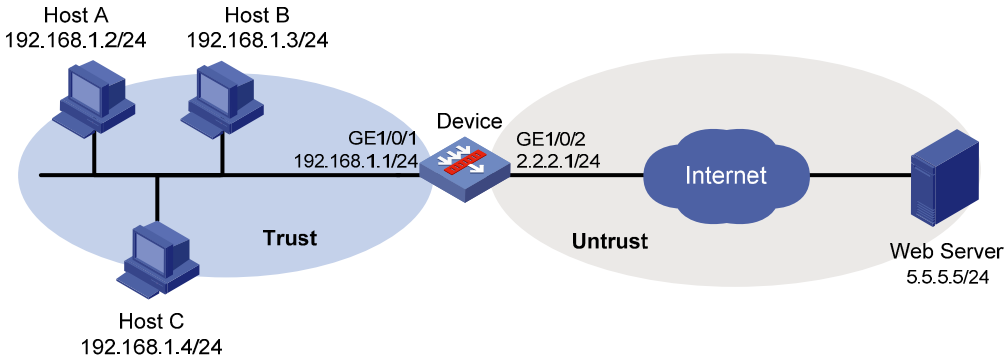
1.5.4 定时自动升级IPS特征库典型配置举例

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 30 分钟。

```
[Device-ips-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 30
[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 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。

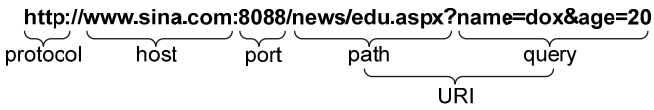
目前，仅支持对基于 HTTP 协议的 URL 进行过滤。

1.1.1 URL过滤原理

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

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。

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。

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 字段进行精确匹配。

匹配主机名字段时，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。例如，规则中配置主机名字符串为 abc.com.cn，则主机名为 abc.com.cn 的 URL 会匹配成功，而主机名为 dfabc.com.cn 的 URL 将与该规则匹配失败。

匹配 URI 字段时，从 URL 中 URI 字段的首字符开始，只要 URI 字段中连续若干个字符与规则中指定的 URI 字符串完全一致，就算匹配成功。例如，规则中配置 URI 字符串为/sina/news，则 URI 为/sina/news、/sina/news/sports 或/sina/news_sports 的 URL 会匹配成功，而 URI 为/sina 的 URL 将与该规则匹配失败。

正则表达式匹配：使用正则表达式对主机名和 URI 字段进行模糊匹配。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。

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，其内容和严重级别不可被修改。

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。

4. URL过滤策略

URL 过滤策略是用于关联所有 URL 过滤配置的一个实体。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。

5. URL过滤黑/白名单规则

URL 过滤黑/白名单规则功能根据应用层的信息进行 URL 过滤。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。

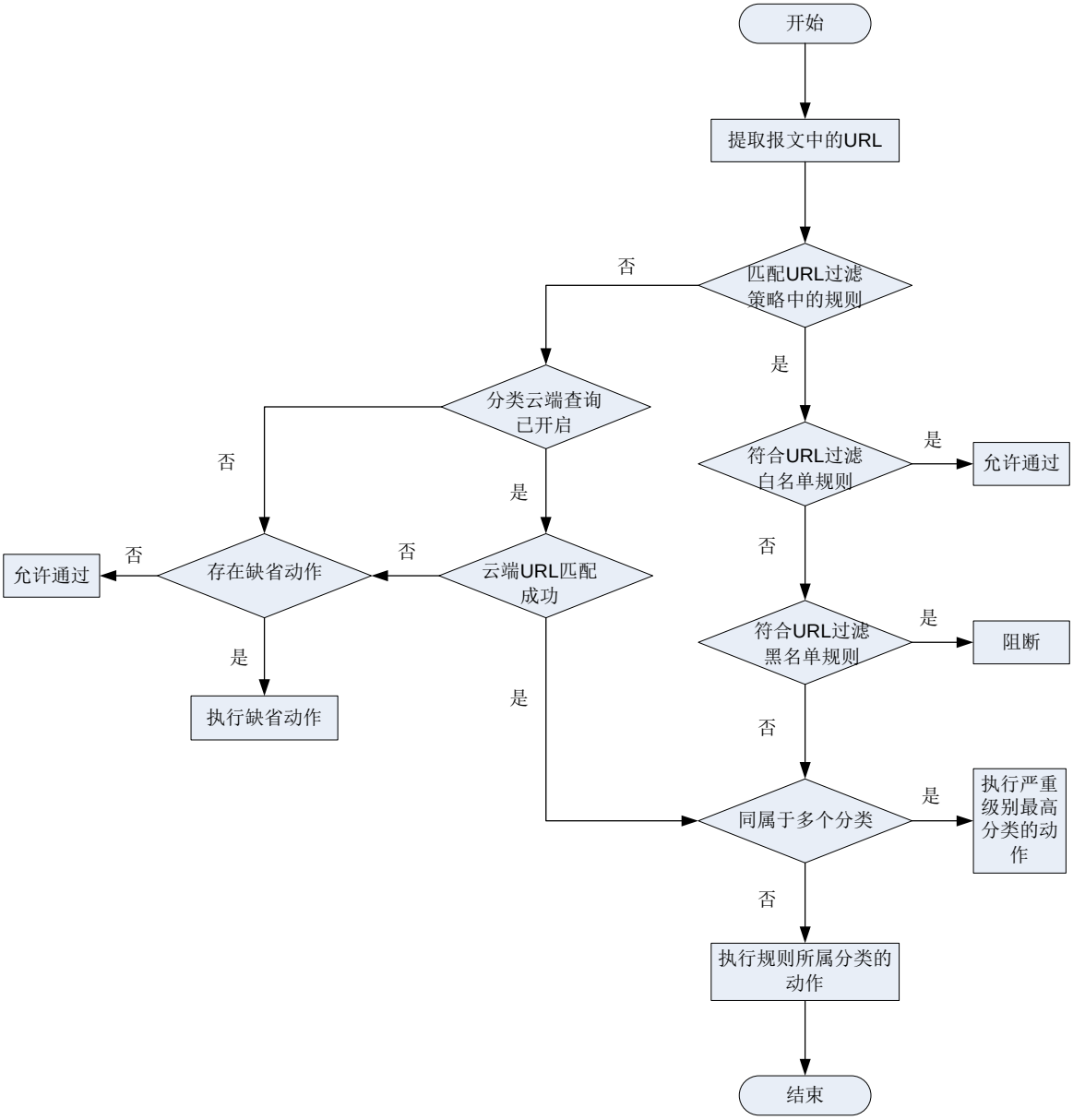
6. URL过滤分类云端查询

在 URL 过滤策略中开启 URL 过滤分类云端查询功能后，如果流经设备 HTTP 报文中的 URL 与该 URL 过滤策略中的过滤规则匹配失败，则此 URL 将会被发向云端 URL 过滤分类服务器进行查询。云端 URL 过滤分类服务器响应该请求，并向设备发送查询结果，该结果中包含 URL 过滤规则及其所属的分类名称，设备会根据该结果执行相应的分类处理动作。如果云端返回的分类在设备上没有与其对应的分类动作或者云端 URL 查询失败，则设备将对此报文执行 URL 过滤策略中的缺省动作。

1.1.2 URL过滤实现流程

在开启URL过滤功能的情况下，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 过滤实现流程如下：

(2) 如果报文匹配了某对象策略规则，且此对象策略规则应用的 DPI 应用 profile 中关联了 URL 过滤策略，则设备提取报文中的URL字段进行URL过滤规则匹配。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) 如果报文与设备上 URL 过滤策略中的过滤规则匹配成功，则将进一步做如下判断：

(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) 如果报文未匹配上任何一条URL过滤策略中的过滤规则，则将进一步判断URL过滤策略中是否开启了 URL 过滤分类云端查询功能。如果分类云端查询功能已开启，则将报文中的 URL 发向云端 URL 过滤分类服务器进行查询，否则进行第 7 步的判断

(7) 如果 URL 云端查询成功，则进行步骤 4 的判断，否则进行步骤 7 的判断。

(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。

1.1.3 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过滤配置任务简介

表1-2 URL 过滤配置任务简介

配置任务	说明	详细配置
配置URL过滤分类	必选	1.3.1
配置URL过滤分类云端查询	可选	1.3.2
配置URL过滤策略	必选	1.3.3
复制URL过滤策略或分类	可选	1.3.4
在DPI应用profile中引用URL过滤策略	必选	1.3.5
在对象策略规则中引用DPI应用profile	必选	1.3.6
在安全域间实例中引用对象策略	必选	1.3.7
配置URL过滤特征库升级和回滚	可选	1.3.8
激活DPI各业务模块的策略配置	可选	1.3.9
开启URL过滤日志信息功能	可选	1.3.10

1.3 配置URL过滤

1.3.1 配置URL过滤分类

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。每个 URL 过滤规则可以同时属于多个 URL 过滤分类。

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。

系统为预定义 URL 过滤分类保留的严重级别为最低，取值范围为 1～999。

表1-3 配置 URL 过滤分类

操作	命令	说明
进入系统视图	**system-view**	-
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
（可选）配置URL过滤分类的描述信息	**description** *text*	缺省情况下，自定义的URL过滤分类中不存在描述信息
配置自定义URL过滤规则	**rule** *rule-id* **host** { **regex** *regex* | **text** *string* } [**uri** { **regex** *regex* | **text** *string* }]	缺省情况下，URL过滤分类中不存在自定义URL过滤规则
（可选）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
（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*	-

1.3.2 配置URL过滤分类云端查询

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 URL 过滤分类服务器学习到的 URL 过滤规则会被缓存在设备上，并在一定时间间隔内下发给应用层检测引擎进行报文匹配。URL 过滤缓存的记录上限、规则的最短保留时间和下发时间间隔都可以根据实际组网环境进行调整。

表1-4 配置 URL 过滤分类云端查询

操作	命令	说明
进入系统视图	**system-view**	-
配置云端URL过滤分类服务器的主机名	**url-filter category-server** *host-name*	缺省情况下，不存在URL过滤分类服务器地址

操作	命令	说明
（可选）配置向应用层检测引擎下发缓存中规则的时间间隔	**url-filter cache deploy-interval** *interval*	缺省情况下，URL过滤缓存规则下发应用层检测引擎的刷新时间间隔为12小时
（可选）配置URL过滤分类缓存区可缓存记录的上限	**url-filter cache size** *cache-size*	缺省情况下，URL过滤分类学习缓存区可缓存记录的上限根据设备内存的实际大小由系统计算得出
（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43200秒
进入URL过滤策略视图	**url-filter policy** *policy-name*	-
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

1.3.3 配置URL过滤策略

在一个 URL 过滤策略中可以配置多个 URL 过滤分类动作，也可以在 URL 过滤策略中为其定义缺省动作。

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。

表1-5 配置 URL 过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
创建URL过滤策略，并进入URL过滤策略视图	**url-filter policy** *policy-name*	缺省情况下，不存在URL过滤策略
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**]	缺省情况下，不存在URL过滤分类动作
（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**]	缺省情况下，不存在缺省动作
（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* }]	缺省情况下，不存在黑/白名单规则
（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*	-

1.3.4 复制URL过滤策略或分类

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

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。

表1-6 复制 URL 过滤策略或分类

操作	命令	说明
进入系统视图	**system-view**	-
复制URL过滤分类	**url-filter copy category** *old-name* [*new-name*] **severity** *severity-level*	-
复制URL过滤策略	**url-filter copy policy** *old-name new-name*	-

1.3.5 在DPI应用profile中引用URL过滤策略

DPI 应用 porfile 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。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。

表1-7 在 DPI 应用 profile 下引用 URL 过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
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”
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

1.3.6 在对象策略规则中引用DPI应用profile

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”。

1. 在IPv4 对象策略中引用DPI应用profile

表1-8 在 IPv4 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv4对象策略	**object-policy ip** *object-policy-name*	-
在IPv4对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass** | **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv4对象策略规则中未引用DPI应用profile

2. 在IPv6 对象策略中引用DPI应用profile

表1-9 在 IPv6 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv6对象策略	**object-policy ipv6** *object-policy-name*	-
在IPv6对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv6对象策略规则中未引用DPI应用profile

1.3.7 在安全域间实例中引用对象策略

有关此功能的详细介绍请参见“安全配置指导”中的“对象策略”。

表1-10 安全域间实例引用对象策略

操作		命令	说明
进入系统视图		**system-view**	-
进入Context系统视图		**switchto context** *context-name*	仅对Context必选
创建源安全域和目的安全域		**security-zone name** *zone-name*	缺省情况下，当首次执行创建安全域的命令时，系统会自动创建以下缺省安全域：Local、Trust、DMZ、Management和Untrust
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*	缺省情况下，不存在安全域间实例
应用对象策略	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用对象策略 二者至少选其一
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

1.3.8 配置URL过滤特征库升级和回滚

注意

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”。

随着互联网业务的不断变化和发展，管理员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. 配置定期自动在线升级URL过滤特征库

如果设备能访问外网，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。

表1-11 配置定期自动在线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
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
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

2. 立即自动在线升级URL过滤特征库

表1-12 立即自动在线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
立即自动在线升级URL过滤特征库	**url-filter signature auto-update-now**	-

3. 手动离线升级URL过滤特征库

如果设备不能访问外网，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。

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。（集中式 IRF 设备）

特征库文件只能存储在当前主控板上，否则设备升级特征库会失败。（分布式设备-独立运行模式）

特征库文件只能存储在当前全局主用主控板上，否则设备升级特征库会失败。（分布式设备-IRF 模式）

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。

表1-13 手动离线升级 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
手动离线升级URL过滤特征库	**url-filter signature update** *file-path*	-

4. 回滚URL过滤特征库

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。

表1-14 回滚 URL 过滤特征库

操作	命令	说明
进入系统视图	**system-view**	-
回滚URL过滤特征库	**url-filter signature rollback** { **factory** | **last** }	-

1.3.9 激活DPI各业务模块的策略配置

当 DPI 各业务模块的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

配置此功能会暂时中断 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”。

表1-15 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.3.10 开启应用层检测引擎日志信息功能

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”。

表1-16 开启应用层检测引擎日志信息功能

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
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

1.4 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1-17 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** [**existence** { **eq** | **lt** | **gt** } *existence-time*] | [**category** *category-name*] | [**hitcount** { **eq** | **lt** | **gt** } *hitnumber*]
显示URL过滤分类信息	**display url-filter 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**

1.5 URL典型配置举例

1.5.1 URL过滤分类典型配置举例

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：

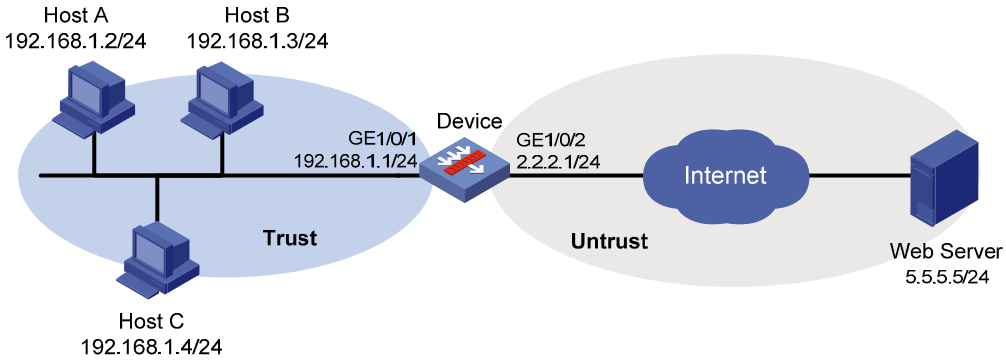
配置 URL 过滤功能，允许 Trust 安全域的主机访问 Untrust 安全域的 Web Server 上的 www.sina.com。

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 URL 过滤分类配置组网图



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
```

(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
```

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

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。

1.5.2 手动离线升级URL过滤特征库典型配置举例

1. 组网需求

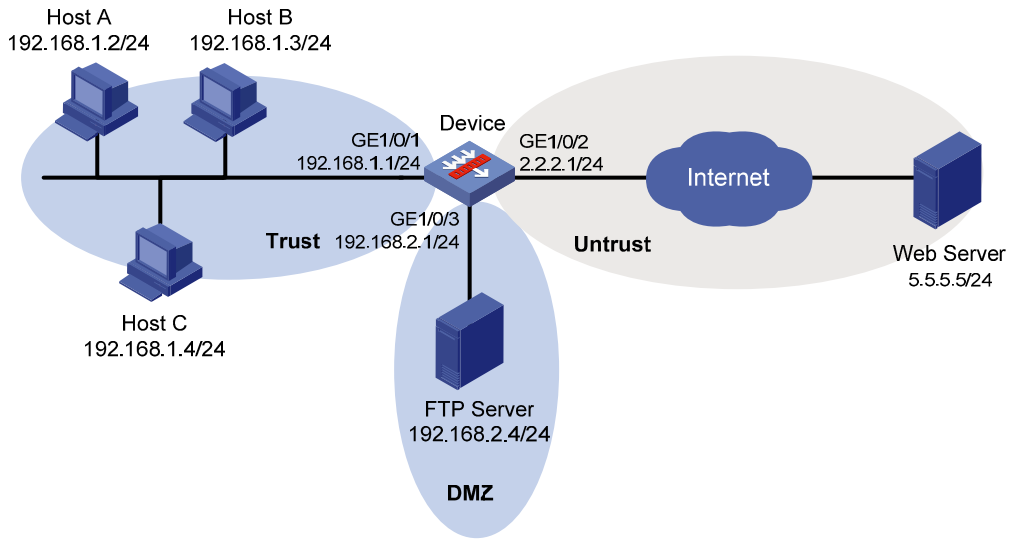
如 图 1-4 所示，位于Trust安全域的局域网用户通过Device可以访问Untrust安全域的Internet资源，以及DMZ安全域的FTP服务器。FTP服务器根目录下保存了最新的URL过滤特征库文件url-1.0.2-encrypt.dat，FTP服务器的登录用户名和密码分别为url和 123。现有组网需求如下：

手动离线升级 URL 过滤特征库，加载最新的 URL 过滤分类。

采用预定义的 URL 过滤分类 Pre-Games，禁止 Trust 安全域的主机访问 Untrust 安全域内关于游戏类的互联网 Web 资源。

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) 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] 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
```

(4) 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
```

(5) 配置 URL 过滤功能

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
```

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，配置预定义 URL 过滤分类 Pre-Games 绑定的动作为丢弃并且生成日志。

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

(6) 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
```

(7) 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
```

(8) 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
```

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

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 都无法访问 Untrust 安全域内的游戏类的互联网 Web 资源。尝试访问 Untrust 安全域内的游戏类的互联网 Web 资源 URL 请求将会被 Device 阻断并且记录日志。日志形式。

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。

1.5.3 定期自动在线升级URL过滤特征库典型配置举例

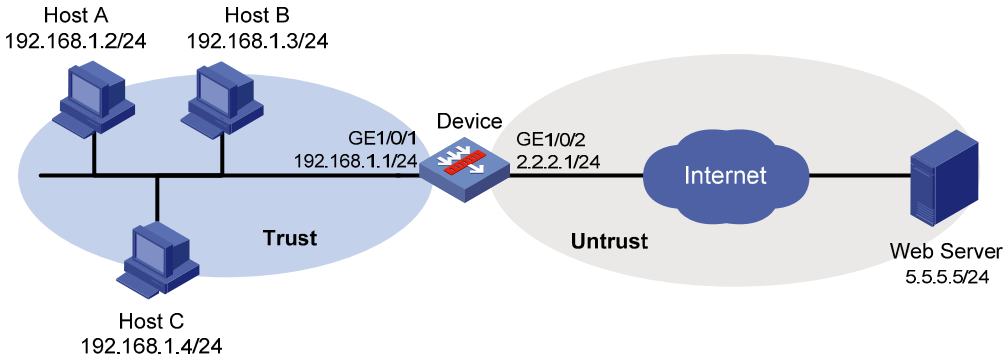
1. 组网需求

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 30 分钟。

```
[Device-url-filter-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 30
[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 数据过滤

1.1 数据过滤简介

数据过滤是一种对流经设备的报文的应用层信息进行过滤的安全防护机制。采用数据过滤功能可以有效防止内网机密信息泄露，禁止内网用户在 Internet 上浏览、发布和传播违规或违法信息。目前，数据过滤功能支持对基于以下应用层协议传输的应用层信息进行检测和过滤。

- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- FTP（File Transfer Protocol，文件传输协议）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

1.1.1 基本概念

1. 数据过滤特征

数据过滤特征是设备上定义的用于识别应层信息特征的字符串。

2. 关键字组

关键字组用来对数据过滤特征进行统一组织和管理。一个关键字组中可以包含 32 个特征，且它们之间是或的关系。

3. 数据过滤规则

数据过滤规则是报文应用层信息安全检测条件及处理动作的集合。在一个规则中可设置关键字组、报文方向、应用类型和动作（丢弃、放行、生成日志）。只有报文成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

1.1.2 数据过滤的实现原理

设备对报文进行数据过滤处理的整体流程如下：

(1) 当设备收到 HTTP、FTP、SMTP 报文时，首先在报文所属的安全域间实例中进行安全策略检查，如果安全域间实例下的某对象策略规则中关联了 DPI 应用 profile，且该 profile 中引用了数据过滤策略，则对报文进行数据过滤处理。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”。

(2) 设备提取报文中的应用层信息与数据过滤规则进行匹配，并根据匹配结果对报文执行动作：

- 如果报文同时与多个规则匹配成功，则执行这些规则中优先级最高的动作，动作优先级从高到低的顺序为：丢弃 > 放行，但是对于生成日志动作只要匹配成功的规则中存在就会执行。
- 如果报文只与一个规则匹配成功，则执行此规则中指定的动作。
- 如果报文未与任何数据过滤规则匹配成功，则设备直接允许报文通过。

1.2 数据过滤配置任务简介

表1-1 数据过滤配置任务简介

配置任务	说明	详细配置
配置关键字组	必选	1.2.2
配置数据过滤策略	必选	1.2.3
在DPI应用profile中应用数据过滤策略	必选	1.2.4
在对象策略规则中引用DPI应用profile	必选	1.2.5
在安全域间实例中引用对象策略	必选	1.2.6
激活DPI各业务模块的策略配置	可选	1.2.7

1.2.2 配置关键字组

一个关键字组中可配置多个数据过滤特征用于定义过滤报文应用层信息的字符串，各特征之间是或的关系。定义数据过滤特征的方式为正则表达式和文本两种。

表1-2 配置关键字组

操作	命令	说明
进入系统视图	**system-view**	-
创建关键字组，并进入关键字组视图	**data-filter keyword-group** *keywordgroup-name*	缺省情况下，不存在关键字组
配置关键字组的描述信息	**description** *string*	缺省情况下，不存在关键字组的描述信息
配置数据过滤特征	**pattern** *pattern-name* { **regex** | **text** } *pattern-string*	缺省情况下，关键字组中不存在数据过滤特征

1.2.3 配置数据过滤策略

一个数据过滤策略中最多可以定义 32 个数据过滤规则，各规则之间是或的关系。每个规则中可配置一个关键字组、多种应用层协议类型、一种报文方向以及多个动作。

表1-3 配置数据过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
创建数据过滤策略，并进入数据过滤策略视图	**data-filter policy** *policy-name*	缺省情况下，不存在数据过滤策略
配置数据过滤策略的描述信息	**description** *string*	缺省情况下，不存在数据过滤策略的描述信息

操作	命令	说明
创建数据过滤规则，并进入数据过滤规则视图	**rule** *rule-name*	缺省情况下，不存在数据过滤规则
指定数据过滤规则采用的关键字组	**keyword-group** *keywordgroup-name*	缺省情况下，未指定数据过滤规则采用的关键字组
配置数据过滤规则的应用层协议类型	**application** { **all** | **type** { **ftp** | **http** | **smtp** } * }	缺省情况下，数据过滤规则未指定应用层协议类型
配置数据过滤规则的匹配方向	**direction** { **both** | **download** | **upload** }	缺省情况下，数据过滤规则的匹配方向为会话的上传方向
配置数据过滤规则的动作	**action** { **drop** | **permit** } [**logging**]	缺省情况下，数据过滤规则的动作为丢弃

1.2.4 在DPI应用profile中引用数据过滤策略

DPI 应用 porfile 是一个安全业务的配置模板，为实现数据过滤功能，必须在 DPI 应用 porfile 中引用指定的数据过滤策略。一个 DPI 应用 profile 中只能引用一个数据过滤策略，如果重复配置，则新的配置会覆盖已有配置。

表1-4 在 DPI 应用 profile 中引用数据过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
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”
在DPI应用profile中引用数据过滤策略	**data-filter apply policy** *policy-name*	缺省情况下，DPI应用profile中未引用数据过滤策略

1.2.5 在对象策略规则中引用DPI应用profile

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”。

1. 在IPv4 对象策略中引用DPI应用profile

表1-5 在 IPv4 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入IPv4对象策略	**object-policy ip** *object-policy-name*	-

操作	命令	说明
在IPv4对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass** | **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，IPv4对象策略规则中未引用DPI应用profile

2. 在IPv6 对象策略中引用DPI应用profile

表1-6 在 IPv6 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入IPv6对象策略	**object-policy ipv6** *object-policy-name*	-
在IPv6对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，IPv6对象策略规则中未引用DPI应用profile

1.2.6 在安全域间实例中引用对象策略

有关此功能的详细介绍请参见“安全配置指导”中的“对象策略”。

表1-7 安全域间实例引用对象策略

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
创建源安全域和目的安全域	**security-zone name** *zone-name*	缺省情况下，当首次执行创建安全域的命令时，系统会自动创建以下缺省安全域：Local、Trust、DMZ、Management和Untrust
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*	缺省情况下，不存在安全域间实例

操作		命令	说明
应用对象策略	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用对象策略 二者至少选其一
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

1.2.7 激活DPI各业务模块的策略配置

当 DPI 各业务模块的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

配置此功能会暂时中断 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”。

表1-8 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.3 数据过滤典型配置举例

1.3.1 数据过滤典型配置举例

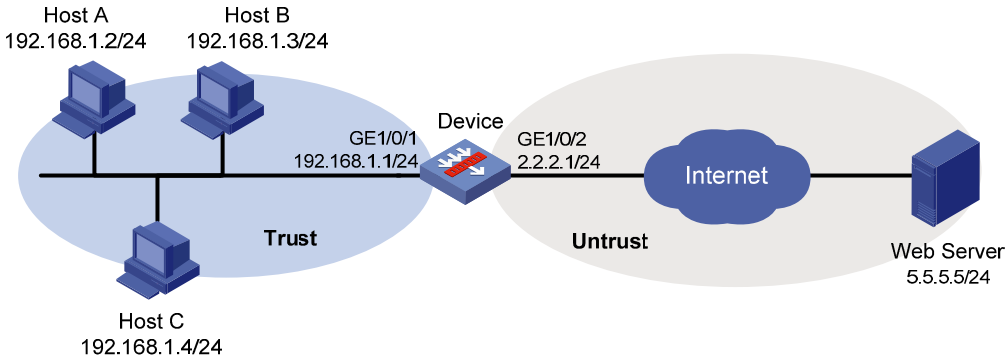
1. 组网需求

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

- 阻止 URI 或者 Body 字段含有“uri”或“abc.*abc”关键字的 HTTP 报文通过。
- 阻止下载文件内容中含有“www.abcd.com”关键字的 FTP 报文通过。
- 对以上被阻止的报文生成日志信息。

2. 组网图

图1-1 数据过滤配置组网图



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 datafilter 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 datafilter
[Device-obj-grp-ip-datafilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-datafilter] quit
```

(4) 配置数据过滤功能

- 配置关键字组

创建关键字组 kg1，并进入关键字组视图。

```
[Device] data-filter keyword-group kg1
```

配置关键字 uri 和正则表示式 abc.*abc。

```
[Device-data-filter-kgroup-kg1] pattern 1 text uri
[Device-data-filter-kgroup-kg1] pattern 2 regex abc.*abc
[Device-data-filter-kgroup-kg1] quit
```

创建关键字组 kg2，并进入关键字组视图。

```
[Device] data-filter keyword-group kg2
```

配置匹配关键字 www.abcd.com。

```
[Device-data-filter-kgroup-kg2] pattern 1 text www.abcd.com
[Device-data-filter-kgroup-kg2] quit
```

- 配置数据过滤策略

创建数据过滤策略 p1，并进入数据过滤策略视图。

```
[Device] data-filter policy p1
```

创建数据过滤规则 r1，并进入数据过滤规则视图。

```
[Device-data-filter-policy-p1] rule r1
```

在规则 r1 中应用关键字组 kg1，配置应用类型为 HTTP，报文方向为会话的双向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r1] keyword-group kg1
[Device-data-filter-policy-p1-rule-r1] application type http
[Device-data-filter-policy-p1-rule-r1] direction both
[Device-data-filter-policy-p1-rule-r1] action drop logging
[Device-data-filter-policy-p1-rule-r1] quit
```

创建数据过滤规则 r2，并进入数据过滤策略视图。

```
[Device-data-filter-policy-p1] rule r2
```

在规则 r2 中应用关键字组 kg2，配置应用类型为 FTP，报文方向为会话的下载方向，动作为丢弃并输出日志。

```
[Device-data-filter-policy-p1-rule-r2] keyword-group kg2
[Device-data-filter-policy-p1-rule-r2] application type ftp
[Device-data-filter-policy-p1-rule-r2] direction download
[Device-data-filter-policy-p1-rule-r2] action drop logging
[Device-data-filter-policy-p1-rule-r2] quit
```

(5) 配置 DPI 应用 profile

创建名称为 profile1 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile profile1
```

在 DPI 应用 profile1 中应用数据过滤策略 p1。

```
[Device-app-profile-profile1] data-filter apply policy p1
[Device-app-profile-profile1] quit
```

(6) 配置对象策略

创建名为 inspect1 的对象策略，并进入对象策略视图。

```
[Device] object-policy ip inspect1
```

对源 IP 地址对象组 datafilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 profile1。

```
[Device-object-policy-ip-inspect1] rule inspect profile1 source-ip datafilter
destination-ip any
[Device-object-policy-ip-inspect1] 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 datafilter 对应的报文进行深度检测的对象策略 inspect1。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-trust-untrust] object-policy apply ip inspect1
[Device-zone-pair-security-trust-untrust] quit
```

(8) 激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

4. 验证配置

完成上述配置后，符合上述条件的 HTTP 报文和 FTP 报文将被阻断，并输出日志信息。

目 录

1 文件过滤

1.1 文件过滤简介

文件过滤是一种根据文件扩展名信息对经设备传输的文件进行过滤的安全防护机制。采用文件过滤功能可以对指定类型的文件进行批量过滤。目前，文件过滤功能支持对基于以下应用层协议传输的文件进行检测和过滤。

- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- FTP（File Transfer Protocol，文件传输协议）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

1.1.1 基本概念

1. 文件过滤特征

文件过滤特征是设备上定义的用于识别文件扩展名特征的字符串。

2. 文件类型组

文件类型组用来对文件过滤特征进行统一组织和管理。一个文件类型组中可以包含 32 个特征，且它们之间是或的关系。

3. 文件过滤规则

文件过滤规则是安全检测条件及处理动作的集合。在一个规则中可配置的检测条件包括文件类型组、报文方向、应用类型，可配置的处理动作包括丢弃、放行和生成日志。只有文件属性（包括文件的应用类型、传输方向和扩展名）成功匹配规则中包含的所有检测条件才算与此规则匹配成功。

1.1.2 文件过滤的实现原理

设备对报文进行文件过滤处理的整体流程如下：

(1) 当设备收到基于 HTTP、FTP、SMTP 协议传输的文件时，首先在文件所属的安全域间实例中进行安全策略检查，如果安全域间实例下的某对象策略规则中关联了 DPI 应用 profile，且该 profile 中引用了文件过滤策略，则对报文进行文件过滤处理。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”。

(2) 设备提取文件的扩展名信息与文件过滤规则进行匹配，并根据匹配结果对文件执行动作：

- 如果文件的扩展名信息同时与多个规则匹配成功，则执行这些规则中优先级最高的动作，动作优先级从高到低的顺序为：丢弃 > 放行，但是对于生成日志动作只要匹配成功的规则中存在就会执行。
- 如果文件的扩展名信息只与一个规则匹配成功，则执行此规则中指定的动作。
- 如果文件的扩展名信息未与任何文件过滤规则匹配成功，则设备直接允许文件通过。

1.2 文件过滤配置任务简介

表1-1 文件过滤配置任务简介

配置任务	说明	详细配置
配置文件类型组	必选	1.2.2
配置文件过滤策略	必选	1.2.3
在DPI应用profile中应用文件过滤策略	必选	1.2.4
在对象策略规则中引用DPI应用profile	必选	1.2.5
在安全域间实例中引用对象策略	必选	1.2.6
激活DPI各业务模块的策略配置	可选	1.2.7

1.2.2 配置文件类型组

一个文件类型组中可配置多个文件过滤特征，各特征之间是或的关系。定义文件过滤特征的方式为文本。

表1-2 配置文件类型组

操作	命令	说明
进入系统视图	**system-view**	-
创建文件类型组，并进入文件类型组视图	**file-filter filetype-group** *group-name*	缺省情况下，不存在文件类型组
配置文件类型组的描述信息	**description** *string*	缺省情况下，不存在文件类型组的描述信息
配置文件过滤特征	**pattern** *pattern-name* **text** *pattern-string*	缺省情况下，文件类型组中不存在文件过滤特征

1.2.3 配置文件过滤策略

一个文件过滤策略中最多可以定义 32 个文件过滤规则，各规则之间是或的关系。每个规则中可配置一个文件类型组、多种应用层协议类型、一种报文方向以及多个动作。

表1-3 配置文件过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
创建文件过滤策略，并进入文件过滤策略视图	**file-filter policy** *policy-name*	缺省情况下，不存在文件过滤策略
配置文件过滤策略的描述信息	**description** *string*	缺省情况下，不存在文件过滤策略的描述信息

操作	命令	说明
创建文件过滤规则，并进入文件过滤规则视图	**rule** *rule-name*	缺省情况下，不存在文件过滤规则
指定文件过滤规则采用的文件类型组	**filetype-group** *group-name*	缺省情况下，未指定文件过滤规则采用的文件类型组
配置文件过滤规则的应用层协议类型	**application** { **all** | **type** { **ftp** | **http** | **smtp** } * }	缺省情况下，文件过滤规则中未指定应用层协议类型
配置文件过滤规则的匹配方向	**direction** { **both** | **download** | **upload** }	缺省情况下，文件过滤规则的匹配方向为上传方向
配置文件过滤规则的动作	**action** { **drop** | **permit** } [**logging**]	缺省情况下，文件过滤规则的动作为丢弃

1.2.4 在DPI应用profile中引用文件过滤策略

DPI 应用 porfile 是一个安全业务的配置模板，为实现文件过滤功能，必须在 DPI 应用 porfile 中引用指定的文件过滤策略。一个 DPI 应用 profile 中只能引用一个文件过滤策略，如果重复配置，则新的配置会覆盖已有配置。

表1-4 在 DPI 应用 profile 中引用文件过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
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”
在DPI应用profile中引用文件过滤策略	**file-filter apply policy** *policy-name*	缺省情况下，DPI应用profile中未引用文件过滤策略

1.2.5 在对象策略规则中引用DPI应用profile

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”。

1. 在IPv4 对象策略中引用DPI应用profile

表1-5 在 IPv4 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入IPv4对象策略	**object-policy ip** *object-policy-name*	-

操作	命令	说明
在IPv4对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass** | **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，IPv4对象策略规则中未引用DPI应用profile

2. 在IPv6 对象策略中引用DPI应用profile

表1-6 在 IPv6 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入IPv6对象策略	**object-policy ipv6** *object-policy-name*	-
在IPv6对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，IPv6对象策略规则中未引用DPI应用profile

1.2.6 在安全域间实例中引用对象策略

有关此功能的详细介绍请参见“安全配置指导”中的“对象策略”。

表1-7 安全域间实例引用对象策略

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
创建源安全域和目的安全域	**security-zone name** *zone-name*	缺省情况下，当首次执行创建安全域的命令时，系统会自动创建以下缺省安全域：Local、Trust、DMZ、Management和Untrust
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*	缺省情况下，不存在安全域间实例

操作		命令	说明
应用对象策略	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用对象策略 二者至少选其一
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

1.2.7 激活DPI各业务模块的策略配置

当 DPI 各业务模块的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

配置此功能会暂时中断 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”。

表1-8 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.3 文件过滤典型配置举例

1.3.1 文件过滤典型配置举例

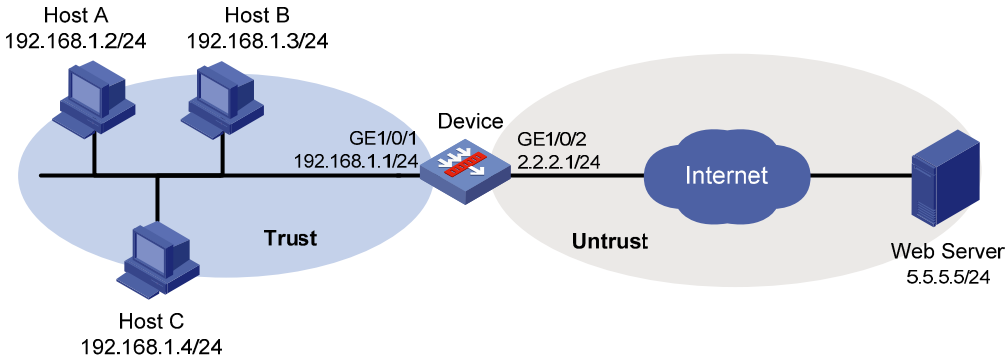
1. 组网需求

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

- 拒绝扩展名为 pptx 和 dotx 的文件通过。
- 对以上被阻止的文件生成日志信息。

2. 组网图

图1-1 文件过滤典型配置组网图



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 filefilter 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 filefilter
[Device-obj-grp-ip-filefilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-filefilter] quit
```

(4) 配置文件过滤功能

- 配置文件类型组

创建文件类型组 fg1，并进入文件类型组视图。

```
[Device] file-filter filetype-group fg1
```

配置文件过滤特征为 pptx 和 dotx。

```
[Device-file-filter-fgroup-fg1] pattern 1 text pptx
[Device-file-filter-fgroup-fg1] pattern 2 text dotx
[Device-file-filter-fgroup-fg1] quit
```

- 配置文件过滤策略

创建文件过滤策略 p1，并进入文件过滤策略视图。

```
[Device] file-filter policy p1
```

创建文件过滤规则 r1，并进入文件过滤规则视图。

```
[Device-file-filter-policy-p1] rule r1
```

在规则 r1 中应用文件类型组 fg1，配置应用类型为 HTTP，报文方向为会话的双向，动作为丢弃并输出日志。

```
[Device-file-filter-policy-p1-rule-r1] filetype-group fg1
[Device-file-filter-policy-p1-rule-r1] application type http
[Device-file-filter-policy-p1-rule-r1] direction both
[Device-file-filter-policy-p1-rule-r1] action drop logging
[Device-file-filter-policy-p1-rule-r1] quit
```

(5) 配置 DPI 应用 profile

创建名称为 profile1 的 DPI 应用 profile，并进入 DPI 应用 profile 视图。

```
[Device] app-profile profile1
```

在 DPI 应用 profile1 中应用文件过滤策略 p1。

```
[Device-app-profile-profile1] file-filter apply policy p1
[Device-app-profile-profile1] quit
```

(6) 配置对象策略

创建名为 inspect1 的对象策略，并进入对象策略视图。

```
[Device] object-policy ip inspect1
```

对源 IP 地址对象组 filefilter 对应的报文进行深度检测，引用的 DPI 应用 profile 为 profile1。

```
[Device-object-policy-ip-inspect1] rule inspect profile1 source-ip filefilter
destination-ip any
[Device-object-policy-ip-inspect1] 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 filefilter 对应的报文进行深度检测的对象策略 inspect1。

```
[Device] zone-pair security source trust destination untrust
[Device-zone-pair-security-trust-untrust] object-policy apply ip inspect1
[Device-zone-pair-security-trust-untrust] quit
```

(8) 激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

4. 验证配置

完成上述配置后，符合上述条件的文件将被丢弃，并输出日志信息。

目 录

1 防病毒

说明

对于本节命令中的 CPU 参数，仅 T5000-M06 产品支持。

说明

防病毒功能需要安装 License 才能使用。License 过期后，防病毒功能可以采用设备中已有的病毒特征库正常工作，但无法升级特征库。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.1 防病毒简介

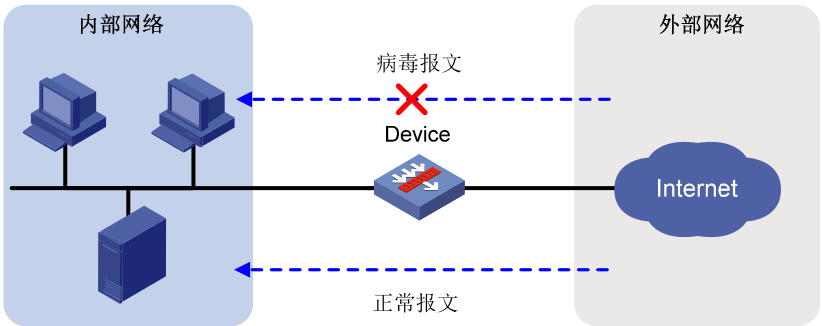
1.1.1 概述

防病毒功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。防病毒功能凭借庞大且不断更新的病毒特征库可有效保护网络安全，防止病毒在网络中的传播。将具有防病毒功能的设备部署在企业网入口，可以将病毒隔离在企业网之外，为企业内网的数据安全提供坚固的防御。目前，该功能支持对基于以下应用层协议传输的报文进行防病毒检测：

- FTP（File Transfer Protocol，文件传输协议）
- HTTP（Hypertext Transfer Protocol，超文本传输协议）
- IMAP（Internet Mail Access Protocol，Internet 邮件访问协议）
- POP3（Post Office Protocol-Version 3，邮局协议的第 3 个版本）
- SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）

1.1.2 应用场景

图1-1 防病毒典型应用场景



如 图 1-1 所示，在如下应用场景中，隔离内网和外网的网关设备上需要部署防病毒策略来保证内部网络安全：

- 内网用户需要访问外网资源，且经常需要从外网下载各种应用数据。
- 内网的服务器需要经常接收外网用户上传的数据。

当在设备上部署防病毒策略后，正常的用户数据可以进入内部网络，携带病毒的报文会被检测出来，并被采取阻断、重定向或生成告警信息等动作。

1.1.3 基本概念

1. 病毒特征

病毒特征是设备上定义的用于识别应用层信息中是否携带病毒的字符串，由系统中的病毒特征库预定义。

2. 病毒例外

缺省情况下，设备对所有匹配病毒特征的报文均进行防病毒动作处理。但是，当管理员认为已检测到的某个病毒为误报时，可以将该病毒特征设置为病毒例外，之后携带此病毒特征的报文经过时，设备将对此报文执行允许动作。

3. 应用例外

缺省情况下，设备基于应用层协议的防病毒动作对符合病毒特征的报文进行处理。当需要对某应用层协议上承载的某一具体应用采取不同的动作时，可以将此应用设置为应用例外。例如，对 HTTP 协议采取的动作是允许，但是需要对 HTTP 协议上承载的游戏类应用采取阻断动作，这时就可以把所有游戏类的应用均设置为应用例外。

4. 防病毒动作

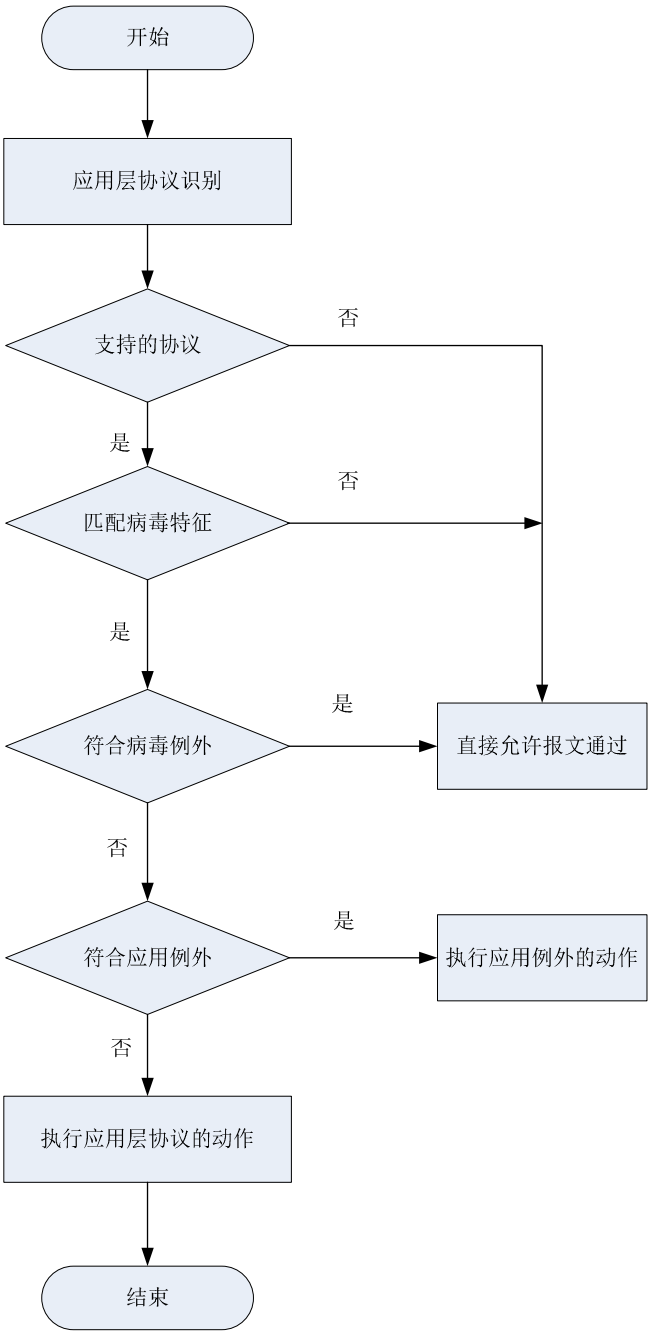
防病毒动作是指对符合病毒特征的报文做出的处理，包括如下几种类型：

- 告警：允许病毒报文通过，同时生成病毒日志。
- 阻断：禁止病毒报文通过，同时生成病毒日志。
- 重定向：将携带病毒的 HTTP 连接重定向到指定的 URL，同时生成病毒日志。

1.1.4 防病毒数据处理流程

设备上部署防病毒策略后，对接收到的用户数据报文处理流程如 图 1-2 所示：

图1-2 防病毒数据处理流程图



防病毒处理的整体流程如下：

(1) 如果报文匹配了某对象策略规则，且此对象策略规则的动作是 **inspect**，则设备将继续识别此报文的应用层协议。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”。

(2) 如果报文的应用层协议为防病毒功能所支持，则设备使用病毒特征库中的病毒特征对此报文进行匹配，否则不对其进行防病毒处理。

(3) 如果报文与病毒特征匹配成功，则进一步判断此病毒报文是否符合病毒例外，否则对其执行允许动作。

(4) 如果病毒报文符合病毒例外，则对此报文执行允许动作，否则继续判断其是否符合应用例外。

(5) 如果病毒报文符合应用例外，则执行应用例外的防病毒动作（告警、阻断和允许），否则执行所属应用层协议的防病毒动作（告警、阻断和重定向）。

1.1.5 病毒特征库升级与回滚

病毒特征库是用来对经过设备的报文进行病毒检测的资源库。随着互联网中病毒的不断变化和发展，需要及时升级设备中的病毒特征库，同时设备也支持病毒特征库回滚功能。

1. 病毒特征库升级

病毒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病毒特征库。
- 立即自动在线升级：管理员手工触发设备立即更新本地的病毒特征库。
- 手动离线升级：当设备无法自动获取病毒特征库时，需要管理员先手动获取最新的病毒特征库，再更新设备本地的病毒特征库。

2. 病毒特征库回滚

如果管理员发现设备当前的病毒特征库对报文进行病毒检测的误报率较高或出现异常情况，可以将其回滚到出厂版本或上一版本。

1.2 防病毒配置任务简介

表1-1 防病毒配置任务简介

配置任务	说明	详细配置
配置防病毒策略	必选	1.3.1
配置防病毒引用的重定向动作参数profile	可选	1.3.2
在DPI应用profile中引用防病毒策略	必选	1.3.3
在对象策略规则中引用DPI应用profile	必选	1.3.4
在安全域间实例中引用对象策略	必选	1.3.5
配置病毒特征库升级和回滚	可选	1.3.6
激活DPI各业务模块的策略配置	可选	1.3.7

1.3 配置防病毒

1.3.1 配置防病毒策略

在防病毒策略中可以配置防病毒的检测条件、对病毒报文的处理动作、病毒例外和应用例外等。

设备上的所有防病毒策略均使用当前系统中的病毒特征库对用户数据进行病毒检测和处理。

表1-2 配置防病毒策略

操作	命令	说明
进入系统视图	**system-view**	-
创建防病毒策略，并进入防病毒策略视图	**anti-virus policy** *policy-name*	缺省情况下，存在一个缺省防病毒策略，名称为default，且其不能被修改和删除
（可选）配置防病毒策略描述信息	**description** *text*	缺省情况下，不存在防病毒策略描述信息
（可选）配置病毒检测的应用层协议类型	**inspect** { **ftp** | **http** | **imap** | **pop3** | **smtp** } [**direction** { **both** | **download** | **upload** }] [**action** { **alert** | **block** | **redirect** }]	缺省情况下，设备对FTP、HTTP和IMAP协议在上传和下载方向传输的报文均进行病毒检测，对POP3协议在下载方向传输的报文进行病毒检测，对SMTP协议在上传方向传输的报文进行病毒检测。设备对FTP、HTTP协议报文的动作为阻断，对IMAP、SMTP和POP3协议报文的动作为告警
（可选）配置病毒例外	**exception signature** *signature-id*	缺省情况下，不存在病毒例外
（可选）配置应用例外并为其指定处理动作	**exception application** *application-name* **action** { **alert** | **block** | **permit** }	缺省情况下，不存在应用例外
（可选）配置有效病毒特征的最低严重级别	**signature severity** { **critical** | **high** | **medium** } **enable**	缺省情况下，所有严重级别的病毒特征都处于生效状态

1.3.2 配置防病毒重定向动作的执行参数

防病毒重定向动作的具体执行参数由应用层检测引擎重定向动作参数 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”。

如果防病毒引用的应用层检测引擎重定向动作参数 profile 不存在或没有引用，则使用系统中重定向动作参数的缺省值。

表1-3 配置防病毒重定向动作的执行参数

操作	命令	说明
进入系统视图	**system-view**	-
配置防病毒引用的应用层检测引擎重定向动作参数profile	**anti-virus redirect parameter-profile** *profile-name*	缺省情况下，防病毒未引用应用层检测引擎重定向动作参数profile

1.3.3 在DPI应用profile中引用防病毒策略

DPI 应用 profile 是一个安全业务的配置模板，为实现防病毒功能，必须在 DPI 应用 profile 中引用指定的防病毒策略。一个 DPI 应用 profile 中只能引用一个防病毒策略，如果重复配置，则新的配置会覆盖已有配置。

表1-4 在 DPI 应用 profile 中引用防病毒策略

操作	命令	说明
进入系统视图	**system-view**	-
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”
在DPI应用profile中引用防病毒策略	**anti-virus apply policy** *policy-name* **mode** { **alert** | **protect** }	缺省情况下，DPI应用profile中未引用防病毒策略

1.3.4 在对象策略规则中引用DPI应用profile

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”。

1. 在IPv4 对象策略中引用DPI应用profile

表1-5 在 IPv4 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv4对象策略	**object-policy ip** *object-policy-name*	-
在IPv4对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass** | **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv4对象策略规则中未引用DPI应用profile

2. 在IPv6 对象策略中引用DPI应用profile

表1-6 在 IPv6 对象策略规则中引用 DPI 应用 profile

操作	命令	说明
进入系统视图	**system-view**	-
进入Context系统视图	**switchto context** *context-name*	仅对Context必选
进入一个IPv6对象策略	**object-policy ipv6** *object-policy-name*	-

操作	命令	说明
在IPv6对象策略规则中引用DPI应用profile	**rule** [*rule-id*] { **drop** | **pass**| **inspect** *app-profile-name* } [[**application** *application-name*] [**app-group** *app-group-name*] [**source-ip** *object-group-name* | **any**] [**destination-ip** *object-group-name* | **any**] [**service** *object-group-name* | **any**] [**vrf** *vrf-name*] [**counting**] [**disable**] [**logging**] [**time-range** *time-range-name*]] *	缺省情况下，在IPv6对象策略规则中未引用DPI应用profile

1.3.5 在安全域间实例中引用对象策略

有关此功能的详细介绍请参见“安全配置指导”中的“对象策略”。

表1-7 安全域间实例引用对象策略

操作		命令	说明
进入系统视图		**system-view**	-
进入Context系统视图		**switchto context** *context-name*	仅对Context必选
创建源安全域和目的安全域		**security-zone name** *zone-name*	缺省情况下，当首次执行创建安全域的命令时，系统会自动创建以下缺省安全域Local、Trust、DMZ、Management和Untrust
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*	缺省情况下，不存在安全域间实例
应用对象策略	应用IPv4对象策略	**object-policy apply ip** *object-policy-name*	缺省情况下，安全域间实例内不应用对象策略 二者至少选其一
	应用IPv6对象策略	**object-policy apply ipv6** *object-policy-name*	

1.3.6 配置病毒特征库升级和回滚

注意

- 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，进而影响防病毒的正常运行。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”。

随着网络病毒攻击的不断变化和发展，管理员需要及时升级设备中的病毒特征库，同时设备也支持病毒特征库回滚功能。

1. 配置定期自动在线升级病毒特征库

如果设备可以访问外网时，可以采用定期自动在线升级方式来对设备上的病毒特征库进行升级。

表1-8 配置定期自动在线升级病毒特征库

操作	命令	说明
进入系统视图	**system-view**	-
开启定期自动在线升级病毒特征库功能，并进入自动在线升级配置视图	**anti-virus signature auto-update**	缺省情况下，定期自动在线升级病毒特征库功能处于关闭状态
配置定期自动在线升级病毒特征库的时间	**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02:01:00至04:01:00之间自动升级病毒特征库

2. 立即自动在线升级病毒特征库

表1-9 立即自动在线升级病毒特征库

操作	命令	说明
进入系统视图	**system-view**	-
立即自动在线升级病毒特征库	**anti-virus signature auto-update-now**	-

3. 手动离线升级病毒特征库

如果设备不能访问外网时，管理员可以采用如下几种方式手动离线升级病毒特征库版本。

- 本地升级：使用本地保存的特征库文件升级系统上的病毒特征库版本。
  - 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。（集中式 IRF 设备）
  - 特征库文件只能存储在当前主控板上，否则设备升级特征库会失败。（分布式设备-独立运行模式）
  - 特征库文件只能存储在当前全局主用主控板上，否则设备升级特征库会失败。（分布式设备-IRF 模式）
- 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，并升级系统上的病毒特征库版本。

表1-10 手动离线升级病毒特征库

操作	命令举例	说明
进入系统视图	**system-view**	-
手动离线升级病毒特征库	**anti-virus signature update** *file-path*	-

4. 回滚病毒特征库

病毒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，当前病毒特征库版本是 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。

表1-11 回滚病毒特征库

操作	命令	说明
进入系统视图	**system-view**	-
回滚病毒特征库	**anti-virus signature rollback** { **factory** | **last** }	-

1.3.7 激活DPI各业务模块的策略配置

当 DPI 各业务模块的策略被创建、修改和删除后，需要配置此功能使其策略配置生效。

配置此功能会暂时中断 DPI 业务的处理，为避免重复配置此功能对 DPI 业务造成影响，请统一部署 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”。

表1-12 激活 DPI 各业务模块的策略配置

操作	命令	说明
进入系统视图	**system-view**	-
激活DPI各业务模块的策略配置	**inspect activate**	缺省情况下，DPI各业务模块的策略被创建、修改和删除时不生效

1.4 防病毒显示和维护

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防病毒的运行情况，通过查看显示信息验证配置的效果。

表1-13 防病毒显示和维护

操作	命令
显示病毒特征信息	**display anti-virus signature** [**severity** { **critical** | **high** | **low** | **medium** }]
显示病毒特征库版本信息	**display anti-virus signature information**
显示防病毒统计信息（分布式设备-独立运行模式/集中式IRF设备）	**display anti-virus statistics** [**policy** *policy-name*] [**slot** *slot-number* [**cpu** *cpu-number*]]
显示防病毒统计信息（分布式设备-IRF设备）	**display anti-virus statistics** [**policy** *policy-name*] [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

1.5 防病毒典型配置举例

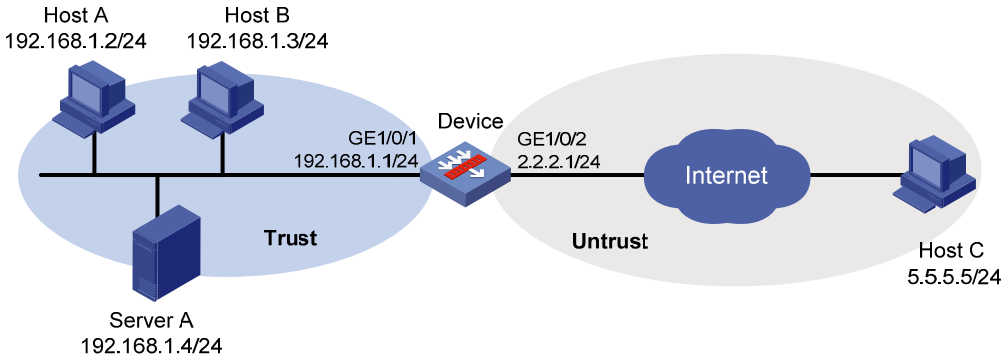
1.5.1 应用缺省防病毒策略的典型配置举例

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。现要求使用设备上的缺省防病毒策略对用户数据报文进行防病毒检测和防御。

2. 组网图

图1-3 应用缺省防病毒策略的配置组网图



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
```

- 配置对象组

创建名为 antivirus 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 antivirus
[Device-obj-grp-ip-antivirus] network subnet 192.168.1.0 24
[Device-obj-grp-ip-antivirus] quit
```

(3) 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 中应用缺省防病毒策略 default，并指定该防病毒策略的模式为 Protect。

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

(4) 配置对象策略

创建名为 antivirus 的 IPv4 对象策略，并进入对象策略视图。

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

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

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

(5) 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 antivirus 对应的报文进行深度检测的对象策略 antivirus。

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

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

4. 验证配置

以上配置生效后，使用缺省防病毒策略可以对已知攻击类型的网络攻击进行防御。

1.5.2 应用自定义防病毒策略的典型配置举例

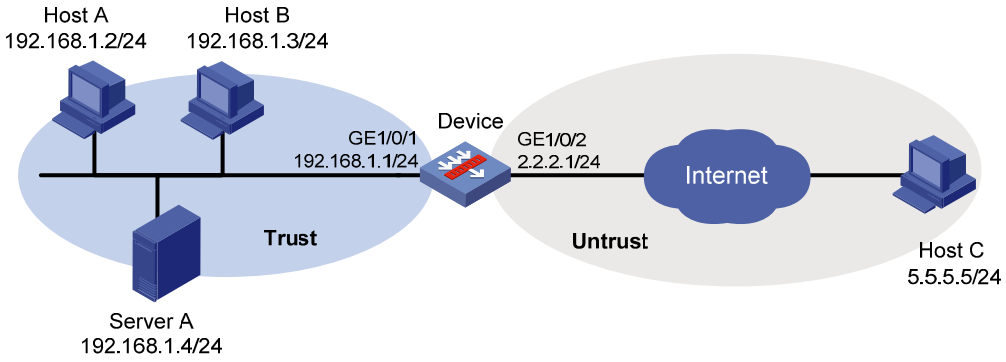
1. 组网需求

如 图 1-4 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 的预定义病毒特征设置为病毒例外。
- 将名称为 126_Web_Email_Send_Email_HTTP 的的应用设置为应用例外。

2. 组网图

图1-4 应用自定义防病毒配置组网图



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 antivirus 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 antivirus
[Device-obj-grp-ip-antivirus] network subnet 192.168.1.0 24
[Device-obj-grp-ip-antivirus] quit
```

(4) 配置防病毒功能

创建一个名称为 antivirus1 的防病毒策略，并进入防病毒策略视图。

```
[Device] anti-virus policy antivirus1
```

将编号为 2 的预定义病毒特征设置为病毒例外。

```
[Device-anti-virus-policy-antivirus1] exception signature 2
```

将名称为 139Email 的应用设置为应用例外，并设置其动作为告警。

```
[Device-anti-virus-policy-antivirus1] exception application 139Email action alert
[Device-anti-virus-policy-antivirus1] 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 中应用防病毒策略 antivirus1，并指定该防病毒策略的模式为 Protect。

```
[Device-app-profile-sec] anti-virus apply policy antivirus1 mode protect
[Device-app-profile-sec] quit
```

(6) 配置对象策略

创建名为 antivirus 的 IPv4 对象策略，并进入对象策略视图。

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

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

```
[Device-object-policy-ip-antivirus] rule inspect sec source-ip antivirus destination-ip any
[Device-object-policy-ip-antivirus] 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 antivirus 对应的报文进行深度检测的对象策略 antivirus。

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

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

4. 验证配置

以上配置生效后，在防病毒策略 antivirus1 中可看到以上有关防病毒策略的配置。

1.5.3 手动离线升级病毒特征库典型配置举例

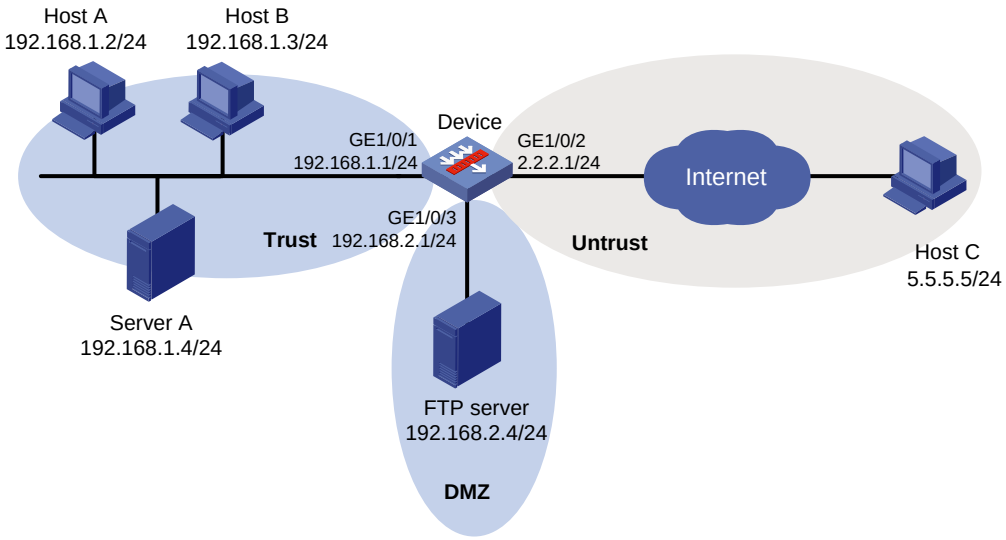
1. 组网需求

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，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病毒特征库文件anti-virus-1.0.2-encrypt.dat，FTP服务器的登录用户名和密码分别为anti-virus和 123。现有组网需求如下：

- 手动离线升级病毒特征库，加载最新的病毒特征。
- 使用设备上的缺省防病毒策略对常见的网络病毒攻击进行防御。

2. 组网图

图1-5 手动离线升级病毒特征库配置组网图



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) 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] 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
```

(4) 配置对象组

创建名为 antivirus 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 antivirus
[Device-obj-grp-ip-antivirus] network subnet 192.168.1.0 24
[Device-obj-grp-ip-antivirus] quit
```

(5) 配置防病毒功能

采用 FTP 方式手动离线升级设备上的病毒特征库，被加载的病毒特征库文件名为 anti-virus-1.0.8-encrypt.dat。

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

(6) 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 中应用缺省防病毒策略 default，并指定该防病毒策略的模式为 Protect。

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

(7) 配置对象策略

创建名为 antivirus 的 IPv4 对象策略，并进入对象策略视图。

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

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

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

(8) 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 antivirus 对应的报文进行深度检测的对象策略 antivirus。

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

激活 DPI 各业务模块的策略配置。

```
[Device] inspect activate
```

4. 验证配置

以上配置生效后，使用缺省防病毒策略可以对已知攻击类型的网络攻击进行防御。

病毒特征库升级后，可以通过 **display anti-virus signature information** 命令查看当前特征库的版本信息。

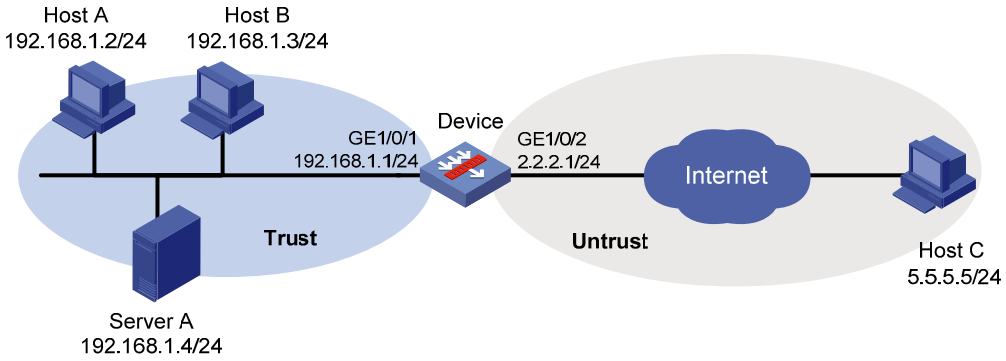
1.5.4 定时自动升级病毒特征库典型配置举例

1. 组网需求

如 图 1-6 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病毒特征库。

2. 组网图

图1-6 定时自动升级病毒特征库配置组网图



3. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置定期自动在线升级病毒特征库

开启设备自动升级病毒特征库功能，并进入自动升级配置视图。

```
<Device> system-view
[Device] anti-virus signature auto-update
```

设置定时自动升级病毒特征库计划为：每周六上午 9:00:00 自动升级，抖动时间为 30 分钟。

```
[Device-anti-virus-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 30
[Device-anti-virus-autoupdate] quit
```

4. 验证配置

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