

H3C SecPath M9000 系列 多业务安全网关

DPI 深度安全配置指导(V7)

Copyright © 2021-2024 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本配置指导主要介绍 DPI（Deep Packet Inspection，深度报文检测）的相关功能原理及配置。
前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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. 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。

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	1-4
1.3 DPI 深度安全配置限制和指导	1-4
1.4 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。传统安全防护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、APR 特征库、防病毒特征库、WAF 特征库、IP 信誉特征库、URL 信誉特征库和域名信誉特征库。

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”
WAF	WAF（Web application firewall，Web应用防火墙）用于阻断Web应用层攻击，保护内网用户和内部Web服务器。
IP信誉特征库	IP信誉根据IP信誉特征库中的IP地址信息对网络流量进行过滤
URL信誉特征库	URL信誉功能用于对恶意的URL进行过滤，允许或禁止用户访问某些网站，达到规范用户上网行为的目的
域名信誉特征库	域名信誉根据域名信誉特征库中的域名信息对网络流量进行过滤，允许或禁止用户访问某些网站，达到规范用户上网行为的目的

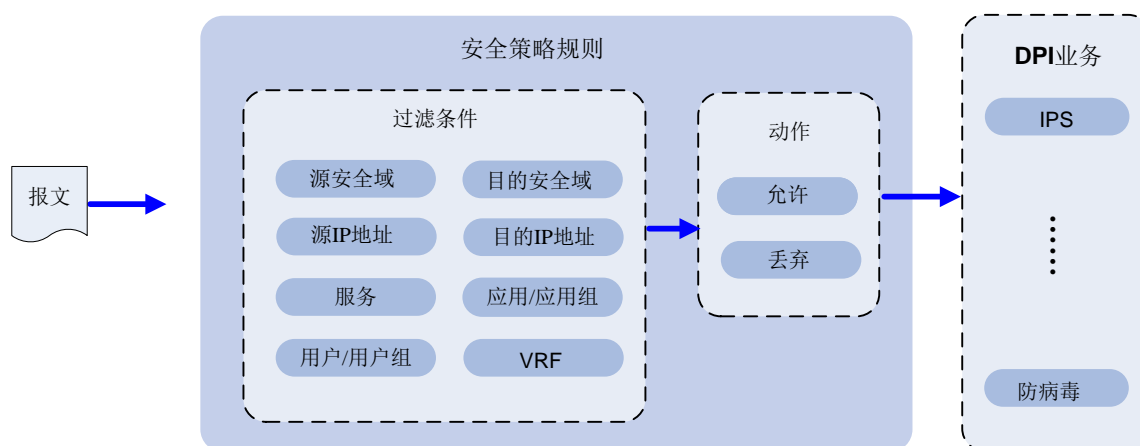
1.1.4 DPI 深度安全的处理流程

DPI 深度安全功能可基于安全策略和对象策略实现。

1. 基于安全策略实现 DPI 深度安全功能

当符合安全策略过滤条件的报文经过设备时，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



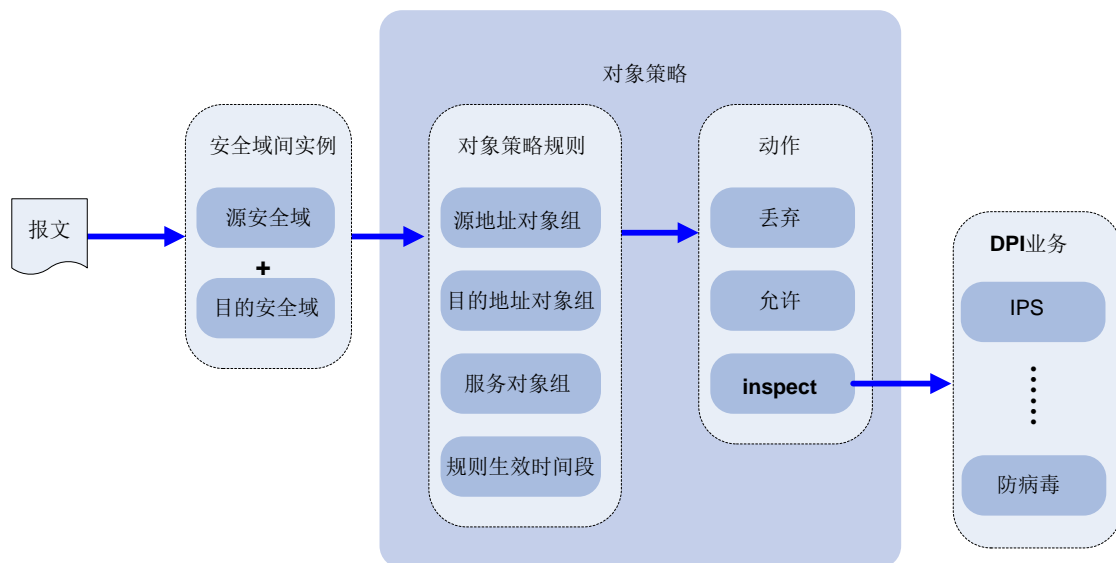
DPI 深度安全处理流程具体如下：

- (2) 报文将与安全策略规则进行匹配。安全策略规则中定义了用来进行报文匹配的源安全域、目的安全域、源 IP 地址、目的 IP 地址和服务类型等过滤条件，仅当报文与所有过滤条件都匹配时才认为成功匹配安全策略规则。有关安全策略规则的详细介绍，请参见“安全配置指导”中的“安全策略”。
- (3) 如果报文未与任何一条安全策略规则匹配成功，则此报文将会被丢弃。
- (4) 如果报文成功匹配安全策略规则，设备将执行此规则中指定的动作。
 - 如果动作为“丢弃”，则设备将阻断此报文；
 - 如果动作为“允许”，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“允许”，且引用的 DPI 业务不存在，则设备将允许此报文通过。

2. 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 1-2 所示。

图1-2 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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV防火墙业务板	支持
	Blade V防火墙业务板	支持
	NAT业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V防火墙业务板	支持
M9008-S M9012-S	Blade IV防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V防火墙业务板	支持
M9000-AK001	Blade V防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI防火墙业务板	支持

1.3 DPI深度安全配置限制和指导

与对象策略相比，安全策略可以基于用户对报文进行控制，使网络管理更加灵活和可视。优先推荐使用基于安全策略的方式 DPI 深度安全功能。

1.4 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 1-3](#)和[图 1-4](#)所示。

图1-3 DPI 深度安全配置指导图（基于安全策略实现）

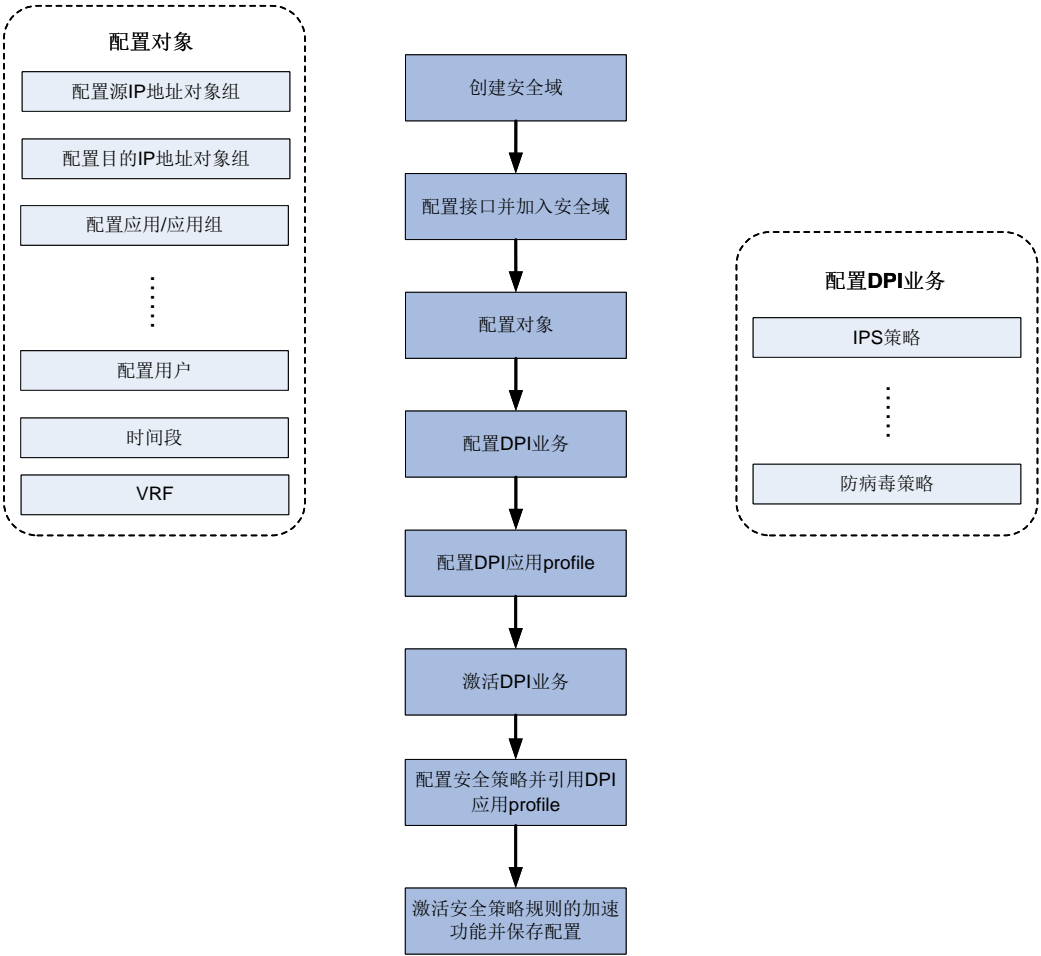
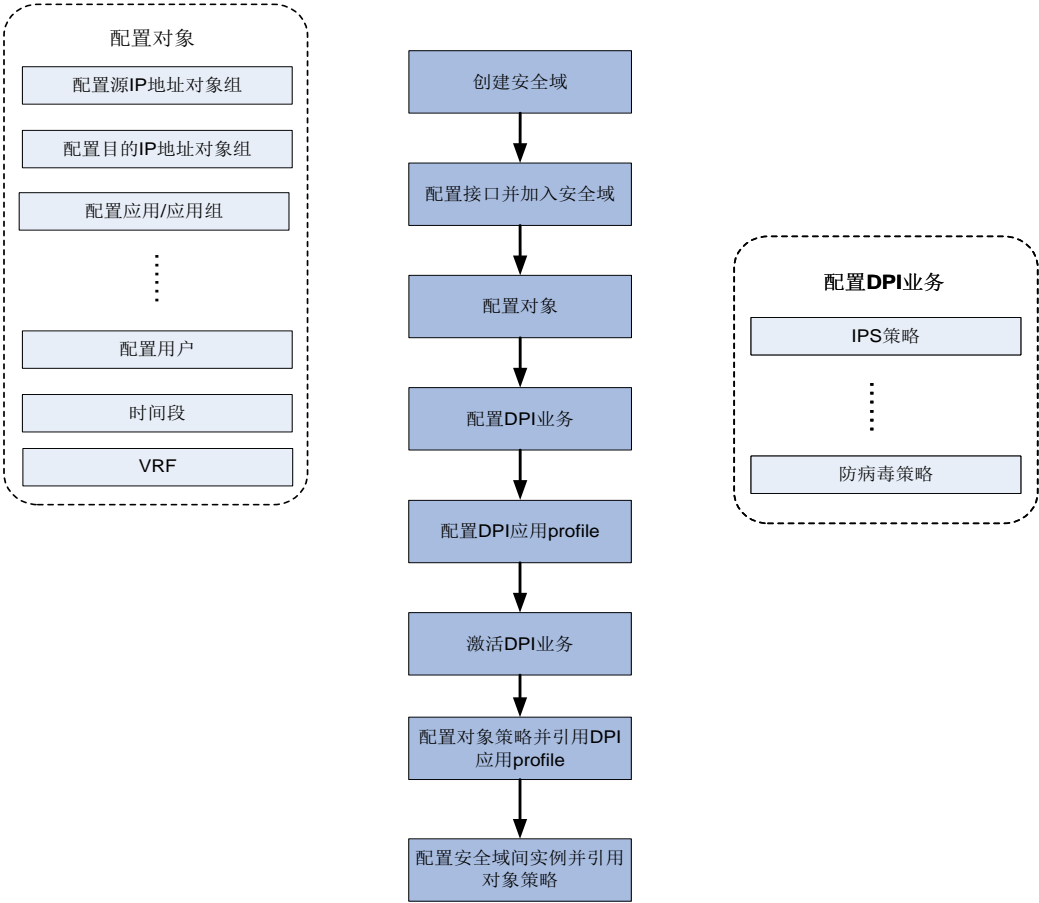


图1-4 DPI 深度安全配置指导图（基于对象策略实现）



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	1-2
1.3 vSystem 相关说明	1-3
1.4 应用层检测引擎配置任务简介	1-3
1.5 配置 DPI 应用 Profile	1-4
1.6 激活 DPI 业务模块的策略和规则配置	1-5
1.7 配置应用层检测引擎动作参数	1-6
1.7.1 配置源阻断动作参数	1-6
1.7.2 配置捕获动作参数	1-6
1.7.3 配置日志动作参数	1-7
1.7.4 配置重定向动作参数	1-8
1.7.5 配置邮件动作参数	1-8
1.7.6 配置防病毒告警动作参数	1-9
1.7.7 配置 URL 过滤告警动作参数	1-10
1.8 优化应用层检测引擎性能	1-10
1.9 配置应用层检测引擎 CPU 门限响应功能	1-11
1.10 配置应用层检测引擎检测参数	1-11
1.10.1 配置应用层检测引擎检测率模式	1-11
1.10.2 配置应用层检测引擎对报文的最大检测长度限制功能	1-12
1.10.3 配置应用层检测引擎检测固定长度文件功能	1-13
1.10.4 配置应用层检测引擎计算固定长度文件 MD5 值功能	1-13
1.10.5 配置应用层检测引擎对所有文件进行 MD5 哈希运算	1-14
1.10.6 配置应用层检测引擎解压缩参数	1-14
1.10.7 配置应用层检测引擎解压缩文件的总次数上限值	1-15
1.10.8 配置应用层检测引擎记录 NFS 协议文件名数量的上限值	1-16
1.11 配置应用层检测引擎扩展功能	1-16
1.11.1 开启基于源端口的应用识别功能	1-16
1.11.2 配置 DPI 业务特征库在线升级所使用的代理服务器	1-16
1.11.3 配置特征库在线升级时访问的特征库服务器所属的 VPN 实例	1-17

1.11.4 配置特征库在线升级时发送给服务器的请求报文的源 IP 地址	1-17
1.11.5 配置 DPI 业务云端服务器	1-18
1.11.6 开启 DPI 业务支持 HA 双主模式功能	1-18
1.11.7 开启 WAF 日志记录报文详情功能	1-19
1.11.8 配置 IPS 日志记录报文详情功能	1-19
1.11.9 配置日志统计信息的上送地址	1-20
1.11.10 配置特征库版本信息的上送地址	1-20
1.11.11 关闭应用层检测引擎透传 DPI 业务流量功能	1-21
1.12 配置真实源 IP 地址提取功能	1-21
1.12.1 开启真实源 IP 地址提取功能	1-21
1.12.2 配置真实源 IP 地址提取模式	1-22
1.12.3 开启真实源 IP 地址复用功能	1-22
1.12.4 配置 X-Forwarded-For 字段检测结果的提取位置	1-23
1.12.5 配置 TCP Option 字段的检测参数	1-24
1.13 关闭应用层检测引擎功能	1-24
1.13.1 关闭应用层检测引擎所有检测功能	1-24
1.13.2 关闭应用层检测引擎对指定协议报文的检测功能	1-25
1.14 应用层检测引擎显示和维护	1-25

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。

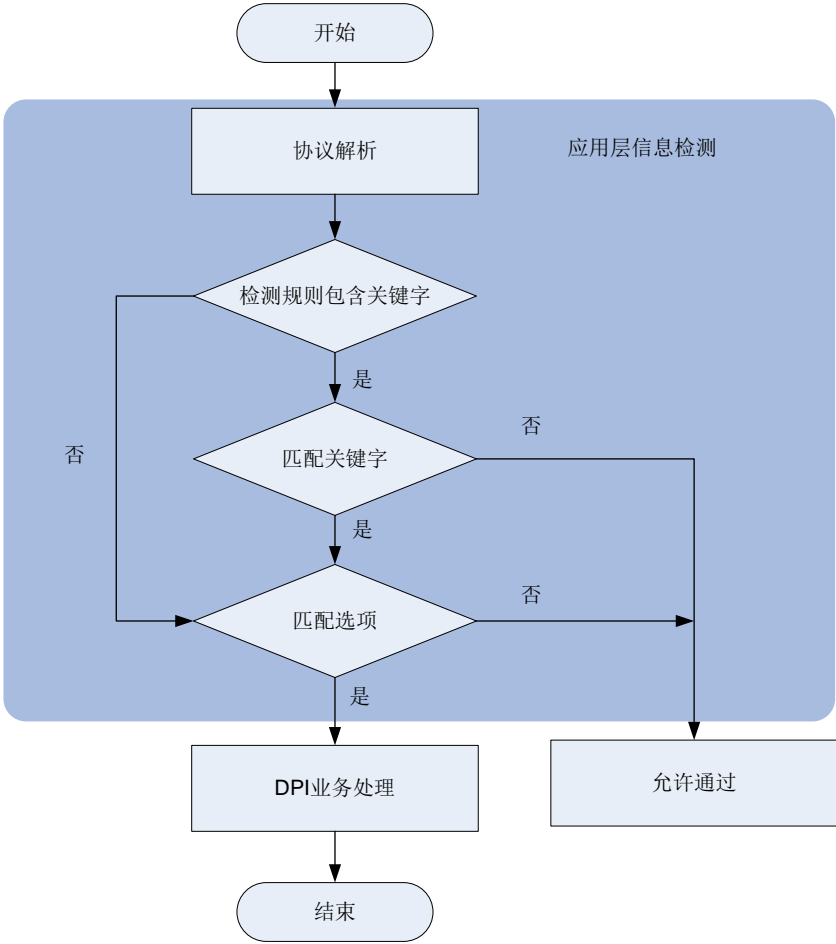
- 关键字：标识报文特征的不少于 3 个字节的字符串，也称作“AC 关键字”。
- 选项：非关键字的辅助匹配项，例如报文的端口号、协议类型等。

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：

- (1) 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。
- (2) 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。
- (3) 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。
- (4) 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。
- (5) 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。

设备型号	业务板类型	说明
M9006	Blade IV防火墙业务板	支持

M9010 M9014	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.3 vSystem 相关说明

非缺省 vSystem 支持本特性部分功能，具体包括：

- 配置 DPI 应用 Profile
- 激活 DPI 业务模块的策略规则配置
- 配置应用层检测引擎动作参数



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.4 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参数](#)
 - [配置应用层检测引擎检测率模式](#)
 - [配置应用层检测引擎对报文的最大检测长度限制功能](#)
 - [配置应用层检测引擎检测固定长度文件功能](#)
 - [配置应用层检测引擎计算固定长度文件 MD5 值功能](#)
 - [配置应用层检测引擎对所有文件进行 MD5 哈希运算](#)
 - [配置应用层检测引擎解压缩参数](#)
 - [配置应用层检测引擎解压缩文件的总次数上限值](#)
 - [配置应用层检测引擎记录 NFS 协议文件名数量的上限值](#)
- (7) (可选) [配置应用层检测引擎扩展功能](#)
 - [开启基于源端口的应用识别功能](#)
 - [配置 DPI 业务特征库在线升级所使用的代理服务器](#)
 - [配置特征库在线升级时访问的特征库服务器所属的 VPN 实例](#)
 - [配置特征库在线升级时发送给服务器的请求报文的源 IP 地址](#)
 - [配置 DPI 业务云端服务器](#)
 - [开启 DPI 业务支持 HA 双主模式功能](#)
 - [开启 WAF 日志记录报文详情功能](#)
 - [配置 IPS 日志记录报文详情功能](#)
 - [配置日志统计信息的上送地址](#)
 - [配置特征库版本信息的上送地址](#)
 - [关闭应用层检测引擎透传 DPI 业务流量功能](#)
- (8) [配置真实源 IP 地址提取功能](#)
- (9) [关闭应用层检测引擎功能](#)

1.5 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 被安全策略规则或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”。
- 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 mode { alert | protect }`
 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”。
- 在 DPI 应用 `profile` 下引用 WAF 策略。
`waf apply policy policy-name mode { protect | alert }`
 缺省情况下，未关联 DPI 业务策略。

1.6 激活DPI业务模块的策略和规则配置

1. 功能简介

缺省情况下，当任意一个 DPI 业务模块（比如 URL 过滤业务）发生配置变更时（即策略或规则被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时执行一次激活操作，使这些策略和规则的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对发生变化的业务的策略或规则立即进行激活，可执行 `inspect activate` 命令手工激活。

2. 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、修改和删除后系统会自动激活配置。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.7 配置应用层检测引擎动作参数

1.7.1 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。

1.7.2 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（例如 **tftp://192.168.100.100/upload**）。

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. 配置限制和指导

当设备检测到硬盘/U 盘在位时，会直接将 IPS 捕获文件保存到硬盘/U 盘中，而不会上送到指定的 URL。

当设备检测到与其对接的安全威胁发现与运营管理平台已开启捕获文件上送功能时，会直接通过 HTTPS 协议将 IPS 捕获文件上送到该平台，而不会上送到指定的 URL。有关安全威胁发现与运营管理平台的相关介绍，请参考该平台配套的配置指导手册。

当设备检测到硬盘/U 盘在位，且与其对接的安全威胁发现与运营管理平台已开启捕获文件上送功能时，会将 IPS 捕获文件保存到硬盘/U 盘中，并通过 HTTPS 协议将 IPS 捕获文件上送到安全威胁发现与运营管理平台。

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。

1.7.3 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和输出语言。

2. 配置限制和指导

配置记录 IPS 日志使用的语言为中文后，仅 IPS 日志的威胁名称字段使用中文描述，其它日志信息仍然为英文。

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。

- (4) 配置记录 IPS 日志使用的语言为中文。

```
log language chinese
```

缺省情况下，记录 IPS 日志使用的语言为英文。

1.7.4 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. 配置限制和指导

重定向报文的 URL 必须以 **http://**或 **https://**开头，例如 **https://www.example.com**。

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。

1.7.5 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。

邮件服务器的地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。采用主机名时，需要确保设备能通过静态或动态域名解析方式获得邮件服务器的 IP 地址，并与之路由可达。否则邮件发送会失败。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”。

- (4) 配置发件人地址。

```
sender addr-string
```

缺省情况下，未配置发件人地址。

- (5) 配置收件人地址。

receiver *addr-string*

缺省情况下，未配置收件人地址。

(6) (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。

(7) (可选) 配置以邮件方式输出日志的限制条件。

email-limit interval *interval* **max-number** *value*

缺省情况下，5 分钟内，设备最多可向外发送 10 封邮件。

(8) (可选) 配置日志邮件使用的语言。

language { **chinese** | **english** }

缺省情况下，日志邮件使用的语言为中文。

目前仅 IPS、防病毒和 WAF 业务支持发送中文的日志邮件，且各业务日志邮件中仅部分字段支持使用中文，具体字段说明请参见命令参考手册。

1.7.6 配置防病毒告警动作参数

1. 功能简介

告警动作参数 **profile** 用来为防病毒模块的告警动作提供动作参数，在此 **profile** 中可以导入告警文件，告警文件中可配置设备向客户端发送的具体告警信息。

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防病毒告警动作参数 **profile**，并进入告警动作参数 **profile** 视图。

inspect warning parameter-profile *profile-name*

(3) 导入告警文件。

import block warning-file *file-path*

缺省情况下，设备使用缺省文件里的告警信息：The site you are accessing has a security risk and thereby is blocked.

(4) (可选) 重置告警文件内容。

reset block warning-file

配置本命令后，设备会将告警文件中的告警信息重置为缺省文件中的告警信息。

1.7.7 配置 URL 过滤告警动作参数

1. 功能简介

URL 过滤告警动作参数 **profile** 用来为 URL 过滤模块的告警动作提供具体的执行参数，在此 **profile** 中可以导入告警信息文件，告警信息文件中可配置设备向客户端发送的具体告警信息。

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 URL 过滤告警动作参数 **profile**，并进入 URL 过滤告警动作参数 **profile** 视图。

inspect url-filter warning parameter-profile *profile-name*

- (3) 导入 URL 过滤告警信息文件。

import warning-file *file-path*

缺省情况下，存在一个名称为 **uflt-xxx.html** 的告警信息文件，其中 **xxx** 表示 URL 过滤告警动作参数 **profile** 的名称。文件中包含缺省的告警信息，具体内容请参见“DPI 深度安全命令参考”中的“应用层检测引擎”手册中对本命令行缺省情况的详细介绍。

- (4) （可选）重置 URL 过滤告警信息文件内容。

reset warning-file

配置本命令后，设备会将 URL 过滤告警信息文件中的内容恢复为缺省告警信息。

1.8 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数目为 32。

- (3) 配置应用层检测引擎缓存待检测选项的数目。

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
```

应用层检测引擎的所有优化调试功能处于关闭状态。

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。

1.9 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，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。
- 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，系统会恢复应用层检测引擎的检测功能。

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。

当 CPU 突发压力过大时，即使 CPU 利用率未达到设备上配置的 CPU 利用率阈值，系统也将会针对部分流量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 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。

1.10 配置应用层检测引擎检测参数

1.10.1 配置应用层检测引擎检测率模式

1. 功能简介

为适应不同场景对设备性能和检测率的不同需求，应用层检测引擎支持如下几种选项供选择：

- **balanced:** 适用于大多数场景，设备在性能和检测率之间可以达到平衡状态。此模式下，应用层检测引擎对 FTP 协议、HTTP 协议、SMB 协议、NFS 协议和与 E-mail 相关协议数据流的最大检测长度均为 32 千字节；MD5 最大检测长度为 2048 千字节。
- **large-coverage:** 适用于对检测率要求较高的场景，设备将提升检测率，但同时会对性能产生一定影响。此模式下，应用层检测引擎对 FTP 协议、HTTP 协议、SMB 协议、NFS 协议和与 E-mail 相关协议数据流的最大检测长度均为 128 千字节；MD5 最大检测长度为 5120 千字节。
- **high-performance:** 适用于对设备性能要求较高的场景，设备可在保证一定检测率的前提下，提升性能。此模式下，应用层检测引擎对 FTP 协议、HTTP 协议、SMB 协议、NFS 协议和与 E-mail 相关协议数据流的最大检测长度均为 32 千字节。MD5 最大检测长度为 32 千字节。
- **user-defined:** 适用于对检测率和性能有精确要求的场景。此模式下，可以自定义应用层检测引擎对各协议数据流的最大检测长度（通过 **inspect stream-fixed-length** 命令配置）和 MD5 最大检测长度（通过 **inspect md5-fixed-length** 命令配置）。

当检测率模式由其他模式切换为自定义模式时，数据流最大检测长度和 MD5 最大检测长度将保持切换前模式下的取值。用户可以此作为参考，调整各检测长度。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎检测率模式。

```
inspect coverage { balanced | large-coverage | high-performance |
user-defined }
```

缺省情况下，应用层检测引擎检测率模式为平衡模式。

1.10.2 配置应用层检测引擎对报文的最大检测长度限制功能

1. 功能简介

本功能用于限制应用层检测引擎对协议报文和音视频应用报文的最大检测长度，当引擎已检测的报文长度达到限制值时，引擎将不对后续报文进行检测。调高最大检测长度后，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，调低最大检测长度后，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。请用户根据实际情况进行配置。

2. 配置限制和指导

本功能仅在应用层检测引擎检测率模式为自定义模式时（通过 **inspect coverage user-defined** 命令配置）支持配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎对报文的最大检测长度。

```
inspect stream-fixed-length { audio-video | dns | email | ftp | http |
https | imaps | nfs | pop3s | rtmp | sip | smb | smtps | telnet | tftp }
* length
```

缺省情况下，应用层检测引擎对 FTP 协议、HTTP 协议、NFS 协议、SMB 协议和与 E-mail 相关协议（包括 SMTP、POP3 和 IMAP 协议）报文最大检测长度为 32 千字节，对音频和视频类应用报文以及 DNS 协议、HTTPS 协议、IMAPS 协议、POP3S 协议、RTMP 协议、SIP 协议、SMTPS 协议、Telnet 协议和 TFTP 协议报文的检测长度不进行限制。

- (3) （可选）关闭应用层检测引擎对报文的最大检测长度限制功能。

inspect stream-fixed-length disable

缺省情况下，应用层检测引擎对报文的最大检测长度限制功能处于开启状态。

当组网环境中对应用层信息识别的成功率要求较高时，可通过关闭应用层检测引擎对报文的最大检测长度限制功能，提升应用层信息识别的成功率。

1.10.3 配置应用层检测引擎检测固定长度文件功能

1. 功能简介

本功能用于配置应用层检测引擎对每条数据流中传输文件的固定检测长度，超过长度的文件内容将不再进行检测。由于病毒特征一般都位于文件的前半部分，可配置文件的固定检测长度，对超过长度的文件内容不进行检测，从而提高设备的检测效率。

2. 配置限制和指导

由于文件在数据流中传输，所以配置的文件固定检测长度必须小于等于数据流固定检测长度。

本功能仅在应用层检测引擎检测率为自定义模式时（通过 **inspect coverage user-defined** 命令配置）支持配置。

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文件功能。

inspect file-fixed-length enable

缺省情况下，应用层检测引擎检测固定长度文件功能处于关闭状态。

- (3) 配置应用层检测引擎检测文件的固定长度。

**inspect file-fixed-length { email | ftp | http | nfs | smb } *
length-value**

缺省情况下，应用层检测引擎对基于 FTP 协议、HTTP 协议、NFS 协议、SMB 协议和与 E-mail 相关协议传输的文件固定检测长度均为 32 千字节。

如果一条数据流中包含多个文件，则每个文件均仅检测配置的固定长度内的内容。

1.10.4 配置应用层检测引擎计算固定长度文件 MD5 值功能

1. 功能简介

防病毒业务中，设备除了特征匹配之外，还可以通过对文件进行 MD5 哈希运算，并使用计算出的 MD5 值与特征库中的 MD5 规则匹配，来实现病毒检测。如果 MD5 值与 MD5 规则匹配成功，则表示该文件携带病毒。有关防病毒检测功能的详细介绍请参见“DPI 深度安全配置指导”中的“防病毒”。

应用层检测引擎对报文的特征检测和文件 MD5 值检测会同时进行，当引擎检测的报文长度达到固定数据流检测长度后，将不再进行特征检测。此时，如果希望 MD5 值检测可以继续进行，则需要开启 MD5 固定检测长度功能，并配置检测长度大于固定数据流检测长度。引擎将继续进行 MD5 值检测，直到检测长度达到配置的 MD5 固定检测长度后，仅计算检测范围内文件的 MD5 值，超出长度的文件内容不会计算在内。

调高 MD5 固定检测长度后，设备性能会下降，但是 MD5 检测的成功率会提高；调低 MD5 固定检测长度后，设备性能会提升，但是 MD5 检测的成功率会降低。

2. 配置限制和指导

本功能仅在应用层检测引擎检测率模式为自定义模式时（通过 **inspect coverage user-defined** 命令配置）支持配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启应用层检测引擎 MD5 固定检测长度功能。

```
inspect md5-fixed-length enable
```

缺省情况下，应用层检测引擎 MD5 固定检测长度功能处于开启状态。

- (3) 配置应用层检测引擎 MD5 固定检测长度。

```
inspect md5-fixed-length { email | ftp | http | nfs | smb } * length
```

缺省情况下，应用层检测引擎对 FTP 协议、HTTP 协议、SMB 协议、NFS 协议和与 E-mail 相关协议数据流中文件的 MD5 固定检测长度均为 2048 千字节。

1.10.5 配置应用层检测引擎对所有文件进行 MD5 哈希运算

1. 配置限制和指导

开启此功能后将对设备业务处理性能产生影响，请管理员根据设备实际情况进行配置。

2. 配置步骤

- (1) 配置步骤进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎对所有文件进行 MD5 哈希运算。

```
inspect md5-verify all-files
```

缺省情况下，只对可执行文件、office 文件和压缩文件等类型的文件进行 MD5 哈希运算。

1.10.6 配置应用层检测引擎解压缩参数

1. 功能简介

当设备收到压缩文件时，应用层检测引擎会对文件进行解压缩，并对解压缩后的数据进行特征匹配等处理。管理员可根据实际需求，对引擎可解压缩的文件层数和单个文件中可解压缩的数据大小进行配置。

- 可解压缩数据上限：设备解压一个文件时可解压缩数据的最大值。到达上限后，该文件的剩余数据不再进行解压，直接按照压缩文件格式进行特征匹配等处理。

- 可解压缩文件层数上限：设备最多可解压缩的文件的层数。当超过配置的层数时，设备将不会对超出层数上限的文件进行解压，直接按照压缩文件格式进行特征匹配等处理。

2. 配置限制和指导

仅支持解压缩 ZIP 和 GZIP 格式的文件。

如果配置的解压缩参数过大，当设备频繁收到过大或压缩层数较多的压缩文件时，将一直解压缩一个文件，会影响后续文件的解压缩，并消耗大量的设备内存，影响设备的转发性能，但是对文件内容的识别率会有所提升；如果配置的解压缩参数过小，可能导致压缩文件中的原始文件内容无法正确识别，从而对 DPI 业务（例如防病毒和数据过滤业务）的检测结果产生影响，但是会降低对设备转发性能的影响。请管理员合理配置此参数。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎可解压缩数据上限。

```
inspect file-uncompr-len max-size
```

缺省情况下，可解压缩数据上限为 100MB。

- (3) 配置应用层检测引擎可解压缩文件层数上限。

```
inspect file-uncompr-layer max-layer
```

缺省情况下，可解压缩文件层数上限为 3。当此参数配置为 0 时，表示不对文件进行解压缩。

1.10.7 配置应用层检测引擎解压缩文件的总次数上限值

1. 功能简介

应用层检测引擎每进行一次解压缩操作都会消耗一定的设备内存。当解压缩的次数较多时，可能会消耗大量的设备内存，导致设备整机的并发性能下降。此时，可通过配置解压缩次数的上限值来控制对内存的占用。

2. 配置限制和指导

调低上限值，可降低对内存的消耗，但应用层检测引擎的检测成功率可能会降低；调高上限值，可能会提升应用层检测引擎的检测成功率，但同时会降低设备的并发性能。请管理员根据实际需求配置此功能。

仅支持在缺省 Context 下配置本命令。有关 Context 的详细介绍，请参见“虚拟化技术配置指导”中的“Context”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎可解压缩数据上限。

```
inspect uncompress maximum max-number
```

缺省情况下，应用层检测引擎解压缩文件的总次数上限值由设备实际内存计算得出。

1.10.8 配置应用层检测引擎记录 NFS 协议文件名数量的上限值

1. 功能简介

应用层检测引擎在对文件进行检测时，会使用特定的存储结构记录文件名，用于展示在日志中，方便用户获取文件信息。该记录过程会占用一定的内存，且检测的文件数量越多，对内存占用就越大，可能会降低设备的并发性能。当实际组网环境中大量使用 NFS 协议传输文件时，管理员可通过配置本功能，限制应用层检测引擎记录的基于 NFS 协议传输的文件的文件名数量。

2. 配置限制和指导

在对设备并发性能要求较高的场景下，可减少记录的文件名数量，降低对内存的消耗；在对设备并发性能要求较低的场景下，可调高此参数，增加记录的文件名数量，方便用户获取更多的文件信息。请管理员根据实际需求配置此功能。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置应用层检测引擎记录 NFS 协议文件名数量的上限值。

```
inspect record-filename nfs maximum max-number
```

缺省情况下，应用层检测引擎记录 NFS 协议文件名数量的上限值由设备实际内存计算得出。

1.11 配置应用层检测引擎扩展功能

1.11.1 开启基于源端口的应用识别功能

1. 功能简介

如果网络中的流量种类单一、源端口固定，但无法通过目的端口对其进行基于端口的应用识别或无法基于流量特征进行内容识别时，可以开启本功能，对流量进行源端口识别，将源端口为固定端口的流量识别为访问特定类型应用的流量。

开启本功能后，可能会造成应用识别结果的误报，请管理员根据组网环境的实际情况配置。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启基于源端口的应用识别功能。

```
inspect source-port-identify enable
```

1.11.2 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，进行特征库在线升级。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。

1.11.3 配置特征库在线升级时访问的特征库服务器所属的 VPN 实例

1. 功能简介

当设备对特征库进行立即在线升级或定期在线升级时，需要访问官网的特征库服务器来获取特征库文件。如果设备需要通过指定的 VPN 实例访问特征库时，则必须通过配置本命令指定该 VPN，否则会导致特征库升级失败。

2. 配置限制和指导

如果同时配置了特征库在线升级时发送给服务器的请求报文的源 IP 地址（即配置 **inspect signature auto-update source** 命令），需要保证源 IP 地址所属的 VPN 实例与本功能配置的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置特征库在线升级时访问的特征库服务器所属的 VPN 实例。

```
inspect signature auto-update vpn-instance vpn-instance-name
```

缺省情况下，未配置特征库在线升级时访问的特征库服务器所属的 VPN 实例。

1.11.4 配置特征库在线升级时发送给服务器的请求报文的源 IP 地址

1. 功能简介

如果管理员希望特征库在线升级时发送给特征库服务器的请求报文的源 IP 地址是一个特定的地址时，则需要配置此功能。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问特征库服务器时，则需要管理员通过本命令指定一个符合 NAT 地址转换规则的 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文经由 NAT 地址转换后访问特征库服务器。

2. 配置限制和指导

如果同时配置了特征库在线升级时访问的特征库服务器所属的 VPN 实例（即配置 **inspect signature auto-update vpn-instance** 命令），需要保证本功能配置的源 IP 地址所属的 VPN 实例与该特征库服务器所属的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置特征库在线升级时发送给服务器的请求报文的源 IP 地址。

```
inspect signature auto-update source { ip | ipv6 } { ip-address |  
interface interface-type interface-number }
```

缺省情况下，特征库在线升级时发送给服务器的请求报文的源 IP 地址为系统根据路由表项查找到的出接口的地址。

1.11.5 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 过滤分类查询以及防病毒 MD5 值查询。

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**。

1.11.6 开启 DPI 业务支持 HA 双主模式功能

1. 功能简介

在 HA 双主模式下，开启本功能可以保证在报文来回路径不一致的网络环境中正常处理 DPI 业务。有关 HA 的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

2. 配置限制和指导

本功能仅在设备处于 HA 双主模式下生效。

本功能仅在开启 HA 在设备间透传业务流量功能后生效。

开启本功能后可能会降低设备性能，请管理员根据实际情况进行配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 DPI 业务支持 HA 双主模式功能。

```
inspect dual-active enable
```

缺省情况下，DPI 业务支持 HA 双主模式功能处于关闭状态。

1.11.7 开启 WAF 日志记录报文详情功能

1. 功能简介

开启本功能后，设备将缓存 HTTP 报文的详情信息，并记录在 WAF 日志中，方便用户了解报文详情。

对于 HTTP 请求报文和应答报文，WAF 日志会在原有字段的基础上记录不同的详情信息：

- 对于 HTTP 请求报文，开启本功能后，WAF 日志中将记录报文的所有详情信息。关闭本功能后，WAF 日志中仅记录报文的请求行和请求方法。
- 对于 HTTP 应答报文，开启本功能后，WAF 日志中将记录报文的响应行信息；关闭本功能后，WAF 日志中将不记录报文的详情信息。

2. 配置限制和指导

对于已产生的 WAF 日志，本功能并不生效，设备不会记录报文详情，日志中的报文详情字段为空。

建议仅在关心 WAF 处理的 HTTP 报文的详细信息的情况下开启此功能，避免此功能占用系统的缓存资源。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 WAF 日志记录报文详情功能。

```
inspect waf http-log-details enable
```

1.11.8 配置 IPS 日志记录报文详情功能

1. 功能简介

开启 IPS 日志记录报文详情功能后，设备会使用内存来缓存报文中的 HOST、URI 等详情字段，并记录到 IPS 日志中，方便用户通过日志了解报文详情。例如，当设备在 HTTP 响应报文中检测到 IPS 攻击特征时，IPS 日志中将记录其请求报文的 HOST 字段，以及响应报文的响应行信息，包括状态码、状态信息等。

2. 配置限制和指导

开启 IPS 日志记录报文详情功能后，当组网环境中存在大量 HTTP 报文时，可能会消耗大量的设备内存，导致设备整机的并发性能下降。此时，可通过调整内存中可缓存的报文详情字段的存储空间上限值来控制对内存的占用。调低上限值，可降低对内存的消耗，但有些 IPS 日志中可能无法正常显示报文详情字段；调高上限值，可能会提升 IPS 日志显示报文详情字段的成功率，但同时会降低设备的并发性能。请管理员根据实际需求进行调整。

对于已产生的 IPS 日志，IPS 日志记录报文详情功能并不生效，设备不会记录报文详情，日志中的报文详情字段为空。

开启 IPS 日志记录报文详情功能后，会占用系统的缓存资源，建议仅在关心 IPS 报文的详细信息的情况下开启该功能。

内存中可缓存的报文详情字段的存储空间上限值仅支持对 IPS 业务检测的 HTTP 报文缓存的详情字段进行限制。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 IPS 日志记录报文详情功能。

```
inspect ips log-details enable
```

缺省情况下，IPS 日志记录报文详情功能处于关闭状态。

- (3) 配置内存中可缓存的报文详情字段的存储空间上限值。

```
inspect log-details max-size max-size-value
```

缺省情况下，内存中可缓存的报文详情字段的存储空间上限值由设备实际内存计算得出。

1.11.9 配置日志统计信息的上送地址

1. 功能简介

本功能用于安全威胁发现与运营管理平台监控设备与 KAFKA 服务器集群间的日志发送情况。配置本功能后，设备会将上一个小时内发送给 KAFKA 服务器集群的 IPS 日志的总数以及设备产生的所有 IPS 日志的总数等统计信息发送到指定的安全威胁发现与运营管理平台地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置日志统计信息的上送地址。

```
inspect log-statistics-report { ip-address ip-address | ipv6-address  
ipv6-address } port port uri uri [ vpn-instance vpn-instance-name ]  
kafka-server kafka-server
```

缺省情况下，未配置日志统计信息的上送地址。

1.11.10 配置特征库版本信息的上送地址

1. 功能简介

本功能用于安全威胁发现与运营管理平台监控设备的特征库版本信息变动。目前，仅安全威胁发现与运营管理平台可接收特征库版本信息。

配置本功能后，设备会进行如下操作：

- 当 IPS 特征库升级或回滚时，会立即通过 HTTP 协议向指定的目的地址上送特征库版本信息。
- 设备每隔 10 天向指定的目的地址上送最新的 IPS 特征库版本信息。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置特征库版本信息的上送地址。

```
inspect signature version-report { ip-address ip-address | ipv6-address  
ipv6-address } port port uri uri [ vpn-instance vpn-instance-name ]
```

缺省情况下，未配置特征库版本信息的上送地址。

1.11.11 关闭应用层检测引擎透传 DPI 业务流量功能

1. 功能简介

当组网环境中存在非对称流量时，即同一条流量的报文来回路径不一致，可能导致流量的正反向报文被送到不同的设备（如果是分布式设备，还可能被送到不同的安全业务板），这将会导致 DPI 业务无法正常处理，例如防病毒业务无法识别出病毒文件等。为了解决上述问题，应用层检测引擎默认会在设备间、安全业务板间透传 DPI 业务流量，使同一条流量的正反向报文最终会被送到同一台设备或同一块业务板。

但是，透传流量的过程会消耗设备资源，降低设备性能。当组网环境中对设备性能要求较高且可以接受损失一部分 DPI 业务检测准确性的风险时，可通过关闭应用层检测引擎透传 DPI 业务流量功能，降低对设备性能的影响。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 关闭应用层检测引擎透传 DPI 业务流量功能。

```
undo inspect transparent enable
```

缺省情况下，应用层检测引擎透传 DPI 业务流量功能处于开启状态。

1.12 配置真实源 IP 地址提取功能

1.12.1 开启真实源 IP 地址提取功能

1. 功能简介

当客户端使用代理方式访问服务器时，源 IP 地址将会发生改变，设备无法获取客户端的真实 IP 地址，可能会造成一些攻击无法准确识别（例如基于源 IP 地址数量判定是否为攻击的场景）。开启真实源 IP 检测功能后，设备将从客户端请求报文的相关字段获取真正的源 IP 地址，避免上述问题。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启真实源 IP 地址提取功能。

```
inspect real-ip enable
```

缺省情况下，真实源 IP 地址提取功能处于关闭状态。

1.12.2 配置真实源 IP 地址提取模式

1. 功能简介

设备支持多种真实源 IP 地址提取模式，管理员可以根据实际情况选择其中一种进行配置。

- 单字段提取：当管理员可以确定当前组网环境中仅需要针对报文中的某个特定字段提取真实源 IP 地址时，可将真实源 IP 地址提取模式配置为仅提取该字段（即 **XXX-only** 模式）。
- 字段优先级提取：当管理员不确定需要从哪些字段中获取真实源 IP 时，可将真实源 IP 地址提取模式配置为按照字段优先级提取（即 **priority** 模式），并可根据实际需求调整各字段的优先级。此模式下，设备会从报文的多个字段中获取多个客户端的真实源 IP 地址，并将优先级最高的字段中提取出的 IP 地址作为最终的真实源 IP 地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置真实源 IP 地址提取模式。

```
inspect real-ip extraction mode { cdn-src-ip-only | priority |  
tcp-option-only | x-real-ip-only | xff-only }
```

缺省情况下，真实源 IP 地址提取模式为 **xff-only**。

- (3) （可选）配置真实源 IP 地址的字段优先级。

```
inspect real-ip detect-field { cdn-src-ip | tcp-option | x-real-ip | xff }  
priority priority-value
```

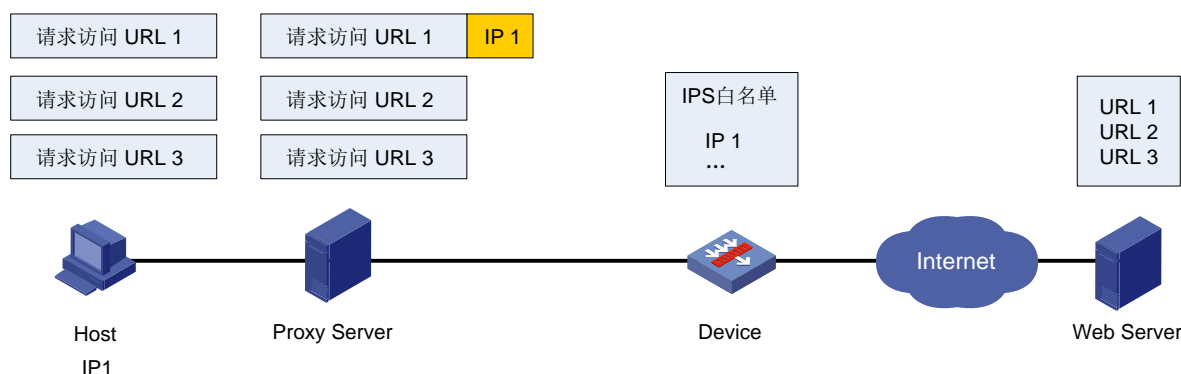
缺省情况下，未配置真实源 IP 地址的字段优先级。设备默认的各真实源 IP 地址字段的优先级从高到底依次为 **xff**、**cdn-src-ip**、**x-real-ip**、**tcp-option**。

本命令仅在真实源 IP 地址提取模式为 **priority** 时生效。

1.12.3 开启真实源 IP 地址复用功能

1. 功能简介

当一个会话中存在多个请求报文时，设备会对会话内的每个请求报文都进行真实源 IP 地址的提取，并分别记录提取结果。缺省情况下，若某个请求报文中未提取到真实源 IP 地址时，则认为该报文的真实源 IP 地址为空。在某些代理场景下，代理服务器只在每个会话的第一个 HTTP 请求报文中携带真实源 IP 地址，这样会导致设备只能提取到第一个报文中的真实源 IP 地址，后续请求报文则无法提取，将会对 IPS 白名单等业务造成影响。如下图所示：



在上述场景中，Host 向 Web Server 发起了 3 个请求，经过 Proxy Server 代理后，只有请求 1 中携带了 Host 的 IP 地址。设备提取到了请求 1 中的真实源 IP 地址 IP1，并将其与 IPS 白名单进行匹配，匹配成功并放行该报文。对于请求 2 和请求 3，由于设备没有提取到真实源 IP 地址，IPS 白名单将匹配失败。此时，管理员可以通过开启真实源 IP 地址功能解决上述问题。开启真实源 IP 地址复用功能后，当设备在请求 2 中提取不到真实源 IP 地址时，会沿用请求 1 提取到的 IP1 作为本次提取结果，这样即可与 IPS 白名单匹配成功。请求 3 同理。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启真实源 IP 地址复用功能。

```
inspect real-ip reuse enable
```

缺省情况下，真实源 IP 地址复用功能处于关闭状态。

1.12.4 配置 X-Forwarded-For 字段检测结果的提取位置

1. 功能简介

在客户端通过 HTTP 代理连接到 Web 服务器的场景中，HTTP 报文的首部可能会携带 X-Forwarded-For 字段。X-Forwarded-For 字段中携带多个地址，标准的格式为 X-Forwarded-For: <client>, <proxy1>, <proxy2>, ... <proxyn>。如果一个报文通过多个代理，则会列出每个代理服务器的 IP 地址。即，最右边（tail）的 proxyn 是最新的代理服务器的 IP 地址，最左边（head）的 client 是原始客户端的 IP 地址。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 X-Forwarded-For 字段检测结果的提取位置。

```
inspect real-ip detect-field xff { head | tail [ number ] }
```

缺省情况下，X-Forwarded-For 字段的提取位置为最后一项。

1.12.5 配置 TCP Option 字段的检测参数

1. 功能简介

当通过检测 TCP Option 字段获取真实源 IP 地址时，首先需要找到一个特定的标志，再基于此标志去获取源 IP 地址。

需要配置的检测参数如下：

- 标志内容 (**hex** *hex-vector*)：TCP Option 字段中，真实源 IP 地址位于一个“标志”的后面，只有检测到标志，设备才会继续向后检测真实源 IP 地址。如果没有检测到标志，则表示不存在真实源 IP 地址，设备会停止对 TCP Option 字段的检测。
- 标志内容的检测范围：包括偏移量 (**offset** *offset-value*) 和检测深度 (**depth** *depth-value*)。偏移量确定了检测的起始位置（从 TCP Option 字段起始位置开始的偏移量），检测深度确定了检测的终止位置。
- 真实源 IP 地址与标志的偏移量 (**ip-offset** *ip-offset-value*)：即检测真实源 IP 地址的起始位置。

2. 配置限制和指导

开启真实源 IP 地址提取功能后，设备默认不从 TCP Option 字段提取真实源 IP 地址，仅在配置 TCP Option 检测参数后才开始检测 TCP Option 字段。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置 TCP Option 字段的检测参数。

```
inspect real-ip detect-field tcp-option hex hex-vector [ offset  
offset-value ] [ depth depth-value ] [ ip-offset ip-offset-value ]
```

缺省情况下，未配置 TCP Option 字段的检测参数，设备不从 TCP Option 字段获取真实源 IP 地址。

1.13 关闭应用层检测引擎功能

1.13.1 关闭应用层检测引擎所有检测功能

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。

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。



注意

关闭应用层检测引擎功能后，系统将不会对接收到的报文进行 DPI 深度安全处理。可能导致其他基于 DPI 功能的业务出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.13.2 关闭应用层检测引擎对指定协议报文的检测功能

1. 功能简介

在如下场景中管理员可能需要关闭应用层检测引擎对指定协议报文的检测功能。

- 场景一：当组网环境中不需要对某些协议的报文进行检测时，可以关闭应用层检测引擎对该协议报文的检测，以减少对设备资源的占用，提升设备性能。
- 场景二：当应用层检测引擎对某个协议报文的检测导致设备出现异常并重启的情况时，可单独关闭引擎对该协议报文的检测功能，避免由于再次检测该协议报文导致设备反复重启的问题，同时又不影响引擎对其他协议报文的检测。

设备支持如下两种方式关闭应用层检测引擎对指定协议报文的检测功能：

- 手动关闭：此方式要求管理员已知需要关闭哪些协议报文的检测功能，适用于场景一和场景二。
- 自动关闭：此方式由设备自动判断需要关闭哪些协议报文的检测功能，适用于场景二。使用此方式后，如果应用层检测引擎对某个协议报文的检测导致设备出现异常并重启的情况时，则当系统重启后，应用层检测引擎将自动关闭对该协议报文的检测功能，跳过对此协议报文的处理。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 关闭应用层检测引擎对指定协议报文的检测功能。

- 手工关闭应用层检测引擎对指定协议报文的检测功能。

```
inspect bypass protocol { dns | ftp | ftp-data | http | https | imap  
| nfs | pop3 | rtmp | sip | smb | smtp | telnet | tftp } *
```

缺省情况下，应用层检测引擎对所有支持的协议都进行检测。

- 自动关闭应用层检测引擎对指定协议报文的检测功能。

```
inspect auto-bypass enable
```

缺省情况下，应用层检测引擎自动关闭指定协议报文的检测功能处于关闭状态。

1.14 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
显示MD5哈希运算配置	display inspect md5-verify configuration

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	1-4
1.4 vSystem 相关说明	1-4
1.5 IPS 配置任务简介	1-4
1.6 配置 IPS 策略	1-5
1.6.1 创建 IPS 策略	1-5
1.6.2 配置筛选 IPS 特征的属性	1-5
1.6.3 配置 IPS 特征库版本基线	1-6
1.6.4 配置 IPS 动作	1-6
1.6.5 配置 IPS 动作参数	1-8
1.7 在 DPI 应用 profile 中引用 IPS 策略	1-9
1.8 激活 IPS 策略配置	1-9
1.9 在安全策略中引用 DPI 应用 profile	1-10
1.10 在对象策略中引用 DPI 应用 profile	1-10
1.11 配置 IPS 特征库升级和回滚	1-11
1.11.1 配置限制和指导	1-11
1.11.2 配置定期自动在线升级 IPS 特征库	1-11
1.11.3 立即自动在线升级 IPS 特征库	1-12
1.11.4 手动离线升级 IPS 特征库	1-12
1.11.5 回滚 IPS 特征库	1-13
1.11.6 开启 IPS 特征库更新日志功能	1-13
1.12 导入和删除 Snort 特征	1-13
1.12.1 导入 Snort 特征	1-13
1.12.2 删除所有导入的 Snort 特征	1-14
1.13 配置自定义 IPS 特征	1-14
1.13.1 创建自定义 IPS 特征	1-14
1.13.2 配置自定义 IPS 特征属性	1-14

1.13.3 配置自定义 IPS 特征规则.....	1-15
1.14 配置 IPS 特征命中统计功能.....	1-17
1.15 配置 IPS 白名单.....	1-17
1.16 IPS 显示和维护.....	1-18
1.17 IPS 典型配置举例	1-18
1.17.1 在安全策略中引用缺省 IPS 策略配置举例	1-18
1.17.2 在安全策略中引用自定义 IPS 策略配置举例	1-20
1.17.3 手动离线升级 IPS 特征库配置举例	1-22
1.17.4 定时自动升级 IPS 特征库配置举例	1-25
1.17.5 在对象策略中引用缺省 IPS 策略配置举例	1-27
1.17.6 在对象策略中引用自定义 IPS 策略配置举例	1-28
1.17.7 手动离线升级 IPS 特征库配置举例	1-30
1.17.8 定时自动升级 IPS 特征库配置举例	1-32

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、严重级别和方向等。这些属性可作为过滤条件来筛选 IPS 特征，只有筛选出的特征才能与报文进行匹配。

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：包括 Snort 文件导入的 Snort 特征和用户手工配置的自定义特征。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：

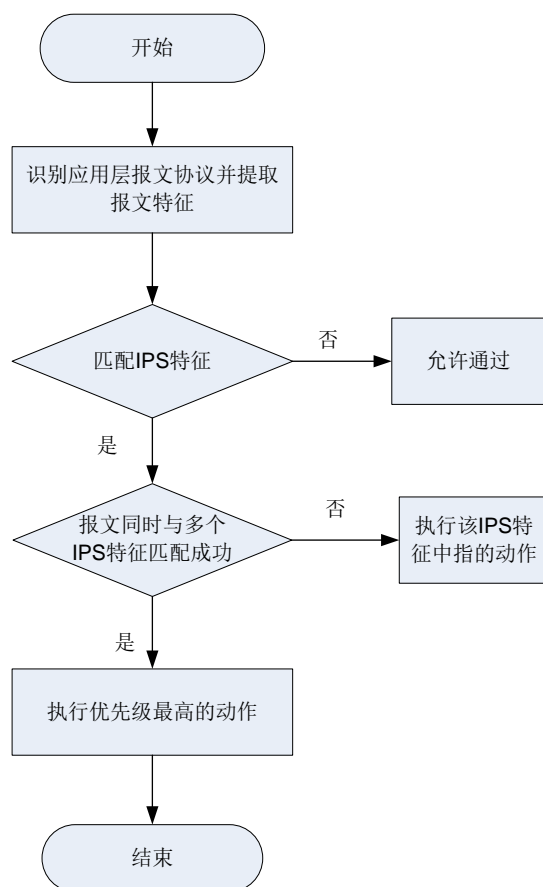
- 重置：通过发送 TCP 的 reset 报文断开 TCP 连接。
- 重定向：把符合特征的报文重定向到指定的 Web 页面上。

- 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，并在安全策略和对象策略中引用 DPI 应用 profile 来实现的，IPS 处理的具体实现流程如下：

- (1) 设备识别应用层报文协议，并提取报文特征。
- (2) 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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06	Blade VI 防火墙业务板	支持

M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10		
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.3 IPS的License要求

IPS 功能需要购买并正确安装 License 后才能使用。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，但无法将特征库升级到 License 过期后官网发布的特征库版本。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.4 vSystem相关说明

非缺省 vSystem 不支持本特性部分功能，具体包括：

- 配置 IPS 特征库升级和回滚
- 配置自定义 IPS 特征
- 配置 IPS 白名单



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.5 IPS配置任务简介

IPS 配置任务如下：

- (1) [配置 IPS 策略](#)
- (2) [在 DPI 应用 profile 中引用 IPS 策略](#)
- (3) （可选）[激活 IPS 策略配置](#)
- (4) 引用 DPI 应用 profile
请选择以下一项任务进行配置：
 - [在安全策略中引用 DPI 应用 profile](#)
 - [在对象策略中引用 DPI 应用 profile](#)
- (5) [配置 IPS 特征库升级和回滚](#)
- (6) （可选）[导入和删除 Snort 特征](#)
- (7) （可选）[配置自定义 IPS 特征](#)
- (8) （可选）[配置 IPS 特征命中统计功能](#)
- (9) （可选）[配置 IPS 白名单](#)

1.6 配置IPS策略

1.6.1 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。

1.6.2 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。

- 配置筛选 IPS 特征的推荐状态属性。

status { disabled | enabled } *

缺省情况下，IPS 策略匹配所有缺省推荐和不推荐使用的特征。

特征的推荐状态属性用于标识特征库中缺省是否推荐使用该特征匹配报文。推荐状态为 **enabled** 时，表示缺省推荐使用该特征；推荐状态为 **disabled** 时，表示缺省不推荐使用该特征。

1.6.3 配置 IPS 特征库版本基线

1. 功能简介

当管理员升级 IPS 特征库后，希望将某个版本之后新增的特征筛选出来，置为非生效状态（即不用于匹配报文）时，可通过本功能将该版本设置为基线版本，IPS 策略会将所有在基线版本之上新增的特征设置为非生效状态，仅使用基线版本的特征与报文进行匹配。

本功能可帮助用户快速筛选出基线版本与当前版本之间有差异的特征，IPS 策略将使用基线版本的特征与报文进行匹配，而不必回滚至基线版本的特征库。

配置本功能后，如果希望将某个非生效状态的特征调整为生效状态、且其它特征状态保持不变时，需要进行如下操作：

- (1) 再次执行本命令，将基线版本调整至该特征所属的特征库版本。
- (2) 在设备的 Web 界面上，查看其它非生效状态的特征 ID。
- (3) 执行 **signature override** 命令，将仍然需要保持非生效状态的特征禁用。

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 特征库版本基线。

signature version-baseline *version-number*

缺省情况下，未配置 IPS 特征库版本基线。

1.6.4 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. 配置限制和指导

当动作配置为 **logging** 时，设备将记录日志并支持如下两种方式输出日志。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

日志信息中，真实源 MAC 地址（RealSrcMacAddr）和真实源目的 MAC 地址（RealDstMacAddr）字段仅当开启跨三层 MAC 地址学习功能后显示取值。有关跨三层 MAC 地址学习功能的详细介绍，请参见“基础配置指导”中的“跨三层 MAC 地址学习”。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

3. 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。

- (5) （可选）修改 IPS 策略中指定特征的严重级别。

```
signature override { pre-defined | user-defined } signature-id severity  
{ critical | high | low | medium }
```

缺省情况下，预定义 IPS 特征使用系统预定义的严重级别。自定义 IPS 特征中，用户手工配置的自定义特征的严重级别在创建时已指定；Snort 特征的严重级别在导入的 Snort 文件中定义。

- (6) 退回系统视图。

```
quit
```

- (7) （可选）配置 IPS 捕获报文时缓存的报文数量。

```
ips capture-cache number
```

缺省情况下，缓存的报文数量为 1，即仅缓存命中报文。

当 IPS 捕获报文时，会缓存命中报文及其前后的报文，方便用户分析威胁信息。当报文缓存结束后，设备会将所有缓存报文写入 IPS 捕获文件中。仅当设备上正确安装了硬盘或 U 盘后，用户才可以到 Web 界面的“威胁日志”页面中下载捕获文件。

1.6.5 配置 IPS 动作参数

1. 功能简介

IPS 动作中，源阻断、捕获和日志仅在配置参数后生效，参数可通过如下方式配置：

- 配置全局动作参数：通过在系统视图下配置 IPS 引用应用层检测引擎动作参数 **profile** 实现，该方式配置的动作参数对所有 IPS 策略均生效。
- 配置策略动作参数：直接在各个 IPS 策略视图下单独配置各动作的执行参数。目前仅支持配置日志动作参数。

2. 配置限制和指导

- 如果 IPS 策略视图下既配置了全局动作参数，又配置了策略动作参数，则以全局动作参数为准。
- 如果需要使策略动作参数生效，则必须保证全局动作参数处于未使能状态。
- 建议在完成全局动作参数的配置之后，再使能全局动作参数。

3. 配置全局动作参数

- (1) 进入系统视图。

```
system-view
```

- (2) 配置全局动作参数。

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

缺省情况下，未配置全局动作参数。

引用的动作参数 **profile** 由应用层检测引擎动作参数 **profile** 提供。如果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。有关应用层检测引擎动作参数 **profile** 的具体配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

4. 配置策略动作参数

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IPS 策略视图。

```
ips policy policy-name
```

- (3) 配置日志动作参数。

```
log { email | syslog }
```

缺省情况下，IPS 日志输出方式为 **syslog**。

- (4) （可选）配置允许以邮件方式输出日志的最低严重级别。

```
email severity-level { critical | high | low | medium }
```

缺省情况下，允许以邮件方式输出日志的最低严重级别为 **low**。

本命令仅当 IPS 日志输出方式为 **email** 时生效。仅当报文命中的 IPS 特征的严重级别不低于本命令配置的最低严重级别时，设备才会将生成的 IPS 日志以邮件方式发送。

- (5) （可选）引用邮件动作参数 **profile**。

email parameter-profile *parameter-profile-name*

缺省情况下，未引用邮件动作参数 **profile**。

仅当 IPS 日志输出方式为 **email** 时需要配置本命令。

引用的邮件动作参数 **profile** 由应用层检测引擎邮件动作参数 **profile** 提供。有关应用层检测引擎邮件动作参数 **profile** 的具体配置请参见“DPI 深度安全命令参考”中的“应用层检测引擎”。

- (6) 去使能全局动作参数。

undo global-parameter enable

缺省情况下，全局动作参数处于使能状态。

1.7 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。

1.8 激活IPS策略配置

1. 功能简介

缺省情况下，当 IPS 策略发生配置变更时（即被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对变更的配置立即进行激活，可执行 **inspect activate** 命令手工激活，使配置立即生效。

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”。

2. 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、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.9 在安全策略中引用DPI应用profile

- (1) 进入系统视图。

```
system-view
```

- (2) 进入安全策略视图。

```
security-policy { ip | ipv6 }
```

- (3) 进入安全策略规则视图。

```
rule { rule-id | [ rule-id ] name rule-name }
```

- (4) 配置安全策略规则的动作作为允许。

```
action pass
```

缺省情况下，安全策略规则动作是丢弃。

- (5) 配置安全策略规则引用 DPI 应用 profile。

```
profile app-profile-name
```

缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.10 在对象策略中引用DPI应用profile

- (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。

1.11 配置IPS特征库升级和回滚

1.11.1 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”。
- 同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.11.2 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。

1.11.3 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
```

1.11.4 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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 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 [ vpn-instance  
vpn-instance-name ] [ source { ip | ipv6 } { ip-address | interface  
interface-type interface-number } ]
```

1.11.5 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，再执行回滚到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 }
```

1.11.6 开启 IPS 特征库更新日志功能

1. 功能简介

开启本功能后，当 IPS 特征库升级或回滚成功时，设备将记录特征库变更的时间，并在每日按照配置的时间发送日志。

2. 配置限制和指导

目前，仅支持以快速日志方式发送 IPS 特征库更新日志，配置本功能后，还需要配置 IPS 快速日志使用国家电网格式（即配置 `customlog format dpi ips sgcc` 命令）并允许设备向指定的日志主机发送 IPS 模块的日志（即配置 `customlog host` 命令）。有关快速日志输出功能的详细介绍，请参见“网络管理和监控命令参考”中的“快速日志输出”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 IPS 特征库更新日志记录功能并配置每日发送日志的时间。

```
ips signature update-log send-time time
```

1.12 导入和删除 Snort 特征

1.12.1 导入 Snort 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 Snort 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
```

1.12.2 删除所有导入的 Snort 特征

- (1) 进入系统视图。

```
system-view
```

- (2) 删除导入的所有 Snort 特征。

```
ips signature remove snort
```

1.13 配置自定义IPS特征

1.13.1 创建自定义 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，可通过手工配置方式自定义创建所需的 IPS 特征。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建自定义 IPS 特征，并进入自定义 IPS 特征视图。

```
ips signature user-defined name signature-name
```

缺省情况下，不存在自定义 IPS 特征。

- (3) （可选）配置自定义 IPS 特征的描述信息。

```
description text
```

1.13.2 配置自定义 IPS 特征属性

1. 功能简介

特征具有多种属性，包括动作、检测方向、严重级别和特征下规则间的逻辑关系。

一个自定义特征下可以配置多条规则作为特征的匹配条件，如果规则间是逻辑与的关系，报文需要匹配该自定义特征的所有规则才结束匹配过程；如果规则间是逻辑或的关系，一旦报文与某条规则匹配成功就结束此匹配过程。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入自定义 IPS 特征视图。

ips signature user-defined name *signature-name*

缺省情况下，不存在自定义 IPS 特征。

- (3) 配置自定义 IPS 特征属性。

- 配置自定义 IPS 特征的动作。

action { **block-source** | **drop** | **permit** | **reset** } [**capture** | **logging**]
*

缺省情况下，自定义 IPS 特征的动作作为 **permit**。

- 配置自定义 IPS 特征的检测方向。

direction { **any** | **to-client** | **to-server** }

缺省情况下，自定义 IPS 特征的检测方向为 **any**。

- 配置自定义 IPS 特征的严重级别。

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

缺省情况下，自定义 IPS 特征的严重级别为 **low**。

- 配置自定义 IPS 特征下规则间的逻辑关系。

rule-logic { **and** | **or** }

缺省情况下，自定义 IPS 特征下规则间的逻辑关系为 **or**。

1.13.3 配置自定义 IPS 特征规则

1. 功能简介

设备支持以下两种类型自定义 IPS 特征规则：

- 关键字类型
- 数值类型

规则下可以配置匹配条件以及检查项。仅当报文与规则的匹配条件匹配成功后，才会对规则的检查项进行检测。

一条规则可以配多个检查项，用于精确匹配报文中所需检测的内容。检查项之间为逻辑与的关系，匹配顺序为配置顺序，只有所有检查项都匹配成功，规则才算成功匹配。

触发检查项是同一规则下检查项的触发条件，只有关键字类型自定义特征规则才需要配置触发检查项。如果一条规则的触发检查项匹配失败，则该规则匹配失败，不会再对该规则下的检查项进行检测。

2. 配置限制和指导

- 检查项仅检测指定协议字段范围内的数据。
- 配置检查项匹配的协议字段时，建议依据 HTTP 协议中各协议字段顺序进行配置，否则可能会影响设备的检测结果。
- 对于关键字类型的自定义特征规则，在配置检查项之前，必须先配置触发检查项。删除触发检查项后，将一并删除所有的检查项。

- 可使用偏移量、检测深度或者相对偏移量、相对检测深度两组参数精确定位检测的起始和终止位置。其中，偏移量、检测深度和相对偏移量、相对检测深度两组参数只可配置一组。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入自定义 IPS 特征视图。

```
ips signature user-defined name signature-name
```

- (3) 创建自定义 IPS 特征规则，并进入自定义 IPS 特征规则视图。

```
rule rule-id l4-protocol l4-protocol-name l5-protocol l5-protocol-name  
pattern-type { keyword | integer }
```

缺省情况下，不存在自定义 IPS 特征规则。

- (4) 配置自定义 IPS 特征规则的匹配条件。

- 配置自定义 IPS 特征规则匹配的源 IP 地址。

```
source-address ip ip-address
```

缺省情况下，自定义 IPS 特征规则匹配所有源 IP 地址。

- 配置自定义 IPS 特征规则匹配的的目的 IP 地址。

```
destination-address ip ip-address
```

缺省情况下，自定义 IPS 特征规则匹配所有目的 IP 地址。

- 配置自定义 IPS 特征规则匹配的源端口。

```
source-port start-port [ to end-port ]
```

缺省情况下，自定义 IPS 特征规则匹配所有源端口。

- 配置自定义 IPS 特征规则匹配的的目的端口。

```
destination-port start-port [ to end-port ]
```

缺省情况下，自定义 IPS 特征规则匹配所有目的端口。

- 配置自定义 IPS 特征规则匹配的 HTTP 报文请求方法。

```
http-method method-name
```

缺省情况下，自定义 IPS 特征规则匹配所有 HTTP 报文请求方法。

- (5) 配置关键字类型自定义 IPS 特征规则的触发检查项和检查项。

- 配置触发检查项。

```
trigger field field-name include { hex hex-string | text text-string }  
[ offset offset-value ] [ depth depth-value ]
```

- 配置检查项。

```
detection-keyword detection-id field field-name match-type { exclude  
| include } { hex hex-string | regex regex-pattern | text text-string }  
[ offset offset-value [ depth depth-value ] | relative-offset  
relative-offset-value [ relative-depth relative-depth-value ] ]
```

- (6) 配置数值类型自定义 IPS 特征规则的检查项。

```
detection-integer field field-name match-type { eq | gt | gt-eq | lt |  
lt-eq | nequ } number
```

1.14 配置IPS特征命中统计功能

1. 功能简介

本功能用于统计 IPS 策略中每个特征的命中次数，管理员可在设备的 Web 界面查看统计数据。

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) 开启 IPS 特征命中统计功能。

```
statistics signature-hit enable
```

缺省情况下，IPS 特征命中统计功能处于关闭状态。

1.15 配置IPS白名单

1. 功能简介

当用户通过查看 IPS 日志发现存在误报的情况时，可配置 IPS 白名单功能，将日志中获取到的特征 ID、URL 和源 IP 地址加入白名单，设备将放行匹配白名单的报文，降低误报率。

当白名单表项中同时存在特征 ID、URL 和源 IP 地址中的两者或以上时，需要同时匹配才认为匹配成功。

2. 配置限制和指导

如果设备中开启了真实源 IP 地址提取功能（即执行了 **inspect real-ip enable** 命令），则当设备提取到了真实源 IP 地址后，会使用真实源 IP 地址与白名单中的源 IP 地址进行匹配；如果未提取到真实源 IP 地址，则使用报文的源 IP 地址与白名单中的源 IP 地址进行匹配。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 IPS 白名单功能。

```
ips whitelist enable
```

缺省情况下，IPS 白名单功能处于关闭状态。

- (3) 创建并进入 IPS 白名单表项视图。

```
ips whitelist entry-id
```

- (4) 配置 IPS 白名单描述信息。

```
description text
```

缺省情况下，未配置 IPS 白名单描述信息。

- (5) 向 IPS 白名单表项中添加匹配信息。请至少选择其中一项进行配置。

- 向 IPS 白名单表项中添加特征 ID。

```
signature-id sig-id
```

缺省情况下，IPS 白名单表项中不存在特征 ID。

- 向 IPS 白名单表项中添加 URL。

```
url match-type { accurate | substring } url-text
```

缺省情况下，IPS 白名单表项不存在 URL。

- 向 IPS 白名单表项中添加源 IP。

```
source-address { ip ipv4-address | ipv6 ipv6-address }
```

缺省情况下，IPS 白名单表项不存在源 IP 地址。

- (6) 退回到系统视图。

```
quit
```

- (7) 激活 IPS 白名单配置。

```
ips whitelist activate
```

当创建、修改和删除含有 URL 的 IPS 白名单后，需要执行本命令使其生效。

1.16 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 <i>policy-name</i>
显示IPS特征库版本信息	display ips signature library
显示IPS特征属性列表	display ips signature [pre-defined user-defined { snort user-config }] [direction { any to-client to-server }] [category <i>category-name</i> fidelity { high low medium } protocol { icmp ip tcp udp } severity { critical high low medium }] *
显示指定预定义IPS特征的详细属性	display ips signature pre-defined <i>signature-id</i>
显示指定自定义IPS特征的详细属性	display ips signature user-defined { snort user-config } <i>signature-id</i>
显示IPS自定义特征解析失败的信息	display ips signature user-defined parse-failed

1.17 IPS典型配置举例

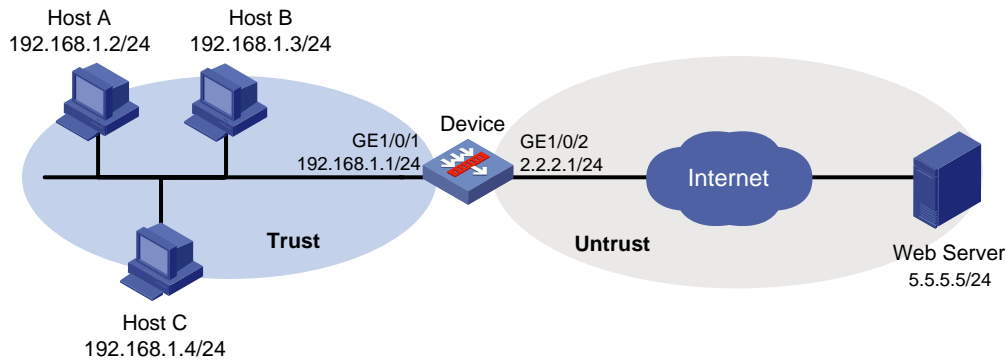
1.17.1 在安全策略中引用缺省 IPS 策略配置举例

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 在安全策略中引用缺省 IPS 策略配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 DPI 应用 profile 并激活 IPS 策略配置

创建名为 sec 的 DPI 应用 profile，在 sec 中引用名称为 default 的缺省 IPS 策略，并指定该 IPS 策略的模式为 protect。

```
[Device] app-profile sec
[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) 配置安全策略

配置名称为 **trust-untrust** 的安全策略规则,使内网用户可以访问外网,并对交互报文进行 IPS 防御。具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name trust-untrust
```

```
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
```

```
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
```

```
[Device-security-policy-ip-10-trust-untrust] action pass
```

```
[Device-security-policy-ip-10-trust-untrust] profile sec
```

```
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
```

```
[Device-security-policy-ip] 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-2014-7187) 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。

1.17.2 在安全策略中引用自定义 IPS 策略配置举例

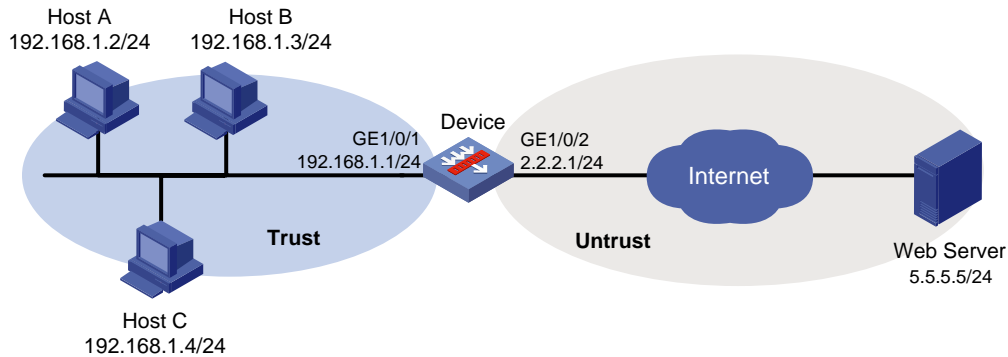
1. 组网需求

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 在安全策略中引用自定义 IPS 策略配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 IPS 策略

创建一个名称为 ips1 的 IPS 策略，配置 IPS 策略保护所有对象、启用编号为 2 的预定义 IPS 特征，并配置动作为丢弃、捕获报文并记录日志、禁用编号为 4 的预定义 IPS 特征、启用编号为 6 的预定义 IPS 特征。

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

```
[Device-ips-policy-ips1] protect-target all
[Device-ips-policy-ips1] signature override pre-defined 2 enable drop capture logging
[Device-ips-policy-ips1] signature override pre-defined 4 disable
[Device-ips-policy-ips1] signature override pre-defined 6 enable
[Device-ips-policy-ips1] quit
```

(5) 配置 DPI 应用 profile 并激活 IPS 策略配置

创建名为 sec 的 DPI 应用 profile，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
[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) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 IPS 检测。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] 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。

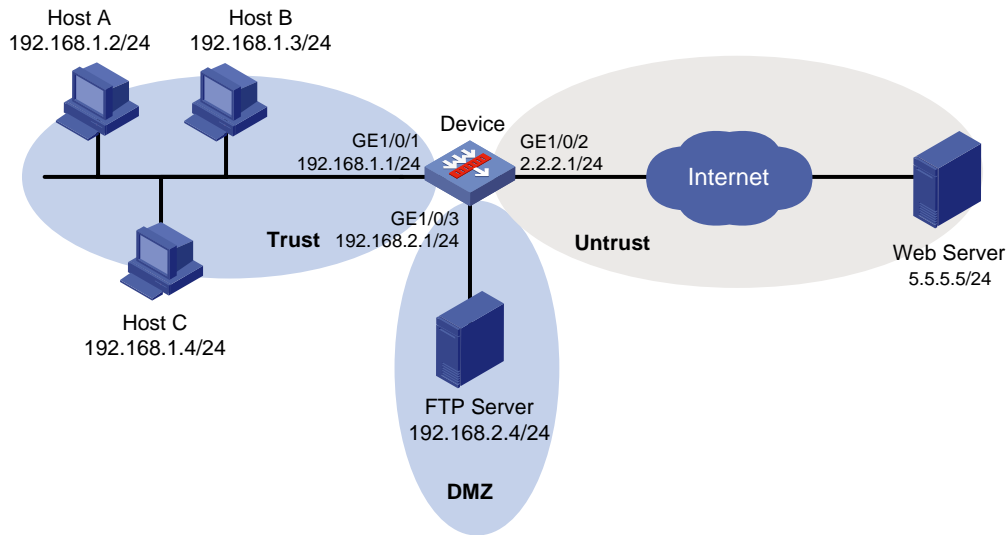
1.17.3 手动离线升级 IPS 特征库配置举例

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。现需要手动离线升级 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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

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

(4) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Trust 到 DMZ 安全域的流量，使内网用户可以访问 DMZ 安全域中的服务器

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-dmz
[Device-security-policy-ip-11-trust-dmz] source-zone trust
[Device-security-policy-ip-11-trust-dmz] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-11-trust-dmz] destination-zone dmz
[Device-security-policy-ip-11-trust-dmz] action pass
[Device-security-policy-ip-11-trust-dmz] quit
```

- 配置安全策略规则放行设备与 FTP 服务器之间的流量，使设备可以访问 FTP 服务器，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name ftplocalout
[Device-security-policy-ip-12-ftplocalout] source-zone local
[Device-security-policy-ip-12-ftplocalout] destination-zone dmz
[Device-security-policy-ip-12-ftplocalout] destination-ip-subnet 192.168.2.0 24
[Device-security-policy-ip-12-ftplocalout] application ftp
[Device-security-policy-ip-12-ftplocalout] application ftp-data
[Device-security-policy-ip-12-ftplocalout] action pass
[Device-security-policy-ip-12-ftplocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 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 library** 命令查看当前特征库的版本信息。

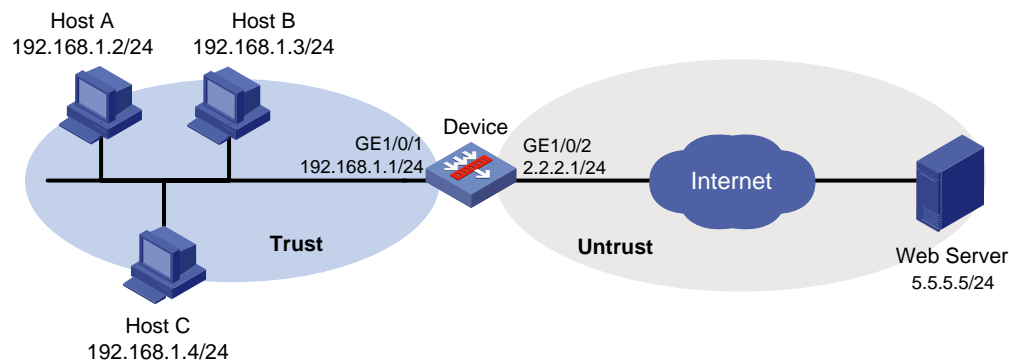
1.17.4 定时自动升级 IPS 特征库配置举例

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，开始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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

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

(4) 配置 DNS 服务器地址

指定 DNS 服务器的 IP 地址为 10.72.66.36，确保 Device 可以获取到官网的 IP 地址，具体配置步骤如下。

```
[Device] dns server 10.72.66.36
```

(5) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Local 到 Untrust 安全域的流量，使设备可以访问官网的特征库服务专区，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-11-downloadlocalout] source-zone local
[Device-security-policy-ip-11-downloadlocalout] destination-zone untrust
[Device-security-policy-ip-11-downloadlocalout] action pass
[Device-security-policy-ip-11-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(6) 配置定期自动在线升级 IPS 特征库

设置定时自动升级 IPS 特征库计划为：每周六上午 9:00:00 前后 30 分钟内开始自动在线升级。

```
[Device] ips signature auto-update
[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 library** 命令查看当前特征库的版本信息。

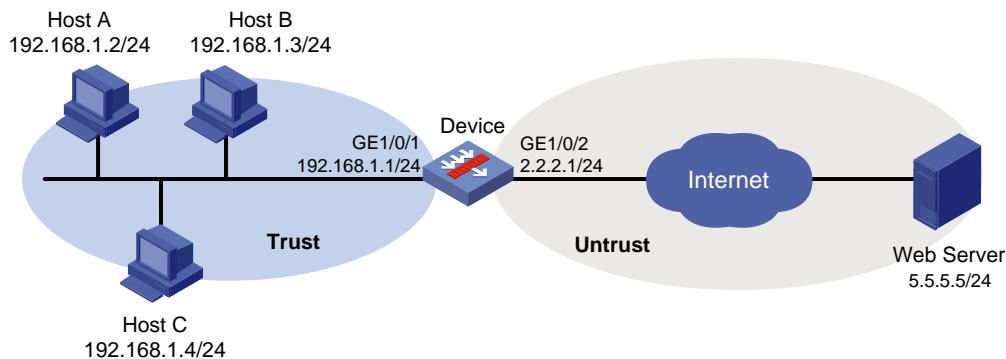
1.17.5 在对象策略中引用缺省 IPS 策略配置举例

1. 组网需求

如图 1-6 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1-6 在对象策略中引用缺省 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 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-2014-7187) 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。

1.17.6 在对象策略中引用自定义 IPS 策略配置举例

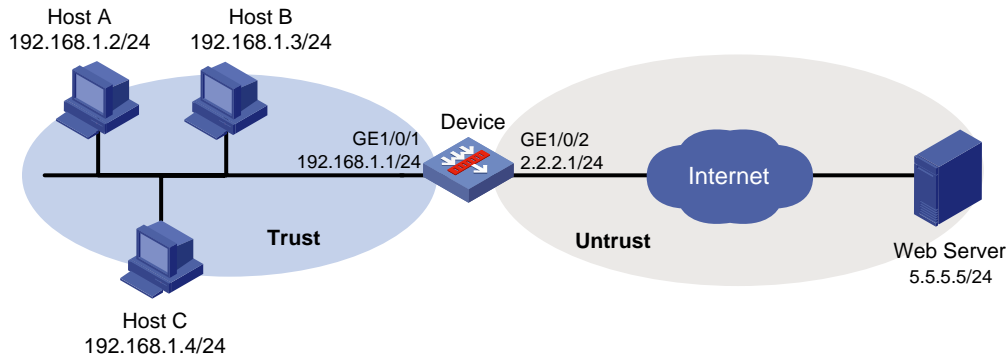
1. 组网需求

如图 1-7 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1-7 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。

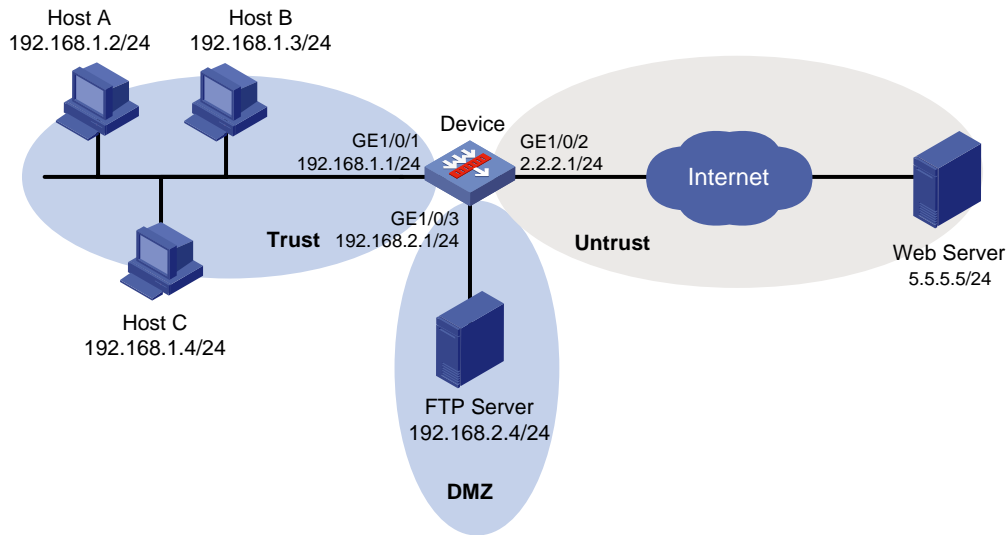
1.17.7 手动离线升级 IPS 特征库配置举例

1. 组网需求

如图 1-8 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1-8 基于对象策略手动离线升级 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 library** 命令查看当前特征库的版本信息。

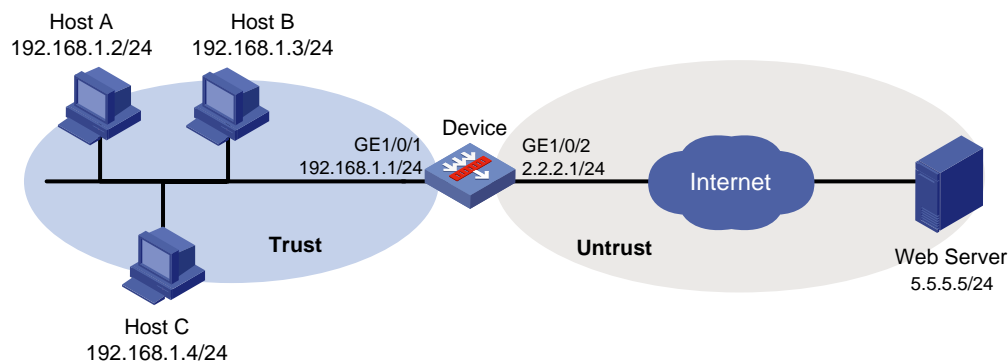
1.17.8 定时自动升级 IPS 特征库配置举例

1. 组网需求

如图 1-9 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1-9 基于对象策略定时自动升级 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 library** 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 信誉	1-2
1.1.5 URL 过滤黑/白名单规则.....	1-2
1.1.6 URL 过滤策略	1-3
1.1.7 URL 过滤实现流程.....	1-3
1.1.8 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.....	1-5
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 配置 URL 过滤分类.....	1-6
1.6 配置 URL 过滤分类云端查询	1-7
1.7 配置 URL 过滤策略.....	1-7
1.7.1 配置任务简介	1-7
1.7.2 基于 URL 过滤分类实现 URL 过滤功能	1-8
1.7.3 基于 URL 过滤白名单实现 URL 过滤功能.....	1-9
1.8 复制 URL 过滤策略或分类.....	1-10
1.8.1 复制 URL 过滤策略	1-10
1.8.2 复制 URL 过滤分类	1-10
1.9 在 URL 过滤策略中引用 URL 过滤告警动作参数 profile.....	1-10
1.10 在 DPI 应用 profile 中引用 URL 过滤策略.....	1-11
1.11 激活 URL 过滤的策略和规则配置	1-11
1.12 在安全策略中引用 URL 过滤业务	1-12
1.13 在对象策略中引用 URL 过滤业务	1-12
1.14 配置 URL 过滤特征库升级和回滚	1-13
1.14.1 配置限制和指导	1-13
1.14.2 配置定期自动在线升级 URL 过滤特征库	1-13
1.14.3 立即自动在线升级 URL 过滤特征库.....	1-13
1.14.4 手动离线升级 URL 过滤特征库	1-14
1.14.5 回滚 URL 过滤特征库	1-14

1.15 配置 URL 信誉特征库升级和回滚	1-15
1.15.1 配置限制和指导	1-15
1.15.2 配置定期自动在线升级 URL 信誉特征库	1-15
1.15.3 立即自动在线升级 URL 信誉特征库	1-16
1.15.4 手动离线升级 URL 信誉特征库	1-16
1.15.5 回滚 URL 信誉特征库	1-17
1.16 开启应用层检测引擎日志信息功能	1-17
1.17 配置 URL 过滤日志信息筛选功能	1-17
1.17.1 功能简介	1-17
1.17.2 配置 URL 过滤仅对网站根目录下资源的访问进行日志记录	1-18
1.17.3 配置 URL 过滤对指定类型网页资源的访问不进行日志记录	1-18
1.18 开启 URL 加速审计功能	1-18
1.19 开启 HTTPS 流量过滤功能	1-19
1.20 URL 过滤显示和维护	1-19
1.21 URL 过滤典型配置举例	1-20
1.21.1 在安全策略中引用 URL 过滤业务配置举例	1-20
1.21.2 手动离线升级 URL 过滤特征库配置举例	1-22
1.21.3 定期自动在线升级 URL 过滤特征库配置举例	1-25
1.21.4 在对象策略中引用 URL 过滤业务配置举例	1-27
1.21.5 手动离线升级 URL 过滤特征库配置举例	1-29
1.21.6 定期自动在线升级 URL 过滤特征库配置举例	1-30

1 URL 过滤

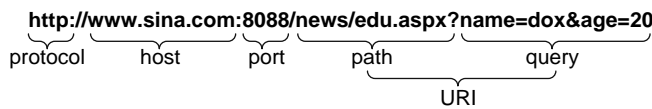
1.1 URL过滤简介

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。

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 信誉

URL 信誉功能用于对恶意的 URL 进行过滤，允许或禁止用户访问某些网站，达到规范用户上网行为的目的。当报文中的 URL 匹配到 URL 信誉特征库中的 URL 后，设备将对报文执行相应的操作。URL 信誉特征库主要是一些恶意 URL 的集合，包含每个 URL 所属的攻击类型等信息。

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 过滤策略

一个 URL 过滤策略中可以配置如下内容：

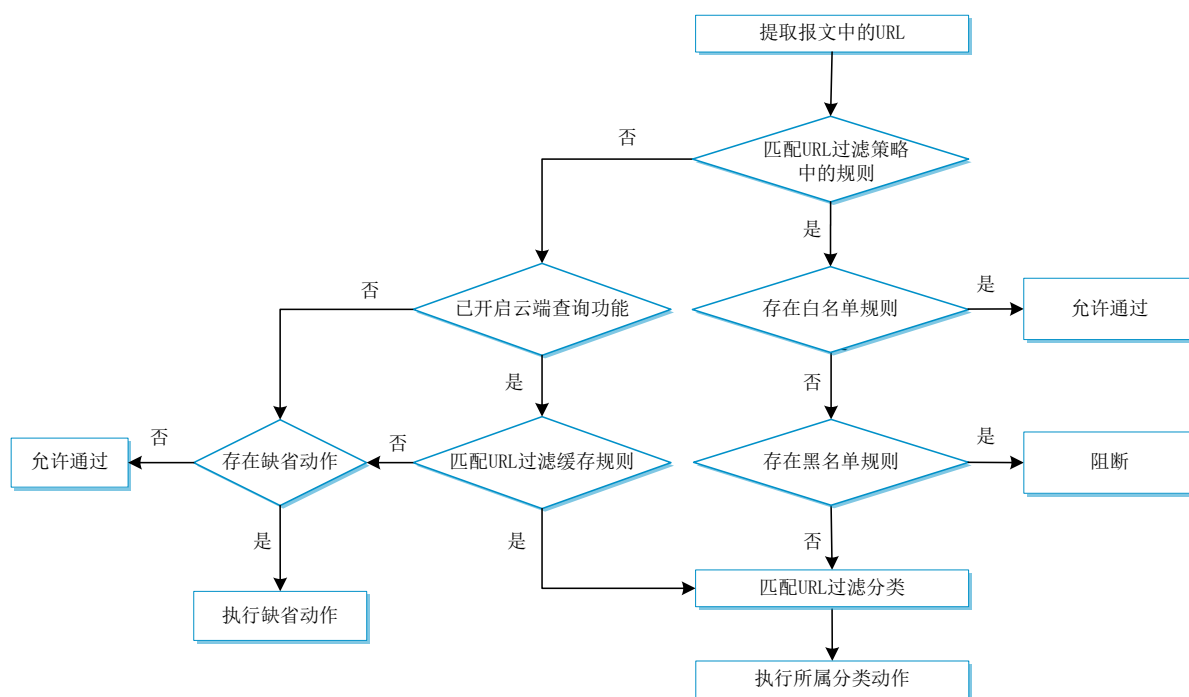
- URL 过滤分类及其处理动作。其中，处理动作包括：丢弃、允许、阻断、重置、重定向和生成日志。
- URL 过滤黑/白名单规则。
- URL 信誉功能。
- URL 过滤分类云端查询功能。

以及对于未匹配到 URL 过滤策略（包括 URL 过滤分类、URL 过滤黑/白名单和 URL 信誉）时，设备对报文执行的缺省动作。

1.1.7 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，并在安全策略或对象策略中引用 DPI 应用 profile 来实现的，URL 过滤实现流程如下：

(1) 设备对报文进行规则（即安全策略规则或对象策略规则）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。

有关安全策略的详细介绍请参见“安全配置指导”中的“安全策略”；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”。

- (2) 设备提取报文中的 URL，并将其与 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。
- (3) 首先判断匹配的规则中是否存在 URL 过滤黑/白名单规则，如果存在白名单规则，设备将直接允许此报文通过；如果不存在白名单规则，则继续判断是否存在黑名单规则，如果存在，则设备将直接阻断此报文。其中，如果开启仅支持白名单功能，则仅判断匹配的规则中是否存在白名单规则。如果存在，则允许此报文通过；如果不存在，则将此报文阻断。不再进行后续流程的判断。
- (4) 如果匹配的规则中不存在 URL 过滤黑/白名单规则，则进行如下判断：
 - a. 如果匹配的规则中存在自定义 URL 过滤分类规则，则根据各规则所属分类中严重级别最高的分类的动作对报文进行处理。如果匹配的规则中不存在自定义 URL 过滤分类规则，则继续进行下一步处理。
 - b. 如果设备上启用了 URL 信誉功能，则判断匹配的规则中是否存在 URL 信誉特征库中的某个攻击分类规则。如果存在，则根据该规则所属攻击分类的动作对报文进行处理；如果不存在，则继续进行下一步处理。
 - c. 如果匹配的规则中存在预定义 URL 过滤分类规则，则根据各规则所属分类中严重级别最高的分类的动作对报文进行处理。
- (5) 如果 URL 过滤分类云端查询功能已开启，则判断 URL 是否匹配 URL 过滤缓存规则（该规则为云端服务器的历史查询结果，包含 URL 及其所属分类的名称）。如果匹配成功，则进入步骤（4）中预定义 URL 过滤分类规则的匹配。如果匹配失败，则进入步骤（6）处理，并将报文中的 URL 发往云端服务器进行查询。云端查询后，查询结果将被缓存到 URL 过滤缓存中。如果 URL 过滤分类云端查询功能未开启，则进入步骤（6）的处理。
- (6) 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。

1.1.8 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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV防火墙业务板	支持
	Blade V防火墙业务板	支持
	NAT业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V防火墙业务板	支持
M9008-S M9012-S	Blade IV防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V防火墙业务板	支持
M9000-AK001	Blade V防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI防火墙业务板	支持

1.3 URL过滤的License要求

URL 过滤特征库升级和 URL 过滤分类云端查询功能需要购买并正确安装 License 后才能使用。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，但无法将特征库升级到 License 过期后官网发布的特征库版本，且无法进行 URL 过滤分类云端查询。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) （可选）[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) (可选) [在 URL 过滤策略中引用 URL 过滤告警动作参数 profile](#)
- (6) [在 DPI 应用 profile 中引用 URL 过滤策略](#)
- (7) (可选) [激活 URL 过滤的策略和规则配置](#)
- (8) 引用 DPI 应用 profile
请选择以下一项任务进行配置：
 - [在安全策略中引用 URL 过滤业务](#)
 - [在对象策略中引用 URL 过滤业务](#)
- (9) [配置 URL 过滤特征库升级和回滚](#)
- (10) (可选) [配置 URL 信誉特征库升级和回滚](#)
- (11) (可选) [开启应用层检测引擎日志信息功能](#)
- (12) (可选) [配置 URL 过滤日志信息筛选功能](#)
- (13) (可选) [开启 URL 加速审计功能](#)

1.5 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，管理员可以自行创建 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。

1.6 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。

1.7 配置URL过滤策略

1.7.1 配置任务简介

URL 过滤功能基于 URL 过滤策略实现，请选择以下一项任务进行配置：

- [基于 URL 过滤分类实现 URL 过滤功能](#)
 - 配置 URL 过滤分类动作
 - 配置 URL 过滤分类缺省动作
 - （可选）配置白名单/黑名单规则
- [基于 URL 过滤白名单实现 URL 过滤功能](#)

1.7.2 基于 URL 过滤分类实现 URL 过滤功能

1. License 要求

URL 信誉功能需要购买并正确安装 License 才能使用。License 过期后，URL 信誉功能可以采用设备中已有的特征库正常工作，但无法将特征库升级到 License 过期后官网发布的特征库版本。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

2. 配置限制和指导

当动作配置为 **logging** 时，设备将记录日志并支持如下两种方式输出日志。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

3. 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 过滤规则中存在多个 URL 过滤分类的规则，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）开启内嵌白名单功能。

```
referrer-whitelist enable
```

缺省情况下，内嵌白名单功能处于开启状态，用户可以访问白名单网页下内嵌的其他网页链接。

- (7) （可选）开启 URL 信誉功能。

url-reputation enable

缺省情况下，URL 信誉功能处于关闭状态。

- (8) （可选）配置对指定 URL 信誉攻击分类执行的操作。

```
attack-category attack-id 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，未配置对指定 URL 信誉攻击分类执行的操作，设备对匹配攻击分类的报文执行允许动作，并记录日志。

- (9) （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
```

1.7.3 基于 URL 过滤白名单实现 URL 过滤功能

1. 功能简介

当管理员只希望通过配置白名单指定内部用户可以访问的网站，不想进行其他复杂配置时（例如配置 URL 过滤分类、URL 过滤分类动作和 URL 过滤策略缺省动作），可以开启仅支持 URL 过滤白名单功能。

开启 URL 过滤白名单功能后，设备仅允许用户访问白名单规则中定义的网站，其他网站均不允许访问。

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) 向 URL 过滤策略中添加白名单规则。

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

- (4) （可选）开启内嵌白名单功能。

```
referrer-whitelist enable
```

缺省情况下，内嵌白名单功能处于开启状态，用户可以访问白名单网页下内嵌的其他网页链接。

- (5) 开启仅支持 URL 过滤白名单功能。

```
whitelist-only enable
```

缺省情况下，仅支持 URL 过滤白名单功能处于关闭状态。

1.8 复制URL过滤策略或分类

1.8.1 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
```

1.8.2 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
```

1.9 在URL过滤策略中引用URL过滤告警动作参数profile

1. 功能简介

当设备阻断了客户端访问的 URL 后，会向客户端浏览器返回告警信息。告警信息的具体内容可在 URL 过滤告警动作参数 profile 中配置。管理员可通过在 URL 过滤策略中引用指定的 URL 过滤告警动作参数 profile，为设备提供相应的告警信息。有关 URL 过滤告警动作参数 profile 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) 创建 URL 过滤策略，并进入 URL 过滤策略视图。

```
url-filter policy policy-name
```

- (3) 引用 URL 过滤告警动作参数 profile。

```
warning parameter-profile profile-name
```


缺省情况下，URL 过滤策略中未引用 URL 过滤告警动作参数 **profile**，设备向客户端返回缺省告警信息，具体内容请参见“DPI 深度安全命令参考”中的“URL 过滤”手册中对本命令行缺省情况的详细介绍。

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 **profile** 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

缺省情况下，当 URL 过滤业务发生配置变更时（即策略或规则被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略和规则的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对变更的配置立即进行激活，可执行 **inspect activate** 命令手工激活，使配置立即生效。

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”。

2. 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、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.12 在安全策略中引用URL过滤业务

- (1) 进入系统视图。

system-view

- (2) 进入安全策略视图。

security-policy { ip | ipv6 }

- (3) 进入安全策略规则视图。

rule { rule-id | [rule-id] name rule-name }

- (4) 配置安全策略规则的动作作为允许。

action pass

缺省情况下，安全策略规则动作是丢弃。

- (5) 配置安全策略规则引用 DPI 应用 profile。

profile app-profile-name

缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.13 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。

1.14 配置URL过滤特征库升级和回滚

1.14.1 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”。
- 同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.14.2 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 之间开始自动升级 URL 过滤特征库。

1.14.3 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
```

1.14.4 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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 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 [ vpn-instance vpn-instance-name ]  
[ source { ip | ipv6 } { ip-address | interface interface-type  
interface-number } ]
```



注意

H3C 官方网站上的特征库服务专区根据设备的内存大小以及软件版本为用户提供了不同的特征库。管理员需要根据设备实际情况获取相应的特征库，如果为小内存设备（8GB 以下）升级了适用于大内存设备（8GB 以上）的特征库，可能会导致设备异常，请谨慎操作。

1.14.5 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 }
```

1.15 配置URL信誉特征库升级和回滚

1.15.1 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 信誉功能的正常运行。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 信誉特征库时，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 信誉特征库会失败。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”。

同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.15.2 配置定期自动在线升级 URL 信誉特征库

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 信誉特征库进行升级。

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 信誉特征库功能，并进入自动在线升级配置视图。

```
url-reputation signature auto-update
```

缺省情况下，定期自动在线升级 URL 信誉特征库功能处于关闭状态。

- (3) 配置定期自动在线升级 URL 信誉特征库的时间。

```
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 之间开始自动升级 URL 信誉特征库。

1.15.3 立即自动在线升级 URL 信誉特征库

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 信誉特征库有更新时，可以选择立即自动在线升级方式来及时升级 URL 信誉特征库版本。

执行此命令后，将立即自动升级设备上的 URL 信誉特征库，且会备份当前的 URL 信誉特征库文件。此命令的生效与否，与是否开启了定期自动升级 URL 信誉特征库功能无关。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 立即自动在线升级 URL 信誉特征库。

```
url-reputation signature auto-update-now
```

1.15.4 手动离线升级 URL 信誉特征库

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 信誉特征库版本：

- 本地升级：使用设备本地保存的特征库文件升级系统中的 URL 信誉特征库版本，使用此方式前，请先从官方网站获取特征库文件并导入到设备中。
- 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，并升级系统中的 URL 信誉特征库版本。

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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手动离线升级 URL 信誉特征库。

```
url-reputation signature update file-path [ vpn-instance  
vpn-instance-name ] [ source { ip | ipv6 } { ip-address | interface  
interface-type interface-number } ]
```

1.15.5 回滚 URL 信誉特征库

1. 功能简介

URL 信誉特征库回滚是指将当前的 URL 信誉特征库版本回滚到上一版本的版本。如果管理员发现设备当前 URL 信誉特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前 URL 信誉特征库版本进行回滚。

URL 信誉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 信誉特征库是 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，再执行回滚到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 信誉特征库。

```
url-reputation signature rollback last
```

1.16 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。

1.17 配置 URL 过滤日志信息筛选功能

1.17.1 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

1.17.2 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。

1.17.3 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。

1.18 开启 URL 加速审计功能

1. 功能简介

缺省情况下，设备在软件快速转发流程中通过 URL 过滤功能对报文进行 URL 审计，这种处理方式不仅可以对报文进行 URL 审计，还可以对报文进行阻断或重定向等操作。但是，软件快速转发和 URL 过滤功能均需要 CPU 进行处理，当 CPU 负担较重时，直接影响报文的转发速度。

开启 URL 加速审计功能后，报文直接通过硬件快速转发流程进行转发处理，同时把 HTTP 类型的报文镜像到 CPU 进行 URL 过滤处理。这种处理方式下，当 CPU 负担较重时，可以保障报文的快速转发，只能对报文进行 URL 审计，即对匹配了动作是 **logging** 的 URL 过滤规则的报文进行记录日志。

有关快速转发的详细介绍，请参见“三层技术-IP 业务”中的“快速转发”。

2. 配置限制和指导

- 必须先配置完 URL 过滤功能和开启硬件快速转发功能后，此功能才会生效。
- 此功能适用于对设备转发性能要求比较高，又需要进行 URL 审计但对安全性要求不高的应用场景。
- 此功能不能与需要进行四层以上业务处理的功能（如七层负载均衡、ALG 等功能）同时使用，否则此功能将会失效。
- 开启此功能后，DPI 相关功能将会失效。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 URL 加速审计功能。

```
hardware audit url enable
```

缺省情况下，URL 加速审计功能处于关闭状态。

1.19 开启HTTPS流量过滤功能

1. 功能简介

缺省情况下，设备仅对 HTTP 流量进行 URL 过滤，如果需要对 HTTPS 流量进行 URL 过滤，则可以选择如下方式：

- 使用 SSL 解密功能：先对 HTTPS 流量进行解密，然后再进行 URL 过滤。有关 SSL 解密功能的详细介绍，请参见“DPI 深度安全配置指导”中的“代理策略”。
- 开启 HTTPS 流量过滤功能：不对 HTTPS 流量进行解密，直接对客户端发送的 HTTPS 的 Client HELLO 报文中的 SNI（Server Name Indication extension）字段进行检测，从中获取用户访问的服务器域名，使用获取到的域名与 URL 过滤策略进行匹配。

由于 SSL 解密功能涉及大量的加解密操作，会对设备的转发性能会产生较大的影响，建议在仅需要对 HTTPS 流量进行 URL 过滤业务处理的场景下开启 HTTPS 流量过滤功能。

2. 配置限制和指导

本功能仅支持基于 URL 过滤规则中的 HOST 字段过滤，对于 URI 字段的信息无法匹配。

本功能仅在访问的服务器地址字段为域名的情况下生效，如果服务器地址字段为 IP 地址，本功能不生效。

如果客户端浏览器启用 TLS 1.3 降级强化机制功能选项，报文中的 SNI 字段将会被加密，本功能将失效。

如果同时配置 SSL 解密功能，则本功能失效。

如果 HTTPS 报文不支持 SNI 字段，本功能将失效。

3. 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) 开启 HTTPS 流量过滤功能。

```
https-filter enable
```

缺省情况下，HTTPS 流量过滤功能处于关闭状态，设备仅对 HTTP 流量进行 URL 过滤。

1.20 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。

其中，**display url-reputation attack-category** 命令仅支持在 URL 过滤策略视图下执行。

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 library
查看URL过滤的统计信息	display url-filter statistics
显示指定URL过滤策略下的URL信誉攻击分类信息	display url-reputation attack-category
显示URL信誉特征库信息	display url-reputation signature library
清除URL过滤的统计信息	reset url-filter statistics

1.21 URL过滤典型配置举例

1.21.1 在安全策略中引用 URL 过滤业务配置举例

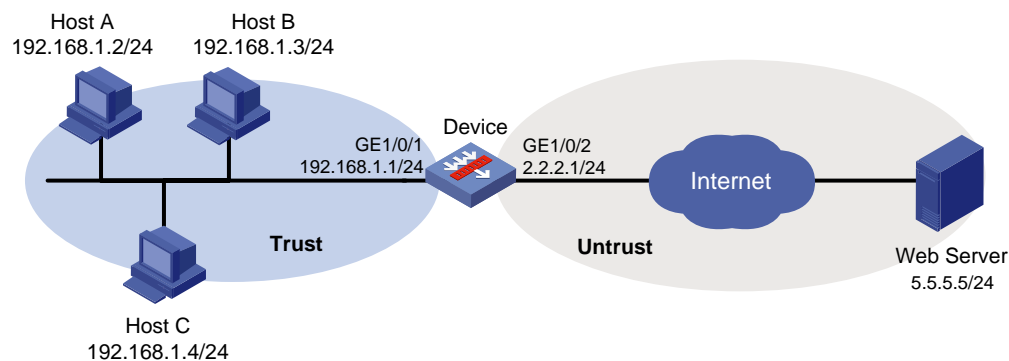
1. 组网需求

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 在安全策略中引用 URL 过滤业务配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 URL 过滤功能

创建名为 news 的自定义 URL 过滤分类，并在分类中添加主机名 www.sina.com。

```
[Device] url-filter category news severity 2000
[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，配置自定义分类 news 的动作为允许、预定义 URL 过滤分类 Pre-Games 的动作为丢弃并生成日志、策略的缺省动作为丢弃和打印日志。

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

(5) 配置 DPI 应用 profile 并激活 URL 过滤策略和规则配置

创建名为 sec 的 DPI 应用 profile，并在 DPI 应用 profile sec 中应用 URL 过滤策略 urlnews。

```
[Device] app-profile sec
[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) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 URL 过滤检测。具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name trust-untrust
```

```
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
```

```
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
```

```
[Device-security-policy-ip-10-trust-untrust] action pass
```

```
[Device-security-policy-ip-10-trust-untrust] profile sec
```

```
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
```

```
[Device-security-policy-ip] 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。

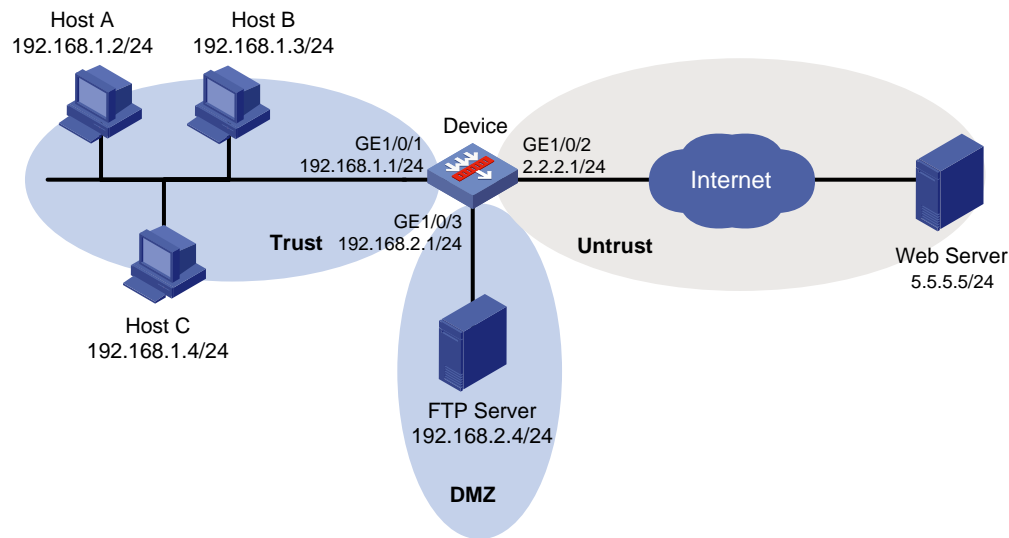
1.21.2 手动离线升级 URL 过滤特征库配置举例

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`。现需要手动离线升级 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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

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

(4) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Trust 到 DMZ 安全域的流量，使内网用户可以访问 DMZ 安全域中的服务器

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-dmz
[Device-security-policy-ip-11-trust-dmz] source-zone trust
[Device-security-policy-ip-11-trust-dmz] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-11-trust-dmz] destination-zone dmz
[Device-security-policy-ip-11-trust-dmz] action pass
[Device-security-policy-ip-11-trust-dmz] quit
```

- 配置安全策略规则放行设备与 FTP 服务器之间的流量，使设备可以访问 FTP 服务器，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-12-downloadlocalout] source-zone local
[Device-security-policy-ip-12-downloadlocalout] destination-zone dmz
[Device-security-policy-ip-12-downloadlocalout] destination-ip-subnet 192.168.2.0 24
[Device-security-policy-ip-12-downloadlocalout] application ftp
[Device-security-policy-ip-12-downloadlocalout] application ftp-data
[Device-security-policy-ip-12-downloadlocalout] action pass
[Device-security-policy-ip-12-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 手动升级 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 library** 命令查看当前特征库的版本信息。

1.21.3 定期自动在线升级 URL 过滤特征库配置举例

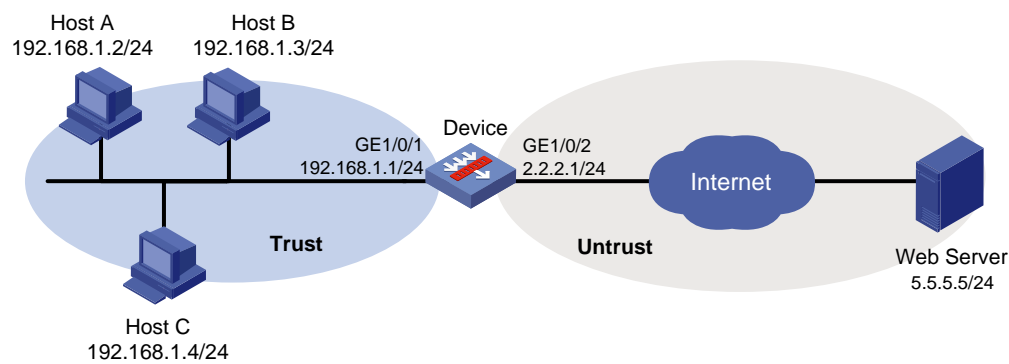
1. 组网需求

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，开始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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
```

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

(4) 配置 DNS 服务器地址

指定 DNS 服务器的 IP 地址为 10.72.66.36，确保 Device 可以获取到官网的 IP 地址，具体配置步骤如下。

```
[Device] dns server 10.72.66.36
```

(5) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Local 到 Untrust 安全域的流量，使设备可以访问官网的特征库服务专区，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-11-downloadlocalout] source-zone local
[Device-security-policy-ip-11-downloadlocalout] destination-zone untrust
[Device-security-policy-ip-11-downloadlocalout] action pass
[Device-security-policy-ip-11-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(6) 配置定期自动在线升级 URL 过滤特征库

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 前后 30 分钟内开始自动在线升级。

```
[Device] url-filter signature auto-update
[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 library** 命令查看当前特征库的版本信息。

1.21.4 在对象策略中引用 URL 过滤业务配置举例

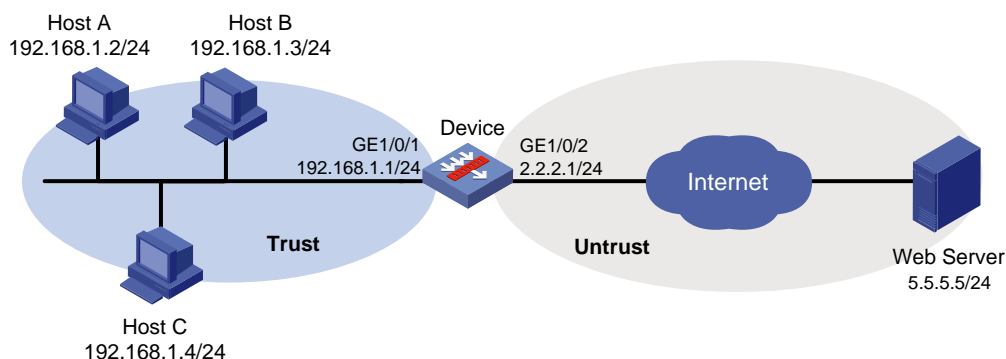
1. 组网需求

如图 1-6 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1-6 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。

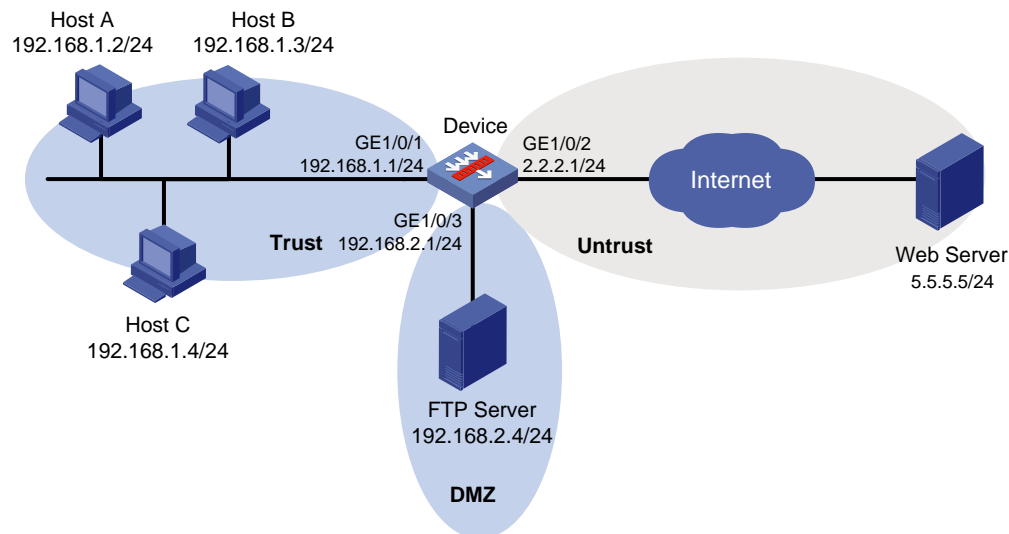
1.21.5 手动离线升级 URL 过滤特征库配置举例

1. 组网需求

如图 1-7 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1-7 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 Server 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) 升级特征库

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 library** 命令查看当前特征库的版本信息。

1.21.6 定期自动在线升级 URL 过滤特征库配置举例

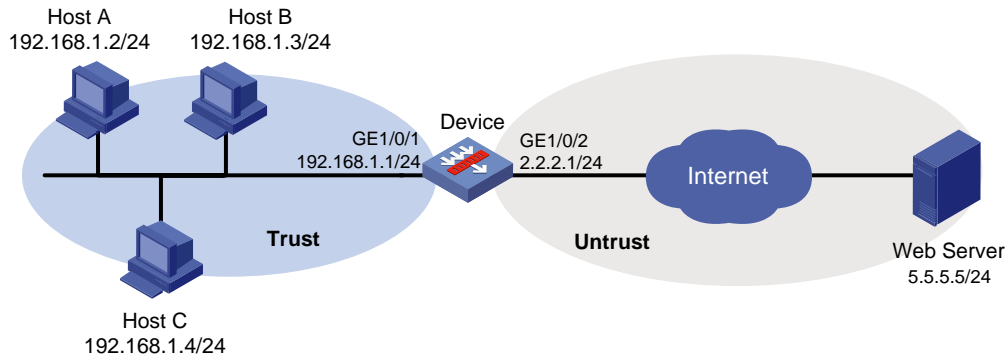
1. 组网需求

如图 1-8 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1-8 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 library** 命令查看当前特征库的版本信息。

目 录

1 数据过滤	1-1
1.1 数据过滤简介	1-1
1.1.1 基本概念	1-1
1.1.2 数据过滤的实现原理	1-1
1.2 数据过滤与硬件适配关系	1-1
1.3 数据过滤配置任务简介	1-2
1.4 配置关键字组	1-3
1.5 配置数据过滤策略	1-3
1.6 在 DPI 应用 profile 中引用数据过滤策略	1-4
1.7 激活数据过滤策略和规则配置	1-5
1.8 在安全策略中引用数据过滤业务	1-5
1.9 在对象策略中引用数据过滤业务	1-6
1.10 数据过滤典型配置举例	1-6
1.10.1 在安全策略中引用数据过滤业务配置举例	1-6
1.10.2 在对象策略中引用数据过滤业务配置举例	1-9

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 HTTP、FTP、SMTP、IMAP、NFS、POP3、RTMP 和 SMB 协议传输的应用层信息进行检测和过滤。

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用层信息特征的字符串，包括以下类型：

- 预定义特征：系统预先定义配置，包括手机号、银行卡号、信用卡号和身份证号。
- 自定义特征：用户自定义配置，支持文本匹配方式和正则表达式匹配方式。

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。

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

数据过滤功能是通过在 DPI 应用 profile 中引用数据过滤策略，并在安全策略或对象策略中引用 DPI 应用 profile 来实现的，设备对报文进行数据过滤处理的整体流程如下：

- (1) 当设备收到报文时，将对匹配了策略的报文进行数据过滤处理。有关安全策略的详细介绍请参见“安全配置指导”中的“安全策略”；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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.3 数据过滤配置任务简介

数据过滤配置任务如下：

- (1) [配置关键字组](#)
- (2) [配置数据过滤策略](#)
- (3) [在 DPI 应用 profile 中引用数据过滤策略](#)
- (4) （可选）[激活数据过滤策略和规则配置](#)
- (5) 引用 DPI 应用 profile

请选择以下一项任务进行配置：

- [在安全策略中引用数据过滤业务](#)
- [在对象策略中引用数据过滤业务](#)

1.4 配置关键字组

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建关键字组，并进入关键字组视图。

```
data-filter keyword-group keywordgroup-name
```

- (3) （可选）配置关键字组的描述信息。

```
description string
```

缺省情况下，未配置关键字组的描述信息。

- (4) 配置数据过滤特征。

- 配置自定义数据过滤特征。

```
pattern pattern-name { regex | text } pattern-string
```

缺省情况下，未配置自定义数据过滤特征。

- 启用预定义数据过滤特征。

```
pre-defined-pattern name { bank-card-number | credit-card-number |  
id-card-number | phone-number }
```

缺省情况下，未启用预定义数据过滤特征。

1.5 配置数据过滤策略

1. 功能简介

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。

2. 配置限制和指导

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

当动作配置为 **logging** 时，设备将记录日志并支持如下两种方式输出日志。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

当使用数据过滤规则对 SMTP 协议数据进行阻断时，由于邮件客户端会不断地尝试发送邮件，可能存在长时间后邮件发送成功的情况。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 创建数据过滤策略，并进入数据过滤策略视图。

data-filter policy *policy-name*

- (3) （可选）配置数据过滤策略的描述信息。

description *string*

缺省情况下，未配置数据过滤策略的描述信息。

- (4) 创建数据过滤规则，并进入数据过滤规则视图。

rule *rule-name*

- (5) 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。

- (6) 配置数据过滤规则的应用层协议类型。

application { **all** | **type** { **ftp** | **http** | **imap** | **nfs** | **pop3** | **rtmp** | **smb** | **smtp** }
* }

缺省情况下，数据过滤规则未指定应用层协议类型。

- (7) 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。

- (8) 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作为丢弃。

1.6 在DPI应用profile中引用数据过滤策略

1. 功能简介

DPI 应用 **profile** 是一个安全业务的配置模板，为实现数据过滤功能，必须在 DPI 应用 **profile** 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。

2. 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。

1.7 激活数据过滤策略和规则配置

1. 功能简介

缺省情况下，当数据过滤业务发生配置变更时（即策略或规则被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略和规则的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对变更的配置立即进行激活，可执行 **inspect activate** 命令手工激活，使配置立即生效。

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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 激活数据过滤策略和规则配置。

```
inspect activate
```

缺省情况下，数据过滤策略和规则被创建、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.8 在安全策略中引用数据过滤业务

- (1) 进入系统视图。

```
system-view
```

- (2) 进入安全策略视图。

```
security-policy { ip | ipv6 }
```

- (3) 进入安全策略规则视图。

```
rule { rule-id | [ rule-id ] name rule-name }
```

- (4) 配置安全策略规则的动作作为允许。

```
action pass
```

缺省情况下，安全策略规则动作是丢弃。

- (5) 配置安全策略规则引用 DPI 应用 profile。

```
profile app-profile-name
```

缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.9 在对象策略中引用数据过滤业务

- (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“基础配置指导”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。

1.10 数据过滤典型配置举例

1.10.1 在安全策略中引用数据过滤业务配置举例

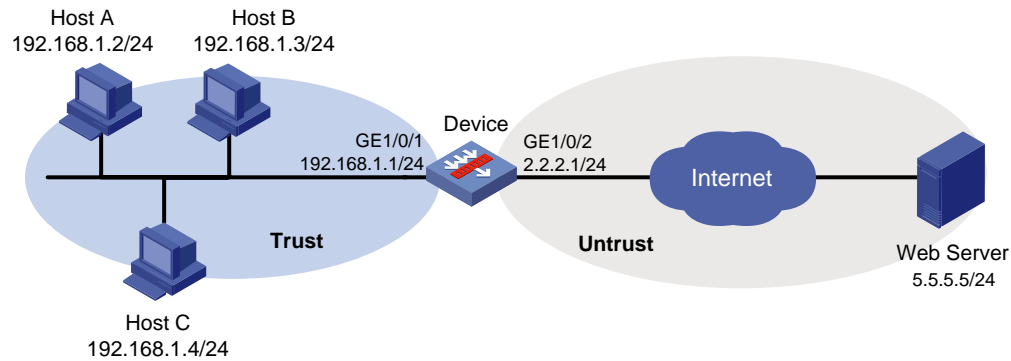
1. 组网需求

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.example.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 在安全策略中引用数据过滤业务配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置数据过滤功能

a. 配置关键字组

创建关键字组 kg1，配置关键字文本 uri 和正则表示式 abc.*abc;

```
[Device] data-filter keyword-group kg1
[Device-data-filter-kg1] pattern 1 text uri
```

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

按照同样的步骤，创建关键字组 kg2，配置匹配关键字文本 www.example.com。

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

b. 配置数据过滤策略

创建数据过滤规则 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
[Device-data-filter-policy-p1] rule r1
[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
```

按照同样的步骤，创建数据过滤规则 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
[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 并激活数据过滤策略和规则配置

创建名称为 sec 的 DPI 应用 profile，在 DPI 应用 sec 中应用数据过滤策略 p1。

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

激活数据过滤策略和规则配置。

```
[Device] inspect activate
```

(6) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网，并对交互报文进行数据过滤检测。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
```

```
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

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。

1.10.2 在对象策略中引用数据过滤业务配置举例

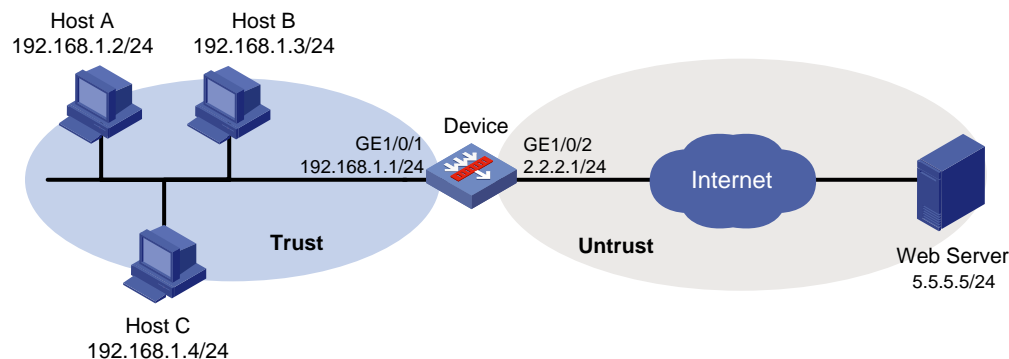
1. 组网需求

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.example.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1-2 在对象策略中引用数据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 **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

a. 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
```

配置关键字文本 **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
```

配置匹配关键字文本 **www.example.com**。

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

b. 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
```

激活数据过滤策略和规则配置。

```
[Device] inspect activate
```

(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
```

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
1.1 文件过滤简介	1-1
1.1.1 基本概念	1-1
1.1.2 文件过滤的实现原理	1-1
1.2 文件过滤与硬件适配关系	1-2
1.3 文件过滤配置任务简介	1-2
1.4 配置文件类型组	1-3
1.5 配置文件过滤策略	1-3
1.6 配置文件扩展名不匹配时动作	1-4
1.7 在 DPI 应用 profile 中引用文件过滤策略	1-5
1.8 激活文件过滤策略和规则配置	1-5
1.9 在安全策略中引用文件过滤业务	1-6
1.10 在对象策略中引用文件过滤业务	1-6
1.11 文件过滤典型配置举例	1-7
1.11.1 在安全策略中引用文件过滤业务配置举例	1-7
1.11.2 在对象策略中引用文件过滤业务配置举例	1-9

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 HTTP、FTP、SMTP、IMAP、NFS、POP3、RTMP 和 SMB 协议传输的文件进行检测和过滤。

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

文件过滤功能是通过在 DPI 应用 profile 中引用文件过滤策略，并在安全策略或对象策略中引用 DPI 应用 profile 来实现的，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 等协议传输的文件时，设备将对匹配了策略的报文进行文件过滤处理。有关安全策略的详细介绍请参见“安全配置指导”中的“安全策略”；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并记录。
- (3) 设备进一步识别文件真实类型，并将识别的结果与扩展名进行匹配：
 - 如果一致，则使用扩展名与文件过滤规则进行匹配，并进入步骤（4）处理；
 - 如果不一致，则查看文件扩展名不匹配时动作，如果动作为丢弃，则直接丢弃报文，不再进行文件过滤规则的匹配；如果动作为允许，则使用文件的真实类型与文件过滤规则进行匹配，并进入步骤（4）处理。
- (4) 与文件过滤规则进行匹配，并根据匹配结果对报文执行以下动作：
 - 如果文件的扩展名信息/真实类型同时与多个文件过滤规则匹配成功，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 > 允许，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/真实类型只与一个文件过滤规则匹配成功，则执行此规则中指定的动作；

- 如果文件的扩展名信息/真实类型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。
- (5) 如果设备不能识别出文件真实类型，则根据文件扩展名与文件过滤规则进行匹配，并进入步骤（4）处理。

1.2 文件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。

设备型号	业务板类型	说明
M9006	Blade IV防火墙业务板	支持
M9010	Blade V防火墙业务板	支持
M9014	NAT业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V防火墙业务板	支持
M9008-S M9012-S	Blade IV防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V防火墙业务板	支持
M9000-AK001	Blade V防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI防火墙业务板	支持

1.3 文件过滤配置任务简介

文件过滤配置任务如下：

- (1) [配置文件类型组](#)
- (2) [配置文件过滤策略](#)
- (3) [配置文件扩展名不匹配时动作](#)
- (4) [在 DPI 应用 profile 中引用文件过滤策略](#)

- (5) （可选）[激活文件过滤策略和规则配置](#)
- (6) 引用 DPI 应用 profile
 - 请选择以下一项任务进行配置：
 - [在安全策略中引用文件过滤业务](#)
 - [在对象策略中引用文件过滤业务](#)

1.4 配置文件类型组

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建文件类型组，并进入文件类型组视图。

```
file-filter filetype-group group-name
```

- (3) （可选）配置文件类型组的描述信息。

```
description string
```

缺省情况下，未配置文件类型组的描述信息。

- (4) 配置文件过滤特征。

```
pattern pattern-name text pattern-string
```

缺省情况下，未配置文件过滤特征。

1.5 配置文件过滤策略

1. 功能简介

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。

2. 配置限制和指导

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

当动作配置为 **logging** 时，设备将记录日志并支持如下两种方式输出日志。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建文件过滤策略，并进入文件过滤策略视图。

```
file-filter policy policy-name
```

- (3) （可选）配置文件过滤策略的描述信息。

```
description string
```

缺省情况下，未配置文件过滤策略的描述信息。

- (4) 创建文件过滤规则，并进入文件过滤规则视图。

```
rule rule-name
```

- (5) 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。

- (6) 配置文件过滤规则的应用层协议类型。

```
application { all | type { ftp | http | imap | nfs | pop3 | rtmp | smb | smtp }  
* }
```

缺省情况下，文件过滤规则中未指定应用层协议类型。

- (7) 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。

- (8) 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作为丢弃。

1.6 配置文件扩展名不匹配时动作

1. 功能简介

设备对报文进行文件过滤处理时，会将识别出的文件真实类型与文件扩展名进行对比，当二者不一致时，需要根据本配置进行判断。如果配置动作为允许，则根据识别出的真实的文件类型与文件过滤规则进行匹配，并执行文件过滤规则中的动作；如果配置动作为丢弃，则直接丢弃报文，不再进行文件过滤规则的匹配。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置文件扩展名不匹配时动作

```
file-filter false-extension action { drop | permit }
```

缺省情况下，文件的真实类型与扩展名不匹配时执行的动作为允许。

1.7 在DPI应用profile中引用文件过滤策略

1. 功能简介

DPI 应用 **profile** 是一个安全业务的配置模板，为实现文件过滤功能，必须在 DPI 应用 **profile** 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。

2. 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。

1.8 激活文件过滤策略和规则配置

1. 功能简介

缺省情况下，当文件过滤业务发生配置变更时（即策略或规则被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略和规则的配置生效。

如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 激活文件过滤策略和规则配置。

```
inspect activate
```

缺省情况下，文件过滤策略和规则被创建、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.9 在安全策略中引用文件过滤业务

- (1) 进入系统视图。
system-view
- (2) 进入安全策略视图。
security-policy { ip | ipv6 }
- (3) 进入安全策略规则视图。
rule { rule-id | [rule-id] name rule-name }
- (4) 配置安全策略规则的动作作为允许。
action pass
缺省情况下，安全策略规则动作是丢弃。
- (5) 配置安全策略规则引用 DPI 应用 profile。
profile app-profile-name
缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.10 在对象策略中引用文件过滤业务

- (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
缺省情况下，不存在安全域间实例。
有关安全域间实例的详细介绍请参见“基础配置指导”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。

1.11 文件过滤典型配置举例

1.11.1 在安全策略中引用文件过滤业务配置举例

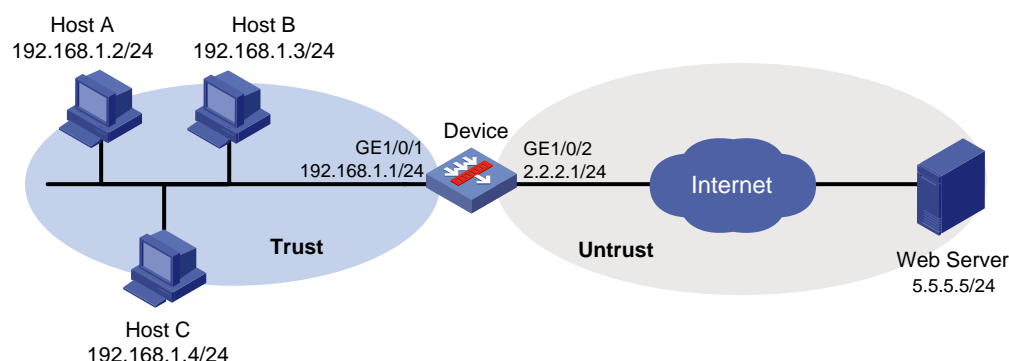
1. 组网需求

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 在安全策略中引用文件过滤业务配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
```



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

(4) 配置文件过滤功能

- a. 创建文件类型组 **fg1**，并配置文件过滤特征为 **pptx** 和 **dotx**。

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

- b. 创建文件过滤规则 **r1**，引用文件类型组 **fg1**，并配置应用类型为 **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
[Device-file-filter-policy-p1] rule r1
[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** 并激活文件过滤策略和规则配置

- # 创建名称为 **sec** 的 DPI 应用 **profile**，在 **sec** 中引用文件过滤策略 **p1**。

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

- # 激活文件过滤策略和规则配置。

```
[Device] inspect activate
```

(6) 配置安全策略

- # 配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行文件过滤检测。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

- # 激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

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。

1.11.2 在对象策略中引用文件过滤业务配置举例

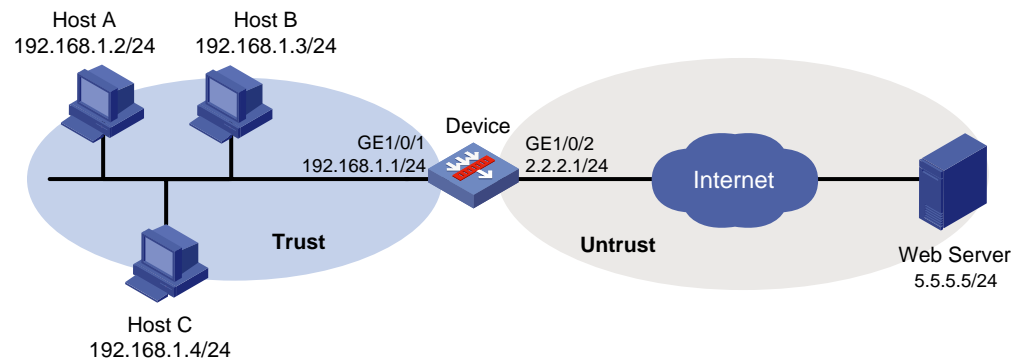
1. 组网需求

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1-2 在对象策略中引用文件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 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

a. 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
```

b. 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
```

激活文件过滤策略和规则配置。

```
[Device] inspect activate
```

(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
```

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	1-1
1.1 防病毒简介	1-1
1.1.1 应用场景	1-1
1.1.2 基本概念	1-1
1.1.3 防病毒检测方式	1-2
1.1.4 防病毒数据处理流程	1-2
1.1.5 病毒特征库升级与回滚	1-4
1.2 防病毒与硬件适配关系	1-4
1.3 防病毒的 License 要求	1-5
1.4 vSystem 相关说明	1-5
1.5 防病毒配置限制和指导	1-5
1.6 防病毒配置任务简介	1-5
1.7 配置防病毒策略	1-6
1.8 配置 MD5 值云端查询功能	1-7
1.9 配置防病毒动作引用应用层检测引擎动作参数 profile	1-8
1.10 在 DPI 应用 profile 中引用防病毒策略	1-9
1.11 激活防病毒策略和规则配置	1-9
1.12 在安全策略中引用 DPI 应用 profile	1-10
1.13 在对象策略中引用 DPI 应用 profile	1-10
1.14 配置病毒特征库升级和回滚	1-10
1.14.1 配置限制和指导	1-10
1.14.2 配置定期自动在线升级病毒特征库	1-11
1.14.3 立即自动在线升级病毒特征库	1-11
1.14.4 手动离线升级病毒特征库	1-11
1.14.5 回滚病毒特征库	1-12
1.15 防病毒显示和维护	1-13
1.16 防病毒典型配置举例	1-13
1.16.1 在安全策略中引用缺省防病毒策略配置举例	1-13
1.16.2 在安全策略中引用自定义防病毒策略配置举例	1-15
1.16.3 手动离线升级病毒特征库配置举例	1-17
1.16.4 定时自动升级病毒特征库配置举例	1-19
1.16.5 在对象策略中引用缺省防病毒策略配置举例	1-21
1.16.6 在对象策略中引用自定义防病毒策略配置举例	1-23

1.16.7 手动离线升级病毒特征库配置举例	1-25
1.16.8 定时自动升级病毒特征库配置举例	1-26

1 防病毒

1.1 防病毒简介

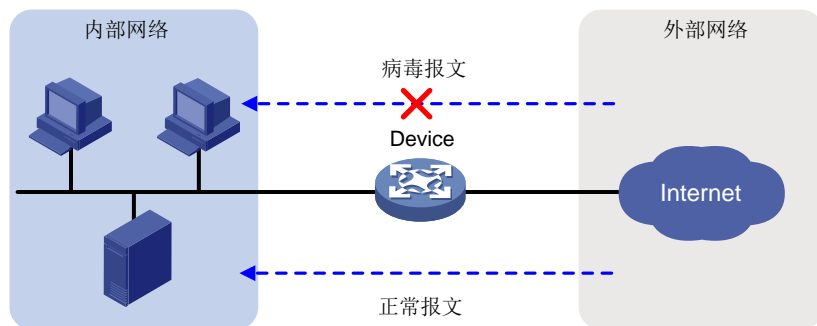
防病毒功能是一种通过对报文应用层信息进行检测来识别和处理病毒报文的安全机制。防病毒功能凭借庞大且不断更新的病毒特征库可有效保护网络安全，防止病毒在网络中的传播。将具有防病毒功能的设备部署在企业网入口，可以将病毒隔离在企业网之外，为企业内网的数据安全提供坚固的防御。

1.1.1 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。

图1-1 防病毒典型应用场景



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。

1.1.2 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. MD5 规则

MD5 规则是设备上定义的用于识别传输文件是否携带病毒的检测规则，由系统中的病毒特征库预定义。

3. 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。

4. 应用例外

缺省情况下，设备基于应用层协议中指定的动作对符合病毒特征的报文进行处理。

当需要对某一具体应用采取的动作与其所属应用层协议的动作不同时，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。

5. MD5 值例外

缺省情况下，设备对所有 MD5 值匹配防病毒规则的报文进行防病毒动作处理。但是，当管理员发现某类检测出病毒的报文被误报时，可以通过查看防病毒日志获取 MD5 值并设置为例外。当后续再有检测出符合该 MD5 值的报文通过时，设备将对其执行允许动作。

6. 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。仅对上传方向有效。

其中，病毒日志支持输出到信息中心或以邮件的方式发送到指定的收件人邮箱。

1.1.3 防病毒检测方式

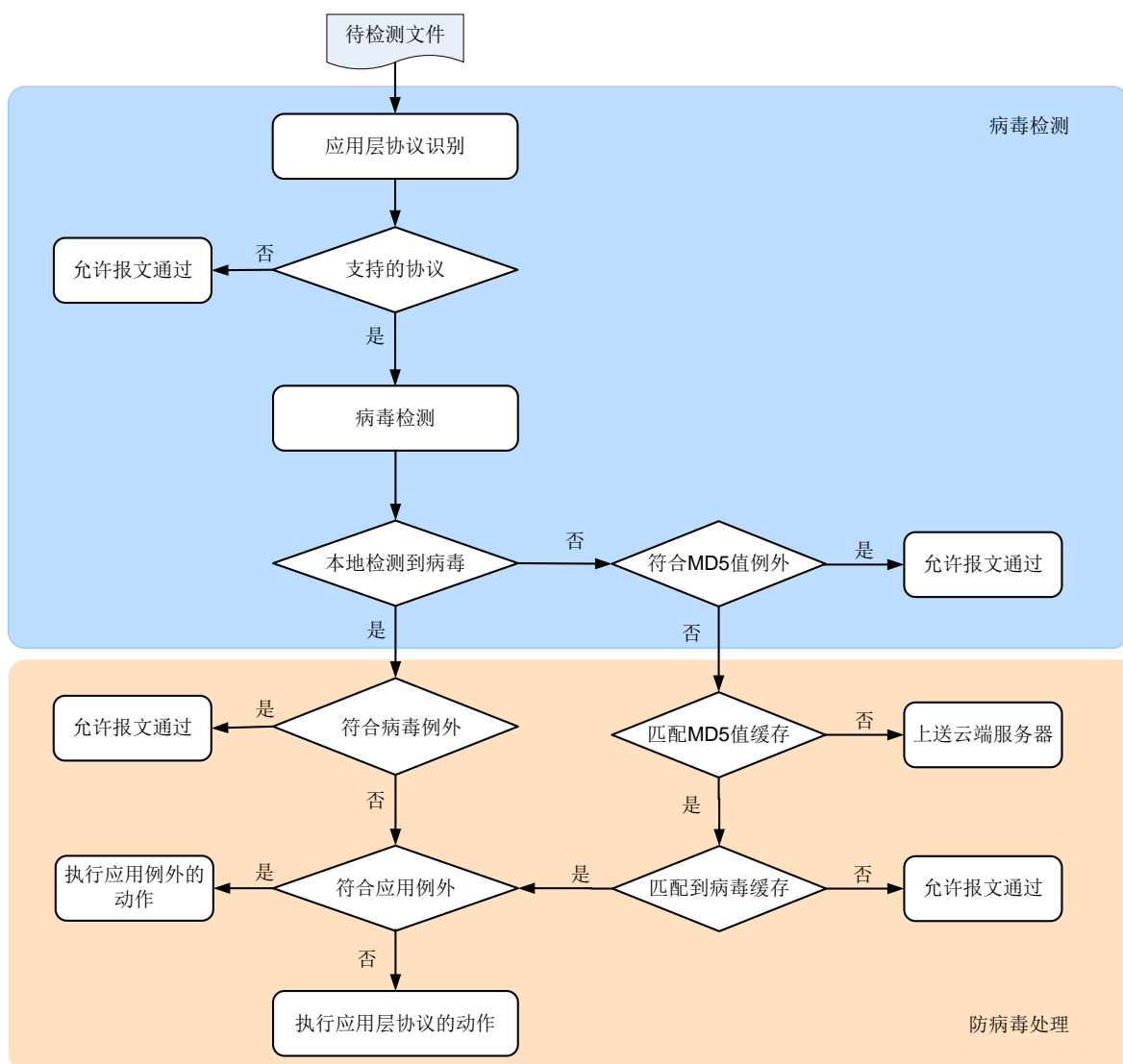
设备支持使用以下方式进行防病毒检测：

- 病毒特征匹配：设备将报文与特征库中的病毒特征进行匹配，如果匹配成功，则表示该报文携带病毒。
- MD5 值匹配：设备首先对待检测文件进行 MD5 哈希运算，再将计算出的 MD5 值与特征库中的 MD5 规则进行匹配，如果匹配成功，则表示该文件携带病毒。

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



防病毒功能是通过在 DPI 应用 profile 中引用防病毒策略，并在安全策略和对象策略中引用 DPI 应用 profile 来实现的，防病毒处理的整体流程如下：

- (1) 设备对应用层协议进行识别，判断协议是否为防病毒功能所支持，如果支持，则进行下一步处理；否则直接允许报文通过，不对其进行防病毒检测。
- (2) 设备对报文进行病毒检测，将报文同时与特征库中的病毒特征和 MD5 规则进行匹配，任意一种匹配成功，则认为该报文携带病毒，并进行下一步处理；如果二者均匹配失败，则判断是否匹配 MD5 值例外，如果符合，则允许报文通过；如果不符合，进入步骤（5）处理。
- (3) 如果报文符合病毒例外，则对此报文执行允许动作，否则继续进行下一步处理。
- (4) 如果报文符合应用例外，则执行应用例外的防病毒动作（告警、阻断和允许），否则执行报文所属应用层协议的防病毒动作（告警、阻断和重定向）。
- (5) 设备将报文与 MD5 值缓存进行匹配，缓存中保存着云端服务器的历史检测结果，包括标识为“病毒”和“非病毒”的 MD5 值。设备将根据报文与 MD5 值缓存的匹配结果进行如下判断：

- a. 如果匹配到标识为“病毒”的缓存，则继续判断报文是否符合应用例外。如果符合，则执行应用例外的动作（告警、阻断和允许），如果不符合，则执行报文所属应用层协议的防病毒动作（告警、阻断和重定向）。
- b. 如果匹配到标识为“非病毒”的缓存，则允许报文通过。
- c. 如果未与任何 MD5 值缓存匹配成功，则判断设备是否开启了云端查询功能。
 - 如果开启了云端查询功能，则放行报文，并同时 will MD5 值上送云端服务器进行病毒检测。检测完成后，设备会将服务器返回的检测结果保存到 MD5 值缓存中，便于后续报文在本地进行病毒检测，而不必再上送云端。
 - 如果未开启云端查询功能，则直接放行报文。

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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持

M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.3 防病毒的License要求

防病毒功能需要购买并正确安装 License 后才能使用。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，且 MD5 值云端查询功能以及联动沙箱进行阻断功能无法使用。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.4 vSystem相关说明

非缺省 vSystem 不支持本特性部分功能，具体包括：

- 配置 MD5 值云端查询功能
- 配置病毒特征库升级和回滚



说明

非缺省 vSystem 对具体命令的支持情况，请见本特性的命令参考。有关 vSystem 的详细介绍请参见“虚拟化技术配置指导”中的“vSystem”。

1.5 防病毒配置限制和指导

防病毒功能支持对基于 FTP、HTTP、HTTPS、IMAP、IMAPS、NFS、POP3、POP3S、SMB、SMTP 和 SMTPS 协议传输的报文进行防病毒检测。其中，HTTPS、IMAPS、POP3S 和 SMTPS 协议需要配合 SSL 代理功能使用，有关 SSL 代理功能的详细介绍，请参见“DPI 深度安全配置指导”中的“代理策略”。

1.6 防病毒配置任务简介

防病毒配置任务如下：

- (1) [配置防病毒策略](#)

- (2) (可选) [配置 MD5 值云端查询功能](#)
- (3) [配置防病毒动作引用应用层检测引擎动作参数 profile](#)
- (4) [在 DPI 应用 profile 中引用防病毒策略](#)
- (5) (可选) [激活防病毒策略和规则配置](#)
- (1) 引用 DPI 应用 profile
请选择以下一项任务进行配置：
 - [在安全策略中引用 DPI 应用 profile](#)
 - [在对象策略中引用 DPI 应用 profile](#)
- (2) [配置病毒特征库升级和回滚](#)

1.7 配置防病毒策略

1. 功能简介

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。

当设备检测出病毒后，支持向客户端发送告警信息。告警信息的具体内容由应用层检测引擎告警动作参数 **profile** 来定义，可通过引用该动作参数 **profile** 为告警信息提供显示内容。有关应用层检测引擎动作参数 **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”。

2. 配置限制和指导

NFS 协议仅支持 NFSv3 版本；SMB 协议支持 SMBv1 和 SMBv2 版本。

防病毒日志支持如下两种方式输出。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

在 RBM 双机热备的非对称组网环境中（即同一条流量的报文来回路径不一致），不支持发送告警信息功能，即使配置了该功能的相关命令，其功能也不会生效。有关 RBM 双机热备的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

开启发送告警信息功能后，设备会对匹配防病毒策略的 HTTP 流量进行代理，将对设备性能产生较大影响，请根据实际情况判断是否需要开启上述功能。

3. 配置步骤

- (3) 进入系统视图。
system-view
- (4) 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。

- (5) (可选) 配置防病毒策略描述信息。

description *text*

- (6) 配置病毒检测的应用层协议类型。

inspect { **ftp** | **http** | **imap** | **nfs** | **pop3** | **smb** | **smtp** } **direction** { **both** | **download** | **upload** } [**cache-file-size** *file-size*] **action** { **alert** | **block** | **redirect** }

缺省情况下，设备对 FTP、HTTP、IMAP、NFS 和 SMB 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、NFS 和 SMB 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，支持缓存的检测文件大小上限为 1MB。因为 POP3 协议只有下载方向，SMTP 协议只支持上传方向，所以对这两种协议类型不支持配置方向属性。

- (7) (可选) 开启发送告警信息功能，并引用告警动作参数 **profile**。

warning parameter-profile *profile-name*

缺省情况下，未引用告警动作参数 **profile**，设备不支持向客户端发送告警信息。

发送告警信息功能仅在病毒检测的应用层协议类型为 HTTP，且动作为 **block** 时生效。

- (8) (可选) 配置病毒例外。

exception signature *signature-id*

- (9) (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** }

- (10) (可选) 配置 MD5 值例外。

exception md5 *md5-value*

- (11) 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。

1.8 配置MD5值云端查询功能

1. 功能简介

开启防病毒 MD5 值云端查询功能后，当设备未检测到病毒时，可将文件的 MD5 值发往云端服务器进行查询。云端服务器响应该请求，并向设备发送查询结果，该结果中包含了 MD5 值并确认其是否为病毒。防病毒模块会将云端服务器返回的查询结果保存到 MD5 值缓存中，便于后续报文在本地进行病毒检测。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. 配置限制和指导

- 云端查询功能支持 FTP、HTTP、HTTPS、IMAP、IMAPS、NFS(仅支持 read 操作)、POP3、POP3S、SMTP 和 SMTPS 协议。其中，HTTPS、IMAPS、POP3S 和 SMTPS 协议需要配合 SSL 代理功能使用，有关 SSL 代理功能的详细介绍，请参见“DPI 深度安全配置指导”中的“代理策略”。

- 对于压缩文件，设备会先对其进行解压缩，直到达到最大解压缩文件层数（通过 **inspect file-uncompr-layer** 命令设置）为止。设备会将压缩文件的 MD5 值以及所有解压缩后子文件的 MD5 值上送云端查询。有关最大解压缩文件层数的详细介绍，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) 配置云端服务器的主机名。

```
inspect cloud-server host-name
```

缺省情况下，云端服务器主机名为 **sec.h3c.com**。

- (3) （可选）配置防病毒 MD5 值缓存中可缓存记录的上限。

```
anti-virus cache size cache-size
```

缺省情况下，防病毒 MD5 值缓存中可缓存记录的上限为 10 万条。

- (4) （可选）配置防病毒 MD5 值缓存条目的最短保留时间。

```
anti-virus cache min-time value
```

缺省情况下，防病毒 MD5 值缓存条目的最短保留时间为 10 分钟。

- (5) 进入防病毒策略视图。

```
anti-virus policy policy-name
```

- (6) 开启 MD5 值云端查询功能。

```
cloud-query enable
```

缺省情况下，MD5 值云端查询功能处于关闭状态。

1.9 配置防病毒动作引用应用层检测引擎动作参数profile

1. 功能简介

防病毒动作的具体执行参数（例如，邮件服务器的地址、输出日志的方式和对报文重定向的 URL）由应用层检测引擎各动作参数 **profile** 来定义，可通过引用各动作参数 **profile** 为防病毒动作提供执行参数。应用层检测引擎动作参数 **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”。

如果防病毒动作没有引用应用层检测引擎动作参数 **profile**，或者引用的动作参数 **profile** 不存在，则使用系统中各动作参数的缺省值。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置防病毒动作引用应用层检测引擎动作参数 **profile**。

```
anti-virus { email | logging | redirect } parameter-profile profile-name
```

缺省情况下，防病毒动作未引用应用层检测引擎动作参数 **profile**。

1.10 在DPI应用profile中引用防病毒策略

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。

2. 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。

1.11 激活防病毒策略和规则配置

1. 功能简介

缺省情况下，当防病毒业务发生配置变更时（即策略或规则被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略和规则的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对变更的配置立即进行激活，可执行 **inspect activate** 命令手工激活，使配置立即生效。

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”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 激活防病毒策略和规则配置。

```
inspect activate
```

缺省情况下，防病毒策略和规则被创建、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.12 在安全策略中引用DPI应用profile

- (1) 进入系统视图。
system-view
- (2) 进入安全策略视图。
security-policy { ip | ipv6 }
- (3) 进入安全策略规则视图。
rule { rule-id | [rule-id] name rule-name }
- (4) 配置安全策略规则的动作为允许。
action pass
缺省情况下，安全策略规则动作是丢弃。
- (5) 配置安全策略规则引用 DPI 应用 profile。
profile app-profile-name
缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.13 在对象策略中引用DPI应用profile

- (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。

1.14 配置病毒特征库升级和回滚

1.14.1 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”。
- 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）防病毒特征库时，需要确保设备能通过静态或动态域名解析方式获得 H3C 官方网站的 IP 地址，并与之路由可达，否则设备升级防病毒特征库会失败。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”。
- 同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.14.2 配置定期自动在线升级病毒特征库

1. 功能简介

如果设备可以访问 H3C 官方网站，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。

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。

- (3) 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。

1.14.3 立即自动在线升级病毒特征库

1. 功能简介

当管理员发现 H3C 官方网站上的特征库服务专区中的病毒特征库有更新时，可以采用立即自动在线升级方式来及时升级病毒特征库版本。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 立即自动在线升级病毒特征库。

```
anti-virus signature auto-update-now
```

1.14.4 手动离线升级病毒特征库

1. 功能简介

如果设备不能访问 H3C 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。
- 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。

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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手动离线升级病毒特征库。

```
anti-virus signature update file-path [ vpn-instance vpn-instance-name ]
[ source { ip | ipv6 } { ip-address | interface interface-type
interface-number } ]
```



注意

H3C 官方网站上的特征库服务专区根据设备的内存大小以及软件版本为用户提供了不同的特征库。管理员需要根据设备实际情况获取相应的特征库，如果为小内存设备（8GB 以下）升级了适用于大内存设备（8GB 以上）的特征库，可能会导致设备异常，请谨慎操作。

1.14.5 回滚病毒特征库

1. 功能简介

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。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 回滚病毒特征库。

anti-virus signature rollback { factory | last }

1.15 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。



说明

非缺省 vSystem 不支持部分显示和维护命令，具体情况请参见本特性的命令参考。

表1-1 防病毒显示和维护

操作	命令
显示防病毒缓存信息	(独立运行模式) display anti-virus cache [slot slot-number [cpu cpu-number]] (IRF模式) display anti-virus cache [chassis chassis-number slot slot-number [cpu cpu-number]]
显示病毒特征信息	display anti-virus signature [[signature-id] [severity { critical high low medium }]]
显示病毒特征家族信息	display anti-virus signature family-info
显示病毒特征库版本信息	display anti-virus signature library
显示防病毒统计信息	(独立运行模式) display anti-virus statistics [policy policy-name] [slot slot-number [cpu cpu-number]] (IRF模式) display anti-virus statistics [policy policy-name] [chassis chassis-number slot slot-number [cpu cpu-number]]

1.16 防病毒典型配置举例

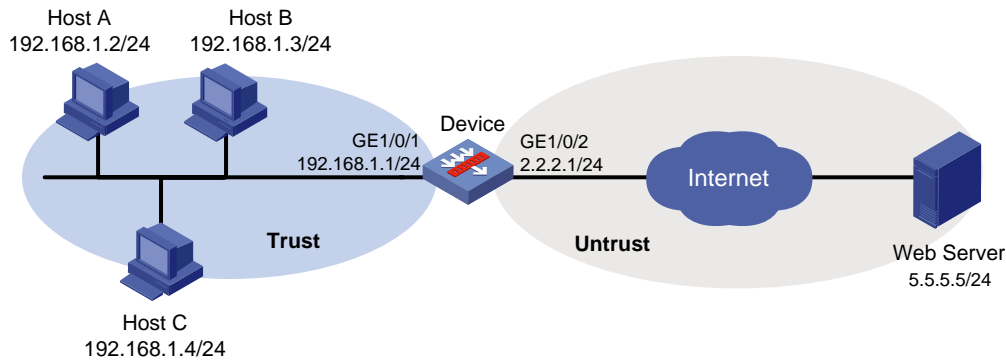
1.16.1 在安全策略中引用缺省防病毒策略配置举例

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 在安全策略中引用缺省防病毒策略配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 DPI 应用 profile 并激活防病毒策略配置

创建名为 sec 的 DPI 应用 profile，在 DPI 应用 profile sec 中引用缺省防病毒策略 default，并指定该防病毒策略的模式为 protect。

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

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

激活防病毒策略配置。

```
[Device] inspect activate
```

(5) 配置安全策略

配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行防病毒检测。具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name trust-untrust
```

```
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
```

```
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
```

```
[Device-security-policy-ip-10-trust-untrust] action pass
```

```
[Device-security-policy-ip-10-trust-untrust] profile sec
```

```
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
```

```
[Device-security-policy-ip] quit
```

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。

1.16.2 在安全策略中引用自定义防病毒策略配置举例

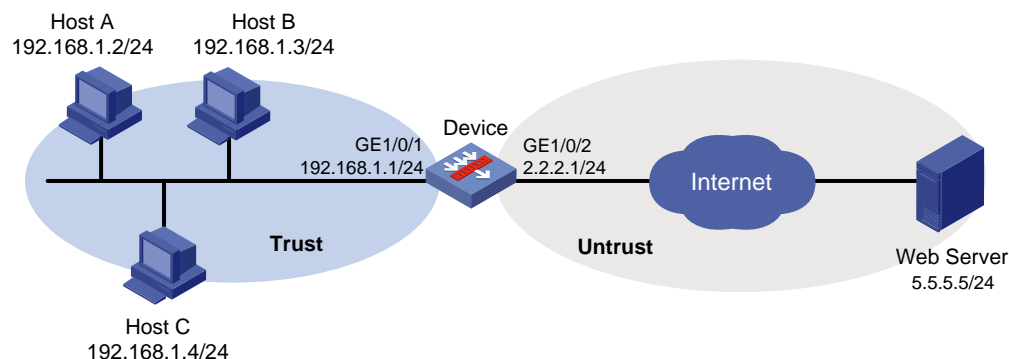
1. 组网需求

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 139Email 的应用设置为应用例外。

2. 组网图

图1-4 在安全策略中引用自定义防病毒配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置防病毒策略

创建一个名称为 antivirus1 的防病毒策略，将编号为 2 的预定义病毒特征设置为病毒例外，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
[Device-anti-virus-policy-antivirus1] exception signature 2
[Device-anti-virus-policy-antivirus1] exception application 139Email action alert
[Device-anti-virus-policy-antivirus1] quit
```

(5) 配置 DPI 应用 profile 并激活防病毒策略配置

创建名为 sec 的 DPI 应用 profile，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
[Device-app-profile-sec] anti-virus apply policy antivirus1 mode protect
[Device-app-profile-sec] quit
```

激活防病毒策略配置。

```
[Device] inspect activate
```

(6) 配置安全策略

配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行防病毒检测。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

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。

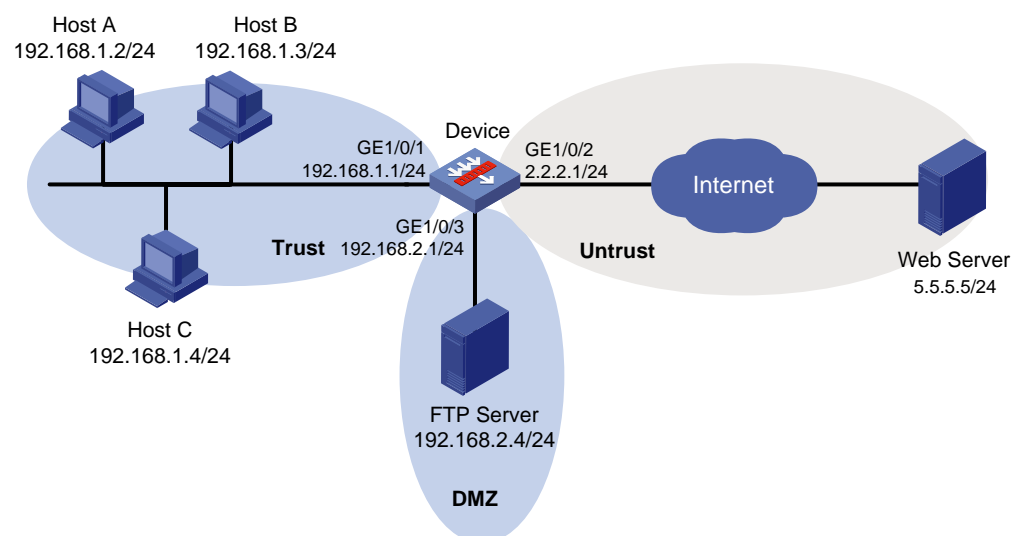
1.16.3 手动离线升级病毒特征库配置举例

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，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-1.0.8-encrypt.dat**，FTP 服务器的登录用户名和密码分别为 **anti-virus** 和 **123**。现需要手动离线升级病毒特征库，加载最新的病毒特征。

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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 1/0/3
[Device-security-zone-DMZ] quit
```

(4) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Trust 到 DMZ 安全域的流量，使内网用户可以访问 DMZ 安全域中的服务器

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-dmz
```



```
[Device-security-policy-ip-11-trust-dmz] source-zone trust
[Device-security-policy-ip-11-trust-dmz] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-11-trust-dmz] destination-zone dmz
[Device-security-policy-ip-11-trust-dmz] action pass
[Device-security-policy-ip-11-trust-dmz] quit
```

- 配置安全策略规则放行设备与 FTP 服务器之间的流量，使设备可以访问 FTP 服务器，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-12-downloadlocalout] source-zone local
[Device-security-policy-ip-12-downloadlocalout] destination-zone dmz
[Device-security-policy-ip-12-downloadlocalout] destination-ip-subnet 192.168.2.0 24
[Device-security-policy-ip-12-downloadlocalout] application ftp
[Device-security-policy-ip-12-downloadlocalout] application ftp-data
[Device-security-policy-ip-12-downloadlocalout] action pass
[Device-security-policy-ip-12-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 手动升级防病毒特征库

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
```

4. 验证配置

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

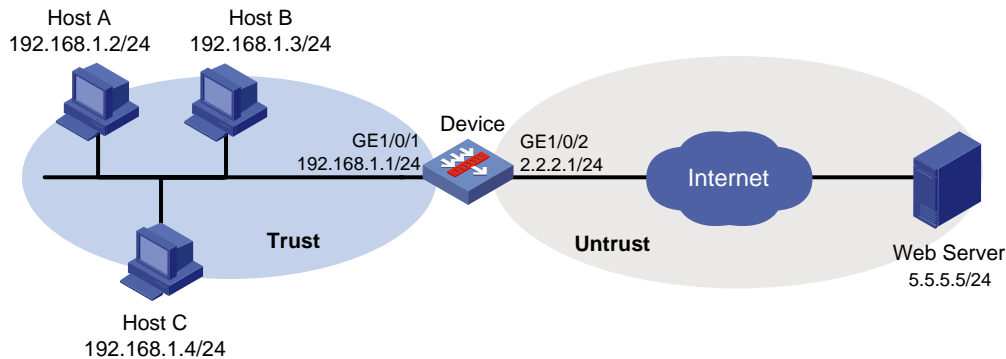
1.16.4 定时自动升级病毒特征库配置举例

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，开始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) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 DNS 服务器地址

指定 DNS 服务器的 IP 地址为 10.72.66.36，确保 Device 可以获取到官网的 IP 地址，具体配置步骤如下。

```
[Device] dns server 10.72.66.36
```

(5) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Local 到 Untrust 安全域的流量，使设备可以访问官网的特征库服务专区，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-11-downloadlocalout] source-zone local
[Device-security-policy-ip-11-downloadlocalout] destination-zone untrust
[Device-security-policy-ip-11-downloadlocalout] action pass
[Device-security-policy-ip-11-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(6) 配置定期自动在线升级病毒特征库

设置定时自动升级病毒特征库计划为：每周六上午 9:00:00 前后 30 分钟内，开始自动升级。

```
[Device] anti-virus signature auto-update
[Device-anti-virus-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 60
[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 library** 命令查看当前特征库的版本信息

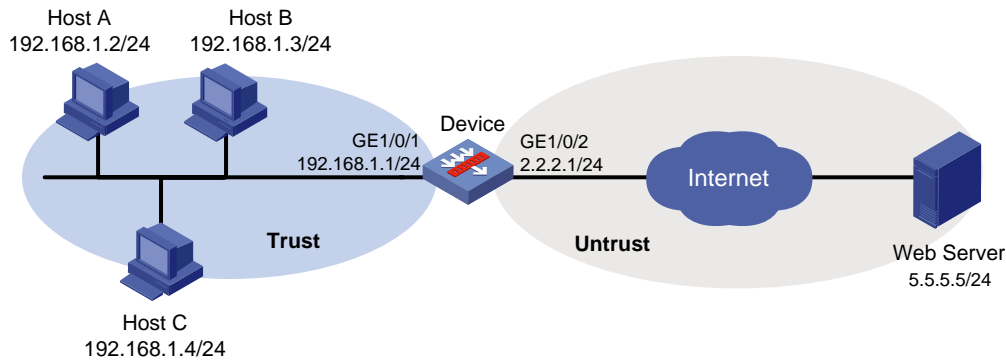
1.16.5 在对象策略中引用缺省防病毒策略配置举例

1. 组网需求

如[图 1-7](#)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1-7 在对象策略中引用缺省防病毒策略配置组网图



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 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 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
```

激活 DPI 各业务模块的策略和规则配置。

```
[Device] inspect activate
```

(5) 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
```

(6) 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
```

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。

1.16.6 在对象策略中引用自定义防病毒策略配置举例

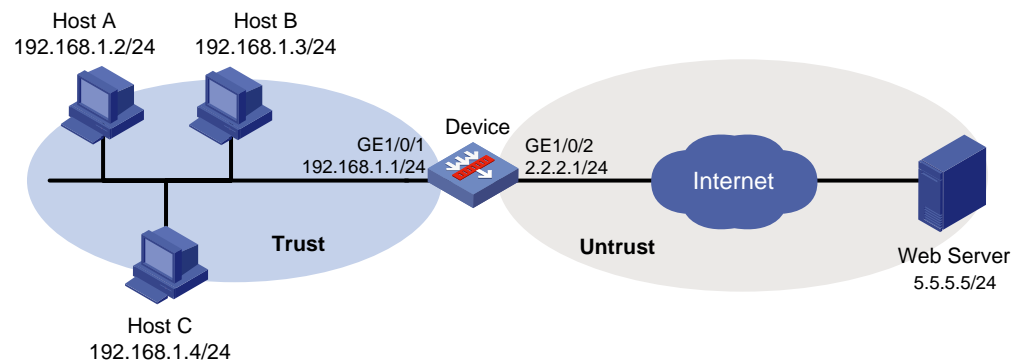
1. 组网需求

如图 1-8 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 139Email 的应用设置为应用例外。

2. 组网图

图1-8 在对象策略中引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
```

激活 DPI 各业务模块的策略和规则配置。

```
[Device] inspect activate
```

(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
```

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。

1.16.7 手动离线升级病毒特征库配置举例

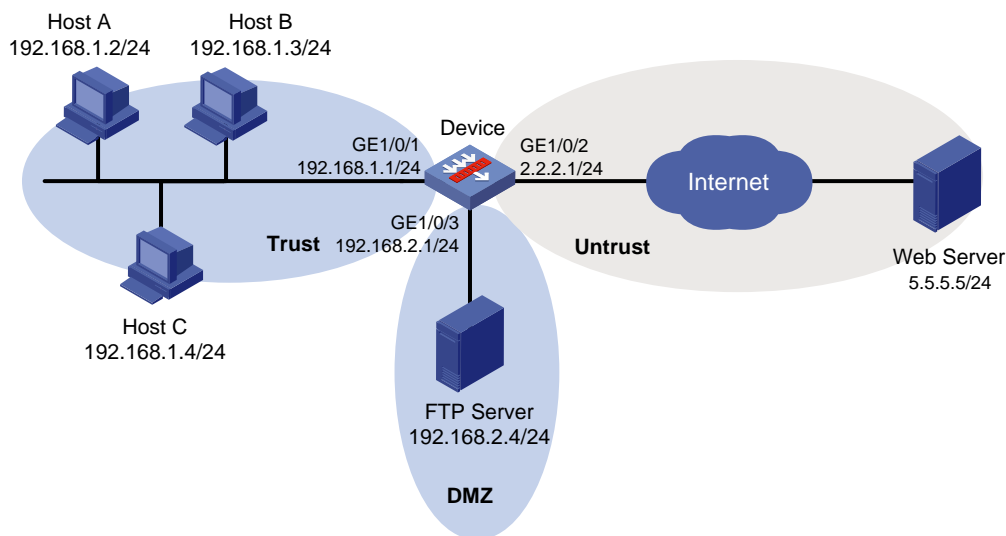
1. 组网需求

如图 1-9 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-1.0.8-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。

2. 组网图

图1-9 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) 手动升级防病毒特征库

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
```

4. 验证配置

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

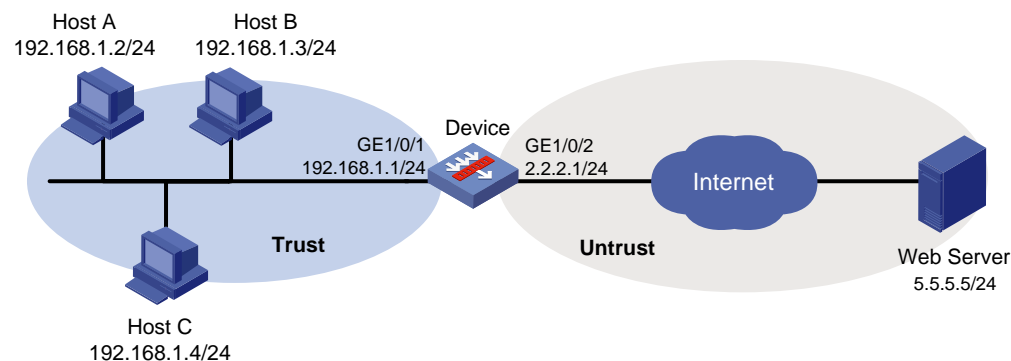
1.16.8 定时自动升级病毒特征库配置举例

1. 组网需求

如图 1-10 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1-10 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) 配置设备解析 H3C 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 60 分钟。

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

```
[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 library** 命令查看当前特征库的版本信息。

目 录

1 数据分析中心	1-1
1.1 数据分析中心简介	1-1
1.1.1 日志信息存储与分析	1-1
1.1.2 流量监控	1-1
1.1.3 报表分析	1-1
1.2 数据分析中心与硬件适配关系	1-1
1.3 数据分析中心配置限制和指导	1-2
1.4 数据分析中心配置任务简介	1-2
1.5 开启日志采集功能	1-2
1.6 开启实时日志展示功能	1-3
1.7 开启实时流量统计功能	1-3
1.8 配置邮件服务器	1-3
1.9 配置报表订阅功能	1-4
1.10 配置数据分析中心存储空间	1-5
1.11 数据分析中心显示和维护	1-5

1 数据分析中心

1.1 数据分析中心简介

DAC（Data Analysis Center，数据分析中心）提供了业务日志信息的数据挖掘和可视化展示服务。它支持日志信息存储与分析、流量监控和报表分析功能，可帮助用户清晰地了解业务流量分布情况以及网络安全现状，为用户制定各业务策略提供了有力的数据支持。

1.1.1 日志信息存储与分析

各业务模块处理报文后，会将产生的日志信息发往数据分析中心，数据分析中心将从中提取相关数据进行汇总和分析。数据分析中心支持内存和硬盘两种存储空间类型，各业务的数据优先保存在硬盘中，只有当硬盘不在位时，才会保存在内存中。

1.1.2 流量监控

数据分析中心实时监控流经设备的网络流量，并根据用户、应用、IP 地址等统计条件对监控数据进行分类统计排行和趋势展示，可帮助管理员监控当前网络流量、检查网络中的安全漏洞以及查看网络攻击的类型等信息，从而方便管理员进行相应的防护控制。

1.1.3 报表分析

数据分析中心可以针对用户不同的需求生成多种类型的分析报表，方便用户查看各业务的统计信息、设备整体运行状况和网络安全现状等。

1.2 数据分析中心与硬件适配关系

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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持

M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V防火墙业务板	支持
M9000-AK001	Blade V防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI防火墙业务板	支持

1.3 数据分析中心配置限制和指导

数据分析中心的结果展示功能仅在 Web 管理方式下支持。CLI（Command Line Interface，命令行接口）管理方式下仅提供相关参数的配置功能，不提供任何分析结果展示功能。

1.4 数据分析中心配置任务简介

数据分析中心配置任务如下：

- [开启日志采集功能](#)
- [开启实时日志展示功能](#)
- [开启实时流量统计功能](#)
- [配置邮件服务器](#)
- [配置报表订阅功能](#)
- [配置数据分析中心存储空间](#)

1.5 开启日志采集功能

1. 功能简介

开启日志采集功能后，数据分析中心将会采集指定业务的日志信息，并从中提取相关数据进行汇总和分析，用于在 Web 界面中进行展示。用户可以在 Web 界面的“概览”和“监控”页面上查看到数据分析中心汇总、分析后的数据。

2. 配置限制和指导

对于 DPI 业务下的流量业务，需要在设备上先开启会话统计功能，数据分析中心才可以采集到日志信息。有关会话统计功能的详细介绍，请参见“安全配置指导”中的“会话管理”。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启业务日志采集功能。

dac log-collect service service-type service-name enable

缺省情况下，各业务日志采集功能的启用状态请以业务注册时的实际情况为准。

1.6 开启实时日志展示功能

1. 功能简介

开启本功能后，数据分析中心会将指定业务产生的日志信息实时展示到 Web 界面，供用户查看，不需要用户手工刷新日志列表。

2. 配置限制和指导

本功能仅在开启指定业务的日志采集功能（通过 **dac log-collect enable** 命令开启）后生效。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启实时日志展示功能。

dac log-display service service-type service-name enable

缺省情况下，各业务实时日志展示功能处于关闭状态。

1.7 开启实时流量统计功能

1. 功能简介

数据分析中心可分别基于用户和应用对流量进行实时的统计，并将统计结果展示到 Web 界面，供用户查看。

2. 配置限制和指导

开启本功能后，会对设备 CPU 性能产生影响。在大流量业务的情况下，请谨慎开启。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启实时流量统计功能。

dac traffic-statistic { application | user } enable [verbose]

缺省情况下，实时流量统计功能处于关闭状态。

1.8 配置邮件服务器

1. 功能简介

当需要实现报表订阅功能时，需要配置邮件服务器，通过邮件将订阅的报表发送到指定的邮箱地址。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 配置数据分析中心的邮件服务器地址。

dac email-server server-address address-string

缺省情况下，未配置数据分析中心的邮件服务器的地址。

邮件服务器的地址既可以是邮件服务器的 IP 地址，也可以是邮件服务器的主机名。采用主机名时，需要确保设备能通过静态或动态域名解析方式获得邮件服务器的 IP 地址，并与之路由可达。否则邮件发送会失败。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) 配置发件人地址。

dac email-server sender address-string

缺省情况下，未配置发件人地址。

- (4) （可选）配置客户端身份验证功能。

- a. 开启客户端身份验证功能。

dac email-server client-authentication enable

- b. 配置登录邮件服务器的用户名。

dac email-server username username

- c. 配置登录邮件服务器的密码。

dac email-server password { cipher | simple } string

- d. （可选）开启安全传输登录邮件服务器的用户信息功能。

dac email-server secure-authentication enable

1.9 配置报表订阅功能

1. 功能简介

报表订阅功能用于生成周期性报表，并定期将生成的报表发送到指定的邮箱。系统默认在凌晨 1 点到 5 点通过邮件服务器向指定的订阅地址发送每日报表，并在每月的 1 日发送上个月的月度报表。发送时间暂不支持配置。支持的报表类型如下：

- 汇总报表：可以将某时间段内各业务的统计排名信息和趋势信息汇总。
- 对比报表：可以将两个时间段内各业务的统计排名信息和趋势信息进行对比分析。其中，每个时间段的天数必须相同。
- 智能报表：可以对某时间段内员工的工作效率、泄密风险和离职风险等情况进行分析。
- 综合报表：可以对某时间段内各业务的重点数据进行抓取和分析，综合展示设备整体运行状况和网络安全现状。

报表中会对各类统计数据进行分析，管理员可以根据实际需求配置报表分析的统计数据范围。例如，配置汇总报表分析排名 Top 20 的统计数据，则生成的汇总报表中，将仅包含各业务的统计排名前 20 的数据的分析结果。

2. 配置准备

为保证成功发送报表，需要对邮件服务器进行配置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置报表订阅参数。

```
dac report type { comparison | integrated | intelligent | summary }  
subscriber mail-address [ language { chinese | english } ]
```

缺省情况下，未配置数据分析中心报表订阅参数。

- (3) 配置报表分析的统计数据范围。

```
dac report type { comparison | integrated | intelligent | summary } top  
number
```

缺省情况下，报表分析排名 Top 5 的统计数据。

1.10 配置数据分析中心存储空间

1. 功能简介

数据分析中心存储各业务的日志信息，设备定时检查日志信息的存储状态，达到存储空间上限或者时间上限都将触发设备执行以下动作：

- 删除：设备将删除保存时间最长天数的数据以便保存新数据，并发送日志信息提示用户。设备不会删除当天的数据。
- 仅记录日志：设备不对历史数据进行删除，也不保存新数据，仅发送日志信息提示用户。

2. 配置限制和指导

当数据保存在内存中时，如果数据存储量达到系统运行的最大规格，系统将会进行滚动覆盖，即自动删除最旧的数据以保存新数据。

当数据保存在硬盘或 U 盘中时，如果数据存储量达到用户配置的存储上限，系统将根据用户配置的上限处理动作对数据进行处理。其中，处理动作为删除时，设备将会进行滚动覆盖，即自动删除最旧的数据以保存新数据。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 配置数据分析中心存储空间。

```
dac storage service service-type service-name limit { hold-time  
time-value | usage usage-value | action { delete | log-only } }
```

缺省情况下，数据分析中心各业务存储空间上限为 20%、存储空间时间上限为 365 天、处理动作为删除。

1.11 数据分析中心显示和维护

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数据分析中心的运行情况，通过查看显示信息验证配置的效果。

表1-1 数据分析中心显示和维护

操作	命令
显示数据分析中心邮件服务器配置信息	display dac email-server
显示业务日志采集功能的配置信息	display dac log-collect { all service service-type service-name }
显示实时日志展示功能的配置信息	display dac log-display { all service service-type service-name }
显示数据分析中心报表订阅信息	display dac report [comparison integrated intelligent summary]
显示数据分析中心存储空间的配置信息	display dac storage [service-type service-name]
显示实时流量统计功能的配置信息	display dac traffic-statistic [application user]

目 录

1 WAF	1-1
1.1 WAF 简介	1-1
1.1.1 WAF 防护功能	1-1
1.1.2 WAF 特征匹配	1-1
1.1.3 语义分析检测	1-3
1.1.4 CC 攻击防护	1-3
1.1.5 WAF 防护功能的处理优先级	1-5
1.1.6 WAF 特征库升级与回滚	1-5
1.2 WAF 的 License 要求	1-6
1.3 WAF 配置任务简介	1-6
1.3.1 WAF 特征匹配配置任务简介	1-6
1.3.2 语义分析检测配置任务简介	1-6
1.3.3 CC 攻击防护配置任务简介	1-6
1.3.4 WAF 策略的公共配置任务简介	1-6
1.4 配置 WAF 特征匹配功能	1-7
1.4.1 创建 WAF 策略	1-7
1.4.2 配置筛选 WAF 特征的属性	1-7
1.4.3 配置 WAF 策略动作	1-8
1.4.4 配置 WAF 策略动作引用的应用层检测引擎动作参数 profile	1-9
1.5 配置语义分析检测功能	1-9
1.5.1 创建 WAF 策略	1-9
1.5.2 开启语义分析检测功能	1-9
1.6 配置 CC 攻击防护功能	1-10
1.6.1 创建 WAF 策略	1-10
1.6.2 创建 CC 攻击防护策略	1-10
1.6.3 创建 CC 攻击防护策略规则	1-10
1.6.4 在 WAF 策略中引用 CC 攻击防护策略	1-11
1.6.5 管理 CC 攻击防护策略规则	1-12
1.7 激活 WAF 策略配置	1-12
1.8 在 DPI 应用 profile 中引用 WAF 策略	1-13
1.9 在安全策略中引用 DPI 应用 profile	1-13
1.10 在对象策略中引用 DPI 应用 profile	1-14
1.11 配置自定义 WAF 特征	1-14

1.11.1 创建自定义 WAF 特征.....	1-14
1.11.2 配置自定义 WAF 特征属性	1-14
1.11.3 配置自定义 WAF 特征规则	1-15
1.12 配置 WAF 特征库升级和回滚	1-17
1.12.1 配置限制和指导	1-17
1.12.2 配置定期自动在线升级 WAF 特征库.....	1-17
1.12.3 立即自动在线升级 WAF 特征库	1-18
1.12.4 手动离线升级 WAF 特征库	1-18
1.12.5 回滚 WAF 特征库	1-19
1.13 配置 WAF 白名单	1-19
1.14 WAF 显示和维护	1-20
1.15 WAF 典型配置举例.....	1-20
1.15.1 在安全策略中引用缺省 WAF 策略配置举例	1-20
1.15.2 在安全策略中引用自定义 WAF 策略配置举例	1-22
1.15.3 手动离线升级 WAF 特征库配置举例	1-24
1.15.4 定时自动升级 WAF 特征库配置举例	1-27
1.15.5 在对象策略中引用缺省 WAF 策略配置举例	1-29
1.15.6 在对象策略中引用自定义 WAF 策略配置举例	1-30
1.15.7 手动离线升级 WAF 特征库配置举例	1-32
1.15.8 定时自动升级 WAF 特征库配置举例	1-34

1 WAF

1.1 WAF简介

WAF（Web application firewall，Web 应用防火墙）用于阻断 Web 应用层攻击，保护内网用户和内部 Web 服务器。当设备收到来自外部的 HTTP 或 HTTPS 请求后，会执行防护策略，对请求内容的安全性和合法性进行检测和验证，对非法的请求予以实时阻断，从而对内网的用户和 Web 服务器进行有效防护。

1.1.1 WAF 防护功能

WAF 支持通过如下功能对 Web 应用层攻击进行检测与防护。

1. WAF 特征匹配

设备通过对攻击行为的特征进行检测，保护内网用户和服务器免受 Web 应用层攻击。

2. 语义分析检测

设备通过对报文中的 SQL 语法进行分析来检测 SQL 注入攻击行为，保护内网用户和服务器免受该类攻击。

3. CC 攻击防护

CC（Challenge Collapsar，挑战黑洞）攻击是 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击的一种，也是一种常见的网站攻击方法。CC 攻击防护功能通过对来自 Web 应用程序客户端的请求进行内容检测、规则匹配和统计计算，对攻击请求予以实时阻断，从而对内网的 Web 服务器进行有效防护。

1.1.2 WAF 特征匹配

设备基于 WAF 策略对攻击报文进行处理。WAF 策略中定义了匹配报文的 WAF 特征和处理报文的 WAF 策略动作。

1. WAF 特征

WAF 特征用来描述网络中的 Web 应用层攻击行为的特征，设备通过将报文与 WAF 特征进行比较来检测和防御攻击。WAF 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 WAF 特征。

设备支持以下两种类型的 WAF 特征：

- 预定义 WAF 特征：系统中的 WAF 特征库自动生成。设备不支持对预定义 WAF 特征的内容进行创建、修改和删除。
- 自定义 WAF 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 WAF 特征，及时阻止网络攻击，否则，不建议用户自定义 WAF 特征。

2. WAF 策略动作

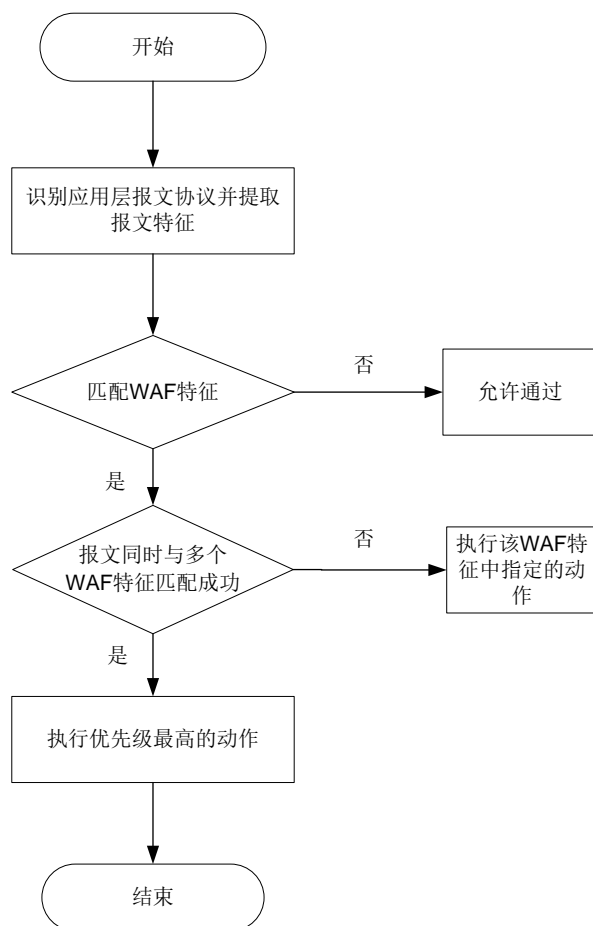
WAF 策略动作是指设备对检测出攻击的报文做出的处理。包括如下几种类型：

- 丢弃：丢弃报文。
- 放行：允许报文通过。
- 重置：通过发送 TCP 的 **reset** 报文断开 TCP 连接。
- 重定向：将报文重定向到指定的 Web 页面上。
- 源阻断：丢弃报文并将该报文的源 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”。
- 捕获：捕获报文。
- 生成日志：记录日志信息。

3. WAF 特征匹配处理流程

WAF 特征匹配处理流程如[图 1-1](#)所示：

图1-1 WAF 特征匹配处理流程图



WAF 特征匹配功能是通过在 DPI 应用 profile 中引用 WAF 策略，并在安全策略或对象策略中引用 DPI 应用 profile 来实现的，WAF 特征匹配处理的具体实现流程如下：

- (1) 设备识别应用层报文协议并提取报文特征。

- (2) 设备将提取的报文特征与 WAF 特征进行匹配，并进行如下处理：
- 如果报文未与任何 WAF 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 WAF 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 WAF 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。

1.1.3 语义分析检测

设备通过对报文中的 SQL 语句进行语法分析来检测是否存在 SQL 注入攻击，并根据检测结果对报文进行相应的处理：

- 如果检测到攻击，则判断是否配置了 WAF 策略动作。如果已配置，则对报文执行指定的动作；如果未配置，则放行报文，并以快速日志方式输出 WAF 日志。有关 WAF 动作的详细介绍，请参见“[1.1.2 2. WAF 策略动作](#)”。
- 如果未检测到攻击，则放行报文。

1.1.4 CC 攻击防护

设备基于 CC 攻击防护策略对 CC 攻击行为进行检测，CC 攻击防护策略中定义了攻击报文的匹配条件、攻击行为的检测方式以及处理报文的动作等。

1. CC 攻击检测方式

设备支持使用请求速率和请求集中度双重检测方式对 CC 攻击进行检测。

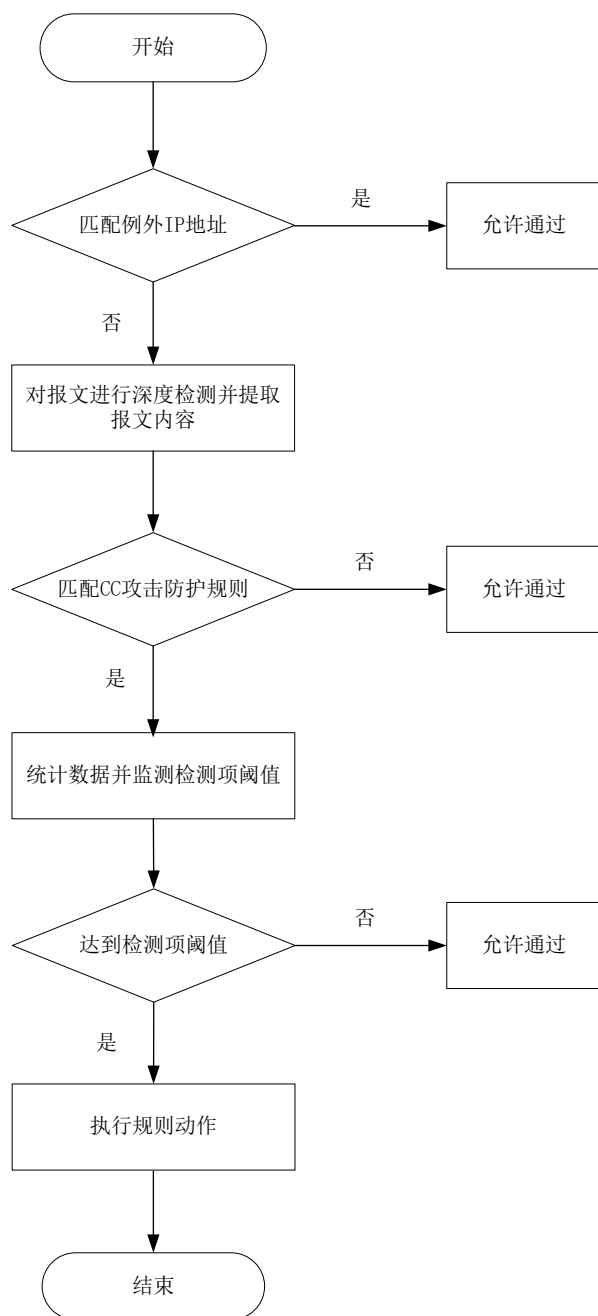
- 请求速率检测：用于检测客户端是否过于频繁地访问某网站。
- 请求集中度检测：用于检测客户端是否主要针对某网站进行访问。

每种检测方式可以分别配置检测阈值，设备将统计到的用户访问网站的结果与检测阈值进行比较，如果统计结果达到任意一个检测阈值，则认为客户端的访问为 CC 攻击。

2. CC 攻击防护实现流程

CC 攻击防护功能是通过在安全策略中引用 WAF 策略，并且在 WAF 策略中引用 CC 攻击防护策略来实现的。当用户的数据流量经过设备时，设备将进行 CC 攻击防护处理。处理流程如[图 1-2](#)所示：

图1-2 CC 攻击防护数据处理流程图



- (1) 如果报文与例外 IP 地址匹配成功，则直接放行该报文；如果未匹配成功，则进入步骤（2）处理。
- (2) 设备对报文进行深度内容检测，并提取报文内容。
- (3) 设备将提取的报文内容与 CC 攻击防护策略规则进行匹配，并进行如下处理：
 - 如果未匹配到任何 CC 攻击防护策略规则，则对报文执行允许动作。
 - 如果匹配到一条 CC 攻击防护策略规则，则不再进行后续规则匹配，进入步骤（4）处理。
- (4) 设备对报文数据进行统计，并与规则下配置的检测项阈值进行比较，并进行如下处理：

- 如果统计结果达到任意一个检测项的阈值，则认为存在 CC 攻击行为，并执行规则下配置的动作，包括允许、黑名单和记录日志。
- 如果未达到阈值，则放行报文。

1.1.5 WAF 防护功能的处理优先级

当 WAF 特征匹配、语义分析检测和 CC 攻击防护功三种功能检测出同一个攻击报文时，则对报文执行三种功能的处理动作中更高优先级的动作。动作优先级从高到低依次为：重置 > 重定向 > 丢弃 > 允许，对于黑名单、日志和捕获三个动作只要处理动作中包含就会执行。

1.1.6 WAF 特征库升级与回滚

WAF 特征库是用来对经过设备的应用层流量进行 Web 攻击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 WAF 特征库，同时设备也支持 WAF 特征库回滚功能。

1. WAF 特征库升级

WAF 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 WAF 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 WAF 特征库。
- 手动离线升级：当设备无法自动获取 WAF 特征库时，需要管理员先手动获取最新的 WAF 特征库，再更新设备本地的 WAF 特征库。

2. WAF 特征库回滚

如果管理员发现设备当前 WAF 特征库对报文进行检测和防御 Web 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。

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。

设备型号	业务板类型	说明
M9006	Blade IV 防火墙业务板	支持
M9010	Blade V 防火墙业务板	支持
M9014	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持

M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.2 WAF的License要求

WAF 功能需要购买并正确安装 License 后才能使用。License 过期后，WAF 功能可以采用设备中已有的 WAF 特征库正常工作，但无法将特征库升级到 License 过期后官网发布的特征库版本。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.3 WAF配置任务简介

1.3.1 WAF 特征匹配配置任务简介

- (1) [创建 WAF 策略](#)
- (2) [配置筛选 WAF 特征的属性](#)
- (3) [配置 WAF 策略动作](#)
- (4) [配置 WAF 策略动作引用的应用层检测引擎动作参数 profile](#)

1.3.2 语义分析检测配置任务简介

- (1) [创建 WAF 策略](#)
- (2) [开启语义分析检测功能](#)

1.3.3 CC 攻击防护配置任务简介

- (1) [创建 WAF 策略](#)
- (2) [创建 CC 攻击防护策略](#)
- (3) [创建 CC 攻击防护策略规则](#)
- (4) [在 WAF 策略中引用 CC 攻击防护策略](#)
- (5) （可选）[管理 CC 攻击防护策略规则](#)

1.3.4 WAF 策略的公共配置任务简介

- (1) （可选）[激活 WAF 策略配置](#)
- (2) [在 DPI 应用 profile 中引用 WAF 策略](#)
- (3) 引用 DPI 应用 profile

请选择以下一项任务进行配置：

- [在安全策略中引用 DPI 应用 profile](#)
- [在对象策略中引用 DPI 应用 profile](#)
- (4) (可选) [配置自定义 WAF 特征](#)
- (5) (可选) [配置 WAF 特征库升级和回滚](#)
- (6) (可选) [配置 WAF 白名单](#)

1.4 配置WAF特征匹配功能

1.4.1 创建 WAF 策略

1. 功能简介

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

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 WAF 策略，并进入 WAF 策略视图。

```
waf policy policy-name
```

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

1.4.2 配置筛选 WAF 特征的属性

1. 功能简介

在 WAF 策略中，可以定义不同类型的属性作为 WAF 特征的过滤条件。如果某个属性中配置了多个参数，则 WAF 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 WAF 策略视图。

```
waf policy policy-name
```

- (3) 配置筛选 WAF 特征的属性。

- 配置筛选 WAF 特征的保护对象属性。

```
protected-target { target [ sub-target subtarget ] | all }
```

缺省情况下，WAF 策略匹配所有保护对象的特征。

- 配置筛选 WAF 特征的攻击分类属性。

```
attack-category { category [ sub-category subcategory ] | all }
```

缺省情况下，WAF 策略匹配所有攻击分类的特征。

- 配置筛选 WAF 特征的动作属性。

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

缺省情况下，WAF 策略匹配所有动作的特征。

- 配置筛选 WAF 特征的方向属性。

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

缺省情况下，WAF 策略匹配所有方向的特征。

- 配置筛选 WAF 特征的严重级别属性。

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

缺省情况下，WAF 策略匹配所有严重级别的特征。

1.4.3 配置 WAF 策略动作

1. 功能简介

缺省情况下，新建 WAF 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 WAF 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：WAF 策略中为指定特征配置的动作 > WAF 策略动作 > WAF 特征自身属性的动作。

2. 配置限制和指导

当动作配置为 **logging** 时，设备将记录日志并支持如下两种方式输出日志。

- 快速日志：此方式生成的日志信息直接发送到管理员指定的日志主机。
- 系统日志：此方式生成的日志信息将发送到信息中心，由信息中心决定日志的输出方向。本业务产生的系统日志不支持输出到控制台和监视终端。如需快速获取日志信息，可通过执行 **display logbuffer** 命令进行查看。

系统日志会对设备性能产生影响，建议采用快速日志方式。

有关 **display logbuffer** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”；有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 WAF 策略视图。

```
waf policy policy-name
```

- (3) 配置 WAF 策略动作。

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

缺省情况下，WAF 策略执行特征属性中的动作。

- (4) （可选）修改 WAF 策略中指定特征的动作和生效状态。

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

缺省情况下，预定义 WAF 特征使用系统预定义的状态和动作。

1.4.4 配置 WAF 策略动作引用的应用层检测引擎动作参数 profile

1. 功能简介

每类 WAF 策略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 WAF 策略动作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 WAF 策略动作引用的应用层检测引擎动作参数 profile。

```
waf { block-source | capture | email | logging | redirect }  
parameter-profile parameter-name
```

缺省情况下，WAF 策略动作未引用应用层检测引擎动作参数 profile。

1.5 配置语义分析检测功能

1.5.1 创建 WAF 策略

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 WAF 策略，并进入 WAF 策略视图。

```
waf policy policy-name
```

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

1.5.2 开启语义分析检测功能

1. 功能简介

开启本功能后，设备将同时使用特征匹配和语义分析功能对 SQL 注入攻击进行检测，可以提升该类攻击的识别率，但同时会对设备性能产生影响，请管理员根据实际情况进行配置。

2. 配置限制和指导

开启本功能后会对设备性能产生影响，建议仅在含有 SQL 注入类攻击的场景中开启。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 WAF 策略视图。

```
waf policy policy-name
```

- (3) 开启语义分析功能。

```
semantic-analysis enable
```

缺省情况下，语义分析检测功能处于关闭状态。

1.6 配置CC攻击防护功能

1.6.1 创建 WAF 策略

1. 功能简介

WAF 策略中未引用 CC 攻击防护策略，用户需要手工新建一个 WAF 策略，并在其中引用 CC 攻击防护策略才能使 CC 攻击防护功能生效。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 WAF 策略，并进入 WAF 策略视图。

```
waf policy policy-name
```

缺省情况下，存在一个缺省 WAF 策略，名称为 **default**，不能被修改或删除，且未引用 CC 攻击防护策略。

1.6.2 创建 CC 攻击防护策略

1. 功能简介

设备基于 CC 攻击防护策略对攻击报文进行处理，管理员可以根据实际需求配置匹配报文的过滤条件以及检测项等。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建 CC 攻击防护策略，并进入 CC 攻击防护策略视图。

```
cc-defense policy policy-name
```

- (3) （可选）配置 CC 攻击防护策略的描述信息。

```
description text-string
```

- (4) （可选）配置 CC 攻击检查项的检测周期。

```
detection-interval interval
```

缺省情况下，CC 攻击检查项的检测周期为 30 秒。

- (5) （可选）配置 CC 攻击防护例外 IP 地址。

```
exception { ipv4 ipv4-address | ipv6 ipv6-address }
```

缺省情况下，未配置 CC 攻击防护例外 IP 地址。

1.6.3 创建 CC 攻击防护策略规则

1. 功能介绍

CC 攻击防护策略规则下可以配置如下内容：

- CC 攻击检测的过滤条件，包括：目的 IP 地址、目的端口号和请求方法。
- CC 攻击防护策略规则防护的路径。

- CC 攻击检测的检查项阈值。
- CC 攻击防护策略规则的动作。

CC 攻击防护策略规则的匹配顺序为配置顺序，当报文与一条规则匹配成功时，则结束匹配过程。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 CC 攻击防护策略视图。

```
cc-defense policy policy-name
```

- (3) 创建 CC 攻击防护策略规则，并进入 CC 攻击防护策略规则视图。

```
rule name rule-name
```

- (4) 配置过滤条件。

- 配置作为 CC 攻击防护策略规则过滤条件的目的 IP 地址。

```
destination-address { ipv4 ipv4-address | ipv6 ipv6-address }
```

- 配置作为 CC 攻击防护策略规则过滤条件的目的端口。

```
destination-port port-number
```

- 配置作为 CC 攻击防护策略规则过滤条件的请求方法。

```
method { connect | delete | get | head | options | post | put | trace } *
```

- (5) 配置 CC 攻击防护策略规则防护的路径。

```
protected-url url-text
```

缺省情况下，未配置 CC 攻击防护策略规则防护的路径。

- (6) 开启 X-Forwarded-For 字段检测功能。

```
xff-detection enable
```

缺省情况下，X-Forwarded-For 字段检测功能处于关闭状态。

- (7) 配置 CC 攻击检测项。

```
cc-detection-item { request-concentration [ concentration-value ]  
[ request-number number ] | request-rate [ rate-value ] }
```

缺省情况下，未配置 CC 攻击检测项，设备不对检查项进行检测。

- (8) 配置规则动作。

```
action { block-source [ block-time ] | permit }
```

缺省情况下，CC 攻击防护策略规则的动作作为 **permit**。

- (9) 开启日志记录功能。

```
logging enable
```

缺省情况下，日志记录功能处于关闭状态。

1.6.4 在 WAF 策略中引用 CC 攻击防护策略

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 WAF 策略视图。

```
waf policy policy-name
```

- (3) 在 WAF 策略中引用 CC 攻击防护策略。

```
apply cc-defense policy policy-name
```

1.6.5 管理 CC 攻击防护策略规则

1. 移动 CC 攻击防护策略规则

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 CC 攻击防护策略视图。

```
cc-defense policy policy-name
```

- (3) 移动 CC 攻击防护策略规则。

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

2. 复制 CC 攻击防护策略规则

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 CC 攻击防护策略视图。

```
cc-defense policy policy-name
```

- (3) 复制 CC 攻击防护策略规则。

```
rule copy rule-name new-rule-name
```

1.7 激活WAF策略配置

1. 功能简介

缺省情况下，当 WAF 策略发生变更时（即被创建、修改和删除），系统将会检测在 20 秒的间隔时间内是否再次发生了配置变更，并根据判断结果执行如下操作：

- 如果间隔时间内未发生任何配置变更，则系统将在下一个间隔时间结束时（即 40 秒时）执行一次激活操作，使这些策略的配置生效。
- 如果间隔时间内再次发生了配置变更，则系统将继续按照间隔时间周期性地检测是否发生配置变更。

如果用户希望对变更的配置立即进行激活，可执行 **inspect activate** 命令手工激活，使配置立即生效。

2. 配置限制和指导

WAF 策略中对语义分析检测功能和 CC 攻击防护功能的修改是即时生效的，不需要配置本功能。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 WAF 策略配置。

inspect activate

缺省情况下，WAF 策略被创建、修改和删除后，系统会自动激活配置使其生效。



注意

执行此命令会暂时中断 DPI 业务的处理，可能导致其他基于 DPI 功能的业务同时出现中断。例如，安全策略无法对应用进行访问控制、七层负载均衡业务无法基于应用进行负载分担等。

1.8 在DPI应用profile中引用WAF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 WAF 功能，必须在 DPI 应用 profile 中引用指定的 WAF 策略。

2. 配置限制和指导

一个 DPI 应用 profile 中只能引用一个 WAF 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 WAF 策略。

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

缺省情况下，DPI 应用 profile 中未引用 WAF 策略。

1.9 在安全策略中引用DPI应用profile

- (1) 进入系统视图。

system-view

- (2) 进入安全策略视图。

security-policy { **ip** | **ipv6** }

- (3) 进入安全策略规则视图。

rule { *rule-id* | [*rule-id*] **name** *rule-name* }

- (4) 配置安全策略规则的动作作为允许。

action pass

缺省情况下，安全策略规则动作是丢弃。

- (5) 配置安全策略规则引用 DPI 应用 profile。

profile *app-profile-name*

缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.10 在对象策略中引用DPI应用profile

- (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。

1.11 配置自定义WAF特征

1.11.1 创建自定义 WAF 特征

1. 功能简介

当需要的 WAF 特征在设备当前 WAF 特征库中不存在时，可通过手工方式创建所需的 WAF 特征。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 创建自定义 WAF 特征，并进入自定义 WAF 特征视图。

```
waf signature user-defined name signature-name
```

缺省情况下，未配置自定义 WAF 特征。

- (3) （可选）配置自定义 WAF 特征的描述信息。

```
description text
```

1.11.2 配置自定义 WAF 特征属性

1. 功能简介

特征具有多种属性，包括动作、检测方向、严重级别和特征下规则间的逻辑关系。

一个自定义特征下可以配置多条规则作为特征的匹配条件，如果规则间是逻辑与的关系，报文需要匹配该自定义特征的所有规则才结束匹配过程；如果规则间是逻辑或的关系，一旦报文与某条规则匹配成功就结束此匹配过程。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入自定义 WAF 特征视图。

```
waf signature user-defined name signature-name
```

缺省情况下，不存在自定义 WAF 特征。

- (3) 配置自定义 WAF 特征属性。

- 配置自定义 WAF 特征的动作。

```
action { block-source | drop | permit | reset } [ capture | logging ]  
*
```

缺省情况下，自定义 WAF 特征的动作作为 **permit**。

- 配置自定义 WAF 特征的检测方向。

```
direction { any | to-client | to-server }
```

缺省情况下，自定义 WAF 特征的检测方向为 **any**。

- 配置自定义 WAF 特征的严重级别。

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

缺省情况下，自定义 WAF 特征的严重级别为 **low**。

- 配置自定义 WAF 特征下规则间的逻辑关系。

```
rule-logic { and | or }
```

缺省情况下，自定义 WAF 特征下规则间的逻辑关系为 **or**。

1.11.3 配置自定义 WAF 特征规则

1. 功能简介

设备支持以下两种类型自定义 WAF 特征规则：

- 关键字类型
- 数值类型

规则下可以配置匹配条件以及检查项。仅当报文与规则的匹配条件匹配成功后，才会对规则的检查项进行检测。

一条规则可以配多个检查项，用于精确匹配报文中所需检测的内容。检查项之间为逻辑与的关系，匹配顺序为配置顺序，只有所有检查项都匹配成功，规则才算成功匹配。

触发检查项是同一规则下检查项的触发条件，只有关键字类型自定义特征规则才需要配置触发检查项。如果一条规则的触发检查项匹配失败，则该规则匹配失败，不会再对该规则下的检查项进行检测。

2. 配置限制和指导

- 检查项仅检测指定协议字段范围内的数据。

- 配置检查项匹配的协议字段时，建议依据 HTTP 协议中各协议字段顺序进行配置，否则可能会影响设备的检测结果。
- 对于关键字类型的自定义特征规则，在配置检查项之前，必须先配置触发检查项。删除触发检查项后，将一并删除所有的检查项。
- 可使用偏移量、检测深度和相对偏移量、相对检测深度两组参数中的任意一组精确定位检查项检测的起始和终止位置。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入自定义 WAF 特征视图。

```
waf signature user-defined name signature-name
```

- (3) 创建自定义 WAF 特征规则，并进入自定义 WAF 特征规则视图。

```
rule rule-id pattern-type { integer | keyword }
```

缺省情况下，未配置自定义 WAF 特征规则。

- (4) 配置自定义 WAF 特征规则的匹配条件。

- 配置自定义 WAF 特征规则匹配的源 IP 地址。

```
source-address ip ip-address
```

缺省情况下，自定义 WAF 特征规则匹配所有源 IP 地址。

- 配置自定义 WAF 特征规则匹配的的目的 IP 地址。

```
destination-address ip ip-address
```

缺省情况下，自定义 WAF 特征规则匹配所有目的 IP 地址。

- 配置自定义 WAF 特征规则匹配的源端口。

```
source-port start-port [ to end-port ]
```

缺省情况下，自定义 WAF 特征规则匹配所有源端口。

- 配置自定义 WAF 特征规则匹配的的目的端口。

```
destination-port start-port [ to end-port ]
```

缺省情况下，自定义 WAF 特征规则匹配所有目的端口。

- 配置自定义 WAF 特征规则匹配的 HTTP 报文请求方法。

```
http-method method-name
```

缺省情况下，自定义 WAF 特征规则匹配所有 HTTP 报文请求方法。

- (5) 配置关键字类型自定义 WAF 特征规则的触发检查项和检查项。

- a. 配置触发检查项。

```
trigger field field-name include { hex hex-string | text text-string }  
[ offset offset-value ] [ depth depth-value ]
```

- b. 配置检查项。

```
detection-keyword detection-id field field-name match-type { exclude  
| include } { hex hex-string | regex regex-pattern | text text-string }  
[ offset offset-value [ depth depth-value ] | relative-offset  
relative-offset-value [ relative-depth relative-depth-value ] ]
```

- (6) 配置数值类型自定义 WAF 特征规则的检查项。

```
detection-integer field field-name match-type { eq | gt | gt-eq | lt |  
lt-eq | neq } number
```

1.12 配置WAF特征库升级和回滚

1.12.1 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 WAF 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）WAF 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 WAF 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”。
- 同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.12.2 配置定期自动在线升级 WAF 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 WAF 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 WAF 特征库功能，并进入自动在线升级配置视图。

```
waf signature auto-update
```

缺省情况下，定期自动在线升级 WAF 特征库功能处于关闭状态。

- (3) 配置定期自动在线升级 WAF 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 WAF 特征库。

- (4) （可选）开启 WAF 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 WAF 特征库时会将当前的特征库文件备份为上一版本。

1.12.3 立即自动在线升级 WAF 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 WAF 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 WAF 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 WAF 特征库。

```
waf signature auto-update-now
```

1.12.4 手动离线升级 WAF 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 WAF 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 WAF 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 WAF 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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手动离线升级 WAF 特征库。

```
waf signature update [ override-current ] file-path [ vpn-instance  
vpn-instance-name ] [ source { ip | ipv6 } { ip-address | interface  
interface-type interface-number } ]
```

1.12.5 回滚 WAF 特征库

1. 功能简介

WAF 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 WAF 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 WAF 特征库。

```
waf signature rollback { factory | last }
```

1.13 配置WAF白名单

1. 功能简介

当管理员通过查看 WAF 日志发现存在误报的情况时，可配置 WAF 白名单功能，将日志中获取到的特征 ID、URL 和源 IP 地址加入白名单，设备将放行匹配白名单的报文，降低误报率。

当白名单表项中同时存在特征 ID、URL 和源 IP 地址中的两者或以上时，需要同时匹配才认为匹配成功。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启 WAF 白名单功能。

```
waf whitelist enable
```

缺省情况下，WAF 白名单功能处于开启状态。

- (3) 创建并进入 WAF 白名单表项视图。

```
waf whitelist entry-id
```

- (4) 配置 WAF 白名单表项描述信息。

```
description text
```

缺省情况下，未配置 WAF 白名单表项描述信息。

- (5) 向 WAF 白名单表项中添加匹配信息。请至少选择其中一项进行配置。

- 向 WAF 白名单表项中添加特征 ID。

```
signature-id [ serial-number ] sig-id
```

缺省情况下，WAF 白名单表项中不存在特征 ID。

- 向 WAF 白名单表项中添加源 IP。

```
source-address { ip ipv4-address | ipv6 ipv6-address }
```

缺省情况下，WAF 白名单表项中不存在源 IP 地址。

- 向 WAF 白名单表项中添加 URL。

```
url match-type { accurate | substring } url-text
```

缺省情况下，WAF 白名单表项中不存在 URL。

(6) (可选) 禁用 WAF 白名单表项。

undo entry enable

缺省情况下，WAF 白名单表项处于启用状态。当某个 WAF 白名单表项暂时不需要时，可配置本命令禁用该白名单表项。

(7) 退回到系统视图。

quit

(8) (可选) 激活 WAF 白名单配置。

waf whitelist activate

缺省情况下，当创建、修改和删除含有 URL 的 WAF 白名单后，系统将在 10 秒后自动激活白名单配置使其生效，如果希望对白名单立即进行激活，可执行本命令手工激活。对于不包含 URL 的 WAF 白名单，不需要激活，立即生效。

1.14 WAF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 WAF 的运行情况，通过查看显示信息验证配置的效果。

表1-1 WAF 显示和维护

操作	命令
显示WAF策略信息	display waf policy <i>policy-name</i>
显示WAF特征库版本信息	display waf signature library
显示WAF特征属性列表	display waf signature [<i>pre-defined</i> <i>user-defined</i>] [<i>direction</i> { <i>any</i> <i>to-client</i> <i>to-server</i> }] [<i>category</i> <i>category-name</i> <i>fidelity</i> { <i>high</i> <i>low</i> <i>medium</i> } <i>severity</i> { <i>critical</i> <i>high</i> <i>low</i> <i>medium</i> }] *
显示WAF预定义特征的详细信息	display waf signature pre-defined <i>signature-id</i>
显示WAF自定义特征的详细信息	display waf signature user-defined <i>signature-id</i>

1.15 WAF典型配置举例

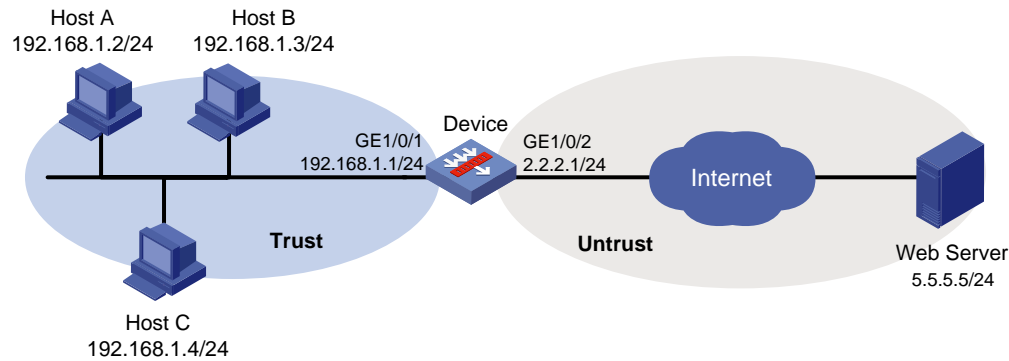
1.15.1 在安全策略中引用缺省 WAF 策略配置举例

1. 组网需求

如图 1-3 所示，Device 分别通过 Trust 安全域和 Untrust 安全域与内部网络和 Internet 相连。现要求使用设备上的缺省 WAF 策略对内部网络进行 Web 攻击防御。

2. 组网图

图1-3 在安全策略中引用缺省 WAF 策略配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 DPI 应用 profile 并激活 WAF 策略配置

创建名为 sec 的 DPI 应用 profile，在 sec 中引用名称为 default 的缺省 WAF 策略，并指定该 WAF 策略的模式为 protect。

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

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

激活 WAF 策略配置。

```
[Device] inspect activate
```

(5) 配置安全策略

配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 WAF 攻击防御。具体配置步骤如下。

```
[Device] security-policy ip
```

```
[Device-security-policy-ip] rule name trust-untrust
```

```
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
```

```
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
```

```
[Device-security-policy-ip-10-trust-untrust] action pass
```

```
[Device-security-policy-ip-10-trust-untrust] profile sec
```

```
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
```

```
[Device-security-policy-ip] quit
```

4. 验证配置

以上配置生效后，使用缺省 WAF 策略可以对已知攻击类型的 Web 攻击进行防御。比如 **GNU_Bash_Remote_Code_Execution_Vulnerability(CVE-2014-6271)** 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 WAF 特征的动作(reset 和 logging) 进行处理。

1.15.2 在安全策略中引用自定义 WAF 策略配置举例

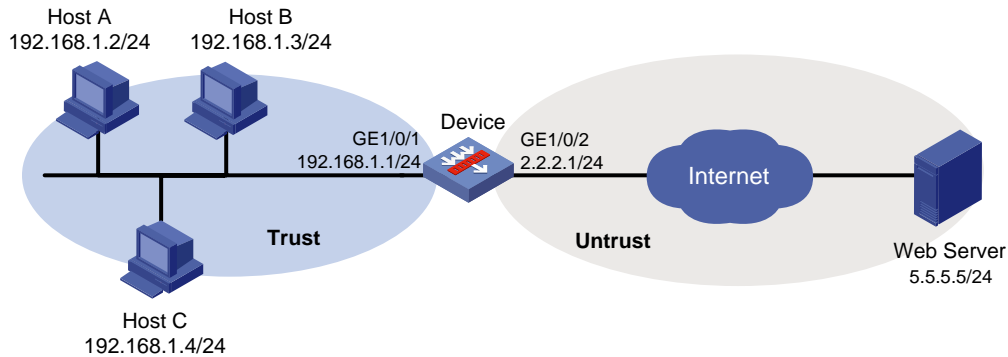
1. 组网需求

如[图 1-4](#)所示，Device 分别通过 Trust 安全域和 Untrust 安全域与内部网络和 Internet 相连。现有组网需求如下：

- 使用设备上的 WAF 策略对内部网络进行 Web 攻击防御。
- 将编号为 2 的预定义 WAF 特征的动作改为丢弃并生成日志。

2. 组网图

图1-4 在安全策略中引用自定义 WAF 策略配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置 WAF 策略

创建一个名称为 waf1 的 WAF 策略，配置筛选 WAF 特征的方向属性为客户端，并配置编号为 2 的预定义 WAF 特征的状态为开启，动作为丢弃并生成日志信息。

```
[Device] waf policy waf1
[Device-waf-policy-waf1] object-dir client
```

```
[Device-waf-policy-waf1] signature override pre-defined 2 enable drop logging
[Device-waf-policy-waf1] quit
```

(5) 配置 DPI 应用 profile 并激活 WAF 策略配置

创建名为 sec 的 DPI 应用 profile，在 DPI 应用 profile sec 中引用 WAF 策略 waf1，并指定该 WAF 策略的模式为 protect。

```
[Device] app-profile sec
[Device-app-profile-sec] waf apply policy waf1 mode protect
[Device-app-profile-sec] quit
```

激活 WAF 策略配置。

```
[Device] inspect activate
```

(6) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 WAF 攻击防御。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

4. 验证配置

以上配置生效后，将有如下验证结果：

- 使用自定义 WAF 策略可以对已知类型的 Web 攻击进行防御。
- 当有报文匹配到编号为 2 的预定义 WAF 特征时，设备将丢弃该报文并生成日志信息。

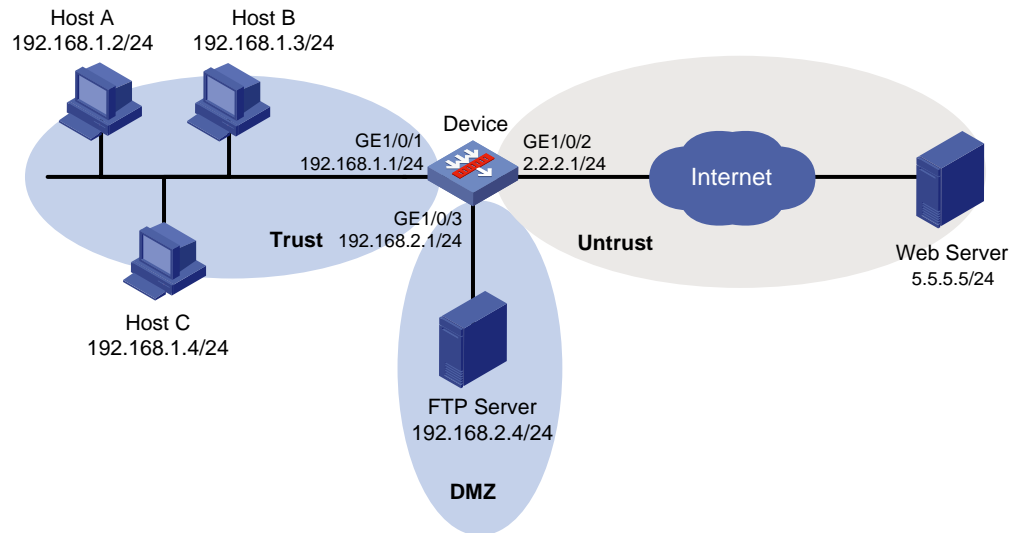
1.15.3 手动离线升级 WAF 特征库配置举例

1. 组网需求

如图 1-5 所示，位于 Trust 安全域的内部网络可通过 Device 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 WAF 特征库文件 waf-1.0.8-encrypt.dat，FTP 服务器的登录用户名和密码分别为 waf 和 123。现需要手动离线升级 WAF 特征库，加载最新的 WAF 特征。

2. 组网图

图1-5 手动离线升级 WAF 特征库配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

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

(4) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Trust 到 DMZ 安全域的流量，使内网用户可以访问 DMZ 安全域中的服务器

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-dmz
[Device-security-policy-ip-11-trust-dmz] source-zone trust
[Device-security-policy-ip-11-trust-dmz] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-11-trust-dmz] destination-zone dmz
[Device-security-policy-ip-11-trust-dmz] action pass
[Device-security-policy-ip-11-trust-dmz] quit
```

- 配置安全策略规则放行设备与 FTP 服务器之间的流量，使设备可以访问 FTP 服务器，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-12-downloadlocalout] source-zone local
[Device-security-policy-ip-12-downloadlocalout] destination-zone dmz
[Device-security-policy-ip-12-downloadlocalout] destination-ip-subnet 192.168.2.0 24
[Device-security-policy-ip-12-downloadlocalout] application ftp
[Device-security-policy-ip-12-downloadlocalout] application ftp-data
[Device-security-policy-ip-12-downloadlocalout] action pass
[Device-security-policy-ip-12-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 手动升级 WAF 特征库

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

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

4. 验证配置

WAF 特征库升级后, 可以通过 `display waf signature library` 命令查看当前特征库的版本信息。

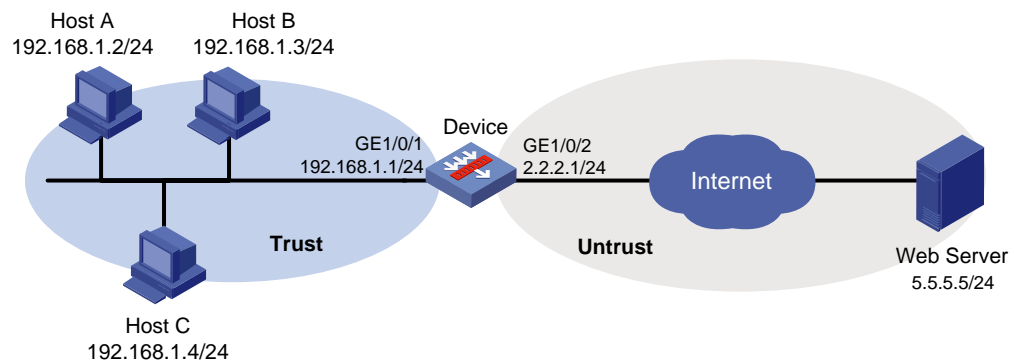
1.15.4 定时自动升级 WAF 特征库配置举例

1. 组网需求

如图 1-6 所示, 位于 Trust 安全域的内部网络可以通过 Device 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, 开始定期自动在线升级设备的 WAF 特征库。

2. 组网图

图1-6 定时自动升级 WAF 特征库配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息, 配置各接口的 IP 地址, 具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址, 具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中, 请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息, 配置静态路由, 本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2, 实际使用中请以具体组网情况为准, 具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息, 将接口加入对应的安全域, 具体配置步骤如下。

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

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

(4) 配置 DNS 服务器地址

指定 DNS 服务器的 IP 地址为 10.72.66.36，确保 Device 可以获取到官网的 IP 地址，具体配置步骤如下。

```
[Device] dns server 10.72.66.36
```

(5) 配置安全策略

- 配置安全策略规则放行 Trust 到 Untrust 安全域的流量，使内网用户可以访问外网资源

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置安全策略规则放行 Local 到 Untrust 安全域的流量，使设备可以访问官网的特征库服务专区，获取特征库文件

```
[Device] security-policy ip
[Device-security-policy-ip] rule name downloadlocalout
[Device-security-policy-ip-11-downloadlocalout] source-zone local
[Device-security-policy-ip-11-downloadlocalout] destination-zone untrust
[Device-security-policy-ip-11-downloadlocalout] action pass
[Device-security-policy-ip-11-downloadlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(6) 配置定期自动在线升级 WAF 特征库

设置定时自动升级 WAF 特征库计划为：每周六上午 9:00:00 前后 30 分钟内，开始自动升级。

```
[Device] waf signature auto-update
[Device-waf-sig-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 60
[Device-waf-sig-autoupdate] quit
```

4. 验证配置

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

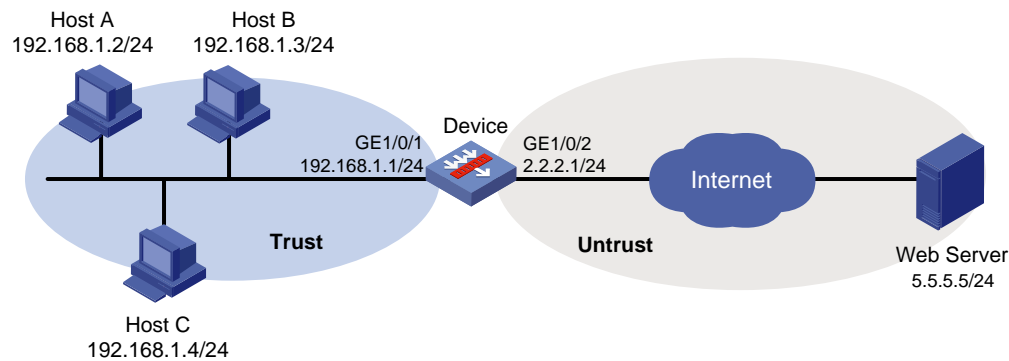
1.15.5 在对象策略中引用缺省 WAF 策略配置举例

1. 组网需求

如图 1-7 所示，Device 分别通过 Trust 安全域和 Untrust 安全域与内部网络和 Internet 相连。现要求使用设备上的缺省 WAF 策略对内部网络进行 Web 攻击防御。

2. 组网图

图1-7 在对象策略中引用缺省 WAF 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 waffilter 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 waffilter
[Device-obj-grp-ip-waffilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-waffilter] 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 WAF 策略 default，并指定该 WAF 策略的模式为 protect。

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

激活 WAF 策略配置。

```
[Device] inspect activate
```

(5) 配置对象策略引用 WAF 业务

创建名为 waffilter 的 IPv4 对象策略，并进入对象策略视图。

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

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

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

```
[Device-object-policy-ip-waffilter] 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 waffilter 对应的报文进行深度检测的对象策略 waffilter。

```
[Device] zone-pair security source trust destination untrust
```

```
[Device-zone-pair-security-Trust-Untrust] object-policy apply ip waffilter
```

```
[Device-zone-pair-security-Trust-Untrust] quit
```

4. 验证配置

以上配置生效后，使用缺省 WAF 策略可以对已知攻击类型的网络攻击进行防御。比如 GNU_Bash_Remote_Code_Execution_Vulnerability(CVE-2014-6271) 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 WAF 特征的动作(reset 和 logging) 进行处理。

1.15.6 在对象策略中引用自定义 WAF 策略配置举例

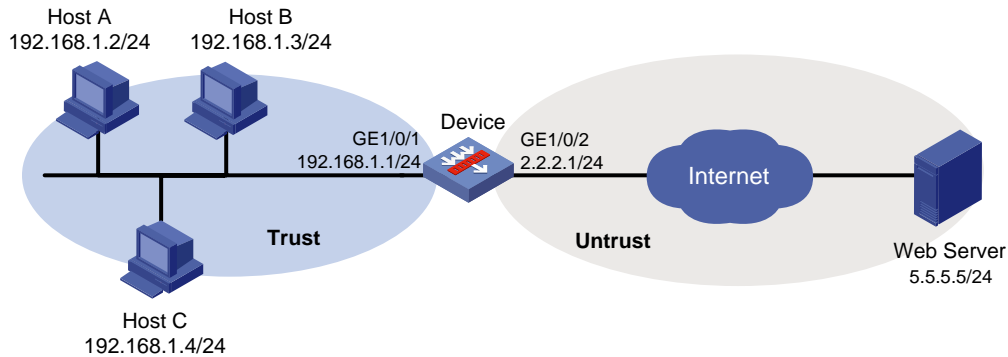
1. 组网需求

如图 1-8 所示，Device 分别通过 Trust 安全域和 Untrust 安全域与内部网络和 Internet 相连。现有组网需求如下：

- 使用设备上的 WAF 策略对内部网络进行 Web 攻击防御。
- 将编号为 2 的预定义 WAF 特征的动作改为丢弃并生成日志。

2. 组网图

图1-8 在对象策略中引用自定义 WAF 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 waffilter 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 waffilter
[Device-obj-grp-ip-waffilter] network subnet 192.168.1.0 24
[Device-obj-grp-ip-waffilter] quit
```

(4) 配置 WAF 策略

创建一个名称为 waf1 的 WAF 策略，并进入 WAF 策略视图。

```
[Device] waf policy waf1
```

配置筛选 WAF 特征的方向属性为客户端。

```
[Device-waf-policy-waf1] object-dir client
```

将编号为 2 的预定义 WAF 特征的状态为开启，动作为丢弃并生成日志信息。

```
[Device-waf-policy-waf1] signature override pre-defined 2 enable drop logging
```

(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 WAF 策略 waf1，并指定该 WAF 策略的模式为 protect。

```
[Device-app-profile-sec] waf apply policy waf1 mode protect
[Device-app-profile-sec] quit
```

激活 WAF 策略配置。

```
[Device] inspect activate
```

(6) 配置对象策略引用 WAF 业务

创建名为 waffilter 的 IPv4 对象策略，并进入对象策略视图。

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

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

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

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

4. 验证配置

以上配置生效后，将有如下验证结果：

- 使用自定义 WAF 策略可以对已知类型的 Web 攻击进行防御。
- 当有报文匹配到编号为 2 的预定义 WAF 特征时，设备将丢弃该报文并生成日志信息。

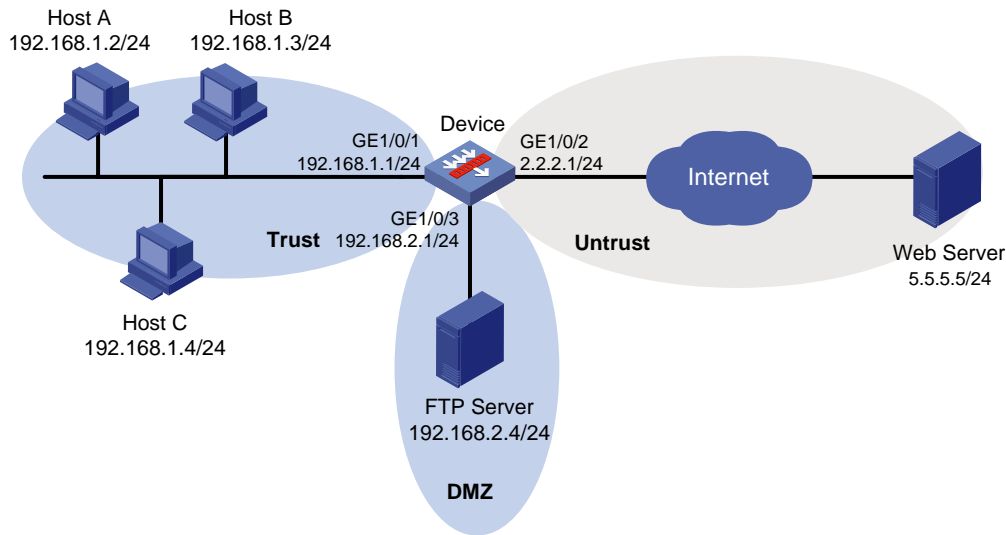
1.15.7 手动离线升级 WAF 特征库配置举例

1. 组网需求

如图 1-9 所示，位于 Trust 安全域的内部网络通过 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 WAF 特征库文件 waf-1.0.8-encrypt.dat，FTP 服务器的登录用户名和密码分别为 waf 和 123。现需求手动离线升级 WAF 特征库，加载最新的 WAF 特征。

2. 组网图

图1-9 基于对象策略手动离线升级 WAF 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 WAF 特征库

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

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

4. 验证配置

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

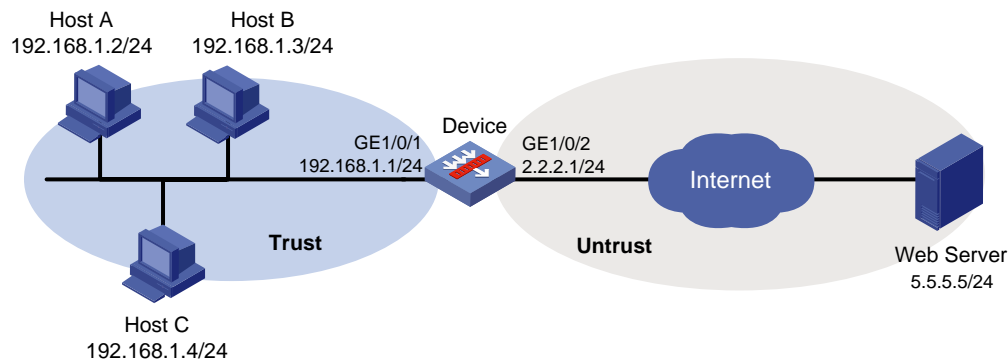
1.15.8 定时自动升级 WAF 特征库配置举例

1. 组网需求

如图1-10所示，位于 Trust 安全域的内部网络通过 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 WAF 特征库。

2. 组网图

图1-10 基于对象策略定时自动升级 WAF 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 WAF 特征库

开启设备自动升级 WAF 特征库功能，并进入自动升级配置视图。

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

设置定时自动升级 WAF 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-waf-sig-autoupdate] update schedule weekly sat start-time 9:00:00 tingle 60
[Device-waf-sig-autoupdate] quit
```

4. 验证配置

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

目 录

1 代理策略	1-1
1.1 代理策略简介	1-1
1.1.1 TCP 代理	1-1
1.1.2 SSL 代理	1-1
1.1.3 代理策略规则	1-5
1.2 代理策略与硬件适配关系	1-7
1.3 代理策略配置限制和指导	1-8
1.4 代理策略配置流程图	1-8
1.5 代理策略配置任务简介	1-9
1.6 代理策略配置准备	1-10
1.7 配置代理策略	1-10
1.7.1 配置代理策略缺省动作	1-10
1.7.2 创建代理策略规则	1-11
1.7.3 配置代理策略规则过滤条件	1-11
1.7.4 配置代理策略规则动作	1-12
1.8 管理代理策略规则	1-12
1.8.1 移动代理策略规则	1-12
1.8.2 禁用代理策略规则	1-12
1.9 配置 SSL 解密证书	1-13
1.9.1 导入 SSL 解密证书	1-13
1.9.2 修改 SSL 解密证书可信度	1-13
1.9.3 删除 SSL 解密证书	1-14
1.10 配置内网服务器证书	1-14
1.10.1 导入内网服务器证书	1-14
1.10.2 删除内网服务器证书	1-14
1.11 配置 SSL 代理域名白名单	1-15
1.11.1 添加自定义域名白名单	1-15
1.11.2 禁用预定义域名白名单	1-15
1.11.3 激活 SSL 代理域名白名单配置	1-15
1.12 代理策略显示和维护	1-16
1.13 代理策略典型配置举例	1-16
1.13.1 代理策略基础配置举例	1-16

1 代理策略

1.1 代理策略简介

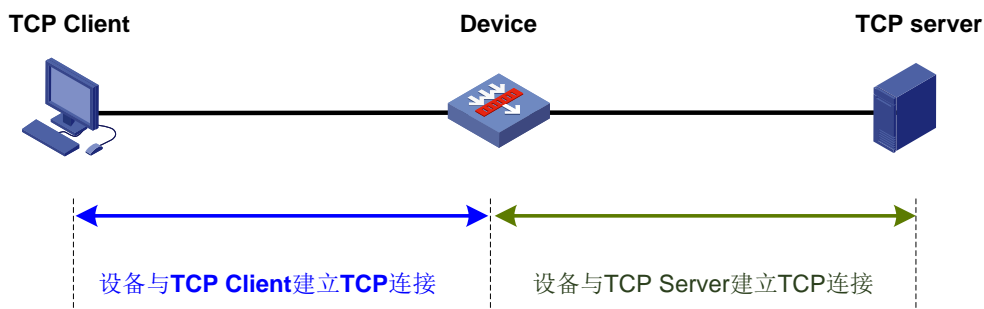
代理策略是一种安全防护策略，通过对客户端和服务端之间的连接进行代理，实现由设备对通过的流量进行检测和控制，避免由于直接访问而出现安全问题。

目前支持 TCP 代理和 SSL 代理功能。

1.1.1 TCP 代理

如下图所示，设备作为 TCP 代理，分别与客户端和服务端之间建立 TCP 连接，为客户端和服务端之间提供 TCP 层隔离，有效地拦截恶意连接和攻击。

图1-1 TCP 代理功能示意图

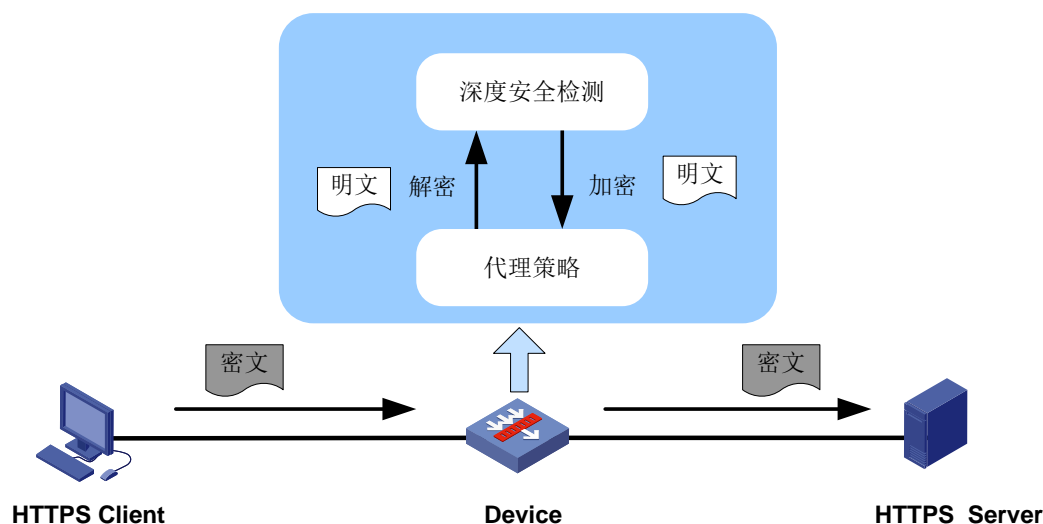


1.1.2 SSL 代理

1. 功能简介

由于 SSL 流量是加密传输的，设备无法对加密的数据进行深度安全检测。在设备上配置 SSL 代理功能后，可解决以上问题。

图1-2 SSL 代理功能示意图



如上图所示，设备根据代理策略判断需要对 HTTPS 客户端的报文进行 SSL 代理，并会分别与客户端和服务端建立 SSL 连接，然后对传输的报文先进行解密，再进行深度安全检测（即进行 DPI 业务处理）。完成深度安全检测后，对放行的报文重新进行加密，并发送到服务器。

有关 DPI 业务的详细介绍，请参见“DPI 深度安全配置指导”。

2. 使用场景

根据 SSL 代理功能防护对象的不同，可分为如下使用场景：

- 保护内网客户端：设备部署在内网客户端所在网络出口处。当内网客户端访问外网服务器时，设备作为代理服务器，会对服务器响应的报文进行解密后再进行 DPI 深度安全等业务的检测，防止内网客户端受到外部恶意网站的攻击。在此场景下，设备使用 SSL 代理服务器证书与内网客户端进行 SSL 协商。有关 SSL 代理服务器证书的介绍，请参见“[3. 基本概念](#)”中的“SSL 代理服务器证书”。
- 保护内网服务器：设备部署在内网服务器所在网络入口处，当外网客户端访问内网服务器时，设备作为代理服务器，会对报文进行解密后再进行 DPI 深度安全等业务的检测，防止外部恶意流量对内网服务器进行攻击。在此场景下，设备使用导入的内网服务器证书与外网客户端进行 SSL 协商。有关内网服务器证书的介绍，请参见“[3. 基本概念](#)”中的“内网服务器证书”。

有关 DPI 深度安全功能的详细介绍，请参见“DPI 深度安全”中的“DPI 深度安全概述”。

3. 基本概念

● SSL 代理服务器证书

保护内网客户端的场景下，设备作为 SSL 代理服务器会代替内网客户端验证外网服务器是否可信。因此，在设备验证了外网服务器的身份后，会基于收到的服务器证书重新签发一个新的服务器证书与内网客户端进行 SSL 协商。这个重新签发的服务器证书就称为 SSL 代理服务器证书，它用来向内网客户端表明设备的身份，同时携带外网服务器是否可信的标识。代理服务器证书支持如下标识：

- 可信：当服务器可信时，设备将标识为“可信”的代理服务器证书发送给客户端，客户端接收到标识为可信的证书后，会通过服务器身份校验，与设备成功建立 SSL 连接。

- 不可信：当服务器不可信时，设备将标识为“不可信”的代理服务器证书发送给客户端，由客户端决定是否继续访问不可信的服务器。
- **SSL 解密证书**

由于设备本身不具备签发证书的功能，需要管理员自行申请具备签发功能的证书并导入到设备中，该证书即为“SSL 解密证书”，设备将使用该证书签发 SSL 代理服务器证书。

管理员将 SSL 解密证书导入到设备时，同时会对证书进行标识：

 - 标识为可信：用于签发可信的 SSL 代理服务器证书。
 - 标识为不可信：用于签发不可信的 SSL 代理服务器证书。
- **内网服务器证书**

在保护内网服务器的场景下，需要管理员先将需要保护的內网服务器的证书导入到设备中。导入证书后，设备将对证书进行解析，生成一个 CER 格式的证书文件和一个密钥文件。

 - **CER 证书**：用于校验服务器身份。设备将计算 CER 证书文件的 MD5 值，并将 MD5 值作为证书的唯一标识。在 SSL 代理过程中，设备收到服务器发来的证书后，会先计算证书的 MD5 值，再与 CER 证书的 MD5 值进行匹配。如果 MD5 值相同，则认为该证书可信，通过校验；如果 MD5 值不同，则认为证书不可信，校验失败，不进行 SSL 代理。
 - **密钥文件**：用于后续 SSL 代理过程中加解密报文。
- **SSL 代理白名单**

SSL 代理白名单是指不需要进行 SSL 代理的网站域名或 IP 地址。配置 SSL 代理白名单功能后，设备将对网站服务器证书匹配 SSL 代理白名单的 SSL 连接不进行代理。

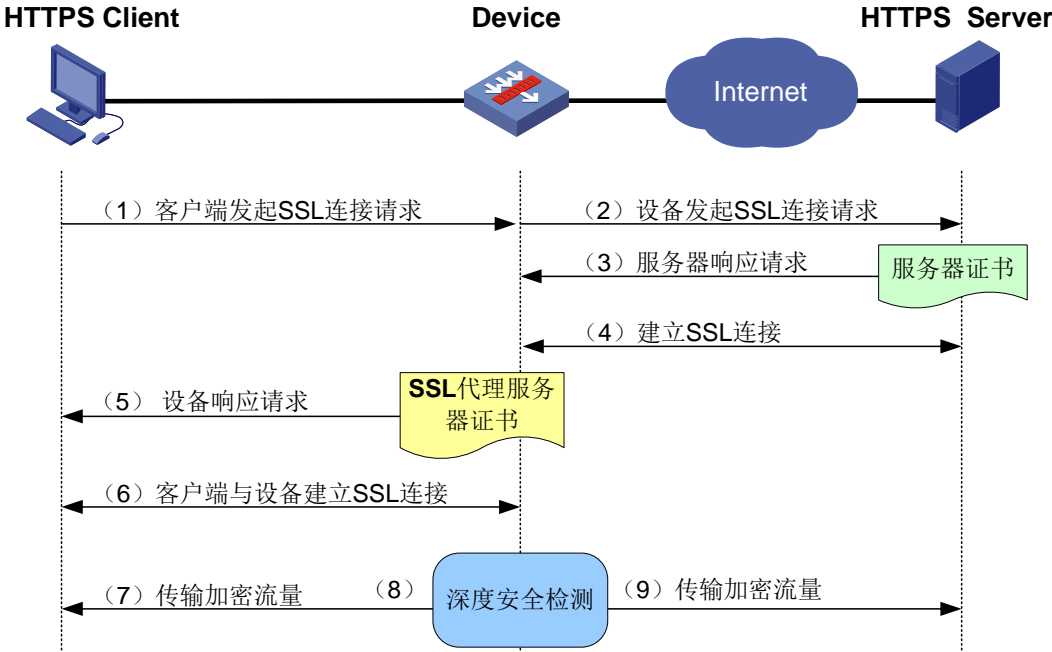
SSL 代理白名单支持的类型如下：

 - 预定义：设备已经预置的 SSL 代理白名单，支持域名白名单和 IP 地址白名单。
 - 自定义：用户手工配置 SSL 代理白名单，仅支持域名白名单。

4. 保护客户端场景下 SSL 代理实现原理

SSL 代理功能是基于 TCP 代理功能实现的，当设备根据代理策略判断需要进行 SSL 代理时，先进行 TCP 代理，建立 TCP 连接，再进行 SSL 代理。在保护内网客户端的场景下，SSL 代理实现流程如[图 1-3](#)所示（以内网客户端访问外网服务器为例）。

图1-3 保护客户端场景下 SSL 代理原理图



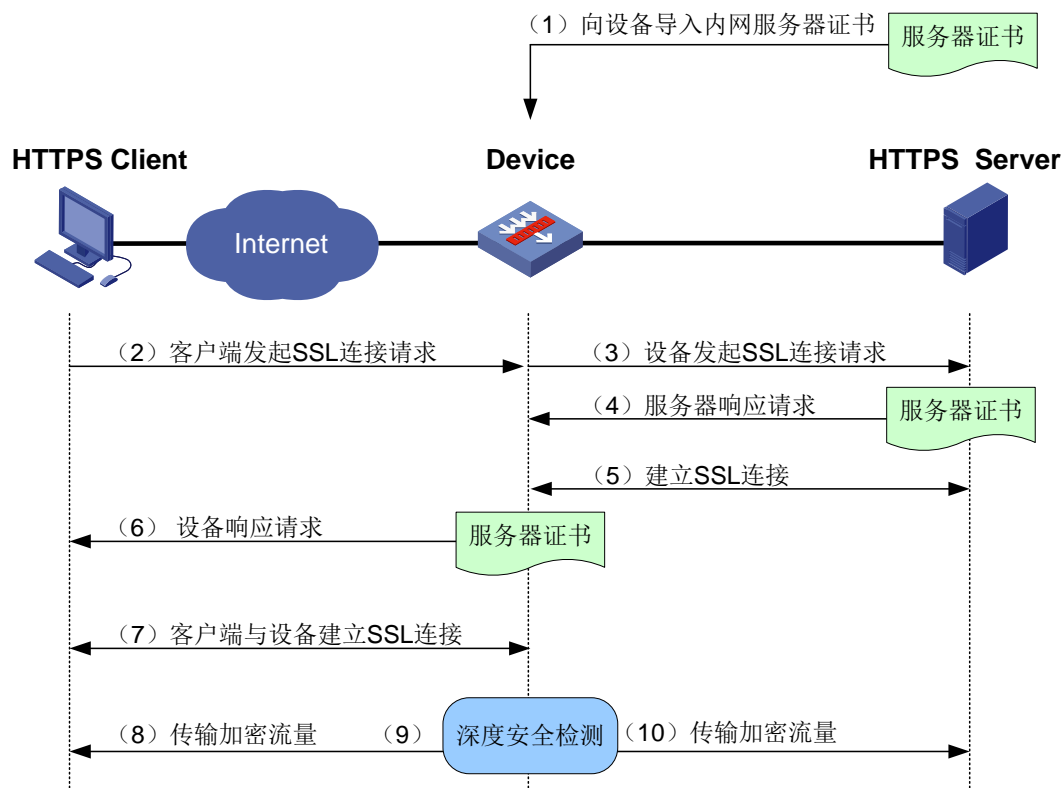
保护内网客户端的场景下，SSL 代理实现流程如下：

- (1) 设备接收到客户端发起的建立 SSL 连接请求。
- (2) 设备作为代理客户端向服务器发起建立 SSL 连接请求。
- (3) 服务器响应请求并发送服务器证书。
- (4) 设备验证服务器证书的合法性，验证通过后与服务器协商加密算法等信息，完成 SSL 握手，成功建立 SSL 连接。
- (5) 设备作为代理服务器，响应客户端请求，并根据服务器证书的内容，使用 SSL 解密证书自己签发 SSL 代理服务器证书，供客户端验证。
- (6) 客户端完成对代理服务器证书的校验后，与设备完成 SSL 握手，建立 SSL 连接。
- (7) 客户端、服务器和设备之间传输加密的 SSL 报文。
- (8) 设备解密 SSL 流量，并进行 DPI 深度安全业务处理。
- (9) 完成 DPI 业务处理后，设备将再次加密后的报文发往服务器。

5. 保护内网服务器场景下 SSL 代理实现原理

SSL 代理功能是基于 TCP 代理功能实现的，当设备根据代理策略判断需要进行 SSL 代理时，先进行 TCP 代理，建立 TCP 连接，再进行 SSL 代理。在保护内网服务器的场景下，SSL 代理实现流程如图 1-4 所示（以外网客户端访问内网服务器为例）。

图1-4 保护内网服务器场景下 SSL 代理原理图



保护内网服务器的场景下，SSL 代理实现流程如下：

- (1) 管理员获取需要保护的內网服务器的证书，并导入到设备中。
- (2) 设备接收到客户端发起的 SSL 连接建立请求。
- (3) 设备作为代理客户端向服务器发起建立 SSL 连接建立请求。
- (4) 服务器响应请求并发送服务器证书。
- (5) 设备验证服务器证书的合法性，验证通过后与服务器协商加密算法等信息，完成 SSL 握手，成功建立 SSL 连接。
- (6) 设备作为代理服务器，响应客户端请求，并将导入的內网服务器证书发送给客户端。
- (7) 客户端完成对服务器证书的校验后，与设备完成 SSL 握手，建立 SSL 连接。
- (8) 客户端、服务器和设备之间传输加密的 SSL 报文。
- (9) 设备解密 SSL 流量，并进行 DPI 深度安全业务处理。
- (10) 完成 DPI 业务处理后，设备将再次加密后的报文发往服务器。

1.1.3 代理策略规则

代理策略对报文的控制是通过代理策略规则实现的，代理策略根据配置的代理策略规则对流量进行划分，对不同的流量进行不同代理方式的处理。规则中可以设置匹配报文的过滤条件以及处理报文的动作。

1. 规则的名称和编号

代理策略中的每条规则都由唯一的名称和编号标识。名称必须在创建规则时由用户手工指定；而编号既可以手工指定，也可以由系统自动分配。

2. 规则的过滤条件

每条规则中均可以配置多种过滤条件，具体包括：源安全域、目的安全域、源 IP 地址、目的 IP 地址、用户、用户组和服务。每种过滤条件中均可以配置多个匹配项，比如源安全域过滤条件中可以指定多个源安全域，任何一个匹配项被匹配成功则认为该过滤条件匹配成功。

3. 规则的匹配顺序

缺省情况下，设备按照规则创建的先后顺序对报文进行匹配，先创建的先匹配，也可以通过手工的方式调整规则的匹配顺序。当一条规则匹配成功后，则结束匹配过程。

建议将规划的所有规则按照“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）进行排序，再按照此顺序配置每一条规则。

4. 规则的动作

设备将根据代理策略规则中配置的动作，对命中策略的流量进行如下处理：

- 动作配置为 **TCP 代理** 时，设备将对命中策略的流量进行 **TCP 代理**。
- 动作配置为 **SSL 解密** 时，设备将对命中策略的流量进行 **SSL 代理**，并基于此对 **SSL 流量** 进行解密，并对解密后的流量进行 **DPI 深度安全检测**。

其中，**SSL 解密** 功能支持如下防护类型：

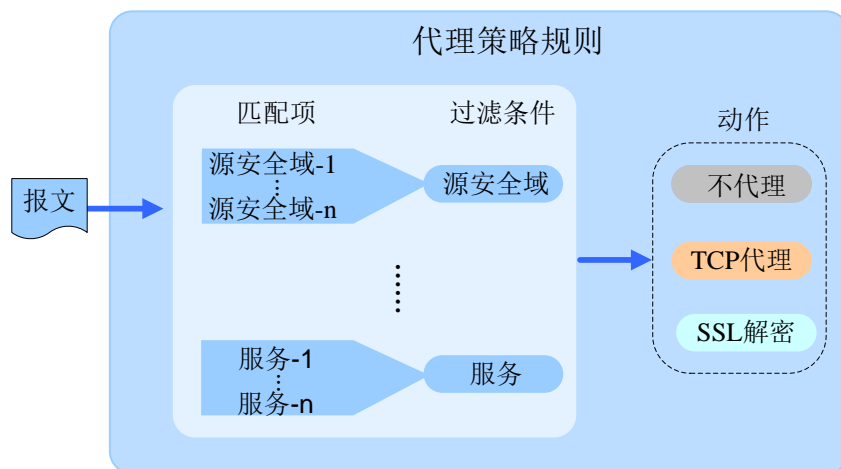
- 客户端：用于保护内网客户端的场景。
- 服务器：用于保护内网服务器的场景。

- 动作配置为不代理时，设备将对命中策略的流量进行透传。

5. 规则的匹配过程

代理策略对规则的匹配过程如[图 1-5](#)所示：

图1-5 代理策略的报文处理流程图



代理策略对报文的处理过程如下：

- (1) 将报文的属性信息与过滤条件中的匹配项进行匹配。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，则报文与此过滤条件匹配失败。
- (2) 若报文与某条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），则报文与此条规则匹配成功。若有一个过滤条件不匹配，则报文与此条规则匹配失败，报文继续匹配下一条规则。以此类推，直到最后一条规则，若报文还未与规则匹配成功，则设备对此报文执行策略配置的缺省动作。
- (3) 若报文与某条规则匹配成功，则结束此匹配过程，并对此报文执行规则中配置的动作。
- (4) 若报文与任何规则都不能匹配成功，则对报文执行代理策略的缺省动作。

1.2 代理策略与硬件适配关系

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。

设备型号	业务板类型	说明
M9006	Blade IV防火墙业务板	支持
M9010	Blade V防火墙业务板	支持
M9014	NAT业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V防火墙业务板	支持
M9008-S	Blade IV防火墙业务板	支持
M9012-S	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V防火墙业务板	支持
M9000-AK001	Blade V防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI防火墙业务板	支持

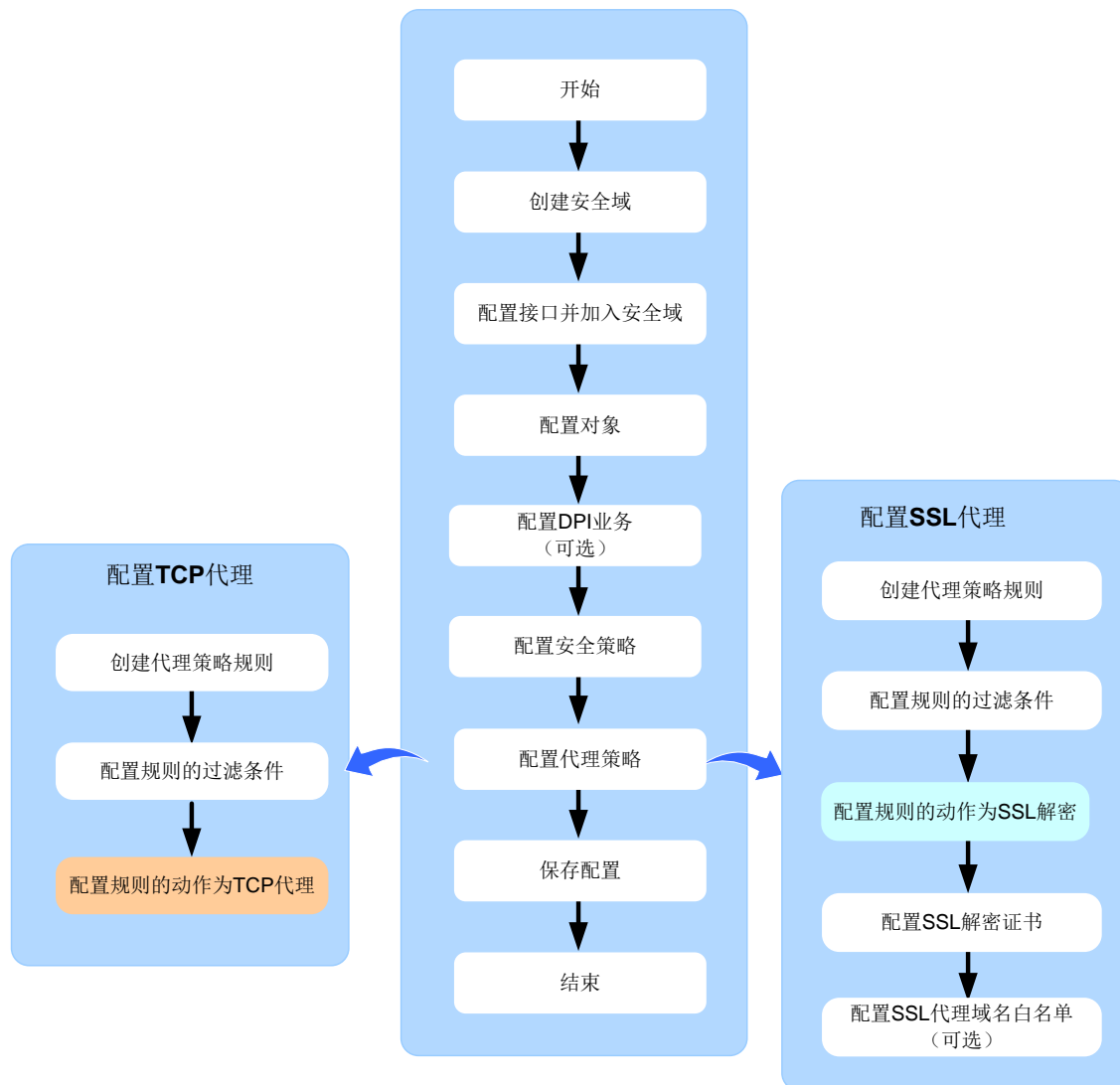
1.3 代理策略配置限制和指导

- TCP 代理与 SSL 代理对设备的转发性能会产生较大的影响，请根据实际情况判断是否需要开启上述功能。
- 配置代理策略时，请尽量细化策略的过滤条件，避免配置过滤条件宽泛的代理策略，影响设备的正常转发。
- 当设备进行 TCP 代理时，如果同时需要进行 NAT 业务的处理，则不支持 ALG 功能。有关 NAT 业务和 ALG 功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“NAT”。
- 如果同时需要配置 SSL 代理和 TCP 代理功能，配置代理策略规则时，请先配置动作为 SSL 解密的规则，避免因为先匹配到动作为 TCP 代理的规则导致 SSL 解密的规则匹配失败。
- 配置 SSL 代理功能时，需要在安全策略中允许源安全域和 Local 域互通。有关安全策略的详细介绍，请参见“安全配置指导”中的“安全策略”。
- 开启 SSL 代理后，IPS 业务的捕获动作将失效。有关捕获动作的详细介绍，请参见“DPI 深度安全配置指导”中的“IPS”。
- 配置 SSL 代理功能时，请务必根据不同的使用场景正确配置 SSL 解密功能的防护类型，并配置相应类型的证书与客户端进行 SSL 协商。
- 在 RBM 双机热备的非对称组网环境中（即同一条流量的报文来回路径不一致），不支持使用 TCP 代理和 SSL 代理功能。即使配置了 TCP 代理或 SSL 代理功能，其功能也不会生效。有关 RBM 双机热备的详细介绍，请参见“高可靠性配置指导”中的“双机热备（RBM）”。

1.4 代理策略配置流程图

代理策略的基本配置思路如[图 1-6](#)所示，在配置代理策略之前需要完成的配置包括：创建安全域、配置接口并加入安全域、配置对象、配置 DPI 业务、配置安全策略。

图1-6 代理策略配置流程图



1.5 代理策略配置任务简介

代理策略配置任务如下：

- (1) [配置代理策略](#)
 - a. [配置代理策略缺省动作](#)
 - b. [创建代理策略规则](#)
 - c. [配置代理策略规则过滤条件](#)
 - d. [配置代理策略规则动作](#)
- (2) (可选) [管理代理策略规则](#)
 - a. [移动代理策略规则](#)
 - b. [禁用代理策略规则](#)
- (3) [配置SSL解密证书](#)

仅当设备需要配置 SSL 代理功能且 SSL 解密防护类型是 **client** 时，才需要进行本配置。

- a. [导入 SSL 解密证书](#)
- b. （可选）[修改 SSL 解密证书可信度](#)
- c. （可选）[删除 SSL 解密证书](#)

(4) [配置内网服务器证书](#)

仅当设备需要配置 SSL 代理功能且 SSL 解密防护类型是 **server** 时，才需要进行本配置。

- a. [导入内网服务器证书](#)
- b. （可选）[删除内网服务器证书](#)

(5) （可选）[配置 SSL 代理域名白名单](#)

- a. [添加自定义域名白名单](#)
- b. [禁用预定义域名白名单](#)
- c. [激活 SSL 代理域名白名单配置](#)

1.6 代理策略配置准备

在配置代理策略之前，需完成以下任务：

- 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”）。
- 配置用户和用户组（请参见“安全配置指导”中的“用户身份识别与管理”）。
- 配置安全域（请参见“基础配置指导”中的“安全域”）。
- 配置安全策略（请参见“安全配置指导”中的“安全策略”）。
- 配置 DPI 业务（请参见“DPI 深度安全配置指导”中的各模块）。

1.7 配置代理策略

1.7.1 配置代理策略缺省动作

1. 功能简介

当不存在代理策略规则或报文未匹配到任何代理策略规则的情况下，设备将对所有经过的报文执行代理策略缺省动作。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入代理策略视图。

```
app-proxy-policy
```

- (3) 配置代理策略默认动作。

```
default action { no-proxy | ssl-decrypt | tcp-proxy }
```

缺省情况下，代理策略缺省动作为不代理。

- (4) 配置代理策略默认动作为 SSL 解密时的 SSL 解密防护类型。

```
default ssl-decrypt protect-mode { client | server }
```

缺省情况下，代理策略默认动作为 SSL 解密时的 SSL 解密防护类型为 **client**。

1.7.2 创建代理策略规则

- (1) 进入系统视图。

system-view

- (2) 进入代理策略视图。

app-proxy-policy

- (3) 创建代理策略规则，并进入代理策略规则视图。

rule { rule-id | [rule-id] name rule-name }

缺省情况下，未配置代理策略规则。

1.7.3 配置代理策略规则过滤条件

1. 配置限制和指导

当代理策略规则中未配置任何过滤条件时，则该规则将匹配所有报文。

当代理策略规则中引用的对象组不存在，或对象组中内容为空时，则该规则将不能匹配任何报文。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 进入代理策略视图。

app-proxy-policy

- (3) 进入代理策略规则视图。

rule { rule-id | [rule-id] name rule-name }

- (4) 配置代理策略规则的过滤条件。

- 配置作为代理策略规则过滤条件的源安全域。

source-zone source-zone-name

缺省情况下，未配置源安全域过滤条件。

- 配置作为代理策略规则过滤条件的目的安全域。

destination-zone destination-zone-name

缺省情况下，未配置目的安全域过滤条件。

- 配置作为代理策略规则过滤条件的源 IP 地址。

source-ip object-group object-group-name

缺省情况下，未配置源 IP 地址过滤条件。

- 配置作为代理策略规则过滤条件的目的 IP 地址。

destination-ip object-group object-group-name

缺省情况下，未配置目的 IP 地址过滤条件。

- 配置作为代理策略规则过滤条件的服务。

service object-group { object-group-name | any }

缺省情况下，未配置服务过滤条件。

- 配置作为代理策略规则过滤条件的用户。


```
user username [ domain domain-name ]
```

缺省情况下，未配置用户过滤条件。

- 配置作为代理策略规则过滤条件的用户组。

```
user-group user-group-name [ domain domain-name ]
```

缺省情况下，未配置用户组过滤条件。

1.7.4 配置代理策略规则动作

- (1) 进入系统视图。

```
system-view
```

- (2) 进入代理策略视图。

```
app-proxy-policy
```

- (3) 进入代理策略规则视图。

```
rule { rule-id | [ rule-id ] name rule-name }
```

- (4) 配置代理策略规则动作。

```
action { no-proxy | ssl-decrypt | tcp-proxy }
```

缺省情况下，代理策略规则动作为不代理。

- (5) 配置 SSL 解密防护类型。

```
ssl-decrypt protect-mode { client | server }
```

缺省情况下，SSL 解密防护类型为 **client**。

本命令仅在代理策略规则动作为 **ssl-decrypt** 时需要配置。

1.8 管理代理策略规则

1.8.1 移动代理策略规则

1. 功能简介

缺省情况下，设备按照规则创建的先后顺序对报文进行匹配，先创建的先匹配，也通过本功能来移动规则的位置，调整规则的匹配顺序。当一条规则匹配成功后，则结束匹配过程。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入代理策略视图。

```
app-proxy-policy
```

- (3) 移动代理策略规则。

```
rule move rule-id before insert-rule-id
```

1.8.2 禁用代理策略规则

- (1) 进入系统视图。

```
system-view
```

- (2) 进入代理策略视图。

```
app-proxy-policy
```

- (3) 进入代理策略规则视图。

```
rule { rule-id | [ rule-id ] name rule-name }
```

- (4) 禁用代理策略规则。

```
disable
```

缺省情况下，代理策略规则处于启用状态。

1.9 配置SSL解密证书

1.9.1 导入 SSL 解密证书

1. 功能简介

设备作为 SSL 代理服务器保护客户端场景下，需要导入 SSL 解密证书。

2. 配置限制和指导

设备上只能存在一份可信证书和一份不可信证书，后续导入的可信或者不可信证书会覆盖原有的证书。

需要在客户端浏览器上安装并信任标识为可信的 SSL 解密证书。

导入成功后，设备将修改证书文件类型为 CER 格式。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 导入 SSL 解密证书。

```
app-proxy ssl-decrypt-certificate import { trusted | untrusted } { pem  
| p12 } filename filename
```

1.9.2 修改 SSL 解密证书可信度

1. 配置限制和指导

设备中只能存在一份可信 SSL 解密证书和一份不可信 SSL 解密证书，若改变证书的可信度，则会覆盖原有的证书。

当 SSL 解密证书成功导入设备后，文件类型会被改为 CER 格式，修改证书时需要将指定的证书后缀名改为.cer。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 修改 SSL 解密证书的可信度。

```
app-proxy ssl-decrypt-certificate modify { trusted | untrusted }  
filename filename
```

1.9.3 删除 SSL 解密证书

1. 配置限制和指导

删除 SSL 解密证书后，设备将不能签发 SSL 代理服务器证书，从而导致客户端因无法验证服务器身份造成 SSL 代理连接失败，设备将直接透传报文。

当证书成功导入设备后，文件类型会被改为 CER 格式，删除证书时需要将指定的证书后缀名改为.cer。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 删除 SSL 解密证书。

```
app-proxy ssl-decrypt-certificate delete filename filename
```

1.10 配置内网服务器证书

1.10.1 导入内网服务器证书

1. 功能简介

设备作为 SSL 代理服务器保护服务器景下，需要导入内网服务器证书。

2. 配置限制和指导

每个保存在设备上的内网服务器证书均有一个 MD5 值，如果导入的内网服务器证书 MD5 值已经存在，设备将覆盖 MD5 值相同的已有证书。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 导入内网服务器证书。

```
app-proxy internal-server-certificate import { p12 | pem } filename  
filename
```

1.10.2 删除内网服务器证书

1. 功能简介

当内网服务器证书过期或不需保护该服务器时，可删除导入的证书。

可通过 **display app-proxy imported internal-server-certificate** 命令查看内网服务器证书的 MD5 值。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 删除内网服务器证书。

```
app-proxy internal-server-certificate delete md5 md5-value
```

1.11 配置SSL代理域名白名单

1.11.1 添加自定义域名白名单

1. 功能简介

对于不需要或不能够以代理方式访问的服务器，可以将这些服务器的域名加入自定义域名白名单。设备对匹配白名单的所有 **SSL** 连接不进行代理。

在如下场景中，设备无法通过客户端或服务器的校验，不能进行 **SSL** 代理，需要配置 **SSL** 代理白名单，使设备直接透传报文：

- 服务器要求对客户端身份进行验证。
- 客户端要求对服务器证书做深度校验。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 添加自定义域名白名单。

```
app-proxy ssl whitelist user-defined-hostname host-name
```

缺省情况下，未配置自定义 **SSL** 代理域名白名单。

1.11.2 禁用预定义域名白名单

- (1) 进入系统视图。

```
system-view
```

- (2) 禁用预定义域名白名单。

```
undo app-proxy ssl whitelist predefined-hostname { chrome-hsts  
[ hostname ] | hostname } enable
```

缺省情况下，预定义 **SSL** 代理域名白名单处于启用状态。

1.11.3 激活SSL代理域名白名单配置

1. 功能简介

需要激活 **SSL** 代理域名白名单配置的场景如下：

- 对自定义 **SSL** 代理域名白名单进行添加、修改和删除操作。
- 对预定义 **SSL** 代理域名白名单进行启用或禁用操作。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 激活 **SSL** 代理域名白名单配置。

```
app-proxy ssl whitelist activate
```

1.12 代理策略显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示代理策略的配置信息、配置白名单和相关证书，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除代理策略使用的 IP 地址白名单和相关证书。

表1-1 代理策略显示和维护

操作	命令
显示代理策略的配置信息	display app-proxy-policy
显示内网服务器证书	display app-proxy imported internal-server-certificate
显示SSL解密证书	display app-proxy ssl-decrypt-certificate
显示服务器证书	(独立运行模式) display app-proxy server-certificate [slot slot-number] (IRF模式) display app-proxy server-certificate [chassis chassis-number slot slot-number [cpu cpu-number]]
显示SSL代理域名白名单	display app-proxy ssl whitelist hostname { user-defined predefined }
显示SSL代理IP地址白名单	(独立运行模式) display app-proxy ssl whitelist { ipv4 ipv6 } { all [slot slot-number] ip-address } (IRF模式) display app-proxy ssl whitelist { ipv4 ipv6 } { all [chassis chassis-number slot slot-number [cpu cpu-number]] ip-address }
清除服务器证书	reset app-proxy server-certificate
清除SSL代理IP地址白名单	reset app-proxy ssl whitelist ip

1.13 代理策略典型配置举例

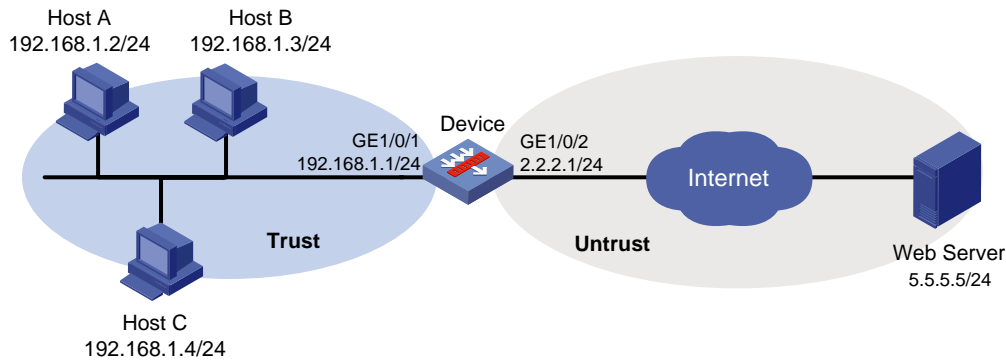
1.13.1 代理策略基础配置举例

1. 组网需求

如图 1-7 所示，Device 作为安全网关部署在内网边界。由于设备无法对 HTTPS 流量进行深度安全检测，导致无法阻断部分网站的访问。现需要配置 SSL 解密功能，对 HTTPS 流量进行 SSL 解密，再进行 DPI 业务检测，保护企业内网用户安全。

2. 组网图

图1-7 代理策略基本配置举例组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[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 obj1 的 IP 地址对象组，并配置其子网地址为 192.168.1.0/24。

```
[Device] object-group ip address obj1
[Device-obj-grp-ip-obj1] network subnet 192.168.1.0 24
[Device-obj-grp-ip-obj1] quit
```

(5) 导入 SSL 解密证书

导入名为 **trust.pem** 的可信 SSL 解密证书和名为 **untrust.pem** 的不可信 SSL 解密证书，分别用于签发标识为可信和不可信的代理服务器证书。

```
[Device] app-proxy ssl-decrypt-certificate import trust pem filename trust.pem
[Device] app-proxy ssl-decrypt-certificate import untrust pem filename untrust.pem
```

(6) 在内网用户浏览器上安装并信任名为 **trust.pem** 的可信 SSL 解密证书（具体配置步骤略）。

(7) 配置代理策略及规则

创建名为 **https** 的代理策略规则，对所有通过 **HTTPS** 协议访问 **Web** 服务器的连接进行 **SSL** 解密。

```
[Device] app-proxy-policy
[Device-app-proxy-policy] rule 1 name https
[Device-app-proxy-policy-rule-1-https] source-zone trust
[Device-app-proxy-policy-rule-1-https] destination-zone untrust
[Device-app-proxy-policy-rule-1-https] source-ip object-group obj1
[Device-app-proxy-policy-rule-1-https] service object-group https
[Device-app-proxy-policy-rule-1-https] action ssl-decrypt
[Device-app-proxy-policy-rule-1-https] quit
```

(8) 配置 URL 过滤功能

创建名称为 **https** 的自定义 URL 过滤分类，并在分类中添加主机名 **www.baidu.com**。

```
[Device] url-filter category https severity 1001
[Device-url-filter-category-https] rule host text www.baidu.com
[Device-url-filter-category-https] quit
```

创建名为 **p1** 的 URL 过滤策略，配置自定义分类 **https** 的动作为重置并生成日志。

```
[Device] url-filter policy p1
[Device-url-filter-policy-p1] category https action reset logging
[Device-url-filter-policy-p1] quit
```

(9) 配置 DPI 应用 profile 并激活 URL 过滤策略和规则配置

创建名为 **sec** 的 DPI 应用 profile，并在 DPI 应用 profile **sec** 中应用 URL 过滤策略 **p1**。

```
[Device] app-profile sec
[Device-app-profile-sec] url-filter apply policy p1
[Device-app-profile-sec] quit
```

激活 URL 过滤策略和规则配置。

```
[Device] inspect activate
```

(10) 配置安全策略

配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 URL 过滤业务检测。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
```

```
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

按照同样的步骤，配置名称为 **untrust-trust** 的安全策略规则，由于使用 **SSL** 代理功能时，设备同时作为代理客户端和代理服务器，需要放行外网到内网的流量。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name untrust-trust
[Device-security-policy-ip-11-untrust-trust] source-zone untrust
[Device-security-policy-ip-11-untrust-trust] destination-zone trust
[Device-security-policy-ip-11-untrust-trust] destination-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-11-untrust-trust] action pass
[Device-security-policy-ip-11-untrust-trust] profile sec
[Device-security-policy-ip-11-untrust-trust] quit
```

按照同样的步骤，配置名称为 **proxyserverlocalin** 和 **proxyserverlocalout** 的安全策略规则，保证设备可作为代理服务器，对客户端向服务器发起的访问流量进行代理。具体配置步骤如下。

```
[Device-security-policy-ip] rule name proxyserverlocalin
[Device-security-policy-ip-12-proxyserverlocalin] source-zone trust
[Device-security-policy-ip-12-proxyserverlocalin] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-12-proxyserverlocalin] destination-zone local
[Device-security-policy-ip-12-proxyserverlocalin] action pass
[Device-security-policy-ip-12-proxyserverlocalin] quit
[Device-security-policy-ip] rule name proxyserverlocalout
[Device-security-policy-ip-13-proxyserverlocalout] source-zone local
[Device-security-policy-ip-13-proxyserverlocalout] destination-zone trust
[Device-security-policy-ip-13-proxyserverlocalout] destination-ip-subnet 192.168.1.0
24
[Device-security-policy-ip-13-proxyserverlocalout] action pass
[Device-security-policy-ip-13-proxyserverlocalout] quit
```

按照同样的步骤，配置名称为 **proxycientlocalin** 和 **proxycientlocalout** 的安全策略规则，保证设备可作为代理客户端，对服务器发往客户端的流量进行代理。具体配置步骤如下。

```
[Device-security-policy-ip] rule name proxycientlocalin
[Device-security-policy-ip-14-proxycientlocalin] source-zone untrust
[Device-security-policy-ip-14-proxycientlocalin] destination-zone local
[Device-security-policy-ip-14-proxycientlocalin] destination-ip-subnet 192.168.1.0
24
```



```
[Device-security-policy-ip-14-proxyclientlocalin] action pass
[Device-security-policy-ip-14-proxyclientlocalin] quit
[Device-security-policy-ip] rule name proxyclientlocalout
[Device-security-policy-ip-15-proxyclientlocalout] source-zone local
[Device-security-policy-ip-15-proxyclientlocalout] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-15-proxyclientlocalout] destination-zone untrust
[Device-security-policy-ip-15-proxyclientlocalout] action pass
[Device-security-policy-ip-15-proxyclientlocalout] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

4. 验证配置

以上配置完成后，当用户访问 www.baidu.com 时，设备会阻断该访问并打印日志。管理员也可以通过 **display app-proxy server-certificate** 命令查看设备作为 SSL 代理客户端时接收到的客户端访问的服务器证书，可以看到设备进行 SSL 代理的次数、第一次进行 SSL 代理的时间以及最近一次进行 SSL 代理的时间等信息。

目 录

1 IP 信誉	1-1
1.1 IP 信誉简介	1-1
1.2 IP 信誉的报文处理流程	1-1
1.3 IP 信誉与硬件适配关系	1-2
1.4 IP 信誉的 License 要求	1-2
1.5 IP 信誉配置任务简介	1-3
1.6 开启全局 IP 信誉功能	1-3
1.7 配置攻击分类执行的动作	1-3
1.8 配置例外 IP 地址	1-4
1.9 配置 IP 信誉特征库升级和回滚	1-4
1.9.1 配置限制和指导	1-4
1.9.2 配置定期自动在线升级 IP 信誉特征库	1-4
1.9.3 立即自动在线升级 IP 信誉特征库	1-5
1.9.4 手动离线升级 IP 信誉特征库	1-5
1.9.5 回滚 IP 信誉特征库	1-6
1.10 开启 Top 排名统计功能	1-6
1.11 IP 信誉显示和维护	1-7
1.12 IP 信誉典型配置举例	1-7
1.12.1 IP 信誉基础配置举例	1-7

1 IP 信誉

1.1 IP信誉简介

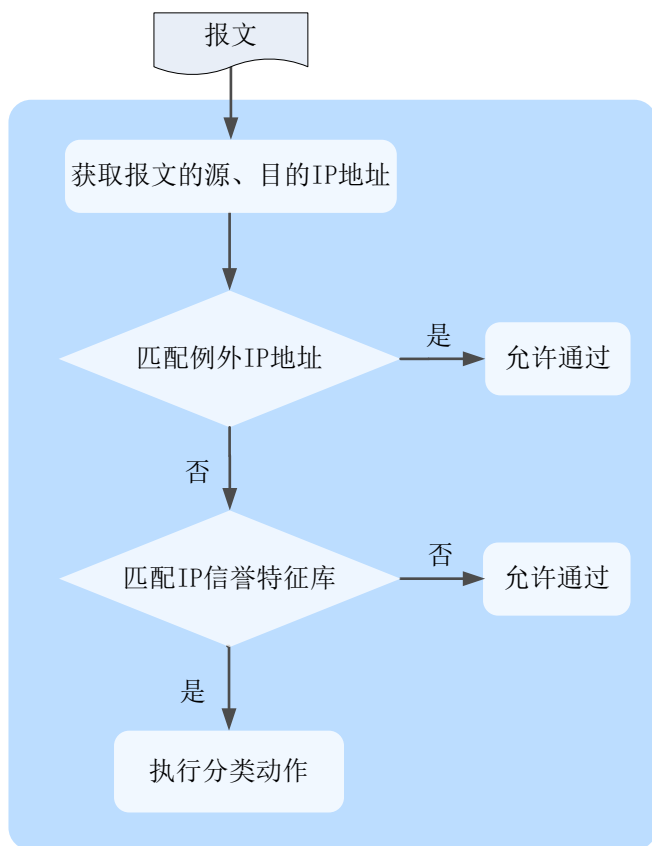
IP 信誉根据 IP 信誉特征库中的 IP 地址信息对网络流量进行过滤。

IP 信誉特征库主要是具有僵尸主机 DDoS 攻击、命令注入攻击、木马下载和端口扫描等风险的 IP 地址集合。特征库中包含每个 IP 地址的方向属性、所属攻击分类、和攻击分类的动作等信息。

1.2 IP信誉的报文处理流程

IP 信誉对报文的处理流程如[图 1-1](#)所示：

图1-1 IP 信誉的报文处理流程图



IP 信誉功能对报文的处理过程如下：

- (1) 设备将报文的源 IP 地址和目的 IP 地址与例外 IP 地址进行匹配。任何一个 IP 地址与例外 IP 地址匹配成功，均放行报文。如果匹配失败，则进入下一步处理。
- (2) 设备将报文的源 IP 地址和目的 IP 地址与特征库中的 IP 地址进行匹配。特征库中的 IP 地址具有方向属性，包含源、目的和双向（既可作为源地址也可作为目的地址）。仅当报文的 IP 地址与特征库中的 IP 地址和方向属性均一致时，才认为匹配成功（如果特征库中 IP 地址的方向

属性是双向，则报文的源 IP 地址和目的 IP 地址均可匹配成功），并执行特征库中 IP 地址所属攻击分类的动作；如果匹配失败，则放行报文。设备支持的攻击分类动作如下：

- 若动作为“允许”，则设备将允许此报文通过。
- 若动作为“丢弃”，则设备将丢弃此报文。
- 若动作为“日志”，则设备将记录 IP 信誉日志。

1.3 IP信誉与硬件适配关系

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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持
M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.4 IP信誉的License要求

IP 信誉功能需要购买并正确安装 License 后才能使用。License 过期后，IP 信誉功能可以使用设备中已有的特征库正常工作，但无法将特征库升级到 License 过期后官网发布的特征库版本。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.5 IP信誉配置任务简介

IP 信誉配置任务如下：

- (1) [开启全局 IP 信誉功能](#)
- (2) [配置攻击分类执行的动作](#)
- (3) （可选）[配置例外 IP 地址](#)
- (4) [配置 IP 信誉特征库升级和回滚](#)
- (5) （可选）[开启 Top 排名统计功能](#)

1.6 开启全局IP信誉功能

1. 功能简介

开启 IP 信誉功能后，设备对报文的源、目的 IP 地址进行匹配，如果命中 IP 信誉库，则执行此 IP 地址所属攻击分类的动作。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IP 信誉视图。

```
ip-reputation
```

- (3) 开启全局 IP 信誉功能。

```
global enable
```

缺省情况下，全局 IP 信誉功能处于关闭状态。

1.7 配置攻击分类执行的动作

1. 功能简介

IP 信誉特征库中，一个 IP 地址可对应多种攻击分类，每种攻击分类都有对应执行的动作。

当 IP 地址只属于一种攻击分类时，设备将对匹配上该 IP 地址的报文执行攻击分类对应的动作；当 IP 地址属于多种攻击分类时，设备将对匹配上该 IP 地址的报文执行多种攻击分类中优先级最高的动作。其中，动作的优先级从高到底依次为：丢弃>允许。

只要 IP 地址所属的任一攻击分类配置了日志动作，则对匹配上该 IP 地址的报文执行记录日志动作。

设备仅支持以快速日志的方式输出 IP 信誉日志，有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IP 信誉视图。

```
ip-reputation
```

- (3) 配置攻击分类执行的动作。

```
attack-category attack-id { action { deny | permit } | logging { disable  
| enable } } *
```

缺省情况下，未配置对指定攻击分类执行的动作，设备执行 IP 信誉特征库中的缺省动作。

1.8 配置例外IP地址

1. 功能简介

若报文的源或目的 IP 地址与例外 IP 地址匹配成功，则设备直接放行该报文。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IP 信誉视图。

```
ip-reputation
```

- (3) 配置例外 IP 地址。

```
exception ipv4 ipv4-address
```

缺省情况下，未配置例外 IP 地址。

1.9 配置IP信誉特征库升级和回滚

1.9.1 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 IP 信誉功能的正常运行。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）IP 信誉特征库时，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 IP 信誉特征库会失败。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”。
- 同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.9.2 配置定期自动在线升级 IP 信誉特征库

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，管理员可以采用定期自动在线升级方式来对设备上的 IP 信誉特征库进行升级。

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 IP 信誉特征库功能，并进入自动在线升级配置视图。

```
ip-reputation signature auto-update
```

缺省情况下，定期自动在线升级 IP 信誉特征库功能处于关闭状态。

- (3) 配置定期自动在线升级 IP 信誉特征库的时间。

```
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 之间开始自动升级 IP 信誉特征库。

1.9.3 立即自动在线升级 IP 信誉特征库

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 IP 信誉特征库有更新时，可以选择立即自动在线升级方式来及时升级 IP 信誉特征库版本。

执行此命令后，设备将立即自动升级 IP 信誉特征库，且会备份当前的 IP 信誉特征库文件到设备存储介质下名为“ipreputation_sigpack_curr.dat”的文件中。

2. 配置限制和指导

本功能生效与否，与是否开启了定期自动升级 IP 信誉特征库功能无关。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 立即自动在线升级 IP 信誉特征库。

```
ip-reputation signature auto-update-now
```

1.9.4 手动离线升级 IP 信誉特征库

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方式手动离线升级 IP 信誉特征库版本：

- 本地升级：使用设备本地保存的特征库文件升级系统中的 IP 信誉特征库版本。
- FTP/TFTP 升级：设备通过 FTP 或 TFTP 方式自动下载远程服务器上保存的特征库文件到本地，再使用本地保存的特征库文件升级系统中的 IP 信誉特征库版本。

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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 配置准备

- 本地升级：使用此方式前，请管理员先从官方网站获取特征库文件并保存到设备中。
- FTP/TFTP 升级：使用此方式前，需要确保设备与远程服务器网络互通。

4. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手动离线升级 IP 信誉特征库。

```
ip-reputation signature update file-path [ vpn-instance  
vpn-instance-name ] [ source { ip | ipv6 } { ip-address | interface  
interface-type interface-number } ]
```

1.9.5 回滚 IP 信誉特征库

1. 功能简介

IP 信誉特征库回滚是指将当前的 IP 信誉特征库版本回滚到上一版本的版本。如果管理员发现设备当前 IP 信誉特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前 IP 信誉特征库版本进行回滚。

IP 信誉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 IP 信誉特征库是 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，再执行回滚到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 IP 信誉特征库。

```
ip-reputation signature rollback last
```

1.10 开启Top排名统计功能

1. 功能简介

开启本功能后，设备将对命中 IP 信誉特征库的 IP 地址进行统计排名。

关闭本功能后，统计信息将自动清空。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入 IP 信誉视图。

```
ip-reputation
```


- (3) 开启 Top 排名统计功能。
- `top-hit-statistics enable`
- 缺省情况下，Top 排名统计功能处于关闭状态。

1.11 IP信誉显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示 IP 信誉的配置信息和 Top 排名统计信息等，通过查看显示信息验证配置的效果。

表1-1 IP 信誉显示和维护

操作	命令
显示IP信誉特征库中的攻击分类信息	<code>display ip-reputation attack-category</code>
显示例外IP地址信息	<code>display ip-reputation exception</code>
显示IP信誉特征库信息	<code>display ip-reputation signature library</code>
显示Top排名统计信息	<div>(独立运行模式) <code>display ip-reputation top-hit-statistics [top-number] [slot slot-id]</code> (IRF模式) <code>display ip-reputation top-hit-statistics [top-number] [chassis chassis-number slot slot-id [cpu cpu-id]]</code></div>
显示IP信誉特征库中的IP地址信息	<code>display ip-reputation ipv4 ipv4-address</code>

1.12 IP信誉典型配置举例

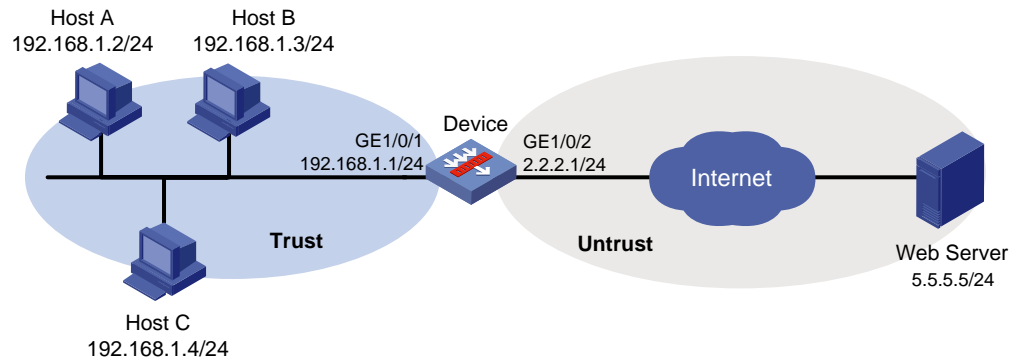
1.12.1 IP 信誉基础配置举例

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。现在需要通过使能 IP 信誉功能，对所有进出 Device 的流量进行控制，并需要开启 Top 统计功能，方便管理员查看攻击统计信息。

2. 组网图

图1-2 IP 信誉基础配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 配置 IP 信誉功能

开启 IP 信誉功能。

```
[Device] ip-reputation
[Device-ip-reputation] global enable
```

开启 Top 排名统计功能。

```
[Device-ip-reputation] top-hit-statistics enable
```

配置 IP 信誉库中编号为 1 的攻击分类对应的动作为丢弃和记录日志。

```
[Device-ip-reputation] attack-category 1 action deny logging enable
[Device-ip-reputation] quit
```

4. 验证配置

配置完成后，当攻击报文匹配到编号为 1 的攻击分类时，设备将对报文执行丢弃动作，并会记录 IP 信誉日志。管理员可到 Web 界面侧查看 IP 信誉 Top 排名统计信息。

目 录

1 域名信誉	1-1
1.1 域名信誉简介.....	1-1
1.2 域名信誉的报文处理流程.....	1-1
1.3 域名信誉的 License 要求.....	1-3
1.4 域名信誉配置任务简介	1-3
1.5 开启全局域名信誉功能	1-3
1.6 配置攻击分类执行的动作.....	1-3
1.7 配置域名例外.....	1-4
1.8 配置域名信誉特征库升级和回滚.....	1-4
1.8.1 配置限制和指导	1-4
1.8.2 配置定期自动在线升级域名信誉特征库	1-5
1.8.3 立即自动在线升级域名信誉特征库	1-5
1.8.4 手动离线升级域名信誉特征库.....	1-5
1.8.5 回滚域名信誉特征库	1-6
1.9 开启命中域名信誉库的 Top 排名统计功能	1-6
1.10 域名信誉显示和维护.....	1-7
1.11 域名信誉典型配置举例	1-7
1.11.1 域名信誉基础配置举例	1-7

1 域名信誉

1.1 域名信誉简介

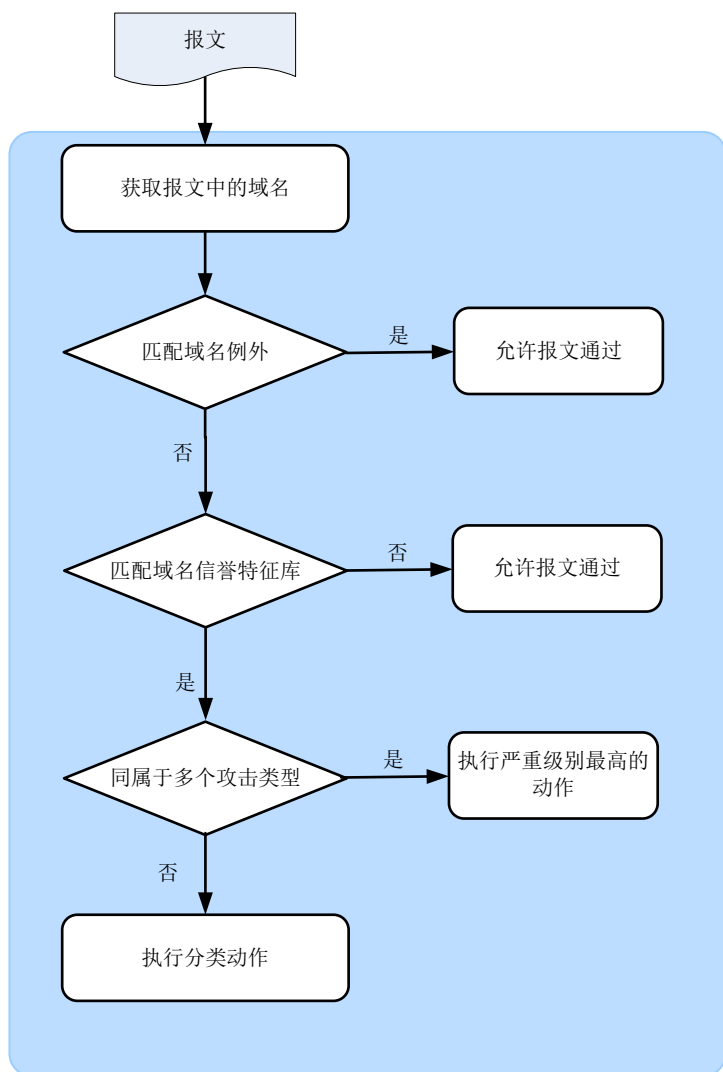
域名信誉根据域名信誉特征库中的域名信息对网络流量进行过滤，允许或禁止用户访问某些网站，达到规范用户上网行为的目的。当 DNS 请求报文中的域名匹配到域名信誉特征库中的域名后，设备将对报文执行相应的操作。

域名信誉特征库主要是具有僵尸主机 DDoS 攻击、命令注入攻击、木马下载和端口扫描等风险的域名集合。特征库中包含每个域名所属的攻击类型等信息。

1.2 域名信誉的报文处理流程

域名信誉对报文的处理流程如[图 1-1](#)所示：

图1-1 域名信誉的报文处理流程图



域名信誉功能对报文的处理过程如下：

- (1) 设备将报文中提取的域名与例外域名进行匹配。如果匹配成功，则放行报文；如果匹配失败，则进入下一步处理。
- (2) 设备将域名与特征库中的域名进行匹配。如果匹配失败，则放行报文；如果匹配成功，则进行如下判断：

- 如果域名属于一个攻击类型，则执行该攻击类型的动作。
- 如果域名同属于多个攻击类型，则执行严重级别最高的动作。

其中，如果动作为“允许”，则设备将允许此报文通过；如果动作为“丢弃”，则设备将丢弃此报文；如果动作为“日志”，则设备将记录域名信誉日志。

1.3 域名信誉的License要求

域名信誉功能需要购买并正确安装 License 才能使用。License 过期后，域名信誉功能可以采用设备中已有的特征库正常工作，但无法将特征库升级到 License 过期后官网发布的特征库版本。关于 License 的详细介绍请参见“基础配置指导”中的“License 管理”。

1.4 域名信誉配置任务简介

域名信誉配置任务如下：

- (1) [开启全局域名信誉功能](#)
- (2) [配置攻击分类执行的动作](#)
- (3) （可选）[配置域名例外](#)
- (4) [配置域名信誉特征库升级和回滚](#)
- (5) （可选）[开启命中域名信誉库的 Top 排名统计功能](#)

1.5 开启全局域名信誉功能

1. 功能简介

开启域名信誉功能后，当 DNS 报文中的域名匹配到域名信誉特征库中域名后，设备将对报文执行此域名所属攻击分类的动作。

2. 配置步骤

- (1) 进入系统视图。
system-view
- (2) 进入域名信誉视图。
domain-reputation
- (3) 开启全局域名信誉功能。
global enable

缺省情况下，全局域名信誉功能处于关闭状态。

1.6 配置攻击分类执行的动作

1. 功能简介

域名信誉特征库中，一个域名可对应多种攻击分类，缺省情况下，每种攻击分类的执行动作均为允许和记录日志，管理员可以根据实际需求，为指定的攻击分类配置执行动作。

当域名只属于一种攻击分类时，设备将对匹配上该域名的报文执行攻击分类对应的动作；当域名属于多种攻击分类时，设备将对匹配上该域名的报文执行多种攻击分类中严重级别最高的动作。其中，动作的严重级别从高到底依次为：丢弃>允许。

只要域名所属的任一攻击分类配置了日志动作，则对匹配上该域名的报文记录日志。

设备仅支持以快速日志的方式输出域名信誉日志，有关快速日志的详细介绍，请参见“网络管理和监控配置指导”中的“快速日志输出”。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入域名信誉视图。

```
domain-reputation
```

- (3) 配置攻击分类执行的动作。

```
attack-category attack-id { action { deny | permit } | logging { disable  
| enable } } *
```

缺省情况下，未配置对指定攻击分类执行的动作，设备执行允许和记录日志动作。

1.7 配置域名例外

1. 功能简介

当管理员信任某些域名，不希望设备对其进行域名信誉检测时，可将该域名设置为例外。

当设备在 DNS 报文中检测到的域名匹配例外域名时，将直接放行报文。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 进入域名信誉视图。

```
domain-reputation
```

- (3) 配置域名例外。

```
exception domain domain-name
```

缺省情况下，未配置域名例外。

1.8 配置域名信誉特征库升级和回滚

1.8.1 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，进而影响域名信誉功能的正常运行。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）域名信誉特征库时，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，否则设备升级域名信誉特征库会失败。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”。

同一时刻只能对一个特征库进行升级，如果当前已有其他特征库正在升级，请稍后再试。

1.8.2 配置定期自动在线升级域名信誉特征库

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域名信誉特征库进行升级。

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域名信誉特征库功能，并进入自动在线升级配置视图。

```
domain-reputation signature auto-update
```

缺省情况下，定期自动在线升级域名信誉特征库功能处于关闭状态。

- (3) 配置定期自动在线升级域名信誉特征库的时间。

```
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 之间自动开始升级域名信誉特征库。

1.8.3 立即自动在线升级域名信誉特征库

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域名信誉特征库有更新时，可以选择立即自动在线升级方式来及时升级域名信誉特征库版本。

执行此命令后，将立即自动升级设备上的域名信誉特征库，且会备份当前的域名信誉特征库文件。此命令的生效与否，与是否开启了定期自动升级域名信誉特征库功能无关。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 立即自动在线升级域名信誉特征库。

```
domain-reputation signature auto-update-now
```

1.8.4 手动离线升级域名信誉特征库

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域名信誉特征库版本：

- **本地升级：**使用设备本地保存的特征库文件升级系统中的域名信誉特征库版本，使用此方式前，请先从官方网站获取特征库文件并导入到设备中。
- **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，并升级系统中的域名信誉特征库版本。

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主控板上，否则设备升级特征库会失败。（独立运行模式）

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全局主用主控板上，否则设备升级特征库会失败。（IRF 模式）

如果管理员希望手动离线升级特征库时发送给 TFTP、FTP 服务器的请求报文的源 IP 地址是一个特定的地址时，可配置 **source** 参数。例如，当组网环境中设备发出的报文需要经过 NAT 地址转换后才能访问 TFTP、FTP 服务器时，则需要管理员通过 **source** 参数指定一个符合 NAT 地址转换规则的源 IP 地址（其中，如果设备需要经过一台独立的 NAT 设备进行地址转换时，本命令指定的 IP 地址必须可以与 NAT 设备三层路由可达），使设备发出的报文可以进行 NAT 地址转换等处理，正常访问 TFTP、FTP 服务器。

2. 配置限制和指导

当同时配置了 **source** 和 **vpn-instance** 参数时，需要保证 **source** 中指定的源 IP 地址或接口所属 VPN 实例与 **vpn-instance** 中配置的 VPN 实例相同。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 手动离线升级域名信誉特征库。

```
domain-reputation signature update file-path [ vpn-instance  
vpn-instance-name ] [ source { ip | ipv6 } { ip-address | interface  
interface-type interface-number } ]
```

1.8.5 回滚域名信誉特征库

1. 功能简介

域名信誉特征库回滚是指将当前的域名信誉特征库版本回滚到上一版本的版本。如果管理员发现设备当前域名信誉特征库版本在检测和防御网络攻击时，误报率较高或出现异常情况，则可以对当前域名信誉特征库版本进行回滚。

域名信誉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。例如当前域名信誉特征库是 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，再执行回滚到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) 回滚域名信誉特征库。

```
domain-reputation signature rollback last
```

1.9 开启命中域名信誉库的Top排名统计功能

1. 功能简介

开启本功能后，设备将对命中域名信誉特征库的域名进行统计排名。

关闭本功能后，统计信息将自动清空。

2. 配置步骤

- (1) 进入系统视图。
`system-view`
 - (2) 进入域名信誉视图。
`domain-reputation`
 - (3) 开启命中域名信誉库的 Top 排名统计功能。
`top-hit-statistics enable`
- 缺省情况下，命中域名信誉库的 Top 排名统计功能处于关闭状态。

1.10 域名信誉显示和维护

在完成上述配置后，在任意视图下执行 `display` 命令可以显示域名信誉的配置信息和命中域名信誉库的 Top 排名统计信息等，通过查看显示信息验证配置的效果。

表1-1 域名信誉显示和维护

操作	命令
显示域名信誉攻击分类信息	<code>display domain-reputation attack-category</code>
显示域名例外信息	<code>display domain-reputation exception</code>
显示域名信誉特征库信息	<code>display domain-reputation signature library</code>
显示命中域名信誉库的Top排名统计信息	(独立运行模式) <code>display domain-reputation top-hit-statistics [top-number] [slot slot-id [cpu cpu-number]]</code> (IRF模式) <code>display domain-reputation top-hit-statistics [top-number] [chassis chassis-number slot slot-id [cpu cpu-number]]</code>
显示域名的域名信誉信息	<code>display domain-reputation domain domain-name</code>

1.11 域名信誉典型配置举例

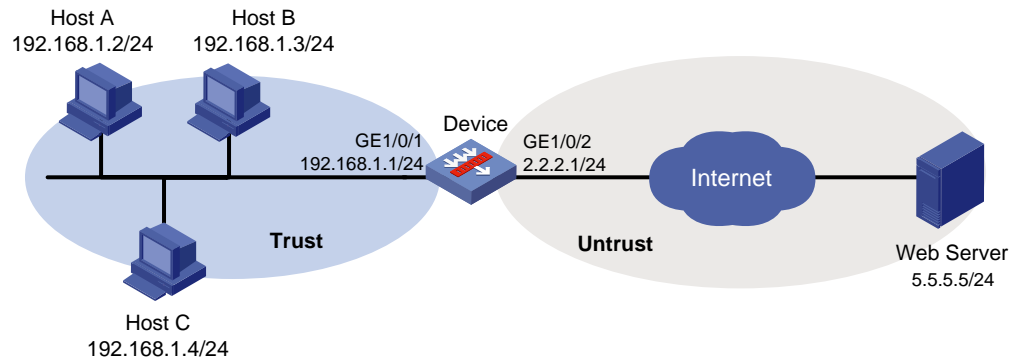
1.11.1 域名信誉基础配置举例

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。现在需要通过使能域名信誉功能，对公司各部门的非法域名请求进行控制。

2. 组网图

图1-2 域名信誉基础配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(3) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(4) 配置安全策略

配置名称为 trust-untrust 的安全策略规则，使内网用户可以访问外网。具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
```

```
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

(5) 配置域名信誉功能

开启域名信誉功能。

```
[Device] domain-reputation
[Device-domain-reputation] global enable
```

开启 Top 排名统计功能。

```
[Device-domain-reputation] top-hit-statistics enable
```

配置域名信誉库中编号为 1 的攻击分类对应的动作为丢弃和记录日志。

```
[Device-domain-reputation] attack-category 1 action deny logging enable
```

4. 验证配置

配置完成后，当攻击报文匹配到编号为 1 的攻击分类时，设备将对报文执行丢弃动作，并会记录日志。管理员可到 Web 界面侧查看域名信誉 Top 排名统计信息。

目 录

1 APT 防御.....	1-1
1.1 APT 防御简介	1-1
1.1.1 APT 防御实现流程	1-1
1.1.2 文件还原条件	1-1
1.1.3 沙箱检测原理	1-2
1.1.4 APT 防御功能与防病毒功能联动	1-2
1.2 配置任务简介	1-2
1.3 配置沙箱联动功能	1-2
1.4 配置 APT 防御策略	1-4
1.5 在 DPI 应用 profile 中引用 APT 防御策略	1-5
1.6 在安全策略中引用 DPI 应用 profile	1-5
1.7 在对象策略中引用 DPI 应用 profile	1-5
1.8 APT 防御显示和维护	1-6
1.9 APT 防御典型配置举例	1-6
1.9.1 在安全策略中引用 APT 防御策略配置举例	1-6

1 APT 防御

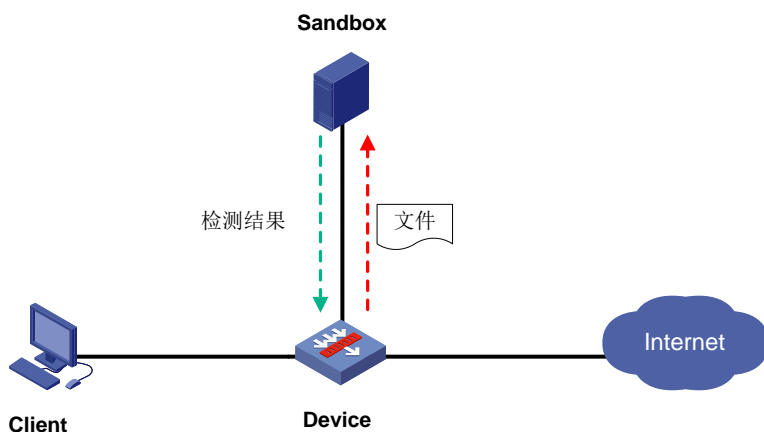
1.1 APT防御简介

APT（Advanced Persistent Threat，高级持续性威胁）攻击，是一种针对特定目标进行长期持续性的网络攻击。目前，沙箱技术是防御 APT 攻击最有效的方法之一，它用于构造隔离的威胁检测环境。设备通过与沙箱进行联动，将网络流量送入沙箱进行隔离分析，由沙箱给出是否存在威胁的结论。如果沙箱检测到某流量为恶意流量，设备将对流量实施阻断等处理。

1.1.1 APT 防御实现流程

设备配置了 APT 防御功能后，当流量经过设备时，设备将进行 APT 防御处理。处理流程如[图 1-1](#)所示。

图1-1 APT 防御实现流程



- (1) Internet 中的攻击者向企业内部发起 APT 攻击，设备对攻击流量进行应用层协议识别以及文件识别。
- (2) 设备对攻击流量中的文件进行还原，并将还原后的文件送往沙箱进行威胁分析。
- (3) 沙箱获取到文件后将运行该文件，并对运行后的行为进行检测分析。检测结束后，会向设备推送检测结果，并将检测结果缓存到 APT 缓存中。
- (4) 如果检测结果是恶意流量，则设备将根据配置的防病毒策略对后续流量进行阻断或告警等处理，保护企业内网免遭攻击。

1.1.2 文件还原条件

仅当满足如下所有条件时，设备才会对报文中的文件进行还原。

- 报文匹配 APT 防御策略：如果未配置 APT 防御策略，则可忽略此条件。
- 报文中文件的大小符合送往沙箱检测的文件大小限制。
- 设备与沙箱已经成功建立连接。

文件还原成功后，设备会将还原后的文件上送沙箱检测。

1.1.3 沙箱检测原理

沙箱可以看作是一个模拟真实网络建造的虚拟检测系统，当未知文件上送沙箱处理后，沙箱会运行该文件，并会对运行后的行为进行记录。沙箱通过将未知文件的行为和沙箱独有的行为特征库进行匹配，最后给出文件是否为威胁的结论。沙箱的行为特征库是通过分析大量的病毒、漏洞、威胁特征，提炼出各种恶意行为的规律和模式，形成的一套判断规则，它能够提供准确的检测结果。

与根据被检测对象的特征进行识别的检测技术（如防病毒）不同的是，沙箱检测是根据被检测对象的行为进行识别。因此具有可以识别未知文件的优点，可以更好的防御未知威胁。

1.1.4 APT 防御功能与防病毒功能联动

设备收到沙箱推送的检测结果后，如果需要对攻击流量进行进一步的处理，则需要与防病毒功能进行联动。配置防病毒功能后，当后续恶意流量流经设备时，设备将识别恶意流量的应用层协议，并与防病毒策略进行匹配，再根据匹配到的防病毒策略中对应的协议报文执行的动作对恶意流量进行处理。

如果用户只想根据检测结果确定当前流量是否为恶意流量，而不需要对流量进行阻断，则对防病毒功能是否配置不作要求。

有关防病毒功能的详细介绍，请参见“DPI 深度安全配置指导”中的“防病毒”。

1.2 配置任务简介

APT 防御配置任务如下：

- (1) [配置沙箱联动功能](#)
- (2) [配置 APT 防御策略](#)
- (3) [在 DPI 应用 profile 中引用 APT 防御策略](#)
- (4) 引用 DPI 应用 profile

请选择以下一项任务进行配置：

- [在安全策略中引用 DPI 应用 profile](#)
- [在对象策略中引用 DPI 应用 profile](#)

1.3 配置沙箱联动功能

1. 功能简介

设备需要配置如下内容实现与沙箱的联动：

- 沙箱的基本参数：包括沙箱地址、登录沙箱的用户名和密码。
- 开启沙箱联动功能。
- 触发设备与沙箱建立连接：当修改沙箱的基本参数或开启/关闭沙箱联动功能后，都将导致与沙箱的连接中断，需要重新触发与沙箱建立连接。

设备根据 RBM 配置同步是否支持同步沙箱配置，分为如下两种沙箱视图：

- **sandbox**：沙箱视图，当设备进行 RBM 配置同步时，此视图下的所有配置都支持同步。

- **sandbox-local**: 沙箱本地视图，当设备进行 RBM 配置同步时，此视图下的所有配置都不支持同步。

上述两种视图下支持配置的内容完全一致，包括沙箱的基本参数、开启沙箱联动功能以及触发设备与沙箱建立连接，请根据实际需求选择相应的视图进行配置。

有关 RBM 的详细介绍，请参见“可靠性配置指导”中的“双机热备（RBM）配置”。

2. 硬件适配关系

本功能中沙箱本地视图（**sandbox-local**）的支持情况与设备型号有关，具体请参见命令参考。

3. 应用场景

用户需要根据实际情况自行判断，在 RBM 配置同步时，是否需要同步沙箱相关参数。如需同步，则沙箱相关参数必须在沙箱视图下进行配置；否则，沙箱相关参数必须在沙箱本地视图下进行配置。例如，在 RBM 主备场景中，两台设备分别连接不同的沙箱（即两台设备的沙箱配置参数不同），用于提升 APT 防御能力。此时，RBM 配置同步时，则不需要同步沙箱相关参数。所以，沙箱相关的参数均需要在沙箱本地视图（**sandbox-local**）下进行配置。

4. 注意事项

两种沙箱视图互斥，视图间切换时需要执行如下操作：

- 如果已经在沙箱视图下配置了沙箱参数，需要切换到沙箱本地视图时，则需要先在沙箱视图下执行 **undo sandbox** 命令，删除沙箱视图下的所有配置并退回到系统视图，再执行 **sandbox-local** 命令，进入沙箱本地视图配置相应的参数。
- 如果已经在沙箱本地视图下配置了沙箱参数，需要切换到沙箱视图时，则可直接在系统视图下执行 **sandbox** 命令，系统会出现提示：“All sandbox local settings will be lost. Continue? [Y/N]:Y”。用户需要选择“Y”，确认删除沙箱本地视图下的所有配置后，进入沙箱视图配置相应的参数。

5. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 选择如下任意一种视图进行配置：

- 进入沙箱视图。

```
sandbox
```

- 进入沙箱本地视图。

```
sandbox-local
```

- (3) 配置沙箱地址。

```
sandbox-address address-string
```

缺省情况下，未配置沙箱地址。

- (4) 配置沙箱登录用户名。

```
username user-name
```

缺省情况，未配置沙箱登录用户名。

- (5) 配置沙箱登录密码。

```
password { cipher | simple } string
```

缺省情况下，未配置登录沙箱的密码。

- (6) (可选) 配置送往沙箱检测的文件大小上限。

file *file-type* **max-size** *max-file-size*

缺省情况下，未配置送往沙箱检测的文件大小上限，设备使用各类文件类型大小上限的缺省值。

为了降低沙箱的检测压力，上传到沙箱检测的文件大小需要一定限制，不符合文件大小限制的文件不上送沙箱检测。用户可以根据自己的需求进行设置，不同文件类型的大小限制不同。

- (7) 开启沙箱联动功能。

linkage enable

缺省情况下，沙箱联动功能处于关闭状态。

- (8) 触发设备与沙箱建立连接。

linkage try

- (9) 退回到系统视图。

quit

- (10) (可选) 配置 APT 防御缓存记录的上限。

apt cache size *cache-size*

缺省情况下，APT 防御缓存区可缓存记录的上限为 10 万条。

1.4 配置APT防御策略

1. 功能简介

在 APT 防御策略中可以配置上送沙箱检测的文件需要符合的条件，包括应用层协议、文件类型和传输方向。仅当文件报文符合所有条件后，才认为成功匹配 APT 防御策略。

2. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 创建 APT 防御策略。

apt policy *policy-name*

- (3) (可选) 配置 APT 防御策略描述信息。

description *description-string*

缺省情况下，未配置 APT 防御策略的描述信息。

- (4) 配置送往沙箱检测的文件的应用层协议。

application { **all** | **type** { **ftp** | **http** | **https** | **imap** | **nfs** | **pop3** | **smb** | **smtp** }
* }

缺省情况下，未配置需要送到沙箱检测的应用层协议类型。

- (5) 配置送往沙箱检测的文件类型。

file-type { **all** | **name** <1-8> }

缺省情况下，未配置需要送往沙箱检测的文件类型。

- (6) 配置送往沙箱检测的文件传输方向。

```
file-direction { both | download | upload }
```

缺省情况下，送往沙箱检测的文件传输方向为 **both**。

1.5 在DPI应用profile中引用APT防御策略

1. 功能简介

DPI 应用 profile 是一个安全业务的配置模板，为使 APT 防御策略生效，需要在 DPI 应用 profile 中引用指定的 APT 防御策略。一个 DPI 应用 profile 中只能引用一个 APT 防御策略，如果重复配置，则新的配置会覆盖已有配置。

2. 配置限制和指导

与防病毒策略联动时，需要在同一个 DPI 应用 profile 中同时引用防病毒策略和 APT 防御策略。

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 APT 防御策略。

```
apt apply policy policy-name
```

缺省情况下，DPI 应用 profile 中未引用 APT 防御策略。

1.6 在安全策略中引用DPI应用profile

- (1) 进入系统视图。

```
system-view
```

- (2) 进入安全策略视图。

```
security-policy { ip | ipv6 }
```

- (3) 进入安全策略规则视图。

```
rule { rule-id | [ rule-id ] name rule-name }
```

- (4) 配置安全策略规则的动作作为允许。

```
action pass
```

缺省情况下，安全策略规则动作是丢弃。

- (5) 配置安全策略规则引用 DPI 应用 profile。

```
profile app-profile-name
```

缺省情况下，安全策略规则中未引用 DPI 应用 profile。

1.7 在对象策略中引用DPI应用profile

- (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。

1.8 APT防御显示和维护

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 APT 防御的运行情况，通过查看显示信息验证配置的效果。

表1-1 APT 防御显示和维护

操作	命令
显示APT防御缓存中的信息	(独立运行模式) <code>display apt cache [slot slot-number [cpu cpu-number]]</code> (IRF模式) <code>display apt cache [chassis chassis-number slot slot-number [cpu cpu-number]]</code>
显示设备与沙箱的连接状态	<code>display apt linkage state</code>

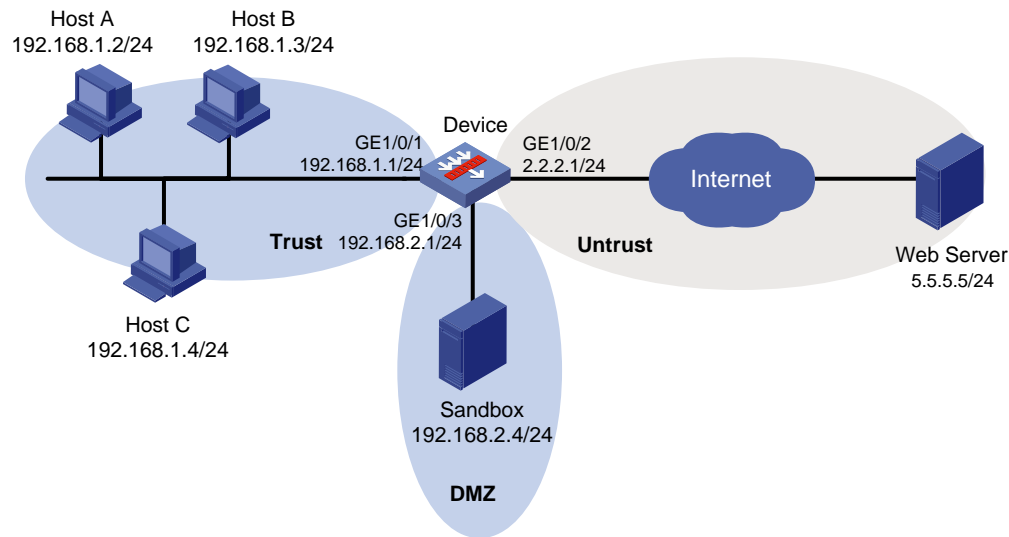
1.9 APT防御典型配置举例

1.9.1 在安全策略中引用 APT 防御策略配置举例

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。企业内网中部署了沙箱，且沙箱与 Device 路由可达。现需要 Device 与沙箱联动，保护内网用户免受 APT 攻击，当沙箱检测到 APT 攻击时，对攻击流量执行阻断操作。

图1-2 在安全策略中引用 APT 防御策略配置组网图



2. 配置步骤

(7) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(8) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达外网 Web Server 的下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[Device] ip route-static 5.5.5.0 24 2.2.2.2
```

(9) 配置接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[Device] security-zone name trust
[Device-security-zone-Trust] import interface gigabitethernet 1/0/1
[Device-security-zone-Trust] quit
[Device] security-zone name untrust
[Device-security-zone-Untrust] import interface gigabitethernet 1/0/2
[Device-security-zone-Untrust] quit
[Device] security-zone name dmz
[Device-security-zone-DMZ] import interface gigabitethernet 1/0/3
```

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

(10) 配置沙箱联动功能

```
[Device] sandbox
[Device-sandbox] sandbox-address 192.168.2.4
[Device-sandbox] username admin
[Device-sandbox] password simple 123456abc
[Device-sandbox] linkage enable
[Device-sandbox] linkage try
```

(11) 配置 APT 防御策略

创建一个名称为 **apt1** 的 APT 防御策略，并配置需要送往沙箱检测的应用层协议为 HTTP、文件类型为 PE、文件传输方向为 upload。

```
[Device] apt policy apt1
[Device-apt-policy-apt1] application type http
[Device-apt-policy-apt1] file-type pe
[Device-apt-policy-apt1] file-direction upload
[Device-apt-policy-apt1] quit
```

(12) 配置 DPI 应用 profile 引用 APT 防御策略和防病毒策略，具体配置步骤如下（本举例假设设备上已经配置了名称为 **antivirus1** 的防病毒策略，策略中将所有传输病毒文件的协议报文的动作设置为阻断，有关防病毒功能的详细介绍，请参见“DPI 深度安全配置指导”中的“防病毒”。）

创建名为 **sec** 的 DPI 应用 profile，并在其中引用名称为 **apt1** 的 APT 防御策略和名称为 **antivirus1** 的防病毒策略。

```
[Device] app-profile sec
[Device-app-profile-sec] apt apply policy apt1
[Device-app-profile-sec] anti-virus apply policy antivirus1 mode protect
[Device-app-profile-sec] quit
```

(13) 配置安全策略

- 配置名称为 **trust-untrust** 的安全策略规则，使内网用户可以访问外网，并对交互报文进行 APT 防御

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-10-trust-untrust] source-zone trust
[Device-security-policy-ip-10-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-10-trust-untrust] destination-zone untrust
[Device-security-policy-ip-10-trust-untrust] action pass
[Device-security-policy-ip-10-trust-untrust] profile sec
[Device-security-policy-ip-10-trust-untrust] quit
```

- 配置名称为 **sandboxlocalout** 的安全策略规则，使设备可将待检测流量上送到沙箱服务器进行检测

```
[Device-security-policy-ip] rule name sandboxlocalout
```

```
[Device-security-policy-ip-11-sandboxlocalout] source-zone local
[Device-security-policy-ip-11-sandboxlocalout] destination-zone dmz
[Device-security-policy-ip-11-sandboxlocalout] destination-ip-subnet 192.168.2.0
24
[Device-security-policy-ip-11-sandboxlocalout] action pass
[Device-security-policy-ip-11-sandboxlocalout] quit
```

- 配置名称为 **sandboxlocalin** 的安全策略规则，使沙箱服务器可将检测结果下发到设备

```
[Device-security-policy-ip] rule name sandboxlocalin
[Device-security-policy-ip-12-sandboxlocalin] source-zone dmz
[Device-security-policy-ip-12-sandboxlocalin] destination-zone local
[Device-security-policy-ip-12-sandboxlocalin] source-ip-subnet 192.168.2.0 24
[Device-security-policy-ip-12-sandboxlocalin] action pass
[Device-security-policy-ip-12-sandboxlocalin] quit
```

激活安全策略配置。

```
[Device-security-policy-ip] accelerate enhanced enable
[Device-security-policy-ip] quit
```

3. 验证配置

以上配置生效后，**Device** 将与沙箱联动，保护内网用户免受 APT 攻击，当沙箱检测到 APT 攻击时，对后续攻击流量执行阻断操作。

目 录

1 DLP	1-1
1.1 DLP 简介	1-1
1.2 DLP 原理	1-1
1.2.1 文件还原	1-2
1.2.2 数据安全检测	1-3
1.3 DLP 与硬件适配关系	1-4
1.4 配置 DLP 功能	1-5
1.5 DLP 显示和维护	1-6
1.6 DLP 典型配置举例	1-6

1 DLP

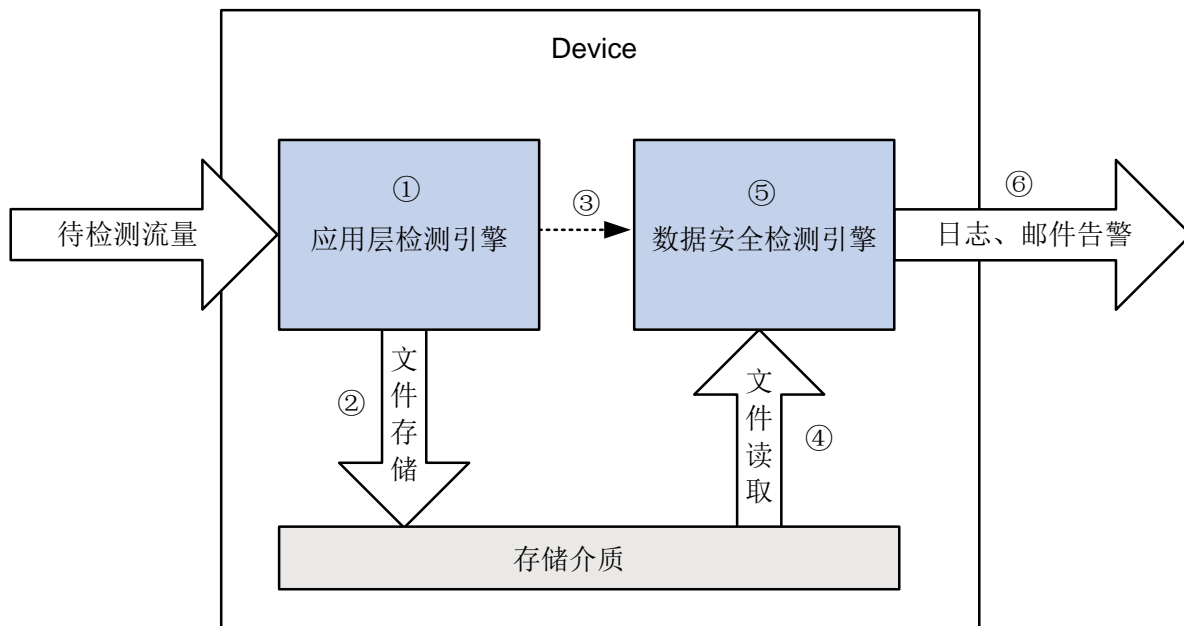
1.1 DLP简介

DLP（Data Loss Prevention，数据防泄漏）是一种针对流经设备的用户敏感文件进行检测和告警的安全技术。通过监控双向流量信息，DLP 功能可以准确发现用户敏感文件的泄露现象，并及时通过日志或邮件形式发出告警，以便用户加固数据安全相关策略。

1.2 DLP原理

如图 1-1 所示，DLP 功能由设备的应用层检测引擎和数据安全检测引擎配合实现。应用层检测引擎提供文件还原功能；数据安全检测引擎提供敏感文件识别功能。关于应用层检测引擎的详细介绍，请参见“DPI 深度安全配置指导”中的“应用层检测引擎”。

图1-1 DLP 功能流程示意图



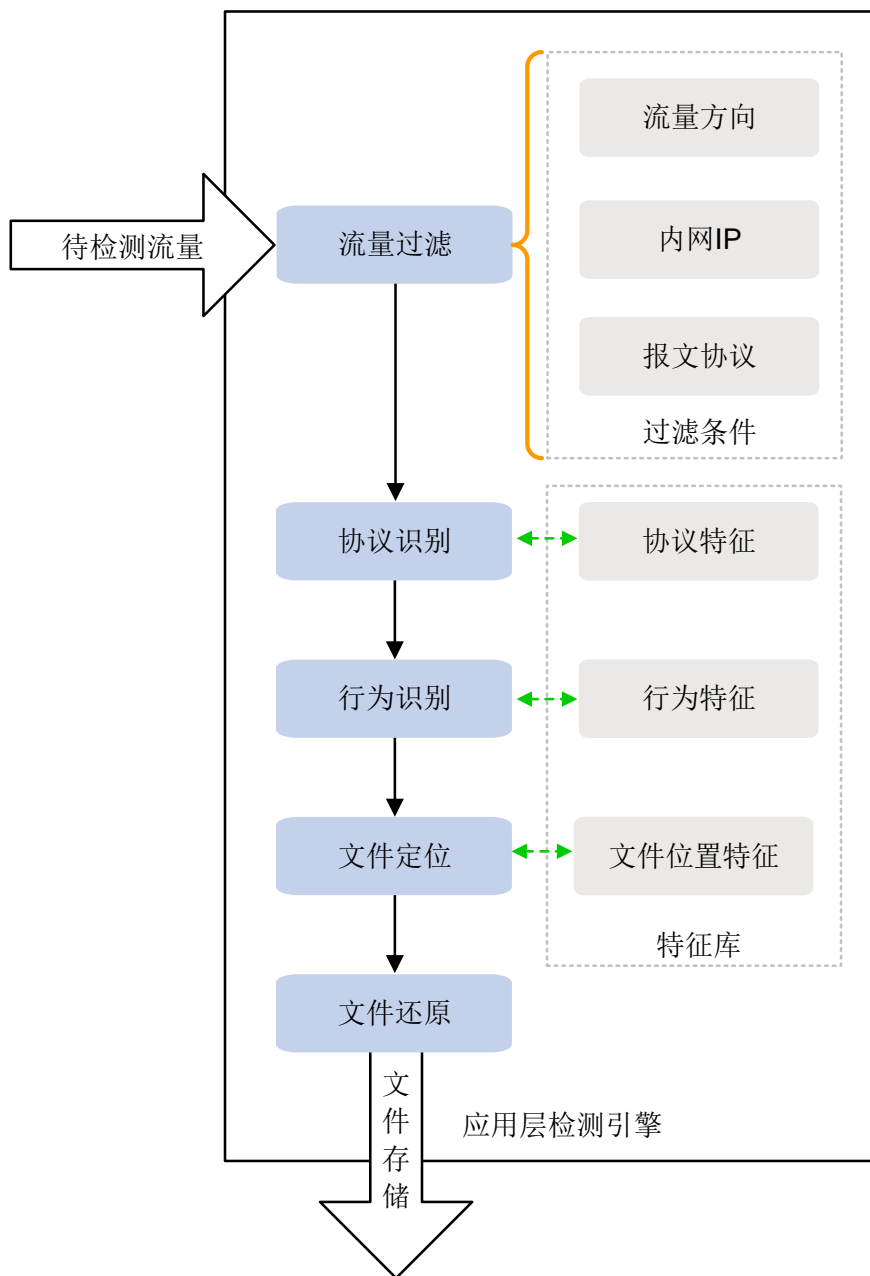
DLP 功能的处理流程如下：

- (1) 应用层检测引擎从待检测流量中还原出待检测文件。
- (2) 应用层检测引擎将还原出的文件存入设备的存储介质中。
- (3) 应用层检测引擎通知数据安全检测引擎进行文件扫描。
- (4) 数据安全检测引擎从设备的存储介质中读取待扫描文件。
- (5) 数据安全检测引擎对文件进行敏感信息检测。
- (6) 数据安全检测引擎根据检测结果以日志或邮件形式进行告警。

1.2.1 文件还原

应用层检测引擎按照如[图 1-2](#)所示流程对报文的应用层信息进行统一识别，进而对报文中嵌入的文件进行还原。

图1-2 文件还原功能流程示意图



文件还原功能的处理流程如下：

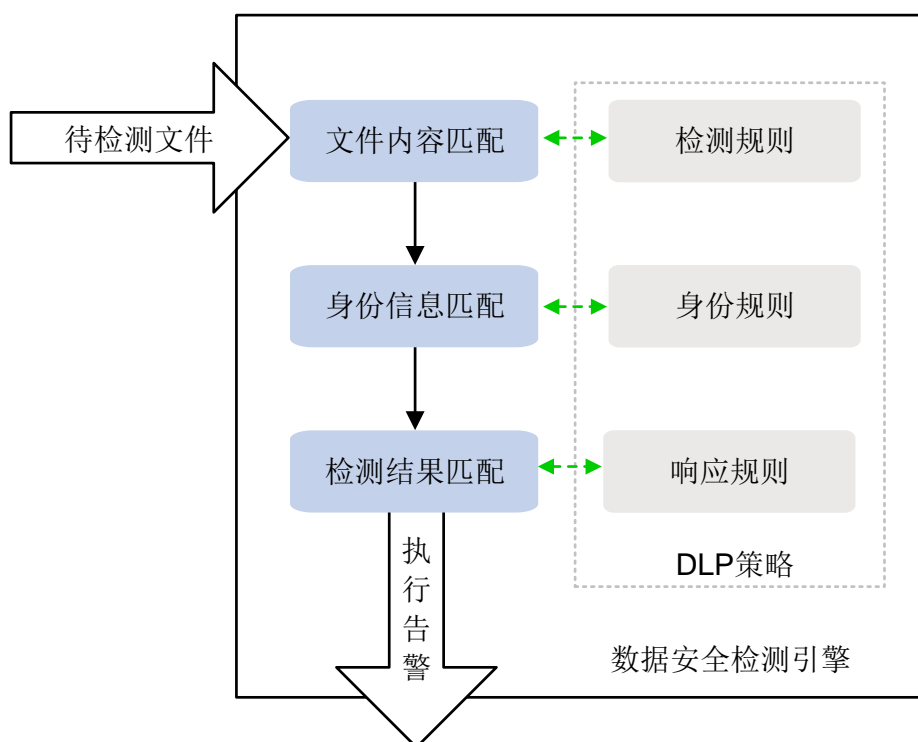
- (1) 流量过滤：筛选匹配所有指定过滤条件的报文进行文件还原操作，包含如下过滤条件。
 - 流量方向：该项用于匹配报文的传输方向，可以为外网向内网、内网向外网或双向。
 - 内网 IP：如果流量方向为外网向内网，该项用于匹配报文的目的 IP 地址；如果流量方向为内网向外网，该项用于匹配报文的源 IP 地址。

- 报文协议：该项用于匹配报文的应用层协议。
- (2) 协议识别：识别报文的应用层协议，例如 **FTP** 或 **SMTP**。
- (3) 行为识别：识别报文的行为特征，例如上传文件或发送邮件。
- (4) 文件定位：检索内置特征库，定位待还原文件在报文中的起始和结束位置。
- (5) 文件还原：提取报文中的文件，并将文件存储在设备本地，并为其分配唯一的 **URL** 供数据安全检测引擎访问。

1.2.2 数据安全检测

如果还原出的文件是压缩文件，数据安全检测引擎支持对压缩文件进行解压缩操作。之后，数据安全检测引擎按照如图 1-3 所示流程对文件进行敏感信息检测。

图1-3 数据安全检测功能流程示意图



数据安全检测功能的处理流程如下：

- (1) 文件内容匹配：使用检测规则对文件内容进行匹配。
- (2) 身份信息匹配：使用身份规则对文件发送者/接收者的身份信息进行匹配。
- (3) 检测结果匹配：完成数据安全检测后，使用响应规则对检测结果（即数据安全事件）进行匹配，确定需要执行的告警动作。
- (4) 执行告警：执行相应的告警动作。

1. 检测规则

检测规则包括如下匹配项：

- 正则表达式：标识敏感文件特征的正则表达式。
- 关键字：标识敏感文件特征的字符串。

- 指纹文件：敏感文件的哈希码。
- 文件名：敏感文件的名称。
- 文件大小：敏感文件的大小。
- 文件类型：敏感文件的类型。
- 协议：传输敏感文件时使用的协议。

待检测文件需要匹配一条检测规则中的所有匹配项才算是与该检测规则匹配成功。需要为一条检测规则设定一个严重等级，待检测文件与该检测规则匹配成功即视作发生了指定严重等级的数据安全事件。

2. 身份规则

身份规则包括如下匹配项：

- IP 地址：文件发送者/接收者的 IP 地址。
- 邮箱地址：文件发送者/接收者的邮箱地址。
- 用户：文件接收者的用户名。

文件发送者/接收者需要匹配一条身份规则中的所有匹配条件（即匹配每个匹配条件中的任一匹配项）才算是与该身份规则匹配成功。需要为一条身份规则设定一个严重等级，文件发送者/接收者与该身份规则匹配成功即视作发生了指定严重等级的数据安全事件。

3. 响应规则

响应规则包括如下匹配项：

- 严重等级：数据安全事件的严重等级。
- 协议：数据安全事件所对应的敏感文件传输使用的协议。

数据安全事件需要匹配一条响应规则中的所有匹配项才算是与该响应规则匹配成功。匹配成功后，数据安全检测引擎将按照响应规则中所配置的响应动作以日志、邮件等方式进行告警。

1.3 DLP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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV 防火墙业务板	支持
	Blade V 防火墙业务板	支持
	NAT 业务板	不支持
M9010-GM	加密业务板	支持
M9016-V	Blade V 防火墙业务板	支持
M9008-S M9012-S	Blade IV 防火墙业务板	支持
	入侵防御业务板	支持
	视频网关业务板	支持
M9008-S-V	Blade IV 防火墙业务板	支持

M9000-AI-E4 M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.4 配置DLP功能

1. 功能简介

DLP 功能需要应用层检测引擎和数据安全检测引擎配合执行，用户需要配置应用层检测引擎进行文件还原操作，配置数据安全检测引擎进行敏感信息检测。

2. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 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。

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) 关闭应用层检测引擎检测固定长度数据流功能。

```
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。

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”。

- (4) 激活 DPI 各业务模块的策略和规则配置。

```
inspect activate
```

缺省情况下，DPI 各业务模块的策略和规则被创建、修改和删除时不生效。

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”。

- (5) 配置 DLP 功能的流量监控方向。

```
dlp flow-monitor file-transfer { all | incoming | outgoing }
```

缺省情况下，DLP 功能不对任何方向的流量进行监控。

- (6) 配置 DLP 功能监控的内网 IP 地址。

- a. 进入 DLP 内网 IP 地址视图。

dlp flow-monitor local-address { ip | ipv6 }

b. 指定 DLP 功能监控的 IP 地址对象组。

object-group object-group-name

缺省情况下，未配置 DLP 功能监控的 IP 地址对象组。

(7) （可选）配置 DLP 功能对指定协议报文的监控。

a. 进入 DLP 协议配置视图。

dlp flow-monitor protocol

b. 关闭 DLP 功能对指定协议报文的监控。

disable protocol { all | type protocol-name }

缺省情况下，DLP 功能对所有支持的协议报文开启监控。

(8) 配置 DLP 策略。

DLP 策略包含检测规则、身份规则和响应规则，仅支持通过 Web 界面进行配置，有关 DLP 策略的配置步骤请参见“DLP 联机帮助”。

(9) 开启 DLP 功能。

undo dlp bypass

缺省情况下，DLP 功能处于开启状态。

1.5 DLP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 DLP 的运行情况。

表1-1 DLP 显示和维护

操作	命令
显示DLP功能监控的内网IPv4地址对象组	display dlp flow-monitor local-address ip config
显示DLP功能监控的内网IPv6地址对象组	display dlp flow-monitor local-address ipv6 config
显示DLP功能监控的报文协议	display dlp flow-monitor protocol config

1.6 DLP典型配置举例

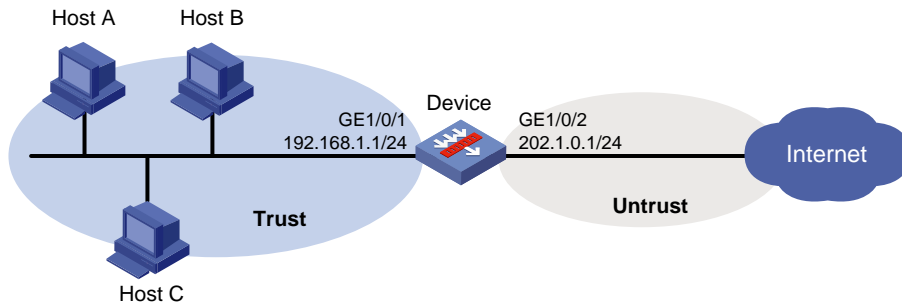
1. 组网需求

公司内部网络出口部署了一台 Device，用于对公司内部敏感文件泄露现象进行检测和告警。具体而言，当发现如下安全事件时，设备记录告警日志：

- 敏感文件 abc.zip 泄露。
- 内网用户向外网敏感邮箱 xyz@mm.com 发送邮件。

2. 组网图

图1-4 DLP 典型配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(3) 配置安全策略

配置名称为 trust-untrust 的安全策略，保证 Trust 安全域内的主机可以访问 Internet，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name trust-untrust
[Device-security-policy-ip-1-trust-untrust] source-zone trust
[Device-security-policy-ip-1-trust-untrust] destination-zone untrust
[Device-security-policy-ip-1-trust-untrust] source-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-1-trust-untrust] action pass
[Device-security-policy-ip-1-trust-untrust] quit
[Device-security-policy-ip] quit
```

(4) 配置 DPI 功能

开启 TCP 数据段重组功能。

```
[Device] inspect tcp-reassemble enable
```

关闭应用层检测引擎检测固定长度数据流功能。

```
[Device] inspect stream-fixed-length disable
```

激活 DPI 各业务模块的策略和规则配置。

```
[Device] inspect activate
```

(5) 配置 DLP 功能的流量过滤参数

配置 DLP 功能监控从内网往外网发送的流量。

```
[Device] dlp flow-monitor file-transfer outgoing
```

配置内网 IP 地址对象组 obj1。

```
[Device] object-group ip address obj1
```

```
[Device-obj-grp-ip-obj1] network subnet 192.168.1.0 24
```

```
[Device-obj-grp-ip-obj1] quit
```

配置 DLP 功能监控的内网 IP 地址。

```
[Device] dlp flow-monitor local-address ip
```

```
[Device-dlp-flow-monitor-local-addr-ip] object-group obj1
```

```
[Device-dlp-flow-monitor-local-addr-ip] quit
```

开启 DLP 功能。

```
[Device] undo dlp bypass
```

(6) 配置 DLP 策略

- a. 登录设备 Web 网管页面，单击导航树中的“策略 > DLP > DLP 策略”菜单项，进入 DLP 策略配置页面。
- b. 单击<新建>按钮，进入新建 DLP 策略页面。
 - 输入策略名称
 - 选择扫描模式
 - 勾选启用规则

图1-5 新建 DLP 策略配置页面

新建DLP策略

策略名称

policy1

(1-31字符)

描述

(1-127字符)

扫描模式

快速扫描

启用策略

☒

检测规则

身份规则

响应规则

添加规则

+ 新建

×

删除

<input type="checkbox"/>	规则名称	严重等级	匹配条件	编辑
--------------------------	------	------	------	----

例外规则

确定

取消

c. 单击添加规则下的<新建>按钮，进入新建检测规则页面。

- 输入名称
- 选择严重等级
- 配置匹配条件（匹配名称为 **abc.zip** 的文件）

图1-6 新建检测规则页面

新建检测规则

?

×

名称

rule1

*(1-31字符)

严重等级

中

匹配条件

+

新建

×

删除

☐ 匹配类型

编辑

☐ 文件名

确定

取消

图1-7 新建匹配条件页面

新建匹配条件

?

×

匹配类型

文件名

文件名

abc.zip

*(1-635字符)

确定

取消

- d. 单击<确定>按钮，完成检测规则配置。选择“身份规则”页签，单击添加规则下的<新建>按钮，进入新建身份规则页面。
- 输入名称
 - 选择严重等级
 - 配置匹配条件（匹配接收者电子邮件地址 xyz@mm.com）

图1-8 新建身份规则页面

新建身份规则

?

×

名称

rule2

(1-31字符)

严重等级

中

匹配条件

+

新建

×

删除

匹配类型

编辑

接收者/用户

确定

取消

图1-9 新建匹配条件页面

新建匹配条件

?

×

提示：电子邮件地址、主机、IP地址和用户配置项为或关系，匹配任意一项视作匹配该身份规则。

匹配类型

接收者/用户

电子邮件地址

xyz@mm.com

(1-315字符)

接收类型

●

全匹配

○

部分匹配

主机

用回车换行区分多个输入项，单个输入项长度不能超过127字

(1-635字符)

IP类型

●

IPv4

○

IPv6

IP地址

请输入IP地址，可用回车换行区分多个输入项

用户

请选择或输入用户

确定

取消

- e. 单击<确定>按钮，完成身份规则配置。选择“响应规则”页签，单击响应规则下拉菜单，单击<新建响应规则>按钮，进入新建响应规则页面。
 - 输入名称
 - 配置匹配条件（匹配严重等级为中的安全事件）
 - 配置动作（配置为发送日志）

图1-10 新建响应规则页面

新建响应规则

名称

rule3

(1-31字符)

描述

(1-127字符)

匹配条件

+

新建

×

删除

<input type="checkbox"/> 匹配类型	操作类型	类型值	编辑
<input type="checkbox"/> 严重等级	属于	中	

动作

+

新建

×

删除

<input type="checkbox"/> 动作类型	类型值	编辑
<input type="checkbox"/> 发送LOG	dlp_syslog_default	

确定

取消

- f. 单击<确定>按钮，完成身份规则配置。
- g. 单击<确定>按钮，完成 DLP 策略配置

4. 验证配置

完成以上配置后，如果设备检测到 abc.zip 文件泄露或存在发往地址 xyz@mm.com 的电子邮件，设备记录日志。

目 录

1 内容风险检测	1-1
1.1 内容风险检测简介	1-1
1.2 内容风险检测原理	1-1
1.2.1 应用层检测引擎	1-2
1.2.2 内容安全检测引擎	1-3
1.3 内容风险检测与硬件适配关系	1-4
1.4 开启内容风险检测结果接收功能	1-5

1 内容风险检测

1.1 内容风险检测简介

内容风险检测是一种针对网络文件传输中的敏感内容进行智能检测和识别的技术，主要功能包括：

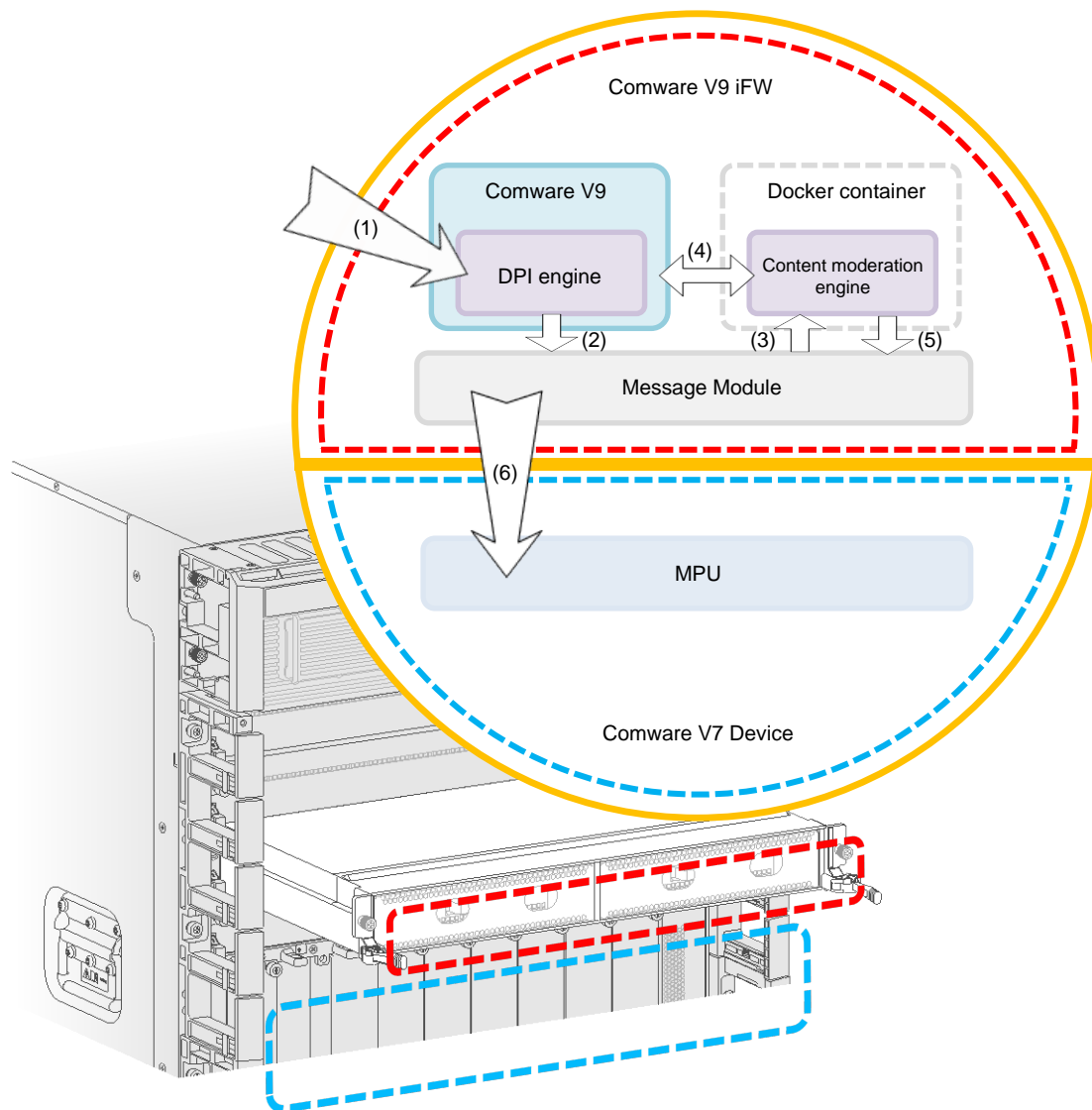
- 图片敏感内容识别：利用由深度学习算法训练生成的图像特征模型，对图片文件中的涉黄、涉恐等敏感内容进行识别和敏感程度度量。
- 视频敏感内容识别：利用由深度学习算法训练生成的视频特征模型，对视频文件中的涉黄、涉恐等敏感内容进行识别和敏感程度度量。

目前，仅支持对采用 **FTP** 和 **SMTP** 协议发送的文件进行内容风险检测。

1.2 内容风险检测原理

如[图 1-1](#)所示，内容风险检测功能由 **Comware V9** 系统的应用层检测引擎和部署于 **Docker** 容器的内容安全检测引擎配合实现。应用层检测引擎提供文件还原、文件解压缩和复合文件拆解功能；内容安全检测引擎提供图片/视频敏感内容识别功能。

图1-1 内容风险检测系统架构图



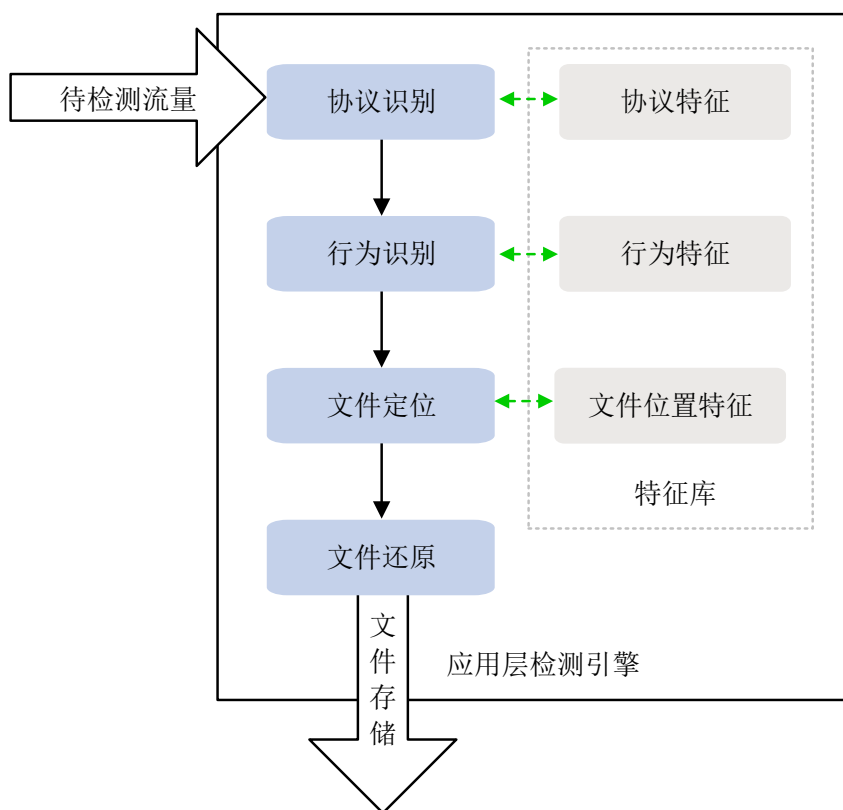
内容风险检测功能的运行流程如下：

- (1) 待检测流量进入 Comware V9 设备的应用层检测引擎进行文件还原操作。
- (2) 应用层检测引擎将还原出的文件信息发送给消息模块。
- (3) 消息模块向内容安全检测引擎提交内容安全检测任务。
- (4) 内容安全检测引擎从 Comware V9 设备本地获取待检测文件后，开启内容安全检测任务。
- (5) 完成检测任务后，内容安全检测引擎将检测结果通知消息模块。
- (6) 消息模块发布检测结果供 Comware V7 设备展示。

1.2.1 应用层检测引擎

应用层检测引擎按照如 [图 1-2](#) 所示流程对报文的应用层信息进行统一识别，进而对报文中嵌入的文件进行还原。

图1-2 应用层检测引擎处理流程图



应用层检测引擎的处理流程如下：

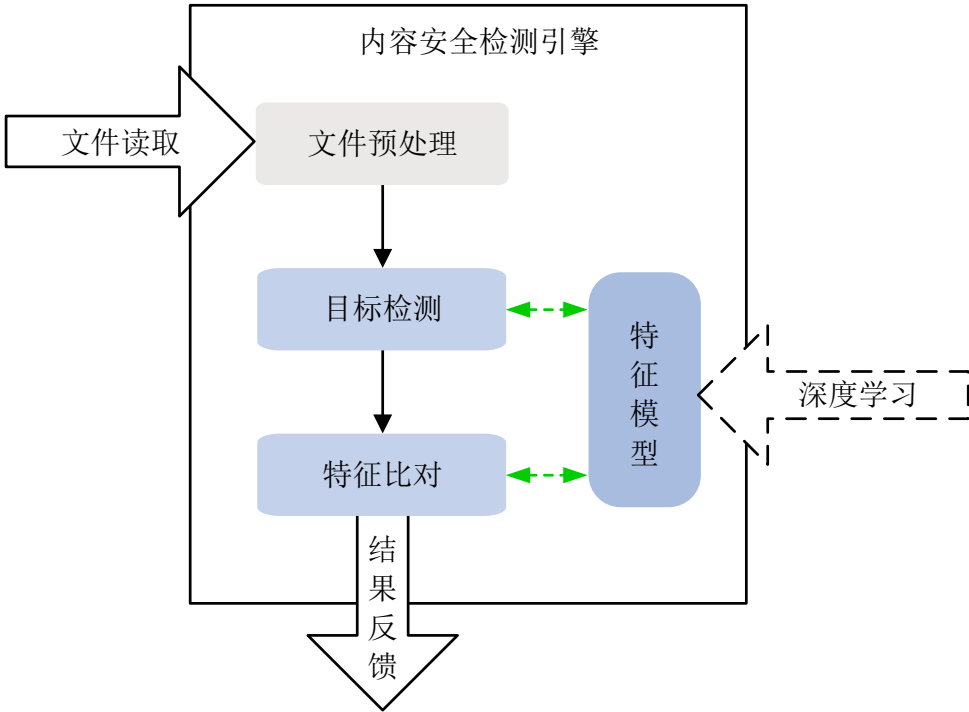
- (1) 协议识别：识别报文的应用层协议，例如 FTP 或 SMTP。
- (2) 行为识别：识别报文的行为特征，例如上传文件或发送邮件。
- (3) 文件定位：检索引擎内置特征库，定位待还原文件在报文中的起始和结束位置。
- (4) 文件还原：引擎提取报文中的文件，并将文件存储在 Comware V9 设备本地，并为其分配唯一的 URL 供内容安全检测引擎访问。

如果还原出的文件是压缩文件，引擎支持对压缩文件进行解压缩操作；如果还原出的文件是复合文件（如嵌有附件的电子邮件），引擎支持将嵌入复合文件中的图片和视频提取出来作为独立的文件。

1.2.2 内容安全检测引擎

内容安全检测引擎上部署了一系列离线敏感内容特征模型，该模型是利用深度学习算法训练生成的神经网络，支持定期更新升级。引擎按照如图 1-3 所示流程对还原出的文件进行敏感内容识别。

图1-3 内容安全检测引擎处理流程图



内容安全检测引擎的处理流程如下：

- (1) 文件读取：引擎通过 URL 访问存储在 Comware V9 设备本地的待检测文件。
- (2) 文件预处理：对图片和视频帧进行光线补偿、灰度调节、噪声过滤等标准化处理。
- (3) 目标检测：利用神经网络对图片和视频帧中的特征（如人脸、旗帜）进行识别和裁剪。
- (4) 特征比对：将特征与敏感内容特征模型进行比对，有效识别敏感信息。
- (5) 结果反馈：将识别结果反馈 Comware V7 设备进行展示。

1.3 内容风险检测与硬件适配关系

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。

设备型号	业务板类型	说明
M9006 M9010 M9014	Blade IV防火墙业务板	不支持
	Blade V防火墙业务板	不支持
	NAT业务板	不支持
M9010-GM	加密业务板	不支持
M9016-V	Blade V防火墙业务板	不支持
M9008-S M9012-S	Blade IV防火墙业务板	不支持
	入侵防御业务板	不支持
	视频网关业务板	不支持

M9008-S-V	Blade IV 防火墙业务板	不支持
M9000-AI-E4	Blade V 防火墙业务板	不支持
M9000-AI-E8 M9000-AI-E16	Blade V 防火墙业务板	支持
M9000-AK001	Blade V 防火墙业务板	不支持
M9000-X06 M9000-X06-B M9000-X06-B-G M9000-X06-G M9000-X10	Blade VI 防火墙业务板	支持
M9000-AI-X06 M9000-AI-X10	Blade VI 防火墙业务板	支持

1.4 开启内容风险检测结果接收功能

1. 功能简介

在内容风险检测业务中, Comware V7 设备作为数据展示平台提供内容风险检测结果的可视化展示。开启本功能后, Comware V7 设备从 Comware V9 设备的内容安全检测引擎获取内容风险检测结果并记录日志。

2. 配置准备

开启本功能前, 用户需要在 Comware V9 设备上配置内容风险检测功能, 具体配置方法请参见相关产品手册。

3. 配置步骤

- (1) 进入系统视图。

```
system-view
```

- (2) 开启内容风险检测结果接收功能。

```
content-moderation enable
```

缺省情况下, 内容风险检测结果接收功能处于关闭状态。

目 录

1 网络资产扫描	1-1
1.1 网络资产扫描简介	1-1
1.2 网络资产扫描原理	1-1
1.3 安全风险防护措施	1-2
1.4 配置网络资产扫描功能	1-2
1.5 网络资产扫描配置举例	1-4
1.5.1 网络资产扫描基本组网配置举例	1-4

1 网络资产扫描

1.1 网络资产扫描简介

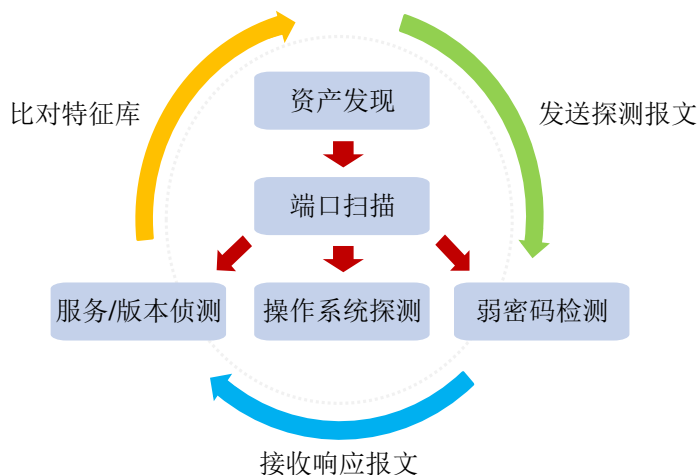
网络资产扫描是一种用于识别和审计指定网络中的主机、服务器、设备等网络资产的技术。通过对指定网络进行探测，网络资产扫描可以发现处于在线状态的网络资产，并对其进行安全审计。网络管理员可以根据网络资产扫描的结果获悉网络资产信息和可能存在的安全风险，进而巩固相应的安全配置。

1.2 网络资产扫描原理

如图 1-1 所示，网络资产扫描包括资产发现、端口扫描、服务/版本侦测、操作系统探测和弱密码检测等五个基本功能，每个功能的基本原理如下：

- 资产发现：设备向指定网络内的所有 IP 地址依次发送不同协议的探测报文，如果设备收到来自探测目标的任何一个响应报文，设备就将该探测目标记录为网络资产。
- 端口扫描：设备向网络资产的指定端口发送 TCP/UDP 探测报文，并根据来自该目标端口的 TCP/UDP 响应报文，判断该端口的开放情况。
- 服务/版本侦测：设备向网络资产的开放端口发送一系列服务探测报文，并将来自该目标端口的响应报文与设备内置的服务特征库进行比对，确定目标端口所提供的服务类型和服务的版本信息。
- 操作系统探测：设备向网络资产的端口（包括至少一个开放端口和关闭端口）发送一系列 TCP/UDP 探测报文，并将来自目标资产的响应报文与设备内置的系统特征库进行比对，确定目标资产上运行的操作系统。
- 弱密码检测：设备使用指定用户名搭配弱密码字典（内含常见的低安全性密码）中的密码，通过指定服务尝试登录网络资产。如果登录成功，说明该用户的密码安全性较低，需要替换为更高安全性的密码。

图1-1 网络资产扫描原理图



1.3 安全风险防护措施

网络资产扫描功能可以发现网络资产上可能存在的端口开放风险、特定服务风险和弱密码风险。网络管理员可以根据表 1-1 所示的安全防护措施，对网络资产及其安全网关进行相应配置，防范资产安全风险。

表1-1 针对不同风险类型的防护措施表

风险类型	防护措施
端口开放风险	<ul style="list-style-type: none">手工关闭网络资产上无需开放的端口配置安全网关的安全策略，拒绝访问网络资产特定端口的报文
特定服务风险	在安全网关上针对网络资产提供的特定服务类型配置攻击检测与防范、IPS等防护策略
弱密码风险	将网络资产上特定用户的弱密码替换为更高安全性的密码

1.4 配置网络资产扫描功能

1. 功能简介

网络资产扫描功能用来对指定目标 IP 地址段中的主机、服务器和设备进行扫描分析，判断其是否存在开放端口、弱密码等风险因素，用户可根据扫描结果巩固相关安全配置。

CLI（Command Line Interface，命令行接口）管理方式下仅提供自动资产扫描功能，设备将按扫描计划自动对目标 IP 地址段发起资产发现、端口扫描、服务/版本侦测、操作系统探测和弱密码检测。扫描结果将展示在设备“监控 > 资产管理 > 资产发现”Web 界面上。

在 Web 管理方式下还支持立即资产扫描功能，设备将根据配置立即发起网络资产扫描任务。有关 Web 管理方式下网络资产扫描功能的详细介绍，请参见“资产发现 Web 联机帮助”。

2. 配置限制和指导

设备必须使用三层接口向目标 IP 地址段发起网络资产扫描。如果设备使用二层接口接入网络，网络资产扫描功能不生效。

设备的安全策略规则需放行 Local 安全域发往目标 IP 地址段所在安全域的报文，否则探测报文无法发送至目标 IP 地址段，造成网络资产扫描功能不生效。

3. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 进入资产扫描视图。

```
asset-scan
```

(3) 配置网络资产扫描的目标 IP 地址段。

○ 配置网络资产扫描的目标 IPv4 地址段。

```
ip { subnet ip-address mask-length | range start-address  
end-address }
```

缺省情况下，不存在网络资产扫描的目标 IPv4 地址段。

- 配置网络资产扫描的目标 IPv6 地址段。

```
ipv6 { subnet ipv6-address prefix-length | range start-address end-address }
```

缺省情况下，不存在网络资产扫描的目标 IPv6 地址段。

(4) (可选) 配置网络资产扫描的目标端口号。

- 配置网络资产扫描的目标 TCP 端口号。

```
tcp-port port-number
```

缺省情况下，目标 TCP 端口号为 23、80、139、443、445、554、631、3389、3872、5800、7080、8000、8080、8088、8180、8443。

- 配置网络资产扫描的目标 UDP 端口号。

```
udp-port port-number
```

缺省情况下，目标 UDP 端口号为 137。

如果既未配置目标 TCP 端口号，又未配置目标 UDP 端口号，设备将针对缺省目标 TCP 端口号和 UDP 端口号进行扫描，否则设备仅针对配置的目标端口号进行扫描。

(5) (可选) 配置弱密码扫描功能。

- 配置弱密码扫描模式。

```
weak-password-scan mode { custom | dict } *
```

缺省情况下，未配置弱密码扫描模式。

可以同时指定 **custom** 和 **dict** 关键字，表示自定义模式下既使用自定义弱密码字典也使用设备预定义弱密码字典进行扫描。

- 配置弱密码扫描所针对的用户名。

```
weak-password-scan user username
```

缺省情况下，未配置弱密码扫描所针对的用户名。

仅弱密码扫描模式配置为自定义模式时，才需要配置弱密码扫描所针对的用户名。

- 配置用户自定义弱密码。

```
weak-password-scan password password
```

缺省情况下，未配置用户自定义弱密码。

仅弱密码扫描模式配置为自定义模式时，才需要配置用户自定义弱密码。

- 配置弱密码扫描所针对的服务类型。

```
weak-password-scan service { ftp | http | mysql | sql-server | ssh } *
```

缺省情况下，未配置弱密码扫描所针对的服务类型。

- 开启弱密码扫描功能。

```
weak-password-scan enable
```

缺省情况下，弱密码扫描功能处于关闭状态。

(6) 配置自动资产扫描计划。

- 配置自动资产扫描计划。

```
schedule every { day start-time | hour start-hour | week week-days start-time }
```

缺省情况下，自动资产扫描计划为每隔 12 小时扫描一次。

- 开启自动资产扫描功能。

auto-scan enable

缺省情况下，自动资产扫描功能处于关闭状态。

1.5 网络资产扫描配置举例

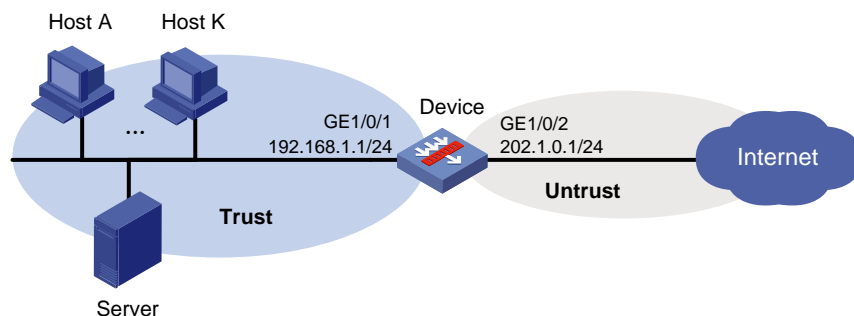
1.5.1 网络资产扫描基本组网配置举例

1. 组网需求

公司内部网络 192.168.1.0/24 中部署了数台主机和服务器，同时其网络出口部署了一台 Device，作为安全网关对内部网络进行安全防护。现在，网络管理员需要每周五 14 时对公司内部网络资产进行扫描和安全审计，定期检测网络资产上可能存在的安全风险。

2. 组网图

图1-2 网络资产扫描配置组网图



3. 配置步骤

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ip address 192.168.1.1 255.255.255.0
[Device-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 将接口加入安全域

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

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

(3) 配置安全策略

配置名称为 local-trust 的安全策略，保证 Device 可以对 Trust 安全域内的网络资产发起扫描，具体配置步骤如下。

```
[Device] security-policy ip
[Device-security-policy-ip] rule name local-trust
[Device-security-policy-ip-1-local-trust] source-zone local
[Device-security-policy-ip-1-local-trust] destination-zone trust
[Device-security-policy-ip-1-local-trust] destination-ip-subnet 192.168.1.0 24
[Device-security-policy-ip-1-local-trust] action pass
[Device-security-policy-ip-1-local-trust] quit
[Device-security-policy-ip] quit
```

(4) 配置网络资产扫描功能

配置网络资产扫描的目标 IPv4 地址段为 192.168.1.0/24。

```
[Device] asset-scan
[Device-asset-scan] ip subnet 192.168.1.0 24
```

配置弱密码扫描功能，扫描模式为预定义模式，服务类型为 FTP、HTTP、MySQL、SQL Server 和 SSH。

```
[Device-asset-scan] weak-password-scan mode dict
[Device-asset-scan] weak-password-scan service ftp http mysql sql-server ssh
[Device-asset-scan] weak-password-scan enable
```

配置自动资产扫描计划，每周五 14 时开始扫描。

```
[Device-asset-scan] schedule every week Fri 14:00
[Device-asset-scan] auto-scan enable
```

4. 验证配置

完成以上配置后，Device 将在每周五 14 时对内网发起网络资产扫描。