目 录

1 攻击检测及防范

1.1 攻击检测及防范简介

攻击检测及防范是一个重要的网络安全特性，它通过分析经过设备的报文的内容和行为，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施，例如输出告警日志、丢弃报文或加入黑名单。

本特性能够检测包攻击、扫描攻击和泛洪攻击等多种类型的网络攻击，并能对各类型攻击采取合理的防范措施。除此之外，该特性还支持流量统计功能，基于接口对 IP 报文流量进行分析和统计。

1.1.1 设备能够防范的网络攻击类型

根据攻击报文表现出的不同特征，设备可以防范的网络攻击类型可以划分为以下三大类：单包攻击、扫描攻击和泛洪攻击。

1. 单包攻击

单包攻击也称为畸形报文攻击。攻击者通过向目标系统发送有缺陷的 IP 报文，如分片重叠的 IP 报文、TCP 标志位非法的报文，使得目标系统在处理这样的 IP 报文时出错、崩溃，给目标系统带来损失，或者通过发送大量无用报文占用网络带宽等行为来造成攻击。

设备可以对表 1-1中所列的各单包攻击行为进行有效防范。

表1-1 单包攻击类型及说明列表

单包攻击类型	说明
Fraggle	攻击者通过向目标网络发送UDP端口为7的ECHO报文或者UDP端口为19的Chargen报文，令网络产生大量无用的应答报文，占满网络带宽，达到攻击目的。
ICMP Redirect	攻击者向用户发送ICMP重定向报文，更改用户主机的路由表，干扰用户主机正常的IP报文转发。
ICMP Unreachable	某些系统在收到不可达的ICMP报文后，对于后续发往此目的地的报文判断为不可达并切断对应的网络连接。攻击者通过发送ICMP不可达报文，达到切断目标主机网络连接的目的。
LAND	攻击者向目标主机发送大量源IP地址和目的IP地址都是目标主机自身的TCP SYN报文，使得目标主机的半连接资源耗尽，最终不能正常工作。
Large ICMP	某些主机或设备收到超大的报文，会引起内存分配错误而导致协议栈崩溃。攻击者通过发送超大ICMP报文，让目标主机崩溃，达到攻击目的。
Route Record	攻击者利用IP报文中的Route Record路由选项对网络结构进行探测。
Smurf	攻击者向目标网络发送ICMP应答请求，该请求包的目的地址设置为目标网络的广播地址，这样该网络中的所有主机都会对此ICMP应答请求作出答复，导致网络阻塞，从而达到令目标网络中主机拒绝服务的攻击目的。
Source Route	攻击者利用IP报文中的Source Route路由选项对网络结构进行探测。

单包攻击类型	说明
TCP Flag	不同操作系统对于非常规的TCP标志位有不同的处理。攻击者通过发送带有非常规TCP标志的报文探测目标主机的操作系统类型，若操作系统对这类报文处理不当，攻击者便可达到使目标主机系统崩溃的目的。
Tracert	攻击者连续发送TTL从1开始递增的目的端口号较大的UDP报文，报文每经过一个路由器，其TTL都会减1，当报文的TTL为0时，路由器会给报文的源IP设备发送一个TTL超时的ICMP报文，攻击者借此来探测网络的拓扑结构。
WinNuke	攻击者向安装（或使用）Windows系统的特定目标的NetBIOS端口（139）发送OOB（out-of-band）数据包，这些攻击报文的指针字段与实际的位置不符，从而引起一个NetBIOS片断重叠，致使已与其他主机建立连接的目标主机在处理这些数据的时候系统崩溃。

2. 扫描攻击

扫描攻击是指，攻击者运用扫描工具对网络进行主机地址或端口的扫描，通过准确定位潜在目标的位置，探测目标系统的网络拓扑结构和启用的服务类型，为进一步侵入目标系统做准备。

3. 泛洪攻击

泛洪攻击是指，攻击者在短时间内向目标系统发送大量的虚假请求，导致目标系统疲于应付无用信息，而无法为合法用户提供正常服务，即发生拒绝服务。

设备支持对以下三种泛洪攻击进行有效防范：

- SYN Flood 攻击

由于资源的限制，TCP/IP 协议栈只能允许有限个 TCP 连接。SYN Flood 攻击者向服务器发送伪造源地址的 SYN 报文，服务器在回应 SYN ACK 报文后，由于目的地址是伪造的，因此服务器不会收到相应的 ACK 报文，从而在服务器上产生一个半连接。若攻击者发送大量这样的报文，被攻击服务器上会出现大量的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时。

- ICMP Flood 攻击

ICMP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMP 请求报文（例如 ping 报文），使其忙于回复这些请求，致使目标系统负担过重而不能处理正常的业务。

- UDP Flood 攻击

UDP Flood 攻击是指，攻击者在短时间内向特定目标发送大量的 UDP 报文，致使目标系统负担过重而不能处理正常的业务。

1.1.2 黑名单功能

黑名单功能是根据报文的源 IP 地址进行报文过滤的一种攻击防范特性。同基于 ACL（Access Control List，访问控制列表）的包过滤功能相比，黑名单进行报文匹配的方式更为简单，可以实现报文的高速过滤，从而有效地将特定 IP 地址发送来的报文屏蔽掉。

黑名单可以由设备动态地进行添加或删除，这种动态添加是与扫描攻击防范功能或者用户登录设备的认证功能配合实现的，动态生成的黑名单表项会在一定的时间之后老化。具体实现是：

- 当设备根据报文的行为特征检测到某特定 IP 地址的扫描攻击企图之后，便将攻击者的 IP 地址自动加入黑名单，之后该 IP 地址发送的报文会被设备过滤掉。

- 当设备检测到某用户通过 FTP、Telnet、SSH、SSL 或 Web 方式尝试登录设备的失败次数达到指定阈值之后，便判定其为恶意攻击用户，并将其源 IP 地址自动加入黑名单，之后来自该 IP 地址且访问本设备的报文将被设备过滤掉。此处所指的认证失败情况包括：用户名错误、密码错误、验证码错误（针对 Web 登录用户）。该功能可以有效防范恶意用户通过不断尝试登录认证，尝试破解登录密码的攻击行为。目前，用户登录失败次数的阈值为 6，黑名单的老化时间为 10 分钟，且均不可配。

除上面所说的动态方式之外，设备还支持手动方式添加或删除黑名单。手动配置的黑名单表项分为永久黑名单表项和非永久黑名单表项。永久黑名单表项建立后，一直存在，除非用户手工删除该表项。非永久黑名单表项的老化时间由用户指定，超出老化时间后，设备会自动将该黑名单表项删除，黑名单表项对应的 IP 地址发送的报文即可正常通过。

1.1.3 流量统计功能

流量统计功能主要用于对内外部网络之间的会话建立情况进行统计与分析，具有一定的实时性，可帮助网络管理员及时掌握网络中各类型会话的统计值，并可作为制定攻击防范策略的一个有效依据。比如，通过分析外部网络向内部网络发起的 TCP 或 UDP 会话建立请求总数是否超过设定的阈值，可以确定是否需要限制该方向的新建会话，或者限制向内部网络某一 IP 地址发起新建会话。

目前，设备支持的流量统计项包括：

- 总会话数
- 新建会话的速率
- TCP 会话数
- 半开状态的 TCP 会话数
- 半闭状态的 TCP 会话数
- TCP 会话的创建速率
- UDP 会话数
- UDP 会话的创建速率
- ICMP 会话数
- ICMP 会话的创建速率
- RAW IP 会话数
- RAW IP 会话的创建速率

说明

- 会话创建速率的统计周期为 5 秒，因此设备上显示的统计值为距离当前时刻最近的一个周期内的会话创建速率统计值。
- 流量统计功能并不关心会话的状态（除 TCP 的半开和半闭状态），只要有会话创建，那么会话数目的统计值就加 1，同理，只要有会话被删除，该统计值就减 1。

1.1.4 TCP Proxy功能

TCP Proxy 功能用来防止服务器受到 SYN Flood 攻击。启用了 TCP Proxy 功能的设备称为 TCP proxy，它位于客户端和服务器之间，能够对客户端与服务器之间的 TCP 连接进行代理。当设备检测到有服务器受到 SYN Flood 攻击时，TCP Proxy 即将该服务器 IP 地址添加为动态受保护的 IP 地址，并对所有向该受保护服务器发起的 TCP 连接的协商报文进行处理，通过对客户端发起的 TCP 连接进行验证，达到保护服务器免受 SYN Flood 攻击的目的。

TCP Proxy 支持两种代理方式：

- 单向代理方式：是指仅对 TCP 连接的正向报文进行处理。
- 双向代理方式：是指对 TCP 连接的正向和反向报文都进行处理。

用户可以根据实际的组网情况选择不同的代理方式。例如：在如图 1-1所示的组网中，从客户端发出的报文经过TCP proxy，而从服务器端发出的报文不经过TCP proxy，此时只能使用单向代理方式；在如图 1-2所示的组网中，从客户端发出的报文经和从服务器端发出的报文都经过TCP proxy，此时可以使用单向代理方式，也可以使用双向代理方式。

图1-1 单向代理组网

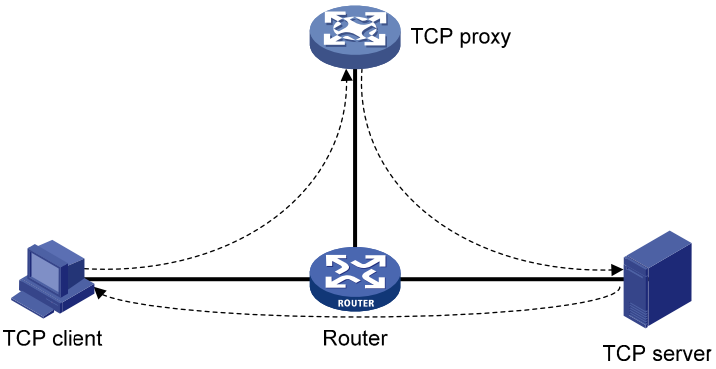
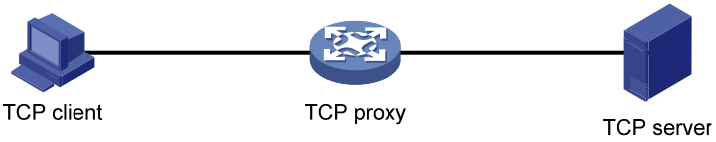


图1-2 双/单向代理组网

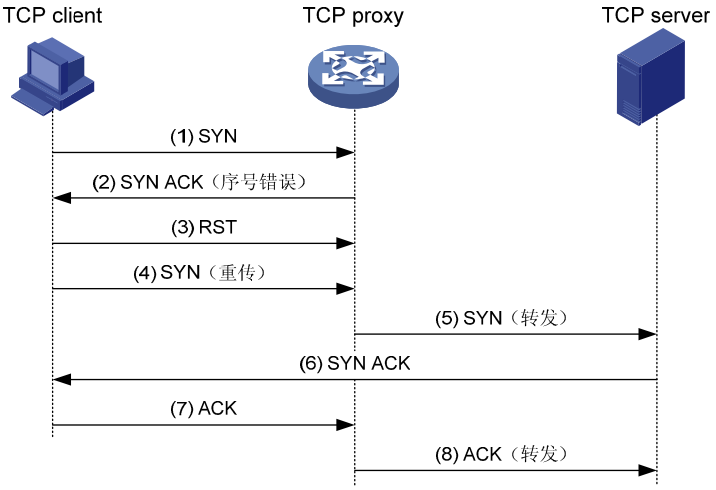


TCP Proxy 处理流程：

- 单向代理

单向代理方式下，TCP Proxy的处理流程如图 1-3所示。

图1-3 单向代理方式的 TCP Proxy 处理流程



TCP proxy 收到某客户端发来的与受保护服务器（匹配某个受保护 IP 地址表项）建立 TCP 连接的请求（SYN 报文）后，先代替服务器向客户端回应序号错误的 SYN ACK 报文。如果 TCP proxy 收到客户端回应的 RST 报文，则认为该 TCP 连接请求通过 TCP 代理的验证。一定时间内，TCP proxy 收到客户端重发的 SYN 报文后，直接向服务器转发该报文，允许客户端和服务器之间直接建立 TCP 连接。TCP 连接建立后，TCP proxy 直接转发后续的报文，不对报文进行处理。

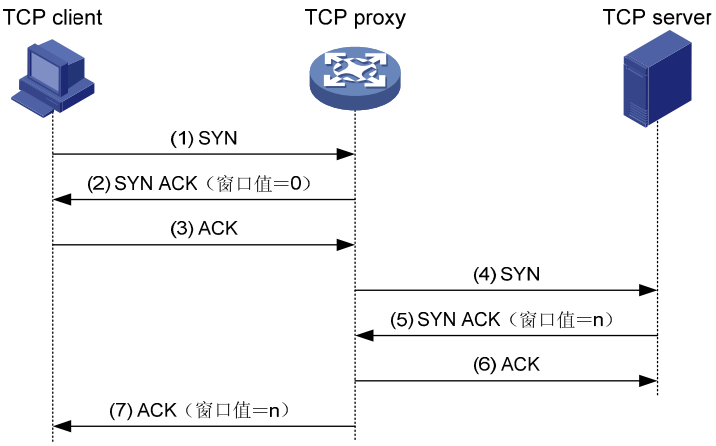
一般而言，应用服务器不会主动对客户端发起恶意连接，因此服务器响应客户端的报文可以不需要经过 TCP proxy 的检查。TCP proxy 仅需要对客户端发往应用服务器的报文进行实时监控，服务器响应客户端的报文可以根据实际需要选择是否经过防火墙，因此单向代理方式能够支持更灵活的组网方式。

由于 TCP proxy 对客户端发起的 TCP 连接进行了干预，因此单向代理方式的实现要求客户端的实现严格遵守 TCP 协议栈的规定，如果客户端的 TCP 协议栈实现不完善，即便是合法用户，也可能由于未通过 TCP proxy 的严格检查而无法访问服务器。而且，该方式依赖于客户端向服务器发送 RST 报文后再次发起请求的功能，因此启用 TCP Proxy 后，客户端发起的每个 TCP 连接的建立时间会有相应增加。

- 双向代理

双向代理方式下，TCP Proxy的处理流程如图 1-4所示。

图1-4 双向代理方式的 TCP Proxy 处理流程



TCP proxy 收到某客户端发来的与受保护服务器建立 TCP 连接的请求（SYN 报文）后，先代替服务器向客户端回应正常的 SYN ACK 报文（窗口值为 0）。如果收到客户端回应的 ACK 报文，则认为该 TCP 连接请求通过 TCP 代理的验证。之后，TCP proxy 再代替客户端向服务器发送 SYN 报文，并通过三次握手与服务器建立 TCP 连接。因此，在客户端和 TCP proxy、TCP proxy 和服务器之间会建立两个 TCP 连接，而且两个 TCP 连接使用的序号不同。

双向代理方式中，TCP proxy 作为虚拟的服务器与客户端交互，同时也作为虚拟的客户端与服务器交互，在为服务器过滤掉恶意连接报文的同时保证了常规业务的正常运行。但该方式要求 TCP proxy 必须部署在所保护的服务器入口和出口的关键路径上，且要保证所有客户端向服务器发送的报文以及服务器向客户端回应的报文都需要经过该设备。

1.2 攻击检测及防范配置任务简介

攻击检测及防范的配置任务从功能上可划分为表 1-2所列的三大类。

- 配置接口上的攻击防范功能首先需要创建一个攻击防范策略，然后在该策略中配置具体类型的攻击防范特性，比如 Smurf 攻击防范、扫描攻击防范、泛洪攻击防范，最后再将该策略应用到具体的接口上。各类型的攻击防范功能之间没有先后顺序，用户可以根据实际需求进行配置。
- 当 SYN Flood 攻击防范策略中指定对 SYN Flood 攻击报文的处理方式为进行 TCP Proxy 时，必须配置 TCP Proxy。
- 黑名单功能既可单独使用，也可以与接口上的扫描攻击防范功能配合使用。
- 流量统计功能可单独使用。

表1-2 攻击防范配置任务简介

配置任务			说明	详细配置
配置接口上的攻击防范	创建攻击防范策略		必选	1.1.1
	配置攻击防范策略	配置单包攻击防范策略	必选 可根据实际组网需求，配置其中的一种或多种	1.3.2 1.
		配置扫描攻击防范策略		1.3.2 2.
		配置泛洪攻击防范策略		1.3.2 3.
	在接口上应用攻击防范策略		必选	1.3.3

配置任务	说明	详细配置
配置TCP Proxy	可选	1.4
配置黑名单	可选	1.5
配置接口上流量统计	可选	1.6

1.3 配置接口上的攻击防范

1.1.1 创建攻击防范策略

在配置攻击防范之前，必须首先创建一个攻击防范策略，并进入该攻击防范策略视图。在该视图下，可以定义一个或多个用于检测攻击的特征项，以及对检测到的攻击报文所采取的防范措施。

在创建攻击防范策略的同时，还可以指定独享该策略的接口，即，该策略仅能被应用在这一个指定的接口上。

表1-3 创建攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
创建一个攻击防范策略，并进入攻击防范策略视图	**attack-defense policy** *policy-number* [**interface** *interface-type interface-number*]	必选 缺省情况下，不存在任何攻击防范策略

1.3.2 配置攻击防范策略

在一个攻击防范策略中，可以根据实际的网络安全需求来配置策略中的具体内容，主要包括针对攻击类型指定检测条件及采取的防范措施。

不同类型的攻击防范策略在配置内容上有所不同，下面将按照攻击类型（单包攻击、扫描攻击、泛洪攻击）分别进行介绍。

1. 配置单包攻击防范策略

单包攻击防范主要通过分析经过设备的报文特征来判断报文是否具有攻击性，一般应用在设备连接外部网络的接口上，且仅对应用了攻击防范策略的接口上的入方向报文有效。若设备检测到某报文具有攻击性，则可以根据配置将检测到的攻击报文做丢弃处理。

表1-4 配置单包攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-

配置步骤	命令	说明
使能对单包攻击的特征检测	**signature-detect** { **fraggle** | **icmp-redirect** | **icmp-unreachable** | **land** | **large-icmp** | **route-record** | **smurf** | **source-route** | **tcp-flag** | **tracert** | **winnuke** } **enable**	必选 缺省情况下，所有类型的单包攻击的特征检测均处于未使能状态
配置启动Large ICMP攻击防范的ICMP报文的长度阈值	**signature-detect large-icmp max-length** *length*	可选 缺省情况下，ICMP报文的长度阈值为4000字节
配置对单包攻击报文的处理方式为丢弃	**signature-detect action drop-packet**	可选 缺省情况下，不处理单包攻击报文
退回到系统视图	**quit**	-
配置攻击防范日志记录功能	**attack-defense logging enable**	可选 缺省情况下，未开启攻击防范日志记录功能

2. 配置扫描攻击防范策略

扫描攻击防范主要通过监测网络使用者向目标系统发起连接的速率，来检测其探测行为，一般应用在设备连接外部网络的接口上，且仅对应用了攻击防范策略的接口上的入方向报文有效。若设备监测到某 IP 地址主动发起的连接速率达到或超过了一定阈值，则可以根据配置将检测到的攻击者的源 IP 地址加入黑名单来丢弃来自该 IP 地址的后续报文。

表1-5 配置扫描攻击防范策略

配置步骤		命令	说明
进入系统视图		**system-view**	-
进入攻击防范策略视图		**attack-defense policy** *policy-number*	-
使能扫描攻击防范		**defense scan enable**	必选 缺省情况下，扫描攻击防范处于未使能状态
配置启动扫描攻击防范的连接速率阈值		**defense scan max-rate** *rate-number*	可选 缺省情况下，启动扫描攻击防范的连接速率阈值为每秒4000个连接数
配置检测到扫描攻击后的黑名单功能	使能扫描攻击防范的黑名单添加功能	**defense scan add-to-blacklist**	可选 缺省情况下，扫描攻击防范的黑名单添加功能处于未使能状态
	配置扫描攻击防范添加的黑名单的老化时间	**defense scan blacklist-timeout** *minutes*	可选 缺省情况下，黑名单的老化时间为10分钟
退回到系统视图		**quit**	-

配置步骤	命令	说明
使能黑名单功能	**blacklist enable**	要使扫描攻击防范添加的黑名单生效，则必选 缺省情况下，黑名单功能处于未使能状态

3. 配置泛洪攻击防范策略

泛洪攻击防范主要用于保护服务器，通过监测向服务器发起连接请求的速率来检测各类泛洪攻击，一般应用在设备连接内部网络的接口上，且仅对应用了攻击防范策略的接口上的出方向报文有效。使能泛洪攻击防范后，设备处于攻击检测状态，当它监测到向某服务器发送报文的速率持续达到或超过了指定的触发阈值时，即认为该服务器受到了攻击，则进入攻击防范状态，并根据配置启动相应的防范措施（默认可配置为对后续新建连接的报文进行丢弃处理或者进行 TCP Proxy）。此后，当设备检测到向该服务器发送报文的速率低于指定的恢复阈值时，即认为攻击结束，则由攻击防范状态恢复为攻击检测状态，并停止执行防范措施。

为保护指定 IP 地址，攻击防范策略中支持基于 IP 地址的攻击防范配置。对于没有专门配置攻击防范策略的 IP 地址，则采用全局的参数设置来进行保护。

(1) SYN Flood 攻击防范策略

表1-6 配置 SYN Flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
使能SYN Flood攻击防范	**defense syn-flood enable**	必选 缺省情况下，SYN Flood攻击防范处于未使能状态
配置SYN Flood攻击防范的全局参数（触发阈值、恢复阈值）	**defense syn-flood rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，触发阈值（**high**）为每秒1000个报文数，恢复阈值（**low**）为每秒750个报文数
对指定IP地址配置SYN Flood攻击防范参数（触发阈值、恢复阈值）	**defense syn-flood ip** *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，未对任何指定IP地址配置SYN Flood攻击防范参数
配置对SYN Flood攻击报文的处理方式为丢弃或进行TCP Proxy	**defense syn-flood action { drop-packet | trigger-tcp-proxy }**	可选 缺省情况下，对SYN Flood攻击报文不进行任何处理

(2) ICMP Flood 攻击防范策略

表1-7 配置 ICMP Flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-

配置步骤	命令	说明
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
使能ICMP Flood攻击防范	**defense icmp-flood enable**	必选 缺省情况下，ICMP Flood攻击防范处于未使能状态
配置ICMP Flood攻击防范的全局参数（触发阈值、恢复阈值）	**defense icmp-flood rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，触发阈值（**high**）为每秒1000个报文数，恢复阈值（**low**）为每秒750个报文数
对指定IP地址配置ICMP Flood攻击防范参数（触发阈值、恢复阈值）	**defense icmp-flood ip** *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，未对任何指定IP地址配置ICMP Flood攻击防范参数
配置对ICMP Flood攻击报文的处理方式为丢弃	**defense icmp-flood action drop-packet**	可选 缺省情况下，对ICMP Flood攻击报文不处理

(3) UDP Flood 攻击防范策略

表1-8 配置 UDP Flood 攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
使能UDP Flood攻击防范	**defense udp-flood enable**	必选 缺省情况下，UDP Flood攻击防范处于未使能状态
配置UDP Flood攻击防范的全局参数（触发阈值、恢复阈值）	**defense udp-flood rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，触发阈值（**high**）为每秒1000个报文数，恢复阈值（**low**）为每秒750个报文数
对指定IP地址配置UDP Flood攻击防范参数（触发阈值、恢复阈值）	**defense udp-flood ip** *ip-address* **rate-threshold high** *rate-number* [**low** *rate-number*]	可选 缺省情况下，未对任何指定IP地址配置UDP Flood攻击防范参数
配置对UDP Flood攻击报文的防范动作为丢包	**defense udp-flood action drop-packet**	可选 缺省情况下，对UDP Flood攻击报文不处理

1.3.3 在接口上应用攻击防范策略

通过下面的配置，使已配置的攻击防范策略在具体的接口上生效。

表1-9 配置在接口上应用攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置在接口上应用攻击防范策略	**attack-defense apply policy** *policy-number*	必选 缺省情况下，接口上未应用任何攻击防范策略 在接口上应用的攻击防范策略必须是已经存在的

1.4 配置TCP Proxy

通过在设备连接外部网络的接口上使能 TCP Proxy，可以保护内部网络中的应用服务器免受 SYN Flood 攻击。一般应用在设备连接外部网络的接口上，且仅对配置了 TCP Proxy 的接口上的入方向报文有效。当设备监测到某服务器受到了 SYN Flood 攻击时，会根据配置启动相应的防范措施。若防范措施配置为对攻击报文进行 TCP Proxy，则设备会将该服务器 IP 地址添加到受保护 IP 表项中，并按照指定的 TCP Proxy 工作模式，对后续新建 TCP 连接的协商报文进行合法性检查，过滤非法客户端发起的 TCP 连接报文。

表1-10 配置 TCP Proxy

配置步骤		命令	说明
进入系统视图		**system-view**	-
配置TCP Proxy工作模式	单向代理模式	**tcp-proxy mode unidirection**	可选 缺省情况下，TCP Proxy工作模式为双向代理模式
	双向代理模式	**undo tcp-proxy mode**	
进入接口视图		**interface** *interface-type interface-number*	-
使能接口上的TCP Proxy功能		**tcp-proxy enable**	必选 缺省情况下，接口上的TCP Proxy功能处于关闭状态

1.5 配置黑名单

通过配置黑名单功能可以对来自指定 IP 地址的报文进行过滤。

黑名单的配置包括使能黑名单功能和添加黑名单表项。添加黑名单表项的同时可以选择配置黑名单表项的老化时间，若不配置，那么该黑名单表项永不老化，除非用户手动将其删除。

表1-11 配置黑名单

配置步骤	命令	说明
进入系统视图	**system-view**	-
使能黑名单功能	**blacklist enable**	必选 缺省情况下，黑名单功能处于未使能状态
添加黑名单表项	**blacklist ip** *source-ip-address* [**timeout** *minutes*]	可选 扫描攻击防范功能可以自动添加黑名单表项

说明

黑名单表项除了可以手工添加之外，还可以通过扫描攻击防范自动添加。具体来讲就是，在黑名单功能使能的前提下，若配置了扫描攻击防范及相应的黑名单添加功能，则可以将检测到的扫描攻击方IP地址添加到黑名单中。扫描攻击防范添加的黑名单必定会老化，老化时间可配。关于扫描攻击防范的相关配置请参见“1.3.2 2. 配置扫描攻击防范策略”。

1.6 配置接口上的流量统计

为了得到接口上的流量统计信息，需要通过下面的配置在具体接口上使能流量统计。设备支持两种方式的流量统计功能：

- 基于接口入方向/出方向的流量统计：对接口上收到或发送的报文进行流量统计。
- 基于源 IP 地址/目的 IP 地址的流量统计：对接口上收到的报文按照源 IP 地址进行流量统计，或对接口上发送的报文按照目的 IP 地址进行流量统计。

表1-12 使能接口上的流量统计功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
使能接口上的流量统计功能	**flow-statistics enable** { **destination-ip** | **inbound** | **outbound** | **source-ip** }	必选 缺省情况下，未使能任何类型的流量统计

1.7 攻击检测及防范显示和维护

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攻击检测及防范的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，执行 **reset** 命令可以清除攻击检测及防范的统计信息。

表1-13 攻击检测及防范配置的显示和维护

操作	命令
显示接口上的攻击防范统计信息	**display attack-defense statistics interface** *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示攻击防范策略的配置信息	**display attack-defense policy** [*policy-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示黑名单信息	**display blacklist** { **all** | **ip** *source-ip-address* [**slot** *slot-number*] | **slot** *slot-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示接口上的流量统计信息	**display flow-statistics statistics interface** *interface-type interface-number* { **inbound** | **outbound** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示接口上基于IP地址的流量统计信息	**display flow-statistics statistics** [**slot** *slot-number*] { **destination-ip** *dest-ip-address* | **source-ip** *src-ip-address* } [**vpn-instance** *vpn-instance-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示受TCP Proxy保护的IP表项信息	**display tcp-proxy protected-ip** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除接口上的攻击防范统计信息	**reset attack-defense statistics interface** *interface-type interface-number*

1.8 攻击检测及防范典型配置举例

1.8.1 配置接口上的攻击防范

1. 组网需求

Router 上的接口 GigbitEthernet3/0/1 与内部网络连接，接口 GigbitEthernet3/0/2 与外部网络连接，接口 GigbitEthernet3/0/3 与一台内部服务器连接。现有如下安全需求：

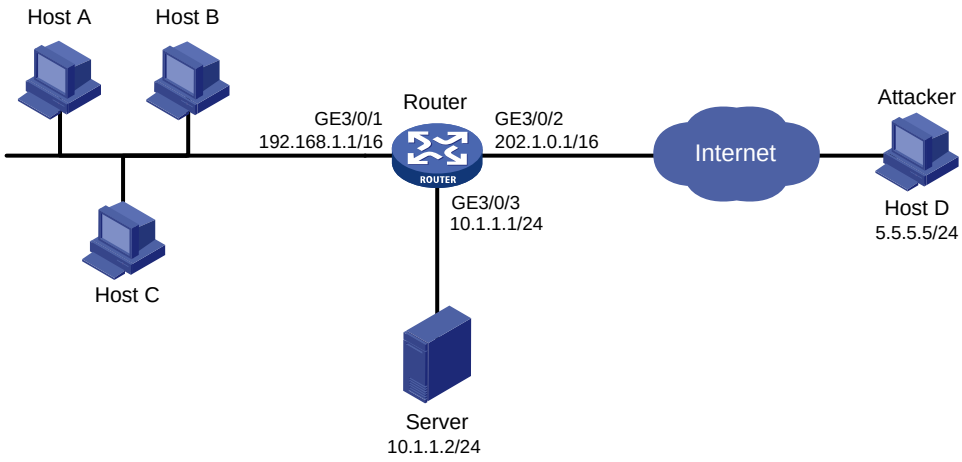
- 防范外部网络对内部网络主机的 Smurf 攻击和扫描攻击；
- 防范外部网络对内部服务器的 SYN Flood 攻击。

为满足以上需求，需要在 Router 上做如下配置：

- 在接口 GigabitEthernet3/0/2 上配置 Smurf 攻击防范和扫描攻击防范，设置扫描攻击防范的黑名单添加功能，并配置启动扫描攻击防范的连接速率阈值为每秒 4500 个连接数。
- 在接口 GigabitEthernet3/0/3 上配置 SYN Flood 攻击防范，当设备监测到向某 IP 地址每秒发送的 SYN 报文数持续达到或超过 5000 时，阻断发往该服务器的后续 SYN 报文；当设备监测到该值低于 1000 时，认为攻击结束，允许继续向该服务器发送 SYN 报文。

2. 组网图

图1-5 接口上的攻击防范配置典型组网图



3. 配置步骤

配置各接口的 IP 地址，略。

使能黑名单功能。

```
<Router> system-view
[Router] blacklist enable
```

创建攻击防范策略 1。

```
[Router] attack-defense policy 1
```

使能 Smurf 攻击防范。

```
[Router-attack-defense-policy-1] signature-detect smurf enable
```

使能扫描攻击防范。

```
[Router-attack-defense-policy-1] defense scan enable
```

配置启动扫描攻击防范的连接速率阈值为 4500。

```
[Router-attack-defense-policy-1] defense scan max-rate 4500
```

将扫描攻击防范检测到的源 IP 地址加入黑名单。

```
[Router-attack-defense-policy-1] defense scan add-to-blacklist
[Router-attack-defense-policy-1] quit
```

在接口 GigabitEthernet3/0/2 上应用攻击防范策略 1。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] attack-defense apply policy 1
[Router-GigabitEthernet3/0/2] quit
```

创建攻击防范策略 2。

```
[Router] attack-defense policy 2
```

使能 SYN Flood 攻击防范。

```
[Router-attack-defense-policy-2] defense syn-flood enable
```

为保护 IP 地址为 10.1.1.2 的内部服务器，配置针对 IP 地址 10.1.1.2 的 SYN Flood 攻击防范参数，触发阈值为 5000，恢复阈值为 1000。

```
[Router-attack-defense-policy-2] defense syn-flood ip 10.1.1.2 rate-threshold high 5000 low
1000
```

配置发现 SYN Flood 攻击后，对后续报文进行丢弃处理。

```
[Router-attack-defense-policy-2] defense syn-flood action drop-packet
[Router-attack-defense-policy-2] quit
```

在接口 GigabitEthernet3/0/3 上应用攻击防范策略 2。

```
[Router] interface gigabitethernet 3/0/3
[Router-GigabitEthernet3/0/3] attack-defense apply policy 2
[Router-GigabitEthernet3/0/3] quit
```

4. 验证配置结果

完成以上配置后，可以通过 **display attack-defense policy** 命令查看配置的攻击防范策略 1 和 2 的具体内容。

如果接口 GigabitEthernet3/0/2 上收到 Smurf 攻击报文，设备输出告警日志；如果接口 GigabitEthernet3/0/2 上收到扫描攻击报文，设备输出告警日志，并将攻击者的 IP 加入黑名单；如果接口 GigabitEthernet3/0/3 上收到 SYN Flood 攻击报文，设备输出告警日志，并对后续报文进行丢弃处理。

之后，可以通过 **display attack-defense statistics interface** 命令查看各接口上攻击防范的统计信息。若有扫描攻击发生，还可以通过 **display blacklist** 命令查看由扫描攻击防范自动添加的黑名单信息。

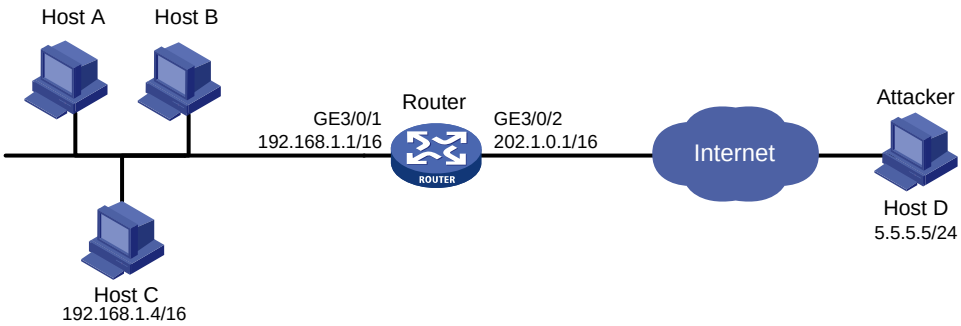
1.8.2 配置黑名单

1. 组网需求

网络管理员通过流量分析发现外部网络中存在一个攻击者 Host D，需要将来自 Host D 的报文在 Router 上永远过滤掉。另外，网络管理员为了暂时控制内部网络 Host C 的访问行为，需要将 Router 上收到的 Host C 的报文阻止 50 分钟。

2. 组网图

图1-6 黑名单配置典型组网图



3. 配置步骤

配置各接口的 IP 地址，略。

使能黑名单功能。

```
<Router> system-view
[Router] blacklist enable
```

将 Host D 的 IP 地址 5.5.5.5 添加到黑名单中，缺省永不老化。

```
[Router] blacklist ip 5.5.5.5
```

将 Host C 的 IP 地址 192.168.1.4 添加到黑名单中，老化时间为 50 分钟。

```
[Router] blacklist ip 192.168.1.4 timeout 50
```

4. 验证配置结果

完成以上配置后，可以通过 **display blacklist all** 命令查看已添加的黑名单信息。

```
[Router] display blacklist all
                    Blacklist information
------------------------------------------------------------------------------
Blacklist                               : enabled
Blacklist items                         : 2
------------------------------------------------------------------------------
IP              Type    Aging started       Aging finished      Dropped packets
                        YYYY/MM/DD hh:mm:ss YYYY/MM/DD hh:mm:ss

Total blacklist items on slot 0         : 2
5.5.5.5         manual 2008/04/09 16:02:20 Never               0
192.168.1.4     manual 2008/04/09 16:02:26 2008/04/09 16:52:26 0
```

配置生效后，Router 对来自 Host D 的报文一律进行丢弃处理，除非管理员认为 Host D 不再是攻击者，通过 **undo blacklist ip 5.5.5.5** 将其从黑名单中删除；如果 Router 接收到来自 Host C 的报文，则在 50 分钟之内，一律对其进行丢弃处理，50 分钟之后，才进行正常转发。

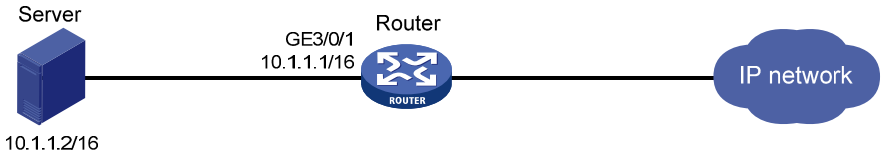
1.8.3 配置流量统计

1. 组网需求

管理员在 Router 的 GigabitEthernet3/0/1 接口上配置流量统计功能对出方向的流量进行统计和监测，并配合 UDP Flood 攻击防范配置来防范外网对内部服务器的攻击。

2. 组网图

图1-7 流量统计配置典型组网图



3. 配置步骤

配置各接口的 IP 地址，略。

创建攻击防范策略 1。

```
<Router> system-view
[Router] attack-defense policy 1
```

使能 UDP Flood 攻击防范。

```
[Router-attack-defense-policy-1] defense udp-flood enable
```

配置启动 UDP Flood 攻击防范的全局触发阈值为每秒 100 个报文数。

```
[Router-attack-defense-policy-1] defense udp-flood rate-threshold high 100
```

配置发现 UDP Flood 攻击后，对后续报文进行丢弃处理。

```
[Router-attack-defense-policy-1] defense udp-flood action drop-packet
[Router-attack-defense-policy-1] quit
```

在接口 GigabitEthernet3/0/1 上应用攻击防范策略 1。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] attack-defense apply policy 1
```

在接口 GigabitEthernet3/0/1 的出方向上使能流量统计功能。

```
[Router-GigabitEthernet3/0/1] flow-statistic enable outbound
```

在接口 GigabitEthernet3/0/1 上使能基于报文目的 IP 地址的流量统计功能。

```
[Router-GigabitEthernet3/0/1] flow-statistic enable destination-ip
```

4. 验证配置结果

若有针对服务器的攻击发生时，可以通过查看接口上的流量统计信息来判断攻击报文的详细情况。

```
[Router-GigabitEthernet3/0/1] display flow-statistics statistics destination-ip 10.1.1.2
                Flow Statistics Information
 ------------------------------------------------------------
 IP Address                              : 10.1.1.2
 ------------------------------------------------------------
 Total number of existing sessions       : 13676
 Session establishment rate              : 2735/s
 TCP sessions                            : 0
 Half-open TCP sessions                  : 0
 Half-close TCP sessions                 : 0
 TCP session establishment rate          : 0/s
 UDP sessions                            : 13676
 UDP session establishment rate          : 2735/s
 ICMP sessions                           : 0
 ICMP session establishment rate         : 0/s
 RAWIP sessions                          : 0
 RAWIP session establishment rate        : 0/s
[Router-GigabitEthernet3/0/1] display flow-statistics statistics interface gigabitethernet
3/0/1 outbound
                Flow Statistics Information
 ------------------------------------------------------------
 Interface                               : GigabitEthernet3/0/1
 ------------------------------------------------------------
 Total number of existing sessions       : 13676
 Session establishment rate              : 2735/s
 TCP sessions                            : 0
 Half-open TCP sessions                  : 0
 Half-close TCP sessions                 : 0
 TCP session establishment rate          : 0/s
 UDP sessions                            : 13676
 UDP session establishment rate          : 2735/s
 ICMP sessions                           : 0
 ICMP session establishment rate         : 0/s
 RAWIP sessions                          : 0
 RAWIP session establishment rate        : 0/s
```

可以看到，接口 GigabitEthernet3/0/1 上有大量发送到 10.1.1.2 的 UDP 报文，而且新建连接速率超过了指定阈值，可以判断发生了 UDP Flood 攻击。通过 **display attack-defense statistics** 命令可以查看 UDP Flood 攻击防范生效后的相关统计信息。

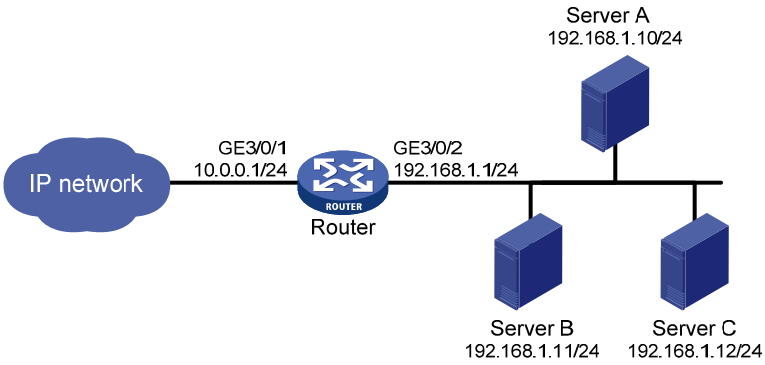
1.8.4 配置TCP Proxy

1. 组网需求

在 Router 上配置 TCP Proxy 功能，保护内网服务器不会受到外网非法用户的 SYN Flood 攻击，并要求在客户端与服务器进行双向代理。

2. 组网图

图1-8 TCP Proxy 配置组网图



3. 配置步骤

配置各接口的 IP 地址，略。

创建攻击防范策略 1。

```
<Router> system-view
[Router] attack-defense policy 1
```

使能 SYN Flood 攻击防范。

```
[Router-attack-defense-policy-1] defense syn-flood enable
```

配置启动 SYN Flood 攻击防范的全局触发阈值为每秒 100 个报文数。

```
[Router-attack-defense-policy-1] defense syn-flood rate-threshold high 100
```

配置发现 SYN Flood 攻击后，对后续报文进行 TCP Proxy。

```
[Router-attack-defense-policy-1] defense syn-flood action trigger-tcp-proxy
[Router-attack-defense-policy-1] quit
```

在接口 GigabitEthernet3/0/2 上应用攻击防范策略 1。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] attack-defense apply policy 1
[Router-GigabitEthernet3/0/2] quit
```

配置 TCP Proxy 的工作模式为双向代理模式。

```
[Router] undo tcp-proxy mode
```

在接口 GigabitEthernet3/0/1 上使能 TCP Proxy 功能。

```
[Router] interface gigabitethernet 3/0/1
[Router-GigabitEthernet3/0/1] tcp-proxy enable
```

```
[Router-GigabitEthernet3/0/1] quit
```

在接口 GigabitEthernet3/0/2 上使能 TCP Proxy 功能。

```
[Router] interface gigabitethernet 3/0/2
[Router-GigabitEthernet3/0/2] tcp-proxy enable
[Router-GigabitEthernet3/0/2] quit
```

4. 验证配置结果

以上配置完成之后，若有针对服务器的 SYN Flood 攻击发生时，可以通过 **display tcp-proxy protected-ip** 命令查看受攻击的服务器的 IP 地址被添加为动态受保护 IP。

```
[Router] display tcp-proxy protected-ip
Protected IP    Port number     Type     Lifetime(min)   Rejected packets
192.168.1.10    any             Dynamic  30              8
```