目 录

1 攻击检测及防范

说明

仅 WX2500H-WiNet 系列不支持 slot 参数。

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，例如输出告警日志或丢弃报文。

本特性能够检测单包攻击、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。

1.2 攻击检测及防范的类型

1.2.1 单包攻击

单包攻击也称为畸形报文攻击，主要包括以下三种类型：

- 攻击者通过向目标系统发送带有攻击目的的 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；
- 攻击者可以通过发送正常的报文，如 ICMP 报文、特殊类型的 IP option 报文，来干扰正常网络连接或探测网络结构，给目标系统带来损失；
- 攻击者还可通过发送大量无用报文占用网络带宽，造成拒绝服务攻击。

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
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。
ICMP type	ICMP报文中，type值的表示不同含义的报文，接收者需要根据不同的类型进行响应，攻击者通过构造特定type类型的ICMP报文来达到影响系统正常处理报文等目的。
ICMPv6 type	ICMPv6报文中，type值的表示不同含义的报文，接收者需要根据不同的类型进行响应，攻击者通过构造特定type类型的ICMPv6报文来达到影响系统正常处理报文等目的。
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。

单包攻击类型	说明
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。
Large ICMPv6	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ICMPv6报文，让目标主机崩溃，达到攻击目的。
IP option	攻击者利用IP报文中的异常选项的设置，达到探测网络结构的目的，也可由于系统缺乏对错误报文的处理而造成系统崩溃。
Fragment	攻击者通过向目标主机发送分片偏移小于5的分片报文，导致主机对分片报文进行重组时发生错误而造成系统崩溃。
Impossible	攻击者通过向目标主机发送源IP地址和目的IP地址相同的报文，造成主机系统处理异常。
Tiny fragment	攻击者构造一种特殊的IP分片来进行微小分片的攻击，这种报文首片很小，未能包含完整的传输层信息，因此能够绕过某些包过滤防火墙的过滤规则，达到攻击目标网络的目的。
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。
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。
Traceroute	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，带外）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。
UDP Bomb	攻击者发送畸形的UDP报文，其IP首部中的报文总长度大于IP首部长度与UDP首部中标识的UDP报文长度之和，可能造成收到此报文的系统处理数据时越界访问非法内存，导致系统异常。
UDP Snork	攻击者向Windows系统发送目的端口为135（Windows定位服务）源端口为135、7或19（UDP Chargen服务）的报文，使被攻击系统不断应答报文，最终耗尽CPU资源。
UDP Fraggle	攻击者通过向目标网络发送源UDP端口为7且目的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。
Teardrop	攻击者通过发送大量分片重叠的报文，致使服务器对这些报文进行重组时造成重叠，因而丢失有效的数据。
Ping of death	攻击者构造标志位为最后一片且长度大于65535的ICMP报文发送给目标主机，可能导致系统处理数据时越界访问非法内存，造成系统错误甚至系统崩溃。

1.2.2 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开放的服务端口，为进一步侵入目标系统做准备。

- IP Sweep 攻击

攻击者发送大量目的 IP 地址变化的探测报文，通过收到的回应报文来确定活跃的目标主机，以便针对这些主机进行下一步的攻击。

- Port scan 攻击

攻击者获取了活动目标主机的 IP 地址后，向目标主机发送大量目的端口变化的探测报文，通过收到的回应报文来确定目标主机开放的服务端口，然后针对活动目标主机开放的服务端口选择合适的攻击方式或攻击工具进行进一步的攻击。

- 分布式 Port scan 攻击

攻击者控制多台主机，分别向特定目标主机发送探测报文，通过收集所有被控制的主机的回应报文，确定目标主机开启的服务端口，以便进一步实施攻击。

1.2.3 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，从而无法为合法用户提供正常服务，即发生拒绝服务。

设备支持对以下几种泛洪攻击进行有效防范：

- SYN flood 攻击

根据 TCP 协议，服务器收到 SYN 报文后需要建立半连接并回应 SYN ACK 报文，然后等待客户端的 ACK 报文来建立正式连接。由于资源的限制，操作系统的 TCP/IP 协议栈只能允许有限个 TCP 连接。攻击者向服务器发送大量伪造源地址的 SYN 报文后，由于攻击报文是伪造的，服务器不会收到客户端的 ACK 报文，从而导致服务器上遗留了大量无效的半连接，耗尽其系统资源，使正常的用户无法访问，直到半连接超时。

- ACK flood 攻击

ACK 报文为只有 ACK 标志位置位的 TCP 报文，服务器收到 ACK 报文时，需要查找对应的连接。若攻击者发送大量这样的报文，服务器需要进行大量的查询工作，消耗正常处理的系统资源，影响正常的报文处理。

- SYN-ACK flood 攻击

由于 SYN ACK 报文为 SYN 报文的后续报文，服务器收到 SYN ACK 报文时，需要查找对应的 SYN 报文。若攻击者发送大量这样的报文，服务器需要进行大量的查询工作，消耗正常处理的系统资源，影响正常的报文处理。

- FIN flood 攻击

FIN 报文用于关闭 TCP 连接。若攻击者向服务器发送大量的伪造的 FIN 报文，可能会使服务器关闭掉正常的连接。同时，服务器收到 FIN 报文时，需要查找对应的连接，大量的无效查询操作会消耗系统资源，影响正常的报文处理。

- RST flood 攻击

RST 报文为 TCP 连接的复位报文，用于在异常情况下关闭 TCP 连接。如果攻击者向服务器发送大量伪造的 RST 报文，可能会使服务器关闭正常的 TCP 连接。另外，服务器收到 RST 报文时，需要查找对应的连接，大量的无效查询操作会消耗系统资源，影响正常的报文处理。

- DNS flood 攻击

DNS 服务器收到任何 DNS Query 报文时都会试图进行域名解析并且回复该 DNS 报文。攻击者通过构造并向 DNS 服务器发送大量虚假 DNS Query 报文，占用 DNS 服务器的带宽或计算资源，使得正常的 DNS Query 得不到处理。

- HTTP flood 攻击

HTTP 服务器收到 HTTP GET 命令时可能进行一系列复杂的操作，包括字符串搜索、数据库遍历、数据组装、格式化转换等等，这些操作会消耗大量系统资源，因此当 HTTP 请求的速率超过了服务器的处理能力时，服务器就无法正常提供服务。攻击者通过构造并发送大量虚假 HTTP GET 请求，使服务器崩溃，无法响应正常的用户请求。

- 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。

- ICMPv6 flood 攻击

ICMPv6 flood 攻击是指，攻击者在短时间内向特定目标发送大量的 ICMPv6 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，占用目标主机的带宽，致使目标主机不能处理正常的业务。

1.2.4 TCP分片攻击

设备的包过滤功能一般是通过判断 TCP 首个分片中的五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议号）信息来决定后续 TCP 分片是否允许通过。RFC 1858 对 TCP 分片报文进行了规定，认为 TCP 分片报文中，首片报文中 TCP 报文长度小于 20 字节，或后续分片报文中分片偏移量等于 8 字节的报文为 TCP 分片攻击报文。这类报文可以成功绕过上述包过滤功能，对设备造成攻击。

为防范这类攻击，可以在设备上配置 TCP 分片攻击防范功能，对 TCP 分片攻击报文进行丢弃。

1.2.5 Login用户字典序攻击

字典序攻击是指攻击者通过收集用户密码可能包含的字符，使用各种密码组合逐一尝试登录设备，以达到猜测合法用户密码的目的。

为防范这类攻击，可以在设备上配置 Login 用户延时认证功能，在用户认证失败之后，延时期间不接受此用户的登录请求。

1.3 攻击检测及防范配置任务简介

表1-2 攻击检测及防范配置任务简介

配置任务		说明	详细配置
创建攻击防范策略		必选	1.4.1
配置攻击防范策略	配置单包攻击防范策略	必选 各类型的攻击防范功能	1.4.2 1.
	配置扫描攻击防范策略		1.4.2 2.

配置任务		说明	详细配置
	配置泛洪攻击防范策略	之间没有先后顺序，可根据实际组网需求，配置其中的一种或多种	1.4.2 3.
	配置攻击防范例外列表	可选	1.4.3
在接口上应用攻击防范策略		二者至少选其一 应用在接口的策略仅对接口生效	1.4.4
在本机应用攻击防范策略		应用在本机的策略对所有目的地址为本机的报文均有效	1.4.5
配置单包攻击防范日志的非聚合输出功能		可选	1.4.6
配置TCP分片攻击防范		可选 通常单独使用	1.5
配置Login用户延时认证功能		可选 通常单独使用	1.6

1.4 配置攻击防范策略

1.4.1 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。

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*	缺省情况下，不存在任何攻击防范策略

1.4.2 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，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，则默认会输出告警日志，另外还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-name*	-
开启指定类型单包攻击报文的特征检测，并设置攻击防范的处理行为	**signature detect** { **fraggle** | **fragment** | **impossible** | **land** | **large-icmp** | **large-icmpv6** | **smurf** | **snork** | **tcp-all-flags** | **tcp-fin-only** | **tcp-invalid-flags** | **tcp-null-flag** | **tcp-syn-fin** | **tiny-fragment** | **traceroute** | **udp-bomb** | **winnuke** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect** { **ip-option-abnormal** | **ping-of-death** | **teardrop** } **action** { **drop** | **logging** } * **signature detect icmp-type** { *icmp-type-value* | **address-mask-reply** | **address-mask-request** | **destination-unreachable** | **echo-reply** | **echo-request** | **information-reply** | **information-request** | **parameter-problem** | **redirect** | **source-quench** | **time-exceeded** | **timestamp-reply** | **timestamp-request** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect icmpv6-type** { *icmpv6-type-value* | **destination-unreachable** | **echo-reply** | **echo-request** | **group-query** | **group-reduction** | **group-report** | **packet-too-big** | **parameter-problem** | **time-exceeded** } [**action** { { **drop** | **logging** } * | **none** }] **signature detect ip-option** { *option-code* | **internet-timestamp** | **loose-source-routing** | **record-route** | **route-alert** | **security** | **stream-id** | **strict-source-routing** } [**action** { { **drop** | **logging** } * | **none** }]	至少选其一 缺省情况下，所有类型的单包攻击的特征检测均处于关闭状态
（可选）配置启动Large ICMP攻击防范的ICMP报文长度的最大值	**signature** { **large-icmp** | **large-icmpv6** } **max-length** *length*	缺省情况下，ICMP报文和ICMPv6报文长度的最大值均为4000字节
（可选）配置对不同级别的单包攻击报文的处理方式	**signature level** { **high** | **info** | **low** | **medium** } **action** { { **drop** | **logging** } * | **none** }	缺省情况下，对**info**和**low**级别的单包攻击的处理行为是发送日志；对**medium**和**high**级别的单包攻击的处理行为是发送日志并丢包
（可选）开启指定级别单包攻击报文的特征检测	**signature level** { **high** | **info** | **low** | **medium** } **detect**	缺省情况下，未开启任何级别的单包攻击报文的特征检测

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，则可以根据配置输出告警日志或者丢弃来自该 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*	-
开启指定级别的扫描攻击防范	**scan detect level** { **high** | **low** | **medium** } **action** { **drop** | **logging** } *	缺省情况下，扫描攻击防范处于关闭状态

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。在接口上应用了泛洪攻击防范策略后，接口处于攻击检测状态，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（输出告警日志或者对后续新建连接的报文进行丢弃处理）。此后，当设备检测到向该服务器发送报文的速率低于恢复阈值（触发阈值的 3/4）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。对于所有非受保护 IP 地址，可以统一开启攻击防范检测，并采用全局的参数设置来进行保护。

(1) 配置 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*	-
对所有非受保护IP地址开启SYN flood攻击防范检测	**syn-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启SYN flood攻击防范检测
配置SYN flood攻击防范的全局触发阈值	**syn-flood threshold** *threshold-value*	缺省情况下，SYN flood攻击防范的全局触发阈值为1000
配置SYN flood攻击防范的全局处理行为	**syn-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的SYN flood攻击采取任何措施
开启对指定IP地址的SYN flood攻击防范检测，并配置触发阈值和处理行为	**syn-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置SYN flood攻击防范检测

(2) 配置 ACK flood 攻击防范策略

表1-7 配置 ACK 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*	-
对所有非受保护IP地址开启ACK flood攻击防范检测	**ack-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启ACK flood攻击防范检测
配置ACK flood攻击防范全局触发阈值	**ack-flood threshold** *threshold-value*	缺省情况下，ACK flood攻击防范的全局触发阈值为1000
配置ACK flood攻击防范的全局处理行为	**ack-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的ACK flood攻击采取任何措施
开启对指定IP地址的ACK flood攻击防范检测，并配置触发阈值和处理行为	**ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置ACK flood攻击防范检测

(3) 配置 SYN-ACK flood 攻击防范策略

表1-8 配置 SYN-ACK 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*	-
对所有非受保护IP地址开启SYN-ACK flood攻击防范检测	**syn-ack-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启SYN-ACK flood攻击防范检测
配置SYN-ACK flood攻击防范的全局触发阈值	**syn-ack-flood threshold** *threshold-value*	缺省情况下，SYN-ACK flood攻击防范的全局触发阈值为1000
配置SYN-ACK flood攻击防范的全局处理行为	**syn-ack-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的SYN-ACK flood攻击采取任何措施
开启对指定IP地址的SYN-ACK flood攻击防范检测，并配置触发阈值和处理行为	**syn-ack-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置SYN-ACK flood攻击防范检测

(4) 配置 FIN flood 攻击防范策略

表1-9 配置 FIN 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*	-

配置步骤	命令	说明
对所有非受保护IP地址开启FIN flood攻击防范检测	**fin-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启FIN flood攻击防范检测
配置FIN flood攻击防范的全局触发阈值	**fin-flood threshold** *threshold-value*	缺省情况下，FIN flood攻击防范的全局触发阈值为1000
配置FIN flood攻击防范的全局处理行为	**fin-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的FIN flood攻击采取任何措施
开启对指定IP地址的FIN flood攻击防范检测，并配置触发阈值和处理行为	**fin-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置FIN flood攻击防范检测

(5) 配置 RST flood 攻击防范策略

表1-10 配置 RST 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*	-
对所有非受保护IP地址开启RST flood攻击防范检测	**rst-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启RST flood攻击防范检测
配置RST flood攻击防范的全局触发阈值	**rst-flood threshold** *threshold-value*	缺省情况下，RST flood攻击防范的全局触发阈值为1000
配置全局的RST flood攻击防范的全局处理行为	**rst-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的RST flood攻击采取任何措施
开启对指定IP地址的RST flood攻击防范检测，并配置触发阈值和处理行为	**rst-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置RST flood攻击防范检测

(6) 配置 ICMP flood 攻击防范策略

表1-11 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**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IPv4地址开启ICMP flood攻击防范检测	**icmp-flood detect non-specific**	缺省情况下，未对任何非受保护IPv4地址开启ICMP flood攻击防范检测
配置ICMP flood攻击防范的全局触发阈值	**icmp-flood threshold** *threshold-value*	缺省情况下，ICMP flood攻击防范的全局触发阈值为1000
配置ICMP flood攻击防范的全局处理动作	**icmp-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的ICMP flood攻击采取任何措施

配置步骤	命令	说明
开启对指定IPv4地址的ICMP flood攻击防范检测，并配置触发阈值和处理行为	**icmp-flood detect ip** *ip-address* [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IPv4地址配置ICMP flood 攻击防范触发阈值

(7) 配置 ICMPv6 flood 攻击防范策略

表1-12 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**	-
进入攻击防范策略视图	**attack-defense policy** *policy-number*	-
对所有非受保护IPv6地址开启ICMPv6 flood攻击防范检测	**icmpv6-flood detect non-specific**	缺省情况下，未对任何非受保护IPv6地址开启ICMPv6 flood攻击防范检测
配置ICMPv6 flood攻击防范的全局触发阈值	**icmpv6-flood threshold** *threshold-value*	缺省情况下，ICMPv6 flood攻击防范的全局触发阈值为1000
配置ICMPv6 flood攻击防范的全局处理行为	**icmpv6-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的ICMPv6 flood攻击采取任何防范措施
开启对指定IPv6地址的ICMPv6 flood攻击防范检测，并配置触发阈值和处理行为	**icmpv6-flood detect ipv6** *ipv6-address* [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IPv6地址配置ICMPv6 flood攻击防范检测

(8) 配置 UDP flood 攻击防范策略

表1-13 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*	-
对所有非受保护IP地址开启UDP flood攻击防范检测	**udp-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启UDP flood攻击防范检测
配置UDP flood攻击防范的全局触发阈值	**udp-flood threshold** *threshold-value*	缺省情况下，UDP flood攻击防范的全局触发阈值为1000
配置UDP flood攻击防范检测的全局处理行为	**udp-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的UDP flood攻击进行任何处理
开启对指定IP地址的UDP flood攻击防范检测，并配置触发阈值和处理行为	**udp-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置UDP flood攻击防范检测

(9) 配置 DNS flood 攻击防范策略

表1-14 配置 DNS 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*	-
对所有非受保护IP地址开启DNS flood攻击防范检测	**dns-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启DNS flood攻击防范检测
配置DNS flood攻击防范的全局触发阈值	**dns-flood threshold** *threshold-value*	缺省情况下，DNS flood攻击防范的全局触发阈值为1000
（可选）配置DNS flood攻击防范的全局检测端口号	**dns-flood port** *port-list*	缺省情况下，DNS flood攻击防范的全局检测端口号为53
配置对DNS flood攻击防范的全局处理行为	**dns-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的DNS flood攻击采取任何措施
开启对指定IP地址的DNS flood攻击防范检测，并配置触发阈值和处理行为	**dns-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置DNS flood攻击防范检测

(10) 配置 HTTP flood 攻击防范策略

表1-15 配置 HTTP 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*	-
对所有非受保护IP地址开启HTTP flood攻击防范检测	**http-flood detect non-specific**	缺省情况下，未对所有非受保护IP地址开启HTTP flood攻击防范检测
配置HTTP flood攻击防范的全局触发阈值	**http-flood threshold** *threshold-value*	缺省情况下，HTTP flood攻击防范的全局触发阈值为1000
（可选）配置HTTP flood攻击防范的全局检测端口号	**http-flood port** *port-list*	缺省情况下，HTTP flood攻击防范的全局检测端口号为80
配置对HTTP flood攻击防范的全局处理行为	**http-flood action** { **drop** | **logging** } *	缺省情况下，不对检测到的HTTP flood攻击采取任何措施
开启对指定IP地址的HTTP flood攻击防范检测，并配置触发阈值和处理行为	**http-flood detect** { **ip** *ip-address* | **ipv6** *ipv6-address* } [**port** *port-list*] [**threshold** *threshold-value*] [**action** { { **drop** | **logging** } * | **none** }]	缺省情况下，未对任何指定IP地址配置HTTP flood攻击防范检测

1.4.3 配置攻击防范例外列表

攻击防范例外列表用于过滤不需要进行攻击防范检测的主机报文，与指定的 ACL permit 规则匹配的报文将不会受到任何类型的攻击防范检测。该配置用于过滤某些被信任的安全主机发送的报文，可以有效的减小误报率，并提高服务器处理效率。

需要注意的是，例外列表引用的 ACL 的 permit 规则中仅源地址、目的地址、源端口、目的端口、协议号和非首片分片标记参数用于匹配报文。

表1-16 配置攻击防范例外列表

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*	-
配置攻击防范例外列表	**exempt acl** [**ipv6**] { *acl-number* | **name** *acl-name* }	缺省情况下，应用了攻击防范策略的接口收到的所有报文都需要进行攻击防范检测

1.4.4 在接口上应用攻击防范策略

通过在接口上应用攻击防范策略，使已配置的攻击防范策略在具体的接口上生效。

当在全局接口上应用攻击防范策略时，为保证扫描攻击防范策略与泛洪攻击防范策略能够正确检测并防御攻击，需要指定处理当前接口流量的业务处理板。

表1-17 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-name*	缺省情况下，接口上未应用任何攻击防范策略

1.4.5 在本机应用攻击防范策略

通过在本机应用攻击防范策略，使已配置的攻击防范策略对目的地址为本机的报文生效。

当接口和本机均应用了攻击防范策略时，先进行接口上攻击防范策略的检测，若报文未被丢弃，则还会进行本机上攻击防范策略的检测。

表1-18 配置在本机应用攻击防范策略

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置在本机应用攻击防范策略	**attack-defense local apply policy** *policy-name*	缺省情况下，本机未应用任何攻击防范策略

1.4.6 配置单包攻击防范日志的非聚合输出功能

对日志进行聚合输出是指，在一定时间内，对在同一个接口上检测到的相同攻击类型、相同攻击防范动作以及相同的源/目的地址的单包攻击的所有日志聚合成一条日志输出。

通常不建议开启单包攻击防范的日志非聚合输出功能，因为在单包攻击较为频繁的情况下，它会导致大量日志信息输出，占用控制台的显示资源。

表1-19 配置单包攻击防范日志的非聚合输出功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
开启对单包攻击防范日志的非聚合输出功能	**attack-defense signature log non-aggregate**	缺省情况下，单包攻击防范的日志信息经系统聚合后再输出

1.5 配置TCP分片攻击防范

设备上开启 TCP 分片攻击防范功能后，能够对收到的 TCP 分片报文的长度以及分片偏移量进行合法性检测，并丢弃非法的 TCP 分片报文。

需要注意的是，如果设备上开启了 TCP 分片攻击防范功能，并应用了单包攻击防范策略，则 TCP 分片攻击防范功能会先于单包攻击防范策略检测并处理入方向的 TCP 报文。

表1-20 配置 TCP 分片攻击防范

操作	命令	说明
进入系统视图	**system-view**	-
开启TCP分片攻击防范功能	**attack-defense tcp fragment enable**	缺省情况下，TCP分片攻击防范功能处于开启状态

1.6 配置Login用户延时认证功能

Login 用户登录失败后，若设备上配置了重新进行认证的等待时长，则系统将会延迟一定的时长之后再允许用户进行认证，可以有效地避免设备受到 Login 用户字典序攻击。

表1-21 配置 Login 用户失败延时认证功能

配置步骤	命令	说明
进入系统视图	**system-view**	-
配置Login用户登录失败后重新进行认证的等待时长	**attack-defense login reauthentication-delay** *seconds*	缺省情况下，Login用户登录失败后重新进行认证不需要等待

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1-22 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* [**slot** *slot-number*]
显示本机攻击防范统计信息	**display attack-defense statistics local** [**slot** *slot-number*]
显示攻击防范策略的配置信息	**display attack-defense policy** [*policy-name*]
显示扫描攻击者的IPv4地址表项	**display attack-defense scan attacker ip** [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local**] [**count**]
显示扫描攻击者的IPv6地址表项	**display attack-defense scan attacker ipv6** [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local**] [**count**]
显示扫描攻击被攻击者的IPv4地址表项	**display attack-defense scan victim ip** [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local**] [**count**]
显示扫描攻击被攻击者的IPv6地址表项	**display attack-defense scan victim ipv6** [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local**] [**count**]
显示IPv4 flood攻击防范统计信息	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ip** [*ip-address*] [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local** [**slot** *slot-number*]] [**count**]
显示IPv6 flood攻击防范统计信息	**display attack-defense** { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **statistics ipv6** [*ipv6-address*] [**interface** *interface-type interface-number* [**slot** *slot-number*] | **local** [**slot** *slot-number*]] [**count**]
显示flood攻击防范的IPv4类型的受保护IP表项	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmp-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ip** [*ip-address*] [**slot** *slot-number*] [**count**]
显示flood攻击防范的IPv6类型的受保护IP表项	**display attack-defense policy** *policy-name* { **ack-flood** | **dns-flood** | **fin-flood** | **flood** | **http-flood** | **icmpv6-flood** | **rst-flood** | **syn-ack-flood** | **syn-flood** | **udp-flood** } **ipv6** [*ipv6-address*] [**slot** *slot-number*] [**count**]
清除接口上的攻击防范统计信息	**reset attack-defense statistics interface** *interface-type interface-number*
清除本机攻击防范的统计信息	**reset attack-defense statistics local**
清除flood攻击防范受保护IP表项的统计信息	**reset attack-defense policy** *policy-name* **flood protected** { **ip** | **ipv6** } **statistics**