目 录

1 TCP攻击防御

1.1 TCP攻击防御简介

攻击者可以利用 TCP 连接的建立过程对设备进行攻击。为了避免上述攻击带来的危害，设备提供了以下功能：

- SYN Cookie 功能
- 防止 Naptha 攻击功能

下面将详细介绍上述功能可以防止的攻击类型、工作原理，以及配置过程。

1.2 配置SYN Cookie功能

一般情况下，TCP 连接的建立需要经过三次握手，即：

(1) TCP 连接请求的发起者向目标服务器发送 SYN 报文；

(2) 目标服务器收到 SYN 报文后，建立处于 SYN_RECEIVED 状态的 TCP 半连接，并向发起者回复 SYN ACK 报文，等待发起者的回应；

(3) 发起者收到 SYN ACK 报文后，回应 ACK 报文，这样 TCP 连接就建立起来了。

利用 TCP 连接的建立过程，一些恶意的攻击者可以进行 SYN Flood 攻击。攻击者向服务器发送大量请求建立 TCP 连接的 SYN 报文，而不回应服务器的 SYN ACK 报文，导致服务器上建立了大量的 TCP 半连接。从而，达到耗费服务器资源，使服务器无法处理正常业务的目的。

SYN Cookie 功能用来防止 SYN Flood 攻击。当服务器收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。服务器接收到发起者回应的 ACK 报文后，才建立连接，并进入 ESTABLISHED 状态。通过这种方式，可以避免在服务器上建立大量的 TCP 半连接，防止服务器受到 SYN Flood 攻击。

表1-1 配置 SYN Cookie 功能

操作	命令	说明
进入系统视图	**system-view**	-
使能SYN Cookie功能	**tcp syn-cookie enable**	必选 缺省情况下，SYN Cookie功能处于使能状态

说明

- 如果启用了在建立 TCP 连接时进行 MD5 认证的功能，则 SYN Cookie 功能不会生效。取消在建立 TCP 连接时进行 MD5 认证功能后，之前配置的 SYN Cookie 功能会自动生效。关于在建立 TCP 连接时进行 MD5 认证功能的介绍，请参见“三层技术-IP 路由配置指导”中“BGP”手册中“配置 BGP 建立 TCP 连接时进行 MD5 认证”章节的内容。
- 使能 SYN Cookie 功能后，建立 TCP 连接时只协商最大报文段长度选项，而不协商窗口缩放因子和时间戳选项。

1.3 配置防止Naptha攻击功能

Naptha 攻击类似于 SYN Flood 攻击，所不同的是 Naptha 攻击可利用 TCP 连接的 CLOSING、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2、LAST_ACK 和 SYN_RECEIVED 六种状态来达到攻击目的，而 SYN Flood 只是利用 SYN_RECEIVED 状态。

Naptha 攻击通过控制大量主机与服务器建立 TCP 连接，并使这些连接处于同一种状态（上述六种状态中的一种），而不请求任何数据，从而达到消耗服务器的内存资源，导致服务器无法处理正常业务的目的。

防止 Naptha 攻击功能通过加速 TCP 状态的老化，来降低服务器遭受 Naptha 攻击的风险。使能防止 Naptha 攻击功能后，设备周期性地检测处于上述六种状态的 TCP 连接数（设备只记录其作为 TCP 服务器的 TCP 连接数）。如果检测到某个状态的 TCP 连接数目超过设定的最大连接数，则认为设备受到 Naptha 攻击，就会加速该状态下 TCP 连接的老化。当该状态下的 TCP 连接数低于最大连接数的 80%（最小值为 1），则取消该状态下 TCP 连接的加速老化。

表1-2 配置防止 Naptha 攻击功能

操作	命令	说明
进入系统视图	**system-view**	-
使能防止Naptha攻击功能	**tcp anti-naptha enable**	必选 缺省情况下，防止Naptha攻击功能处于关闭状态
配置某一状态下的最大TCP连接数	**tcp state** { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** | **syn-received** } **connection-number** *number*	可选 缺省情况下，六种TCP状态下的最大连接数均为5 如果TCP状态下的最大连接数为0，则表示不会加速该状态的老化
配置TCP连接状态的轮询检测时间间隔	**tcp timer check-state** *timer-value*	可选 缺省情况下，TCP状态轮询检测的时间间隔为30秒

1.4 TCP攻击防御显示和维护

在任意视图下执行 **display tcp status** 命令可以显示所有 TCP 连接的状态，用户可以通过显示信息随时监控 TCP 连接。

表1-3 TCP 攻击防御显示和维护

操作	命令
显示所有TCP连接的状态	**display tcp status** [**|** { **begin** | **exclude** | **include** } *regular-expression*]