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 连接的建立过程对与其建立连接的设备进行攻击，为了避免攻击带来的危害，设备提供了相应的技术对攻击进行检测和防范。

下面将详细介绍防攻击技术的原理以及配置。

1.2 配置防止Naptha攻击功能

Naptha 属于 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击方式，主要利用操作系统 TCP/IP 栈和网络应用程序需要使用一定的资源来控制 TCP 连接的特点，在短时间内不断地建立大量的 TCP 连接，并且使其保持在某个特定的状态（CLOSING、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2 和 LAST_ACK 五种状态中的一种），而不请求任何数据，那么被攻击设备会因消耗大量的系统资源而陷入瘫痪。

防止 Naptha 攻击功能通过加速 TCP 状态的老化，来降低设备遭受 Naptha 攻击的风险。开启防止 Naptha 攻击功能后，设备周期性地对各状态的 TCP 连接数进行检测。当某状态的最大 TCP 连接数超过指定的最大连接数后，将加速该状态下 TCP 连接的老化。

表1-1 配置防止 Naptha 攻击功能

操作	命令	说明
进入系统视图	**system-view**	-
开启防止Naptha攻击功能	**tcp anti-naptha enable**	缺省情况下，防止Naptha攻击功能处于关闭状态
（可选）配置TCP连接的某一状态下的最大TCP连接数	**tcp state** { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** } **connection-limit** *number*	缺省情况下，CLOSING、ESTABLISHED、 FIN_WAIT_1、FIN_WAIT_2和LAST_ACK五种状态最大TCP连接数均为50 如果最大TCP连接数为0，则表示不会加速该状态下TCP连接的老化
（可选）配置TCP连接状态的检测周期	**tcp check-state interval** *interval*	缺省情况下，TCP连接状态的检测周期为30秒