目 录

1 TCP攻击防御 ····· 1-1
1.1 TCP攻击防御配置命令 ····· 1-1
1.1.1 display tcp status ····· 1-1
1.1.2 tcp anti-naptha enable ····· 1-2
1.1.3 tcp state ····· 1-2
1.1.4 tcp syn-cookie enable ····· 1-3
1.1.5 tcp timer check-state ····· 1-4

1 TCP攻击防御

1.1 TCP攻击防御配置命令

1.1.1 display tcp status

【命令】

display tcp status [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display tcp status 命令用来显示所有 TCP 连接的状态，使用户随时监控 TCP 连接。

【举例】

显示所有 TCP 连接状态。

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB         Local Add:port       Foreign Add:port     State
03e37dc4      0.0.0.0:4001         0.0.0.0:0            Listening
04217174      100.0.0.204:23       100.0.0.253:65508    Established
```

表1-1 display tcp status 命令显示信息描述表

字段	描述
*: TCP MD5 Connection	如果某个连接前有星号标识，则表示该TCP连接是采用MD5加密算法认证的连接
TCPCB	TCP控制块
Local Add:port	本端IP地址及端口号
Foreign Add:port	对端IP地址及端口号
State	TCP连接的状态

1.1.2 tcp anti-naptha enable

【命令】

tcp anti-naptha enable

undo tcp anti-naptha enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

tcp anti-naptha enable 命令用来使能防止 Naptha 攻击功能。**undo tcp anti-naptha enable** 命令用来关闭防止 Naptha 攻击功能。

缺省情况下，防止 Naptha 攻击功能处于关闭状态。

需要注意的是，关闭防止 Naptha 攻击功能后，**tcp state** 命令和 **tcp timer check-state** 命令的配置都会被删除。

【举例】

使能防止 Naptha 攻击功能。

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
```

1.1.3 tcp state

【命令】

tcp state { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** | **syn-received** } **connection-number** *number*

undo tcp state { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** | **syn-received** } **connection-number**

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

closing：TCP 连接的 CLOSING 状态。

established：TCP 连接的 ESTABLISHED 状态。

fin-wait-1：TCP 连接的 FIN_WAIT_1 状态。

fin-wait-2：TCP 连接的 FIN_WAIT_2 状态。

last-ack：TCP 连接的 LAST_ACK 状态。

syn-received：TCP 连接的 SYN_RECEIVED 状态。

connection-number *number*：处于某个状态的最大 TCP 连接数。*number* 的取值范围为 0～500。

【描述】

tcp state 命令用来配置某一状态下的最大 TCP 连接数，连接数目超过最大连接数后，将加速该状态下 TCP 连接的老化。**undo tcp state** 命令用来恢复缺省情况。

缺省情况下，六种状态下的最大 TCP 连接数均为 5。

需要注意的是，

- 配置本命令前，需要先使能防止 Naptha 攻击功能，否则会提示错误；
- 可以分别配置六种状态下的最大连接数；
- 如果某一状态下的最大连接数为 0，则表示不会加速该状态下 TCP 连接的老化。

相关配置可参考命令 **tcp anti-naptha enable**。

【举例】

配置 ESTABLISHED 状态下的最大 TCP 连接数为 100。

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
[Sysname] tcp state established connection-number 100
```

1.1.4 tcp syn-cookie enable

【命令】

tcp syn-cookie enable

undo tcp syn-cookie enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

tcp syn-cookie enable 命令用来使能 SYN Cookie 功能，防止设备受到 SYN Flood 攻击。**undo tcp syn-cookie enble** 命令用来关闭 SYN Cookie 功能。

缺省情况下，SYN Cookie 功能处于使能状态。

【举例】

使能 SYN Cookie 功能。

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

1.1.5 tcp timer check-state

【命令】

tcp timer check-state *time-value*

undo tcp timer check-state

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

time-value：TCP 连接状态的轮询检测时间间隔，取值范围为 1～60，单位为秒。

【描述】

tcp timer check-state 命令用来配置 TCP 连接状态的轮询检测时间间隔。**undo tcp timer check-state** 命令用来恢复缺省情况。

缺省情况下，TCP 连接状态的轮询检测时间间隔为 30 秒。

设备周期性地检测处于六种状态的 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时，则加速该状态下 TCP 连接的老化。

需要注意的是，配置本命令前，需要先使能防止 Naptha 攻击功能，否则会提示错误。

相关配置可参考命令 **tcp anti-naptha enable**。

【举例】

配置 TCP 连接状态的轮询检测时间间隔为 40 秒。

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
[Sysname] tcp timer check-state 40
```