Contents

TCP attack prevention commands ····· 1
tcp anti-naptha enable ····· 1
tcp check-state interval ····· 1
tcp state ····· 2

TCP attack prevention commands

tcp anti-naptha enable

Use **tcp anti-naptha enable** to enable Naptha attack prevention.

Use **undo tcp anti-naptha enable** to disable Naptha attack prevention.

Syntax

tcp anti-naptha enable

undo tcp anti-naptha enable

Default

Naptha attack prevention is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After you enable Naptha attack prevention, the device periodically checks the number of TCP connections in each state. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in that state. The check interval is set by the **tcp check-state interval** command. The TCP connection limits are set by the **tcp state** command.

Examples

Enable Naptha attack prevention.

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

Related commands

tcp state

tcp check-state interval

tcp check-state interval

Use **tcp check-state interval** to set the interval for checking the number of TCP connections in each state.

Use **undo tcp check-state interval** to restore the default.

Syntax

tcp check-state interval *interval*

undo tcp check-state interval

Default

The interval for checking the number of TCP connections in each state is 30 seconds.

Views

System

Predefined user roles

network-admin

Parameter

interval: Specifies the check interval in the range of 1 to 60 seconds.

Usage guidelines

This command takes effect after you enable Naptha attack prevention.

After you enable Naptha attack prevention, the device checks the number of TCP connections in each state at intervals. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in that state.

Examples

Set the interval to 40 seconds for checking the number of TCP connections in each state.

```
<Sysname> system-view
[Sysname] tcp check-state interval 40
```

Related commands

tcp anti-naptha enable

tcp state

tcp state

Use **tcp state** to set the maximum number of TCP connections in a state.

Use **undo tcp state** to restore the default.

Syntax

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

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

Default

The maximum number of TCP connections in each state (CLOSING, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, and LAST_ACK) is 50.

Views

System view

Predefined user roles

network-admin

Parameters

closing: Specifies the CLOSING state.

established: Specifies the ESTABLISHED state.

fin-wait-1: Specifies the FIN_WAIT_1 state.

fin-wait-2: Specifies the FIN_WAIT_2 state.

last-ack: Specifies the LAST_ACK state.

connection-limit *number*: Specifies the maximum number of TCP connections, in the range of 0 to 500. The value of 0 represents that the device does not accelerate the aging of the TCP connections in a state.

Usage guidelines

This command takes effect after you enable Naptha attack prevention. If the number of TCP connections in a state exceeds the limit, the device will accelerate the aging of the TCP connections in the state.

Examples

Set the maximum number of TCP connections in the ESTABLISHED state to 100.

```
<Sysname> system-view
[Sysname] tcp state established connection-limit 100
```

Related commands

tcp anti-naptha enable

tcp check-state interval