Contents

Attack detection and prevention commands

attack-defense login reauthentication-delay

Use **attack-defense login reauthentication-delay** to enable the login delay feature.

Use **undo attack-defense login reauthentication-delay** to restore the default.

Syntax

attack-defense login reauthentication-delay *seconds*

undo attack-defense login reauthentication-delay

Default

The login delay feature is disabled. The device does not delay accepting a login request from a user who has failed a login attempt.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the delay period in the range of 4 to 60 seconds.

Usage guidelines

The login delay feature delays the device to accept a login request from a user after the user fails a login attempt. This feature can slow down login dictionary attacks.

The login delay feature is independent of the login attack prevention feature.

Examples

Enable the login delay feature and set the delay period to 5 seconds.

```
<Sysname> system-view
[Sysname] attack-defense login reauthentication-delay 5
```

attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable TCP fragment attack prevention.

Use **undo attack-defense tcp fragment enable** to disable TCP fragment attack prevention.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

TCP fragment attack prevention is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to drop attack TCP fragments to prevent TCP fragment attacks that the packet filter cannot detect. As defined in RFC 1858, attack TCP fragments refer to the following TCP fragments:

- First fragments in which the TCP header is smaller than 20 bytes.
- Non-first fragments with a fragment offset of 8 bytes (FO=1).

TCP fragment attack prevention takes precedence over single-packet attack prevention. When both are used, incoming TCP packets are processed first by TCP fragment attack prevention and then by the single-packet attack defense policy.

Examples

Enable TCP fragment attack prevention.

```
<Sysname> System-view
[Sysname] attack-defense tcp fragment enable
```