Tamper Detection

Tamper detection is a security feature implemented in Cisco 8000 Series Secure Routers to identify potential tampering events. Each router is shipped from the manufacturer with its chassis cover securely fastened. If the chassis cover is opened after shipment, the hardware records all chassis cover open and close events in tamper-proof memory, regardless of whether the device is powered on or off.

On boot up, the software reads the latest event index and compares it with previously known indices. When there is a discrepancy, the software generates a SYSlog message during startup to report the tamper event. When the device is in fully powered up state, software will generate syslog message and SNMP trap immediately.

Benefits

Tamper Detection notification detects unauthorized physical access or attempts to compromise the device, helping protect sensitive data and network integrity.

Limitations

Tamper Detection feature is currently not supported on SDWAN/SD-Routing mode.

Configure Tamper Detection

Tamper detection is enabled by default on the router. The open or close events of the chassis cover are auto recorded.

The tamper event notification can be enabled or disabled using these commands in config mode.

- Enable the Tamper Detection notification using this command in config mode (enabled by default):

```
Router(config)#platform tamper detection
```

- Disable the Tamper Detection notification using the command in config mode:

```
Router(config)#no platform tamper detection
```

Mark tamper detection events

A Tamper event marking is a feature that

- allows authorized users to prevent specific activities from appearing as tamper events,
- enables the system to distinguish between authorized and unauthorized access, and
- maintains the accuracy of tamper event logs.

Configure tamper detection events

To prevent authorized activities from appearing as tamper events in logs. Follow these steps.

Procedure

Step 1 Generate a challenge to obtain the consent token using the below command.

Example:

```
request consent-token generate-challenge tamper-auth auth-timeout <mins>
```

This step ensures that the consent token is generated only by an authorized user.

Step 2 Once the challenge is verified and the consent token is generated, accept the consent token using this command.

Example:

```
request consent-token accept-response tamper-auth <consent token>
```

Step 3 Mark the tamper detection event using the command below

Example:

```
request platform hardware tamper-detection event-mark
```

request platform hardware tamper-detection event-mark command is supported from Cisco IOS XE 17.17.1a

The last known event index and timestamp are marked, preventing authorized activities from appearing as tamper events in the log.

Verify the Tamper Detection events

```
Router# show platform tamper-detection event [power-off | power-on] [all | lastx | new]
```

Option	Description
power off	The **power off** option specifies the tampering events when router doesn't have power cable connected.

Option	Description
power on	The **power on** option specifies the tampering events when the router was powered on.
all	The **all** option specifies all the recorded tampering events. System can show maximum 500 entries; every 500 entries will increase one rollover counter.
lastx	The **lastx** option specifies the number of events to display. For example, "lastx 10" will show the last 10 events.
new	The **new** option specifies the new tampering events since last known events index.

The show command provides an event log which contains these details:

- Current event index
- Current time
- Rollover Status and Rollover Count:
  - When tamper event count <= 500, the Rollover Count is 0, Rollover Status: No
  - For every 500 logs, the Rollover Count will be increased by 1:
  - When 501-1000 overwrites 1-500, the Rollover Count is 1, Rollover Status: Yes
  - When 1001-1500 overwrites 501-1000, the Rollover Count is 2, Rollover Status: Yes
- The events indicating event type and timestamp

Verify events when system is powered off

When the system power is off, the router uses battery power to record any tampering events. The router records the first chassis cover open event between last power off and next power on. If chassis cover was open or closed many times during power off, only the first open event is recorded. An example shows the event log when the system is powere off :

```
Router#show platform tamper-detection event power-off all
Current Time: 2025/04/25 19:55:03       Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------

    #2                          2024/08/08 02:36:41             Chassis is opened
    #1                         2000/00/00 00:00:00            Battery not present or used
 up
```

Verify events when system is partially or fully powered on

When system power is available, the router records all chassis cover open or close events. An example of the event log when the system is partially or fully powered on:

```
Router show platform tamper-detection event power-on lastx 10
Current Time: 2025/04/25 19:54:46      Rollover Status: No     Rollover Count: 0
-------------------------------------------------------------------------------------------------------
Tamper event index      |       Tamper event timestamp  |       Tamper events description
-------------------------------------------------------------------------------------------------------

    #2                  025/04/24 22:10:14             Chassis is opened
    #1                   025/04/24 22:02:33             Chassis is closed
```

Tamper Detection SYSlog

When the router boots up, it reads the current event index from the event log and compares it with the last known index stored previously. If there is a mismatch between the indices or the timestamps differ, IOS will generate a warning-level SYSlog message and send a notification to the controller in controller mode.

This section provides examples of distinct SYSlog events.

- SYSlog for power-on events

  When Tamper Detection is enabled and the system is powered on, a power-on SYSlog message will be displayed during boot-up.

  ```
  Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 0 times and closed 0 times during power up since last known event index 7 at
  2025/04/24 22:11:51
  ```

- SYSlog for power-off events

  When Tamper Detection is enabled and the system is powered off, a power-off SYSlog message will be displayed during boot-up.

  ```
  Apr 25 20:15:01.064: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 0 times and closed 0 times during power down since last known event index 5 at
   2025/04/24 22:11:51
  ```

- SYSlog for runtime events

  ```
  *Aug 29 06:56:34.560: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has been
  opened !!
  *Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 2 times and closed 0 times during power down since last known event index 50
  at 2025/06/04 08:03:06
  *Aug 29 06:56:36.130: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 20 times and closed 20 times during power up since last known event index 1638
   at 2025/06/05 07:08:12

  *Aug 29 06:57:04.563: %CMRP-4-INTRUSION_ALERT: R0/0: cmand: The system cover has been
  closed !!
  *Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 2 times and closed 0 times during power down since last known event index 50
  at 2025/06/04 08:03:06
  *Aug 29 06:57:06.137: %CMRP-4-TAMPER_DETECTION_EVENT_MSG: R0/0: cmand: System cover was
   opened 20 times and closed 21 times during power up since last known event index 1638
   at 2025/06/05 07:08:12
  ```

Note If the Tamper Detection feature is disabled, the SYSlog messages will not be displayed at boot up.