Unexpected Source Address Alerting

You can configure Cisco Unified Border Element (SP Edition) to provide alerts for any unexpected source addresses that are received. After an unexpected source address is received, a log is created and a Simple Network Management Protocol (SNMP) trap is generated.

Cisco Unified Border Element (SP Edition) was formerly known as Integrated Session Border Controller and may be commonly referred to in this document as the session border controller (SBC).

For a complete description of the commands used in this chapter, refer to the *Cisco Unified Border Element (SP Edition) Command Reference: Unified Model* at:

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

To locate documentation for other commands that appear in this chapter, use the command reference master index, or search online.

Note For Cisco IOS XE Release 2.4, this feature is supported in both the unified model and the distributed model.

Feature History for Unexpected Source Address Alerting

Release	Modification
Cisco IOS XE Release 2.4	This feature was introduced for the unified model on the Cisco ASR 1000 Series Aggregation Services Routers.

Contents

This module contains the following sections:

Prerequisites—Implementing Unexpected Source Address Alerting

The following prerequisite is required to implement the unexpected source address alerting feature:

Before implementing unexpected source address alerting, Cisco Unified Border Element (SP Edition) must already be configured.

Restrictions for Unexpected Source Address Alerting

Review the following restrictions for unexpected source address alerting:

- This configuration option should only be enabled on trusted networks where any single such instance might indicate a threat to network security.
- Alerts on the same flow are rate-limited as are the total number of alerts reported at any one time to ensure management systems are not flooded with reports. There is not a 1-to-1 correspondence between alerts and incorrect packets.
- Diagnosing and resolving the issue of rogue packets is beyond the scope of the Cisco Unified Border Element (SP Edition) function.
- Any and all packets from unexpected sources are dropped.

Unexpected Source Address Alerting

If a packet with unexpected source address/port is received by the data border element (DBE) on a media address, port, or (if applicable) Virtual Routing Forwarding (VRF) used by a current call, then the DBE creates a log and generates an SNMP trap on the appropriate media-flow-stats MIB.

The log (level 63) is output to the console automatically (by default). The log is a member of the MEDIA debug log group. The log includes the local address, port, and VRF where the packets were received and also the source address and port of the received packet.

An alert is generated the first time an unexpected packet is received on a port after the port is opened for a call. If additional unexpected packets are received on the same media port, additional alerts are generated. Any additional alerts are rate-limited. After the call is completed, the media port is assigned to a new call, and the state is reset. A new alert is then generated if any additional unexpected packets are subsequently received.

The SNMP trap that is generated will contain the following fields:

- The address and port where the unexpected packet was received.
- The address and port where the unexpected packet originated.

Configuring Unexpected Source Address Alerting

SUMMARY STEPS

1. **configure**
2. **sbc** *sbc-name*
3. **sbe**
4. **unexpected-source-alerting**
5. **end**
6. **show sbc** *sbc-name* **dbe media-flow-stats vrf** *vrf-name* [**ipv4** *A.B.C.D* [**port**] *port number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure`	Enables global configuration mode.
Step 2	**sbc** *sbc-name* **Example:** `Router(config)# sbc mysbc`	Creates the SBC service on Cisco Unified Border Element (SP Edition) and enters into SBC configuration mode.
Step 3	**sbe** **Example:** `Router(config-sbc)# sbe`	Enters the mode of the signaling border element (SBE) function of the SBC.
Step 4	**unexpected-source-alerting** **Example:** `Router(config-sbc-sbe)# unexpected-source-alerting`	Sets alerting for unexpected source addresses. The **no** form of this command removes alerting for any unexpected source addresses that are received.
Step 5	**exit** **Example:** `Router(config-sbc-sbe)# exit`	Exits SBE configuration mode and enters SBC configuration mode.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-sbc)# end`	Exits the SBC configuration mode and returns to Privileged EXEC mode.
Step 7	**show sbc** *service-name* **dbe media-flow-stats vrf** *vrf-name* **[ipv4** *A.B.C.D* **[port** *port-number*]] **Example:** `Router# show sbc mysbc dbe media-flow-stats vrf vpn3 ipv4 10.1.1.1 port 24000`	Displays detailed information about the media flow statistics configured on the DBE.

Examples of Configuring Unexpected Source Address Alerting

This section provides a sample configuration for configuring unexpected source address alerting including an example of the information added to the media flow statistics.

To configure unexpected source address alerting, use the following commands:

```
configure terminal
 sbc mysbc
  sbe
   unexpected-source-alerting
   end
```