

## Unexpected Source Address Alerting

You can configure the Session Border Controller (SBC) 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.



**Note**

For ACE SBC Release 3.0.00, this feature is supported in both the unified model and the distributed model.

For a complete description of commands used in this chapter, refer to [Chapter 39, “Cisco Session Border Controller Commands”](#). To locate documentation for other commands that appear in this chapter, use the command reference master index, or search online.

### Feature History for Unexpected Source Address Alerting

Release	Modification
Release 12.2(33)SRC	Added support for SBC unified model.
Release 12.2(33)SRB1	This feature was introduced on the Cisco 7600 series router.

## Contents

This module contains the following sections:

- [Prerequisites—Implementing Unexpected Source Address Alerting, page 5-1](#)
- [Restrictions for Unexpected Source Address Alerting, page 5-2](#)
- [Unexpected Source Address Alerting, page 5-2](#)
- [Configuring Unexpected Source Address Alerting, page 5-3](#)
- [Examples of Configuring Unexpected Source Address Alerting, page 5-4](#)

## Prerequisites—Implementing Unexpected Source Address Alerting

The following prerequisites are required to implement SBC unexpected source address alerting:

- On the Application Control Engine Module (ACE), you must be an Admin user to enter SBC commands. For more information, see the *Application Control Engine Module Administration Guide* at [http://www.cisco.com/en/US/products/hw/modules/ps2706/products\\_configuration\\_guide\\_book09186a00806838f4.html](http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806838f4.html)
- Before implementing unexpected source address alerting, the SBC must already be created. See the procedures described in [Chapter 2, “ACE Configuration Prerequisites for the SBC”](#).

## 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 SBC 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** *service-name*
3. **dbe**
4. **vdbe** *global*
5. **unexpected-source-alerting**
6. **end**
7. **show services 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	<b>configure</b>  <b>Example:</b> host1/Admin# configure	Enables global configuration mode.
Step 2	<b>sbc</b> <i>service-name</i>  <b>Example:</b> host1/Admin(config)# sbc mysbc	Enters a submode where alerts can be configured for unexpected source addresses.  Use the <i>service-name</i> argument to define the name of the service.
Step 3	<b>dbe</b>  <b>Example:</b> host1/Admin(config-sbc)# dbe	Enters a submode where alerts can be configured for unexpected source addresses.
Step 4	<b>vdbe</b> [ <b>global</b> ]  <b>Example:</b> host1/Admin(config-sbc-dbe)# vdbe	Enters into vDBE configuration submode.   <b>Note</b> In the initial release only one vDBE (the global vDBE) is supported. The vdbe name is not required. If specified, it must be global.
Step 5	<b>unexpected-source-alerting</b>  <b>Example:</b> host1/Admin(config-sbc-dbe-vdbe-global)# unexpected-source-alerting	Sets alerting for unexpected source addresses.  The <b>no</b> form of this command removes alerting for any unexpected source addresses that are received.  <b>Note</b> The <b>unexpected-source-alerting</b> command applies only to DBEs in the distributed model.

	Command or Action	Purpose
Step 6	<b>end</b>  <b>Example:</b> host1/Admin(config-sbc-dbe-vdbe-global)# end	Exits the unexpected-source-alerting mode to DBE mode.
Step 7	<b>show services sbc service-name dbe media-flow-stats vrf vrf-name [ipv4 A.B.C.D [port port-number]]</b>  <b>Example:</b> host1/Admin(config-sbc-dbe)# show services 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 and output 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
  sbc mysbc
  dbe
  vdbe
  global
  unexpected-source-alerting
end
```