



CHAPTER 5

予期せぬ送信元アドレスに対するアラート

予期せぬ送信元アドレスを受信した場合にアラートを生成するように Session Border Controller (SBC; セッション ボーダ コントローラ) を設定できます。予期せぬ送信元アドレスを受信すると、ログが作成され、Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップが生成されます。



(注)

ACE SBC Release 3.0.00 では、この機能は統合モデルと分散モデルの両方でサポートされます。

この章で使用されるコマンドの詳細については、[第 39 章「Cisco セッション ボーダ コントローラ コマンド」](#)を参照してください。この章に記載されたその他のコマンドのマニュアルを特定するには、コマンドリファレンスのマスター インデックスを使用するか、またはオンラインで検索してください。

予期せぬ送信元アドレスに関するアラート機能の履歴

リリース	変更内容
Release 12.2(33)SRC	SBC 統合モデルのサポートが追加されました。
Release 12.2(33)SRB1	この機能が Cisco 7600 シリーズ ルータに追加されました。

この章の構成

この章で説明する内容は、次のとおりです。

- 「[前提条件 - 予期せぬ送信元アドレスに対するアラートの実装](#)」 (P.5-1)
- 「[予期せぬ送信元アドレスに対するアラートの制約事項](#)」 (P.5-2)
- 「[予期せぬ送信元アドレスに対するアラート](#)」 (P.5-2)
- 「[予期せぬ送信元アドレスに対するアラートの設定](#)」 (P.5-3)
- 「[予期せぬ送信元アドレスに対するアラートの設定例](#)」 (P.5-4)

前提条件 - 予期せぬ送信元アドレスに対するアラートの実装

次に、予期せぬ送信元アドレスに関するアラートを SBC に実装するための前提条件を示します。

- Application Control Engine (ACE) モジュールで SBC コマンドを入力するには、Admin ユーザーである必要があります。詳細については、次の URL にある『*Application Control Engine Module Administration Guide*』を参照してください。
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806838f4.html
- 予期せぬ送信元アドレスに対するアラートを実装する前に、SBC を作成しておく必要があります。第 2 章「SBC の ACE を設定するための前提条件」に記載された手順に従ってください。

予期せぬ送信元アドレスに対するアラートの制約事項

予期せぬ送信元アドレスに対するアラートについて、次の制約事項を確認してください。

- 信頼できるネットワークの場合、この設定オプションをイネーブルにする必要があるのは、このような違反がネットワーク セキュリティに対する脅威となりうる場合だけです。
- 管理システムがレポートによってフラッディングしないように、同じフローに対するアラートはレート（同時に報告されるアラートの総数）が制限されます。アラートと不正パケットに 1 対 1 の対応関係はありません。
- SBC 機能は、不正パケット問題の診断および解決に対応していません。
- 予期せぬ送信元からのパケットはすべてドロップされます。

予期せぬ送信元アドレスに対するアラート

予期せぬ送信元アドレス/ポートを含むパケットが、Data Border Element (DBE; データ ボーダ エlement) によって、現在のコールで使用されるメディア アドレス、ポート、または Virtual Routing Forwarding (VRF) (使用可能な場合) 上で受信すると、DBE はログを作成し、該当する media-flow-stats MIB 上で SNMP トラップを生成します。

ログ (レベル 63) はコンソールに自動的に出力されます (デフォルト)。このログは、MEDIA デバッグ ログ グループのメンバーです。このログには、パケットが受信されたローカル アドレス、ポート、VRF、および受信パケットの送信元アドレスやポートが含まれます。

コール用に開かれたポート上に、予期せぬパケットが最初に着信すると、アラートが生成されます。同じメディア ポート上に、予期せぬパケットがさらに着信すると、追加アラートが生成されます。追加アラートはレート制限されます。コールが完了すると、メディア ポートは新しいコールに割り当てられ、状態がリセットされます。以降に予期せぬパケットがさらに着信した場合は、新しいアラートが生成されます。

生成された SNMP トラップには、次のフィールドが含まれます。

- 予期せぬパケットが受信されたアドレスおよびポート
- 予期せぬパケットの送信元アドレスおよびポート

予期せぬ送信元アドレスに対するアラートの設定

手順概要

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]`

詳細手順

	コマンドまたはアクション	目的
ステップ 1	<code>configure</code> 例： host1/Admin# <code>configure</code>	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	<code>sbc service-name</code> 例： host1/Admin(config)# <code>sbc mysbc</code>	予期せぬ送信元アドレスに対してアラートを設定できるサブモードを開始します。 サービス名を定義するには、 <code>service-name</code> 引数を使用します。
ステップ 3	<code>dbe</code> 例： host1/Admin(config-sbc)# <code>dbe</code>	予期せぬ送信元アドレスに対してアラートを設定できるサブモードを開始します。
ステップ 4	<code>vdbe [global]</code> 例： host1/Admin(config-sbc-dbe)# <code>vdbe</code>	VDBE コンフィギュレーション サブモードを開始します。  (注) 初期リリースでは、vDBE (グローバル vDBE) が 1 つだけサポートされています。vdbe 名は省略可能です。指定する場合は、 <code>global</code> を指定する必要があります。
ステップ 5	<code>unexpected-source-alerting</code> 例： host1/Admin(config-sbc-dbe-vdbe-global)# <code>unexpected-source-alerting</code>	予期せぬ送信元アドレスに対するアラートを設定します。 このコマンドの <code>no</code> 形式を使用すると、予期せぬ送信元アドレスが受信された場合に、アラートが生成されなくなります。 (注) <code>unexpected-source-alerting</code> コマンドは、分散モデルの DBE にだけ適用されます。

	コマンドまたはアクション	目的
ステップ 6	<pre>end</pre> <p>例:</p> <pre>host1/Admin(config-sbc-dbe-vdbe-global)# end</pre>	予期せぬ送信元アラート モードを終了して、DBE モードに戻ります。
ステップ 7	<pre>show services sbc service-name dbe media-flow-stats vrf vrf-name [ipv4 A.B.C.D [port port-number]]</pre> <p>例:</p> <pre>host1/Admin(config-sbc-dbe)# show services sbc mysbc dbe media-flow-stats vrf vpn3 ipv4 10.1.1.1 port 24000</pre>	DBE に設定されたメディア フロー統計情報の詳細を表示します。

予期せぬ送信元アドレスに対するアラートの設定例

ここでは、メディア フロー統計情報に追加される情報の例を含む、予期せぬ送信元アドレスに対するアラートの設定例およびその出力例を示します。

予期せぬ送信元アドレスに対するアラートを設定するには、次のコマンドを使用します。

```
configure
  sbc mysbc
  dbe
  vdbe
  global
  unexpected-source-alerting
end
```