CHAPTER 31

DoS 防止およびダイナミック ブラックリスティング

Session Border Controller（SBC; セッション ボーダ コントローラ）は、悪意のあるエンドポイントによるネットワーク攻撃をブロックするために、Denial of Service（DoS; サービス拒絶）防止およびダイナミック ブラックリスティングを使用します。

SBC は、提供している他のサービスを中断しないで、シグナリング トラフィックを監視し潜在的な攻撃をダイナミックに検出する必要があります。攻撃を検出したら内部的または外部的にブロックできます。

一般に DoS 攻撃はインターネット サービスに対して実行され、それによりサービス利用者へのサービス提供ができなくなります。サービス プロバイダーが攻撃対象になることが多く、完全に悪意のある破壊行為であったり恐喝未遂のようなものであったりします。

ブラックリスティングは、発信パケットを送信元 IP アドレスなどのパラメータに基づいて照合し、パラメータと一致するパケットの処理を防ぐプロセスです。

ダイナミック ブラックリストは、SBC を通過するトラフィック フローを中断しようとする行為が検出されたときに SBC により自動的（複数の設定上の制約があります）に実行されます。ダイナミック ブラックリスティングには、管理による干渉は不要です。攻撃の開始から数ミリ秒以内に実行され、攻撃の変化に対応して変化できるため、ネットワークが即座に保護されます。

（注） ACE SBC Release 3.0.00 では、この機能は統合モデルに限りサポートされます。

コーデック制限機能の履歴

リリース	変更内容
ACE SBC Release 3.0.00	この機能は、SBC 統合モデルのサポートとともに 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。

- 「DoS 防止およびダイナミック ブラックリスティングの前提条件」（P.31-2）
- 「DoS 防止およびダイナミック ブラックリスティングの制約事項」（P.31-2）
- 「DoS 防止およびダイナミック ブラックリスティングに関する情報」（P.31-4）
- 「ダイナミック ブラックリスティングの設定方法」（P.31-5）
- 「ダイナミック ブラックリスティングの設定、削除、および表示の例」（P.31-8）

DoS 防止およびダイナミック ブラックリスティングの前提条件

次に、ダイナミック ブラックリスティング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
- SBC を作成しておく必要があります。「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。

DoS 防止およびダイナミック ブラックリスティングの制約事項

ダイナミック ブラックリスティングについて、次の制約事項を確認してください。

- ACE SBC Release 3.0.00 では、Session Initiation Protocol（SIP）トラフィックだけが分析されます。H.323 を通じた攻撃は保護されません。ただし、SIP を通じた攻撃により、結果的に H.323 トラフィックがブロックされることもあります。
- パケットは送信されたポートに従ってシグナリングまたはメディアのいずれかに分類されます。
  - 10,000 番未満のポートはシグナリングです。
  - 10,000 番を超えるポートはメディアです。
- 送信元および宛先のすべてを含んだ総合負荷が CPU の能力を超えないように、グローバルなレート制限が適用されます（デフォルトの制限は 8000 pps/1000 Mbps）。
- 各 IP アドレスにイベント タイプごとにハードコードされた初期設定は、100 ミリ秒の間に 4 つのイベントを保持する設定になっています。この設定値を超えた場合、その IP アドレスは 10 分間ブラックリストに掲載されます。
- 1 つの IP アドレスまたはポートに対して明示的に制限を設定した場合、そのコンフィギュレーションに定義されたトリガーおよびブロック時間の値によってデフォルトは上書きされます。表 31-1 に、任意のメッセージに設定可能な、それぞれのスコープのイベント制限のパラメータを示します。制限値はメッセージの送信元がグローバル アドレス レンジにある場合と VPN にある場合で異なります。
- ブラックリストをイネーブルにするということは、「監視対象のイベント（E：authentication-failure など）が所定の期間（W：trigger-period <>）内に設定回数（N：trigger-size <>）を超えて発生した場合に、タイムアウト期間（T：timeout <>）のダイナミック アクセス コントロール リストをアクティブ化すること」として定義されます。
- DoS 検出ポリシーによる検出の原因として、次のイベントを監視できます。
  - **authentication-failure**：SBC で UA またはピアをローカルで認証している場合、認証失敗が 1 つのイベントと見なされます。
  - **bad-address**：このイベントは、SBC に予期せぬ送信元からのパケットが到達した場合に生成されます。このようなパケットはドロップされます。
  - **routing-failure**：このイベントは、トラフィックがルーティング ポリシーに適合しなかった場合に生成されます。

  - **endpoint-registration**：このイベントは、SBC を通じたエンドポイントの登録が拒否された場合に生成されます。
  - **corrupt-message**：このイベントは、アプリケーションでシグナリング メッセージをデコードできない場合、またはシグナリング メッセージにプロトコル例外/違反が含まれる場合に生成されます。
  - **policy-rejection**：原則として CAC ポリシー障害（つまり、CAC ポリシーからの否定の結果）を監視する複雑なカテゴリです。そのため、このカテゴリにはレート、カウント、および帯域幅制限が含まれますが、それらの区別は行われません。
- 任意のエンドポイントに対して、所定の時間にポート単位、アドレス単位、および VPN 単位で監視するブラックリスト イベントを最大で 3 つ設定できます。アドレスの送信元タイプ内では、次の優先順位があります。
  - 特定の IPv4 アドレスごとに設定された制限
  - 親 VRF アドレス レンジのデフォルト制限
  - グローバル アドレス レンジのデフォルト制限（親 VRF と異なる場合）
  - ハードコードされたアドレス制限
- グローバル アドレス レンジのブラックリストだけが定義されている場合（VRF 固有のブラックリストが定義されていない場合）、その定義に基づいて、設定されているすべての VRF 内のアドレスがブラックリストに掲載されます。
- VRF ベースのブラックリスト制限は、送信元単位またはアドレス単位の設定済みのデフォルト制限よりも優先されます。IP アドレス単位スコープを使用して、VRF レンジの動作を上書きすることはできません。
- ブラックリストによって作成されたダイナミック ACL がアクティブの場合、そのスコープに一致するすべてのセッション（アクティブ セッションを含む）が影響を受けます。
- 「T」の期限に達するか、ブラックリスト コンフィギュレーションがクリアされるまで、ダイナミック ACL はアクティブのままです。
- ポート固有のブラックリスト コンフィギュレーションは不可能です。
- ブラックリストがアクティブ化されると、SBC によって SNMP トラップが生成されます。

表 31-1　イベント制限パラメータのプライオリティ

イベント制限のスコープ	イベント制限パラメータ送信元（プライオリティの高い順）	
	グローバル アドレス レンジ	VPN
ポート	1. このポートに対する明示的な制限 2. この IP アドレスに対するデフォルト	1. このポートに対する明示的な制限 2. この IP アドレスに対するデフォルト

表 31-1　イベント制限パラメータのプライオリティ （続き）

イベント制限のスコープ	イベント制限パラメータ送信元（プライオリティの高い順）	
	グローバル アドレス レンジ	VPN
アドレス	1. このアドレスに対する明示的な制限 2. グローバル IP アドレスに対するデフォルト 3. ハードコードされている初期設定	1. このアドレスに対する明示的な制限 2. この VPN のアドレスに対するデフォルト 3. グローバル IP アドレスに対するデフォルト 4. ハードコードされている初期設定
VPN	グローバル アドレス レンジに対する明示的な制限	1. この VPN に対する明示的な制限 2. グローバル アドレス レンジに対する制限セット

DoS 防止およびダイナミック ブラックリスティングに関する情報

ブラックリスティングの原因となる動作を示唆するイベントには、ローレベル攻撃とハイレベル攻撃の 2 種類があります。

- ローレベル攻撃

  パケットごとに相当量の処理を実行するデバイスにラインレートで送信される大量のトラフィックです。

- ハイレベル攻撃

  シグナリング プレーンまたはアプリケーション レイヤ内のボトルネックに対する攻撃です。

SBC Packet Filter（SPF）は、ローレベル攻撃を防ぐために設計された新しいコンポーネントです。SPF は、Media Packet Forwarder（MPF）コンポーネントとともに Network Processing Unit（NPU）上に存在し、スタンドアロン Data Border Element（DBE; データ ボーダ エレメント）および統合 SBC の配置シナリオにローレベルの DoS 防止を提供します。

ハイレベル攻撃を検出し、その攻撃に基づいてダイナミック ブラックリストを作成するためには、新しいコンポーネントが Signaling Border Element（SBE; シグナリング ボーダ エレメント）に追加されます。ダイナミック ブラックリストは、Command Line Interface（CLI; コマンドライン インターフェイス）を使用して設定します。他の SBE コンポーネントからイベントを受信し、アラートを生成して特定のメッセージのブラックリスティングの開始または停止を行います。ハイレベル攻撃に該当する可能性のあるイベントは他の SBE コンポーネントによって検出され、SBE ダイナミック ブラックリスティング コンポーネントに送信されて、発生頻度に関する統計情報が収集されます。

ダイナミック ブラックリスティングの制限事項

- メディア パケットはフロー テーブル内の有効なエントリと一致する必要があります。一致しない場合はドロップされます。
- 有効なメディア パケットはコール シグナリングで確立された帯域幅制限を超えてはなりません。準拠しないパケットはドロップされます。
- シグナリング パケットは、大きなパケット フラッディングを早期に停止させる過程で送信元ポートによりレート制限されます（デフォルトの制限は 1000 pps/100 Mbps）。

- 有効なローカル ポートを宛先としないシグナリング パケットはドロップされます。
- シグナリング パケットは宛先ポートによりレート制限されます（デフォルトの制限は 4000 pps/500 Mbps）。
- VPN ID、IP アドレス、または特定 IP アドレスのポートを送信元とする特定のイベントを対象に、制限を設定できます。
- VPN 上のすべての送信元 IP アドレスおよび特定の IP アドレスのすべてのポートを対象に、イベント レートのデフォルト制限を定義できます。各 IP アドレスのデフォルト制限は 1 日の開始時に自動的に設定されますが、これらのパラメータは再設定できます。デフォルトでは、ポートにイベント制限は設定されていません。

デフォルトでは、SBC は IP アドレスごとにイベントを監視します。VPN 全体または特定ポートを監視するように SBC を設定することもできます。設定のあとに VPN の何らかの制限を超過した場合は、VPN 全体がブラックリストに掲載されます。ポートの制限を超過した場合は、ポートおよびその IP アドレスがブラックリストに掲載されます。

SBC によりデフォルトのイベント制限が各制限送信元に適用されますが、これらは変更できます。

ダイナミック ブラックリスティングの設定方法

次の各項の説明に従って、ダイナミック ブラックリスティングを設定できます。

- 「IP アドレス、ポート、または VPN に対するブラックリスト パラメータの設定」（P.31-5）
- 「ブラックリスティングの終了の設定」（P.31-8）

IP アドレス、ポート、または VPN に対するブラックリスト パラメータの設定

特定の送信元に対してイベント制限を設定するには、次のコマンドを使用します。

手順概要

1. **configure**
2. **sbc** *service-name* **sbe blacklist** *source*
3. **description** *text*
4. **reason** *event*
5. **trigger-size** *number*
6. **trigger-period** *time*
7. **timeout** *timeframe*
8. **exit**
9. **exit**
10. **show services sbc** *service-name* **sbe blacklist configured-limits**
11. **show services sbc** *service-name* **sbe blacklist** *source*
12. **show services sbc** *service-name* **sbe blacklist current-blacklisting**

詳細手順

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `host1/Admin# configure`	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	**sbc** *service-name* **sbe blacklist** *source* **例：** `host1/Admin(config)# sbc mysbc sbe blacklist ipv4 25.25.25.5`	所定の送信元に対してイベント制限を設定するサブモードを開始します。 サービス名を定義するには、*service-name* 引数を使用します。 制限をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。 **（注）** イベント制限パラメータのうち、このサブモードで設定されないものは次のデフォルト値に設定されます。 port = アドレスに対応するポートのデフォルト値 IP address = VPN に対応するアドレスのデフォルト値 VPN = グローバル アドレス レンジに対応する値 global address space = 制限なし
ステップ 3	**description** *text* **例：** `host1/Admin(config-sbc-sbe-blacklist)# description NAT of XYZ Corp`	読み取り可能なテキスト ストリング形式を使用して、送信元およびそのイベント制限に関する説明を追加します。 説明を削除するには、このコマンドの **no** 形式を使用します。 この説明は、この送信元に対して **show** コマンドを使用すると表示されます。
ステップ 4	**reason** *event* **例：** `host1/Admin(config-sbc-sbe-blacklist)# reason authentication-failure`	送信元の特定のイベント タイプに制限を設定するサブモードを開始します。 イベント制限をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。 event には次のものがあります。 • authentication-failure（要求の認証失敗） • bad-address（予期せぬアドレスからのパケット） • routing-failure（SBC による要求ルーティングの失敗） • endpoint-registration（すべてのエンドポイント登録） • policy-rejection（設定されているポリシーによる要求の拒否） • corrupt-message（シグナリング パケットがひどく破損して該当するプロトコルで解析不能）
ステップ 5	**trigger-size** *number* **例：** `host1/Admin(config-sbc-sbe-blacklist-reason# trigger-size 5`	ブラックリストがトリガーされて指定の送信元からのすべてのパケットがブロックされるまでに、その送信元に対して許可するイベント数を定義します。 範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 6	**trigger-period** *time* **例：** `host1/Admin(config-sbc-sbe-blacklist-reason)# trigger-period 20 milliseconds`	イベントの判定期間を定義します。 *time* は *number unit* として表現します。*number* は整数で、*unit* は milliseconds、seconds、minutes、hours、または days のいずれかです。 デフォルトの期間は 10 ミリ秒～ 23 日の間です。
ステップ 7	**timeout** *time* **例：** `host1/Admin(config-sbc-sbe-blacklist-reason)# timeout 180 seconds`	設定されている制限を超過したときに送信元からのパケットをブロックする期間を定義します。 *time* には、次の値を指定できます。 • 0 = 送信元をブラックリストに掲載しない • never = 永続的にブラックリストに掲載する • *number unit*（*number* は整数で、*unit* は seconds、minutes、hours、または days です） デフォルトの期間は 23 日未満です。
ステップ 8	**exit** **例：** `host1/Admin(config-sbc-sbe-blacklist-reason)# exit`	原因モードを終了し、ブラックリスト モードに戻ります。
ステップ 9	**exit** **例：** `host1/Admin(config-sbc-sbe-blacklist)# exit`	ブラックリスト モードを終了し、SBE モードに戻ります。
ステップ 10	**show services sbc** *service-name* **sbe blacklist configured-limits** **例：** `host1/Admin(config-sbc-sbe)# show sbc mysbc sbe blacklist configured-limits`	明示的に設定されている制限の詳細情報を表示します。 各送信元に明示的に定義されていない値はすべてカッコ内に表示されます。
ステップ 11	**show services sbc** *service-name* **sbe blacklist** *source* **例：** `host1/Admin(config-sbc-sbe)# show services sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12`	特定の送信元に現在適用されている制限を表示します（この例では VPN）。デフォルトの制限および明示的に設定されている制限がすべて含まれます。 このアドレスで設定されているスコープより小さいスコープのデフォルト値がある場合は、それも表示されます。 明示的に設定されていない値はカッコ内に表示されます（これらは他のデフォルト値から継承された値です）。
ステップ 12	**show services sbc** *service-name* **sbe blacklist current-blacklisting** **例：** `host1/Admin(config-sbc-sbe)# show services sbc mysbc sbe blacklist current-blacklisting`	送信元をブラックリストに掲載する原因となっている制限をリストします。

ブラックリスティングの終了の設定

ブラックリストから送信元を削除するには、次のコマンドを使用します。

clear services sbc *service-name* **sbe blacklist** *source*

service-name パラメータには、SBC の名前を入力します。

source パラメータには、ブラックリストの名前を入力します。

ダイナミック ブラックリスティングの設定、削除、および表示の例

ここでは、ダイナミック ブラックリスティング、ブラックリストからの送信元の削除、および設定済みの制限の表示を行うための設定例およびその出力例を示します。

ダイナミック ブラックリスティングの設定例

次のブラックリストは、100 ミリ秒の間に取り込まれる可能性のあるすべてのアドレス送信元からの認証失敗が 1 回発生した場合を対象として、グローバル アドレス レンジに対して設定されています。作成される ACL（ブラックリスト）はタイムアウトしません。

```
host1/Admin(config-sbc-sbe)# blacklist
host1/Admin(config-sbc-sbe-blacklist)# address-default
host1/Admin(config-sbc-sbe-blacklist-addr-default)# reason authentication-failure
host1/Admin(config-sbc-sbe-blacklist-addr-default)# timeout never
host1/Admin(config-sbc-sbe-blacklist-addr-default)# trigger-size 1
host1/Admin(config-sbc-sbe-blacklist-addr-default)# trigger-period 100 milliseconds
```

次のブラックリストは、1 分間で予期せぬ送信元からの 5 つのパケットが到達した場合を対象として、グローバル アドレス レンジに対して設定されています。ACL は 24 時間でタイムアウトします。

```
host1/Admin(config-sbc-sbe-blacklist)# ipv4 10.5.1.21
host1/Admin(config-sbc-sbe-blacklist-ipv4)# reason bad-address
host1/Admin(config-sbc-sbe-blacklist-ipv4)# timeout 1 days
host1/Admin(config-sbc-sbe-blacklist-ipv4-reason)# trigger-size 5
host1/Admin(config-sbc-sbe-blacklist-ipv4-reason)# trigger-period 1 minutes
```

ブラックリストからの送信元の削除例

次に、SBC からブラックリストを削除するための構文の例を示します。

```
host1/Admin# clear services sbc mysbc sbe blacklist blacklist
host1/Admin#
```

設定済みのすべての制限の表示例

次に、各種ブラックリスティング用に設定されている制限を表示する例を示します。

```
ACE-105-UUT1-1/Admin# show services sbc uut105-1 sbe blacklist configured-limits
SBC Service ''uut105-1''
```

```
Global
========
Reason Trigger Trigger Blacklisting
Size Period Period
------------------------------------------------------------
Authentication 30 30 secs 30 secs
Bad Address (0) (0 days) (0 days)
Routing (0) (0 days) (0 days)
Registration (0) (0 days) (0 days)
Policy (0) (0 days) (0 days)
Corrupt (0) (0 days) (0 days)

vpn1
======
Reason Trigger Trigger Blacklisting
Size Period Period
------------------------------------------------------------
Authentication (30) (30 secs) (30 secs)
Bad Address (0) (0 days) (0 days)
Routing (0) (0 days) (0 days)
Registration 50 50 secs 50 secs
Policy (0) (0 days) (0 days)
Corrupt (0) (0 days) (0 days)

Default for all addresses
==========================
Reason Trigger Trigger Blacklisting
Size Period Period
------------------------------------------------------------
Authentication (4) (100 ms) (10 mins)
Bad Address (4) (100 ms) (10 mins)
Routing (4) (100 ms) (10 mins)
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
Corrupt 40 40 secs 40 secs

Admin 1.1.1.1
===============
Reason Trigger Trigger Blacklisting
Size Period Period
------------------------------------------------------------
Authentication (4) (100 ms) (10 mins)
Bad Address (4) (100 ms) (10 mins)
Routing 10 20 secs 20 secs
Registration (4) (100 ms) (10 mins)
Policy (4) (100 ms) (10 mins)
Corrupt (40) (40 secs) (40 secs)
ACE-105-UUT1-1/Admin#
```

ブラックリスティングに関する show コマンドの使用例

次に、特定の送信元（この例では VPN）に現在適用されている制限をリストするのに必要なコマンドの例を示します。デフォルトの制限および明示的に設定されている制限がすべて含まれます。このアドレスで設定されているスコープより小さいスコープのデフォルト値がある場合は、それも表示されます。明示的に設定されていない値はカッコ内に表示されます（これらは他のデフォルト値から継承された値です）。

```
host1/Admin# show sbc mysbc sbe blacklist vpn3 ipv4 172.19.12.12

SBC Service "mySbc" SBE dynamic blacklist vpn3 172.19.12.12
```

```
vpn3 172.19.12.12
=================
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication     (20)            10 ms          (1 hour)
Bad address        (20)            10 ms          (1 hour)
Routing            (20)            10 ms          (1 hour)
Registration        (5)           100 ms        (10 hours)
Policy             (20)            10 ms           (1 day)
Corrupt              40            10 ms          (1 hour)

Default for ports of vpn3 172.19.12.12
======================================
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication       20            1 sec            1 hour
Bad address          20            1 sec            1 hour
Routing              20            1 sec            1 hour
Registration          5           30 sec          10 hours
Policy               20            1 sec             1 day
Corrupt              20           100 ms            1 hour
```

次に、送信元をブラックリストに掲載する原因となっている制限をリストするのに必要なコマンドの例を示します。

```
host1/Admin# show sbc mysbc sbe blacklist current-blacklisting
SBC Service "mySbc" SBE dynamic blacklist current members

Global addresses
================
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
125.125.111.123  All      Authentication  15 mins
125.125.111.253  UDP 85   Registration    10 secs
144.12.12.4      TCP 80   Corruption      Never ends

VRF: vpn3
=========
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
132.15.1.2       TCP 285  Registration    112 secs
172.23.22.2      All      Policy          10 hours
```

次に、設定されている制限を表示する例を示します。

```
host1/Admin# show services sbc MySBC sbe blacklist configured-limits
SBC Service "MySBC"

Global
========
Reason            Trigger            Trigger      Blacklisting
                     Size             Period            Period
-----------------------------------------------------------------
Authentication        (0)           (0 days)          (0 days)
Bad Address           (0)           (0 days)          (0 days)
Routing               (0)           (0 days)          (0 days)
Registration          (0)           (0 days)          (0 days)
Policy                (0)           (0 days)          (0 days)
Corrupt               (0)           (0 days)          (0 days)
```

```
Default for all addresses
=========================
Reason            Trigger            Trigger      Blacklisting
                     Size             Period            Period
-----------------------------------------------------------------
Authentication          1             100 ms           Forever
Bad Address           (4)           (100 ms)         (10 mins)
Routing               (4)           (100 ms)         (10 mins)
Registration          (4)           (100 ms)         (10 mins)
Policy                (4)           (100 ms)         (10 mins)
Corrupt               (4)           (100 ms)         (10 mins)

Admin 10.5.1.21
===============
Reason            Trigger            Trigger      Blacklisting
                     Size             Period            Period
-----------------------------------------------------------------
Authentication        (1)           (100 ms)         (Forever)
Bad Address             5             1 mins            1 days
Routing               (4)           (100 ms)         (10 mins)
Registration          (4)           (100 ms)         (10 mins)
Policy                (4)           (100 ms)         (10 mins)
Corrupt               (4)           (100 ms)         (10 mins)
```

（注） デフォルト コンフィギュレーションがすでに適用されていることに注意してください。適用されているコンフィギュレーションだけが変更されます。

次に、現在のブラックリスティングを表示する例を示します。

```
host1/Admin# show services sbc MySBC sbe blacklist current-blacklisting
SBC Service "MySBC" SBE dynamic blacklist current members

Global addresses
================
Source           Source   Blacklist       Time
Address          Port     Reason          Remaining
-------          ------   ---------       ---------
10.5.1.31All      Authentication  Forever
```