DoS 防止およびダイナミック ブラックリスティング

サービス拒否（DoS）防止およびダイナミック ブラックリスティングは、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 SBC によって使用されます。

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。攻撃は、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、その目的は他者へのそのサービスの提供を妨害することです。サービスの提供者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、インバウンド 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インターフェイスが必要ありません。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のでネットワークを即座に保護します。

コーデック制限機能の履歴

リリース	変更内容
リリース 3.4.1	この機能は、Cisco XR 12000 シリーズ ルータで導入されました。
リリース 3.5.0	変更なし。

内容

このモジュールの構成は次のとおりです。

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

次に、ダイナミック ブラックリスティング機能の前提条件を示します。

- 使用される SBC コマンドの適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループとタスク ID の詳細については、『*Cisco IOS XR Session Border Controller Command Reference*』で、コマンドごとに必要な定義済みタスク ID を参照してください。
- SBC ソフトウェアのパッケージ インストレーション エンベロープ（PIE）をインストールしてアクティブにする必要があります。

  PIE のインストールに関する詳細については、『*Cisco IOS XR Getting Started Guide*』の「*Upgrading and Managing Cisco IOS XR Software*」モジュールを参照してください。
- SBC を作成しておく必要があります。「SBC 設定の前提条件」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に関する制約事項

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。

- SIP トラフィックのみがこのリリースで分析されます。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
- すべての送信元および宛先の負荷の合計が CPU の能力を超えないように、グローバル レート制限が適用されます（デフォルトの制限は 8000 pps/1000 mpbs）。
- 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。この設定値を超えると、IP アドレスは 10 分間ブラックリスティングされます。
- 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、その設定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 15 に、任意のメッセージに設定可能な、それぞれの範囲のイベント制限のパラメータを示します。設定値はメッセージの送信元がグローバル アドレス空間にある場合と VPN にある場合で異なります。

表 15　イベント制限パラメータのプライオリティ

イベント制限の範囲	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 アドレス空間	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
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. ハードコード化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. ハードコード化されている初期設定
VPN	グローバル アドレス空間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 アドレス空間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

  装置に回線速度で送信される大量のトラフィック。装置はパケットごとに相当量の処理を実行します。

- 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層内のボトルネックに対する攻撃。

SBC Packet Filter（SPF; SBC パケット フィルタ）は、低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 MPF コンポーネントとともに NPU 上に存在し、スタンドアロン DBE と統合型 SBC 展開シナリオに対して低レベルの DoS 防止機能を提供します。

新しいコンポーネントが SBE に追加され、これによって、ハイレベル攻撃が検出され、この攻撃に基づいたダイナミック ブラックリストが作成されます。ダイナミック ブラックリストは、CLI を使用して設定されます。このインターフェイスで他の SBE コンポーネントからイベントを受信して、特定のメッセージのブラックリスティングを開始または停止するためのアラートが生成されます。ハイレベル攻撃の一部を形成する可能性が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。一致しない場合は廃棄されます。

- 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廃棄されます。
- シグナリング パケットは、大規模なパケット 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（デフォルト値は 1000 pps/100 mpbs）。
- 有効なローカル ポートを宛先としないシグナリング パケットは廃棄されます。
- シグナリング パケットのレート制限は宛先ポートによって行われます（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。ポートの制限が超過した場合、ポートおよびその IP アドレスがブラックリスティングされます。

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

次のセクション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、VPN に対するブラックリスト パラメータの設定」（P.266）
- 「ブラックリスティングの終了の設定」（P.269）

IP アドレス、ポート、VPN に対するブラックリスト パラメータの設定

特定の送信元に対する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。

手順の概要

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. **commit**
11. **show services sbc** *service-name* **sbe blacklist configured-limits**

12. **show services sbc** *service-name* **sbe blacklist** *source*
13. **show services sbc** *service-name* **sbe blacklist current-blacklisting**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure** **例：** `RP/0/0/CPU0:router# 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：** `RP/0/0/CPU0:router(config)# sbc mysbc sbe blacklist ipv4 25.25.25.5`	特定の送信元のイベント制限を設定するためのサブモードを開始します。 *service-name* 引数を使用して、サービスの名前を定義します。 このコマンドの **no** 形式を使用すると、制限はデフォルト値に戻ります。 **（注）** このサブモードで設定されていないイベント制限パラメータは、デフォルトでは次のように設定されます。 ポート = そのアドレスのポート デフォルト値 IP アドレス = VPN のアドレス デフォルト値 VPN = グローバル アドレス空間に対する値 グローバル アドレス空間 = 制限なし
ステップ 3	**description** *text* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-blacklist)# description NAT of XYZ Corp`	判読可能なテキスト ストリング形式を使用し、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。 このコマンドの **no** 形式を使用すると、説明は削除されます。 この説明は、この送信元に対して **show** コマンドを使用したときに表示されます。
ステップ 4	**reason** *event* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-blacklist)# reason authentication-failure`	送信元の特定のイベント タイプに対する制限を設定するためのサブモードを開始します。 このコマンドの **no** 形式を使用すると、イベント制限はデフォルトの値に戻ります。 event には次のものが含まれます。 • authentication-failure（認証を受けられなかった要求） • bad-address（予期せぬアドレスからのパケット） • routing-failure（SBC によってルーティングされなかった要求） • endpoint-registration（すべてのエンドポイントの登録） • policy-rejection（設定済みポリシーによって拒否された要求） • corrupt-message（ひどく破損しているため該当するプロトコルで解析できないシグナリング パケット）

	コマンドまたはアクション	目的
ステップ 5	**trigger-size** *number* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason# trigger-size 5`	指定した送信元からのイベントの許容数を定義します。これを超えるとブラックリスティングがトリガーされ、送信元からのすべてのパケットがブロックされます。 範囲は 0 ～ 65535 です。
ステップ 6	**trigger-period** *time* **例：** `RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# trigger-period 20 milliseconds`	イベントを考慮する期間を定義します。 *time* は <*number*> <*unit*> として表現され、*number* は整数で、*unit* は milliseconds、seconds、minutes、hours、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：** `RP/0/0/CPU0:router(config-sbc-sbe-blacklist-reason)# timeout 180 seconds`	設定された制限を超えた場合に、送信元からのパケットがブロックされる時間を定義します。 *time* には次の値が使用できます。 • 0 = 送信元はブラックリスティングされません。 • never = ブラックリスティングは永続的に行われます。 • <*number*> <*unit*>。*number* は整数で、*unit* は seconds、minutes、hours、days のいずれかです。 デフォルトの期間は 23 日未満です。
ステップ 8	**exit** **例：** `RP/0/0/CPU0:router(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：** `RP/0/0/CPU0:router(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	**commit** **例：** `RP/0/0/CPU0:router(config-sbc-sbe)# commit`	設定変更を保存します。実行コンフィギュレーション ファイルに変更を保存し、コンフィギュレーション セッションを継続するには、**commit** コマンドを使用します。
ステップ 11	**show services sbc** *service-name* **sbe blacklist configured-limits** **例：** `RP/0/0/CPU0:router(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括弧で括られて表示されます。

	コマンドまたはアクション	目的
ステップ 12	**show services sbc** *service-name* **sbe blacklist** *source* **例：** `RP/0/0/CPU0:router(config-sbc-sbe)# show 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範囲より小さい範囲のデフォルト値があれば、それも表示されます。 明示的に設定されていない値は括弧で括られて表示されます（これらは他のデフォルトから継承されている値です）。
ステップ 13	**show services sbc** *service-name* **sbe blacklist current-blacklisting** **例：** `RP/0/0/CPU0:router(config-sbc-sbe)# show services sbc mysbc sbe blacklist current-blacklisting`	送信元がブラックリスティングされた原因となっている制限を一覧表示します。

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、ブラックリストにある送信元の削除、および設定済み制限の表示を行うための設定例と出力例について説明します。

ダイナミック ブラックリスティングの設定例

次の例では、IP アドレス 25.25.25.5 からの許容される認証失敗イベントのレートに対して新しいダイナミック ブラックリスト制限を設定するために必要なコマンドを示します。

```
configure
    sbc mysbc
    sbe
    blacklist ipv4 25.25.25.5
      description NAT of XYZ Corp
      reason authentication-failure
        trigger-size 5
        trigger-period 20 milliseconds
        timeout 180 seconds
        exit
      exit
    commit
```

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。

```
RP/0/0/CPU0:PE7_C12406#clear services sbc mysbc sbe blacklist blacklist
RP/0/0/CPU0:PE7_C12406#
```

設定済みのすべての制限の表示例

次の例では、明示的に設定されている制限を一覧表示するために必要なコマンドを示します。各送信元に対して明示的に定義されていない値は、カッコで囲まれます。

```
configure
    show sbc mysbc sbe blacklist configured-limits

SBC Service "mySbc" SBE dynamic blacklist configured limits

Default for all addresses
=========================
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

Default for addresses on vpn3
=============================
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication       20            1 sec             1 day
Bad address          20            1 sec             1 day
Routing              20            1 sec             1 day
Registration          5           30 sec             1 day
Policy               20            1 sec             1 day
Corrupt              50           100 ms          12 hours

112.234.23.2
============
Reason          Trigger          Trigger      Blacklisting
                   Size           Period            Period
------          -------          -------      ------------
Authentication     2000          (1 sec)          (1 hour)
Bad address        2000          (1 sec)          (1 hour)
Routing            2000          (1 sec)          (1 hour)
Registration        500         (30 sec)        (10 hours)
Policy             2000          (1 sec)           (1 day)
Corrupt            2000         (100 ms)          (1 hour)

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              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
```

ソースの設定済み制限を表示する例

次に、特定の送信元に現在適用されている制限を一覧表示するために必要なコマンドの例を示します（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範囲より小さい範囲のデフォルト値があれば、それも表示されます。明示的に設定されていない値は括弧で括られて表示されます（これらは他のデフォルトから継承されている値です）。

```
configure
   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
```

ブラックリスティングの原因となる制限を表示する例

次に、送信元がブラックリスティングされた原因となっている制限を一覧表示するために必要なコマンドの例を示します。

```
configure
    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
```

その他の関連資料

次の各項では、DoS 防止およびダイナミック ブラックリスティングに関連する資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS XR マスター コマンド リファレンス	*『Cisco IOS XR Master Commands List』*
Cisco IOS XR SBC インターフェイス コンフィギュレーション コマンド	*『Cisco IOS XR Session Border Controller Command Reference』*
Cisco IOS XR ソフトウェアを使用するルータを初回に起動し設定するための情報	*『Cisco IOS XR Getting Started Guide』*
Cisco IOS XR コマンド モード	*『Cisco IOS XR Command Mode Reference』*

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB の場所を特定してダウンロードするには、次の URL にある Cisco MIB Locator を使用して、[Cisco Access Products] メニューからプラットフォームを選択します。 http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html