CHAPTER 33

DoS 防止およびダイナミック ブラックリスティング

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 Cisco Unified Border Element（SP Edition）が使用します。

Cisco Unified Border Element（SP Edition）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します。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、攻撃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、Cisco Unified Border Element（SP Edition）を通過するトラフィックの流れを中断しようとする行為が検出されたときに自動的に実行されます（複数の設定上の制約があります）。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。

Cisco Unified Border Element（SP Edition）は、以前は Integrated Session Border Controller と呼ばれており、このマニュアルでは通常 Session Border Controller（SBC; セッション ボーダー コントローラ）と呼びます。

本章で使用されているコマンドの詳細な説明については、『Cisco Unified Border Element (SP Edition) Command Reference: Unified Model』（http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html）を参照してください。

Cisco IOS のすべてのコマンドについては、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool か、Cisco IOS マスター コマンド リストを使用してください。

（注） Cisco IOS XE Release 2.4 では、この機能は統合モデルだけでサポートされます。

DoS 防止およびダイナミック ブラックリスティングの機能履歴

リリース	変更点
Cisco IOS XE Release 2.4	この機能は、統合モデルのサポートとともに、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに追加されました。

構成内容

ここで説明する内容は、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.33-2）
- 「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制約事項」（P.33-2）
- 「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.33-3）
- 「ダイナミック ブラックリスティングのデフォルトのしきい値の上書き」（P.33-4）
- 「ダイナミック ブラックリスティングの動作」（P.33-5）
- 「ダイナミック ブラックリスティングの設定方法」（P.33-7）
- 「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.33-10）

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。

- 事前に Cisco Unified Border Element（SP Edition）を設定している必要があります。第 2 章「Cisco Unified Border Element の設定（SP Edition）」の手順を参照してください。
- SBE を設定するとき、Cisco Unified Border Element（SP Edition）の使用を開始する前に、デフォルトのブラックリスティングしきい値を上書きするように、ブラックリスティングを設定する必要があります。

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の制約事項は次のとおりです。

- Session Initiation Protocol（SIP; セッション開始プロトコル）トラフィックだけが分析対象です。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。
- ポート固有のブラックリスト設定はできません。

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

Cisco Unified Border Element（SP Edition）は、DoS 検出ポリシーを開始する「理由」となる、次のイベントを監視します。

- **authentication-failure**：Cisco Unified Border Element（SP Edition）は、ローカルで UA またはピアを認証し、その後、あらゆる認証の失敗を 1 イベントとカウントします。
- **bad-address**：このイベントは、予期しない送信元から送られたパケットが Cisco Unified Border Element（SP Edition）に到達したときに生成されます。このパケットは廃棄されます。
- **routing-failure**：このイベントは、トラフィックがルーティング ポリシーと一致しなかったときに生成されます。
- **endpoint-registration**：このイベントは、エンドポイントが Cisco Unified Border Element（SP Edition）を通じて登録しようとしたが拒否されたときに生成されます。
- **corrupt-message**：このイベントは、シグナリング メッセージをアプリケーションで解析できないとき、または、プロトコルの例外や違反が含まれているときに生成されます。
- **policy-rejection**：本来は CAC ポリシー違反（CAC ポリシーとの照合結果がネガティブ）を監視する複雑なカテゴリです。したがって、このカテゴリには、レート、カウント、帯域幅の制限が含まれ、それぞれの間に区別はありません。
- **spam**：エンドポイントは不要なコールやスパム コールを送信する場合があります（これを SPam over Internet Telephony（SPIT）と呼ぶこともあります）。スパムは予期しない大量のシグナリング メッセージの結果発生します。以前に送信された要求と一致しない SIP 応答を受信したり、大量に再送信された SIP メッセージを受信したりする例もスパムに含まれます。

ブラックリスティングの原因となるイベントには、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 レイヤ内のボトルネックに対する攻撃。

ブラックリストの有効化は、監視対象のイベント（'E'vent）（authentication-failure など）が、設定された回数（'N'umber）を超過して（trigger-size <>）ウィンドウ（'W'indow）内に発生し（trigger-period <>）、その後、一定の期間（'T'ime period）（timeout <>）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した場合に定義されます。

任意の指定されたエンドポイントでは、最大 3 種類のブラックリスト イベントをポート単位、アドレス単位、および VPN 単位で指定された時刻に監視できます。アドレス送信元タイプの内部には、次の優先順位があります。

- 指定された IPv4 アドレス単位で制限を設定
- ペアレント VRF アドレス スペースのデフォルト制限
- グローバル アドレスのアドレス スペースのデフォルト制限（ペアレント VRF と異なる場合）
- ハードコード化されたアドレス制限

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 Media Packet Forwarder（MPF; メディア パケット フォワーダ）コンポーネントとともに Network Processing Unit（NPU）に常駐し、スタンドアロンの Data Border Element（DBE）および統合 SBC の導入シナリオに低レベルの DoS 防止機能を提供します。

Signaling Border Element（SBE）に新規コンポーネントが追加され、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、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。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デフォルトのしきい値の上書き

ダイナミック ブラックリスティングはデフォルトでオンに設定されています。デフォルトのしきい値は、トリガー サイズ、トリガー期間、ブラックリスティング期間に対して理由ごとに設定されます。理由となる可能性があるのは、認証の失敗、不正なアドレス、ルーティングの失敗、エンドポイントの登録、ポリシー拒否、メッセージの破損、またはスパムです。

シスコでは、SBE が設定された時点のコールのセットアップと登録メッセージのデフォルトのしきい値を上書きするブラックリスティングを設定してから Cisco Unified Border Element（SP Edition）を起動することをお勧めします。こうすることで、予定したコールのセットアップ速度または登録メッセージの速度によってスパム ブラックリスティングがトリガーされてトラフィックの流れに悪影響が生じることがなくなります。トラフィックが適切に流れるようにするために、コールのセットアップ メッセージまたは登録メッセージのしきい値を各 SIP ベースのコール メッセージまたは登録メッセージの毎秒の速度より高く設定することが重要です。トリガー サイズ、トリガー期間、ブラックリスティング期間のデフォルト値は、毎秒 40 イベントまたは 100 ミリ秒ごとに 4 イベントです。これは、1 秒あたり 40 パケットを超えるトラフィックがあると、ブラックリスティングがトリガーされることを意味します。

次の SIP ベースのコール フローの例では、1 秒あたりのコール セットアップ メッセージに対する適切なトリガー サイズのしきい値を計算する方法を示します。

```
SIP-based call (caller) has:
Send INVITE
Receive 100 Trying
Receive 180 Ringing
Receive 200 OK to confirm Session Establishment
Send ACK to complete Session Establishment
Send BYE
Receive 200 OK
==================================
SIP-based call (callee) has:
Send INVITE
Send 100 Trying
Send 180 Ringing
Send 200 OK to confirm Session Establishment
Receive ACK to complete Session Establishment
Receive BYE
Send 200 OK
==========================================
```

SIP ベースのコールごとに 14 のメッセージまたはパケットがあります。Call Per Second（CPS; 1 秒あたりのコール）が最大 20 のコール セットアップ レートがある場合、14 メッセージ×20 CPS = 1 秒あたり 280 メッセージとなります。したがって、最大 20 の CPS のコール セットアップ レートでは、トリガー サイズのしきい値は 1 秒あたり少なくとも 280 メッセージに設定します。

次の設定例では、トリガー サイズを増やして 1 秒あたり 280 個のメッセージまたはパケットとするように設定しています。

```
blacklist global
 reason spam
  trigger-size 280
  trigger-period 1 seconds
```

1 秒あたりのコール セットアップ メッセージ数の計算と同様、次の例では、メッセージ登録に適切なトリガー サイズのしきい値を計算する方法を示します。

SIP ベースのコールごとに、毎秒 1 メッセージが 1 回登録されます。毎秒 20 回の登録がある場合、1 メッセージ×20 登録 = 1 秒あたり 20 メッセージとなります。したがって、毎秒最大 20 回登録する登録レートでは、トリガー サイズのしきい値は 1 秒あたり少なくとも 20 メッセージに設定されます。

ダイナミック ブラックリスティングはデフォルトではオンですが、何らかの理由でタイムアウトをゼロに設定するとこの機能をオフにできます。ただし、ミリ秒または秒など任意の単位値のタイムアウトをゼロに設定すると、**show run** コマンドで返される単位値は「day」と表示されることに注意が必要です。デフォルトのトリガー サイズ、トリガー期間、タイムアウト、設定されている制限を表示するには、**show sbc sbe blacklist configured-limits** コマンドが使用できます。このコマンドの使用例については、「ブラックリスティングでの show コマンドの使用例」（P.33-12）を参照してください。

ダイナミック ブラックリスティングの動作

次に、ダイナミック ブラックリスティングの動作について説明します。

- 送信元および宛先のすべてを含む総合の負荷が 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 アドレスに対してイベント タイプごとにハードコード化された初期設定は、デフォルトで 100 ミリ秒間に 4 つのイベントを保持する設定となっています。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 33-1 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 スペースにある場合と VPN にある場合で異なります。
- 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。

表 33-1　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 スペース	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 スペース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 スペースに対する制限セット

- 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は宛先ポートによりレート制限されます（デフォルト値は 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、Cisco Unified Border Element（SP Edition）は IP アドレスごとにイベントを監視します。VPN 全体または特定のポートを監視するように Cisco Unified Border Element（SP Edition）を設定することもできます。その後、VPN の何らかの制限が超過した場合は、VPN 全体がブラックリスティングされます。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。
- 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。
- グローバル アドレス スペース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は未定義）、設定済みのすべての VRF でアドレスのブラックリスティングにこの定義が使用されます。
- VRF ベースのブラックリスト制限により、送信元ごとの制限またはすでに設定されているアドレスのデフォルト制限は上書きされます。IP アドレスごとにスコープを使用しても VRF スペースの動作は上書きできません。
- Cisco Unified Border Element（SP Edition）は、ブラックリスティングがアクティブにされると、SNMP トラップを生成します。

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.33-7）
- 「ブラックリスティングの終了の設定」（P.33-10）

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。

（注）　SBE を設定するとき、Cisco Unified Border Element（SP Edition）の使用を開始する前に、デフォルトのブラックリスティングしきい値を上書きするように、ブラックリスティングを設定する必要があります。

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. **end**
9. **show sbc** *service-name* **sbe blacklist configured-limits**
10. **show sbc** *service-name* **sbe blacklist** *source*
11. **show 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：** `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：** `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、制限はデフォルトの値に戻ります。 **（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の値に設定されます。 ポート：アドレスに対応するポートのデフォルト値 IP アドレス：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 スペースに対応する値 グローバル アドレス スペース：制限なし
ステップ 3	**description** *text* **例：** `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：** `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：** `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：** `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* には milliseconds、seconds、minutes、hours、または days のいずれかを指定します。 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：** `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* には seconds、minutes、hours、または days のいずれかを指定します。 デフォルトの期間は 23 日未満です。
ステップ 8	**end** **例：** `Router(config-sbc-sbe-blacklist-reason)# end`	reason モードを終了し、特権 EXEC モードを開始します。
ステップ 9	**show sbc** *service-name* **sbe blacklist configured-limits** **例：** `Router# show sbc mysbc sbe blacklist global 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。
ステップ 10	**show sbc** *service-name* **sbe blacklist** *source* **例：** `Router# 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 11	**show sbc** *service-name* **sbe blacklist current-blacklisting** **例：** `Router# show 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 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、すべての可能なアドレス送信元からの認証が 100 ミリ秒間のウィンドウ内で 1 回失敗するとブラックリストに取り込まれるようにグローバル アドレス スペースを設定します。作成される ACL（ブラックリスト）はタイムアウトしないものとします。

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

次の例では、1 分間のウィンドウ内で予期しない送信元からのパケットが 5 個になるとブラックリスティングするようにグローバル アドレス スペースを設定します。ACL は 24 時間でタイムアウトします。

```
Router(config-sbc-sbe)# blacklist global
Router(config-sbc-sbe-blacklist)# ipv4 10.5.1.21
Router(config-sbc-sbe-blacklist-ipv4)# reason bad-address
Router(config-sbc-sbe-blacklist-ipv4)# timeout 1 days
Router(config-sbc-sbe-blacklist-ipv4-reason)# trigger-size 5
Router(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、Cisco Unified Border Element（SP Edition）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。

```
Router# clear sbc mysbc sbe blacklist blacklist
Router#
```

設定済みのすべての制限の表示例

次に、さまざまなタイプのブラックリスティングに設定されている制限を表示する例を示します。

```
Router# show 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)
Router#
```

ブラックリスティングでの show コマンドの使用例

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）。

```
Router# 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。

```
Router# 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、設定済みの制限を表示する例を示します。

```
Router# show 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） すでに実施されているデフォルトの設定に注意してください。適用済みの設定だけが変更されます。

次に、現在行われているブラックリスティングの例を示します。

```
Router# 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
-------          ------   ---------       ---------
10.5.1.31All      Authentication  Forever
```