脅威の検出

次のトピックでは、脅威検出の統計情報およびスキャン脅威検出を設定する方法について説明します。

脅威の検出

ASA の脅威検出は、攻撃に対して最前線で防御する機能です。脅威検出は、パケット ドロップの統計を分析し、トラフィック パターンに基づいた「トップ」レポートを蓄積することで、レイヤ 3 と 4 にトラフィックのベースラインを作成します。一方、IPS または次世代 IPS サービスを提供するモジュールは、ASA が許可したトラフィックの攻撃ベクトルをレイヤ 7 まで識別して軽減させますが、すでに ASA がドロップしたトラフィックは認識できません。そのため、脅威検出と IPS を一緒に使用することで、より総合的な脅威に対する防御を可能にします。

脅威検出は次の要素から構成されています。

- さまざまな脅威を収集する複数レベルの統計情報

  脅威検出統計情報は、ASA に対する脅威の管理に役立ちます。たとえば、スキャン脅威検出をイネーブルにすると、統計情報を見ることで脅威を分析できます。次の 2 種類の脅威検出統計情報を設定できます。

  - 基本脅威検出統計情報：システムに対する攻撃アクティビティについての全体的な情報を含みます。基本脅威検出統計情報はデフォルトでイネーブルになっており、パフォーマンスに対する影響はありません。「基本脅威検出統計情報 （2 ページ）」を参照してください。

- 拡張脅威検出統計情報：オブジェクトレベルでアクティビティを追跡するので、ASA は個別のホスト、ポート、プロトコル、または ACL についてのアクティビティを報告できます。拡張脅威検出統計情報は、収集される統計情報によってはパフォーマンスに大きく影響するので、デフォルトでは ACL の統計情報だけがイネーブルになっています。「拡張脅威検出統計情報 （3 ページ）」を参照してください。

- ホストがスキャンを実行する時期を決定するスキャン脅威検出機能オプションとして、スキャン脅威であることが特定されたホストを排除できます。「スキャン脅威検出 （3 ページ）」を参照してください。
- IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護するために使用できる VPN サービスの脅威検出。
  - リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。
  - クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。
  - 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。

  アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。VPN サービスの脅威検出の設定 （9 ページ） を参照してください。

基本脅威検出統計情報

ASA は、基本脅威検出統計情報を使用して、次の理由でドロップしたパケットおよびセキュリティ イベントの割合をモニターします。

- ACL による拒否。
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）。
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）。
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）。
- 基本ファイアウォール検査に不合格。このオプションは、このリストのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
- 疑わしい ICMP パケットの検出。
- アプリケーション インスペクションに不合格のパケット。
- インターフェイスの過負荷。

- スキャン攻撃の検出。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニターします。フル スキャン脅威検出では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に排除することによって対処します。
- 不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）。

ASA は、脅威を検出するとただちにシステム ログ メッセージ（733100）を送信します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバーストイベント レートの 2 種類のレートを追跡します。バースト レート間隔は、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。ASA は、受信するイベントごとに平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、ASA は、バースト期間におけるレート タイプごとに最大 1 つのメッセージの割合で 2 つの別々のシステム メッセージを送信します。

基本脅威検出は、ドロップまたは潜在的な脅威が存在した場合にだけパフォーマンスに影響します。このようなシナリオでも、パフォーマンスへの影響はわずかです。

拡張脅威検出統計情報

拡張脅威検出統計情報は、ホスト、ポート、プロトコル、ACL などの個別のオブジェクトについて、許可されたトラフィック レートとドロップされたトラフィック レートの両方を表示します。

注意 拡張統計情報をイネーブルにすると、イネーブルにする統計情報のタイプに応じて、ASA のパフォーマンスが影響を受けます。ホストの統計情報をイネーブルにすると、パフォーマンスに大きく影響します。トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討してください。ただし、ポート統計情報の影響はそれほど大きくありません。

スキャン脅威検出

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック シグニチャに基づく IPS スキャン検出とは異なり、ASA の脅威検出スキャンでは、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

スキャン脅威レートを超過すると、ASA は syslog メッセージ（733101）を送信し、必要に応じて攻撃者を排除します。ASA は、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 1/30 または 10 秒のうち、どちらか大きいほうです。スキャン攻撃の一部と見なされるイベントが検出されるたびに、ASA は平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。

次の表に、スキャン脅威検出のデフォルトのレート制限を示します。

表 *1:* スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
直前の 3600 秒間で 5 ドロップ/秒。	直近の 120 秒間で 10 ドロップ/秒。

注意 スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、ASA のパフォーマンスとメモリに大きく影響することがあります。

脅威検出のガイドライン

セキュリティ コンテキストのガイドライン

高度な脅威統計および VPN サービスを除き、脅威検出はシングルモードのみでサポートされます。マルチモードでは、TCP 代行受信の統計情報が唯一サポートされている統計情報です。

モニター対象トラフィックのタイプ

- 統計では、through-the-box トラフィックのみがモニターされます。to-the-box トラフィックはモニターされません。
- ACL によって拒否されたトラフィックは、スキャン脅威検出をトリガーしません。ASA から許可され、フローを作成したトラフィックだけがスキャン脅威検出の影響を受けます。
- VPN サービスの場合、IPv4 アドレスからの to-the-box トラフィックのみがモニターされます。

脅威検出のデフォルト

基本脅威検出統計情報は、デフォルトでイネーブルになっています。

次の表に、デフォルト設定を示します。これらのデフォルト設定すべてを表示するには、**show running-config all threat-detection** コマンドを [Tools] > [Command Line Interface] で使用します。

高度な統計情報では、ACL の統計情報はデフォルトでイネーブルになっています。

VPN サービス脅威検出では、すべてのサービスがデフォルトで無効になっています。

表 *2:* 基本的な脅威の検出のデフォルト設定

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 400 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 320 ドロップ/秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ/秒。	直近の 20 秒間で 10 ドロップ/秒。
	直前の 3600 秒間で 4 ドロップ/秒。	直近の 120 秒間で 8 ドロップ/秒。
不完全セッションの検出（TCP SYN 攻撃の検出や戻りデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ/秒。	直近の 20 秒間で 200 ドロップ/秒。
	直前の 3600 秒間で 80 ドロップ/秒。	直近の 120 秒間で 160 ドロップ/秒。
ACL による拒否	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 800 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 640 ドロップ/秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ/秒。	直近の 20 秒間で 1600 ドロップ/秒。
	直前の 3600 秒間で 320 ドロップ/秒。	直近の 120 秒間で 1280 ドロップ/秒。

パケット ドロップの理由	トリガー設定	
	平均レート	バースト レート
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ/秒。	直近の 20 秒間で 8000 ドロップ/秒。
	直前の 3600 秒間で 1600 ドロップ/秒。	直近の 120 秒間で 6400 ドロップ/秒。

脅威検出の設定

基本脅威検出統計情報はデフォルトでイネーブルになっており、ユーザーが必要とする唯一の脅威検出サービスである場合があります。さらに脅威検出サービスを実行する場合は、次の手順を使用します。

手順

ステップ 1 基本脅威検出統計情報の設定 （6 ページ）。

基本脅威検出統計情報には、DoS 攻撃（サービス拒絶攻撃）などの攻撃に関連している可能性があるアクティビティが含まれます。

ステップ 2 拡張脅威検出統計情報の設定 （7 ページ）。

ステップ 3 スキャン脅威検出の設定 （8 ページ）。

ステップ 4 VPN サービスの脅威検出の設定 （9 ページ）。

基本脅威検出統計情報の設定

基本脅威検出統計情報は、デフォルトでイネーブルになっています。ディセーブルにすることも、一度ディセーブルにしたあと再度イネーブルにすることもできます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Threat Detection]** を選択します。

ステップ 2 必要に応じて、[Enable Basic Threat Detection] を選択または選択解除します。

ステップ 3 [Apply] をクリックします。

拡張脅威検出統計情報の設定

広範な統計情報を収集するように ASA を設定することができます。デフォルトでは、ACL の統計情報はイネーブルになっています。他の統計情報をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Threat Detection]** を選択します。

ステップ 2 [Scanning Threat Statistics] 領域で、次のオプションのいずれかを選択します。

- [Enable All Statistics]
- [Disable All Statistics]
- [Enable Only Following Statistics]

ステップ 3 [Enable Only Following Statistics] を選択した場合は、次のオプションから 1 つ以上を選択します。

- [Hosts]：ホスト統計情報をイネーブルにします。ホストがアクティブで、スキャン脅威ホストデータベース内に存在する限り、ホスト統計情報は累積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
- [Access Rules]（デフォルトでイネーブル）：アクセス ルールの統計情報をイネーブルにします。
- [Port]：TCP/UDP ポートの統計情報をイネーブルにします。
- [Protocol]：TCP/UDP 以外の IP プロトコルの統計情報をイネーブルにします。
- [TCP-Intercept]：TCP 代行受信によってインターセプトされた攻撃に関する統計をイネーブルにします（TCP 代行受信をイネーブルにする方法については、SYN フラッド DoS 攻撃からのサーバーの保護（TCP 代行受信） を参照してください）。

ステップ 4 ホスト、ポート、およびプロトコルの統計情報については、収集するレート間隔の数を変更できます。[Rate Intervals] 領域で、統計タイプのそれぞれに対して [1 hour]、[1 and 8 hours]、または [1, 8 and 24 hours] を選択します。デフォルトの間隔は [1 hour] で、メモリ使用量が低く抑えられます。

ステップ 5 TCP 代行受信の統計情報については、次のオプションを [TCP Intercept Threat Detection] 領域で設定できます。

- [Monitoring Window Size]：履歴モニタリングの時間枠のサイズを 1 ～ 1440 分の範囲内で設定します。デフォルトは 30 分です。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

- [Burst Threshold Rate]：syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
- [Average Threshold Rate]：syslog メッセージ生成の平均レートのしきい値を 25 ～ 2147483647 の範囲内で設定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。

デフォルト値を復元するには、[Set Default] ボタンをクリックします。

ステップ 6 [Apply] をクリックします。

スキャン脅威検出の設定

攻撃者を識別し、必要に応じて排除するため、スキャン脅威検出を設定できます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。デフォルトでは、ホストが攻撃者として識別されると、システム ログ メッセージ 730101 が生成されます。ホストから大量のメッセージが送信されることが予想される場合は、アドレスを排除から除外するようにしてください。たとえば、Pluggable Interface Module（PIM）マルチキャストを有効にした場合、PIM ルータまたは PIM メッセージがドロップされます。

手順

ステップ 1 **[Configuration]** > **[Firewall]** > **[Threat Detection]** を選択します。

ステップ 2 [Enable Scanning Threat Detection] を選択します。

ステップ 3 （任意）ASA がホストを攻撃者と識別した場合に自動的にホスト接続を終了させるには、[Shun Hosts detected by scanning threat] を選択し、必要に応じて次のオプションを入力します。

- ホスト IP アドレスを回避対象から除外するには、[Networks excluded from shun] フィールドにアドレスまたはネットワーク オブジェクト名はを入力します。複数のアドレスまたはサブネットは、カンマで区切って入力できます。IP アドレス オブジェクトのリストからネットワークを選択するには、[...] ボタンを押します。
- （任意）攻撃ホストの除外期間を設定するには、[Set Shun Duration] を選択し、10 ～ 2592000 秒の間の値を入力します。デフォルトの期間は 3600 秒（1 時間）です。デフォルト値を復元するには、[Set Default] をクリックします。

ステップ 4 [Apply] をクリックします。

VPN サービスの脅威検出の設定

VPN サービスの脅威検出を有効にして、IPv4 アドレスからのサービス妨害（DoS）攻撃を防ぐことができます。次のタイプの攻撃に使用できる個別のサービスがあります。

- リモートアクセス VPN ログイン認証攻撃者が、パスワードスプレー攻撃でログイン試行を繰り返し開始することで認証試行に使用されるリソースを消費し、実数のユーザーが VPN にログインできなくなる可能性があります。
- クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。パスワードスプレー攻撃と同様に、この攻撃はリソースを消費し、有効なユーザーが VPN に接続できなくなる可能性があります。
- 無効な VPN サービス、つまり内部使用専用サービスに接続しようとします。この接続を試みる IP アドレスは、ただちに排除されます。

これらのサービスを有効にすると、システムはしきい値を超えたホストを自動的に排除して、それ以上の試行されないようにします。アドレスに対して **no shun** コマンドを使用して、排除を手動で削除できます。

サービスのカウンタを手動で 0 にリセットするには、**clear threat-detection service** コマンドを使用します。

始める前に

適切なホールドダウン値としきい値を決定する場合は、環境での NAT の使用を検討してください。PAT を使用して、同じ IP アドレスから多数の要求を送信できるようにする場合は、認証失敗とクライアント開始サービスの値を大きくして、有効なユーザーが接続を完了するのに十分な時間を確保できるようにする必要があります。たとえば、多くのお客様が非常に短い時間内に接続を試みるホテルなどです。

手順

ステップ 1 **[設定（Configuration）] > [ファイアウォール（Firewall）] > [脅威検出（Threat Detection）]** の順に選択します。

VPN サービスの脅威検出を有効にするには、次の手順を実行します。CLI の手順は次のとおりです。

a) リモートアクセス VPN クライアントの開始に対して脅威検出を有効にするには、[リモートアクセスクライアントの開始試行を記録するサービス（Service for recording remote access client initiation attempts）] を選択します。
b) VPN クライアントの開始に関して次のオプションを設定します。
   - [ホールドダウン（Hold Down）] は、最後の開始からのホールドダウン期間を定義します。クライアントの IPv4 アドレスの排除をトリガーするには、前回の開始とのホールドダウン期間内に、連続する開始のしきい値カウントに達する必要があります。た

とえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した開始が 20 回あり、2 つの連続した開始間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。デフォルトに戻すには、[デフォルトを設定（Set Default）] をクリックします。

- [しきい値（Threshold）] は、排除をトリガーするためにホールドダウン期間内に発生する必要がある開始の数を定義します。5 ～ 100 のしきい値を指定できます。デフォルトに戻すには、[デフォルトを設定（Set Default）] をクリックします。

c) [適用（Apply）] をクリックし、変更内容を保存して展開します。

ステップ 2 リモートアクセス VPN 認証失敗の脅威検出を有効にします。

threat-detection service remote-access-authentication hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の失敗からのホールドダウン期間を定義します。攻撃者の IPv4 アドレスの排除をトリガーするには、前回の失敗とのホールドダウン期間内に連続失敗のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した認証失敗が 20 回あり、2 つの連続した失敗間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。
- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある試行の失敗数を定義します。1 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-authentication

例：

次の例では、20 分以内に 10 回の失敗のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

ステップ 3 リモートアクセス VPN クライアント開始の脅威検出を有効にします。

threat-detection service remote-access-client-initiations hold-down *minutes* **threshold** *count*

それぞれの説明は次のとおりです。

- **hold-down** *minutes* は、最後の開始からのホールドダウン期間を定義します。クライアントの IPv4 アドレスの排除をトリガーするには、前回の開始とのホールドダウン期間内に、連続する開始のしきい値カウントに達する必要があります。たとえば、ホールドダウン期間が 10 分でしきい値が 20 で、単一の IPv4 アドレスからの連続した開始が 20 回あり、2 つの連続した開始間のタイムスパンが 10 分を超えない場合、送信元 IPv4 アドレスは排除されます。1 ～ 1440 分の時間を指定できます。
- **threshold** *count* は、排除をトリガーするためにホールドダウン期間内に発生する必要がある開始の数を定義します。5 ～ 100 のしきい値を指定できます。

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service remote-access-client-initiations

例：

次の例では、20 分以内に 10 回の開始のメトリックを設定します。

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

ステップ 4 無効な VPN サービスへの接続試行の脅威検出を有効にします。

threat-detection service invalid-vpn-access

サービスを無効化するには、次のコマンドを使用します。

no threat-detection service invalid-vpn-access

例：

次の例では、Invalid VPN Access サービスを有効にしています。

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

脅威検出のモニタリング

次のトピックでは、脅威検出のモニタリングとトラフィック統計情報を表示する方法を説明します。

基本脅威検出統計情報のモニタリング

基本脅威検出統計情報を表示するには、[Home] > [Firewall Dashboard] > [Traffic Overview] を選択します。

拡張脅威検出統計情報のモニタリング

次のダッシュボードを使用して拡張脅威検出統計情報をモニタリングできます。

- [Home] > [Firewall Dashboard] > [Top 10 Access Rules]：最も多くヒットしたアクセス ルールを表示します。許可および拒否はこのグラフでは区別されません。拒否されたトラフィックは、[Traffic Overview] > [Dropped Packets Rate] グラフで追跡できます。
- [Home] > [Firewall Dashboard] > [Top Usage Statistics]： [Top 10 Sources] および [Top 10 Destinations] タブには、ホストの統計情報が表示されます。脅威検出アルゴリズムに起因して、フェールオーバー リンクとステート リンクの組み合わせとして使用されるインターフェイスは上位 10 個のホストに表示されることがあります。これは予期された動作であり、表示される IP アドレスは無視できます。

[Top 10 Services] タブには、ポートとプロトコルの両方の統計情報が表示され（表示するには、両方がイネーブルに設定されている必要があります）、TCP/UDP ポートと IP プロトコル タイプを組み合わせた統計情報が表示されます。TCP（プロトコル 6）と UDP（プロトコル 17）は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ（ポートまたはプロトコル）の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。

- [Home] > [Firewall Dashboard] > [Top Ten Protected Servers under SYN Attack]：TCP 代行受信の統計情報を表示します。[Detail] ボタンをクリックすると、履歴サンプリング データが表示されます。ASA はレート間隔の間に攻撃の数を 30 回サンプリングするので、デフォルトの 30 分間隔では、60 秒ごとに統計情報が収集されます。

VPN サービスの脅威検出のモニタリング

次のトピックで説明するように、syslog および show コマンドを使用して、VPN サービスの脅威検出をモニターできます。

VPN サービスの脅威検出の Syslog モニタリング

これらのサービスに関連する次の syslog メッセージが表示される場合があります。

- %ASA-6-733200: Threat-detection Info: *message*

  このメッセージは、脅威検出に関する一般的な情報イベントを報告します。

- %ASA-4-733201: Threat-detection: Service[*service*] Peer[*peer*]: threshold of *threshold-value* was exceeded. Adding shun to interface *interface.Additional_message*

  このメッセージは、指定されたサービスの不審なアクティビティが原因で、脅威検出サービスが IP アドレスを排除したことを示しています。メッセージには追加情報が含まれている場合があります。たとえば、RA VPN クライアント開始試行の場合、追加情報は「SSL（または IKEv2）：RA 過剰なクライアント開始要求（SSL (or IKEv2): RA excessive client initiation requests.）」のようになります。

  show shun コマンドを使用して、排除されたホストのリストを表示できます。IP アドレスが攻撃者ではないことがわかっている場合は、**no shun** コマンドを使用して排除を削除できます。

VPN サービスの脅威検出の show コマンドによるモニタリング

次のコマンドを使用して、VPN サービスの脅威検出の統計情報を表示します。

show threat-detection service [*service*] [**entries** | **details**]

必要に応じて、特定のサービス（**remote-access-authentication**、**remote-access-client-initiations**、または **invalid-vpn-access**）にビューを制限できます。次のパラメータを追加することで、ビューをさらに制限できます。

- **entries**：追跡対象のエントリのみを表示します。たとえば、認証試行に失敗した IP アドレスです。
- **details**：サービスの詳細とサービスエントリの両方を表示します。

選択したオプションに基づいて、ディスプレイ出力には次の情報が表示されます。

- サービスの名前
- サービスの状態：有効または無効
- サービスホールドダウン設定
- サービスしきい値設定
- サービスアクション統計情報
  - [失敗（Failed）]：報告された発生の処理中に障害が発生しました。
  - [ブロッキング（Blocking）]：報告された発生はホールドダウン期間内であり、しきい値に達したか超過しました。その結果、サービスは、不正なピアをブロックするための排除を自動的にインストールしました。
  - [記録（Recording）]：報告された発生がホールドダウン期間外であるか、しきい値に達したか超過しました。その結果、サービスは発生を記録します。
  - [サポート対象外（Unsupported）]：報告された発生は、現在自動排除をサポートしていません。
  - [無効（Disabled）]：発生が報告されました。ただし、サービスは無効になっています。

例

次の例では、すべてのサービスが有効になっており、リモートアクセス認証サービスについて潜在的な攻撃者が追跡されています。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
```

```
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

次に、**show threat-detection service entries** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

次に、**show threat-detection service details** コマンドの例を示します。

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

VPN サービス違反に適用された排除の削除

次のコマンドを使用して、VPN サービスに適用された排除をモニターし、排除を削除できます。VPN サービスの脅威検出によって適用される排除は、**show threat-detection shun** コマンドには表示されないことに注意してください。このコマンドは、スキャン脅威検出にのみ適用されます。

- **show shun** [*ip_address*]

  VPN サービスの脅威検出によって自動的に排除されたホスト、または **shun** コマンドを使用して手動で排除されたホストを含む、排除されたホストを表示します。必要に応じて、指定した IP アドレスにビューを制限できます。

- **no shun** *ip_address* [**interface** *if_name*]

  指定した IP アドレスからのみ排除を削除します。アドレスが複数のインターフェイスで排除され、一部のインターフェイスで排除をそのままにしておく場合は、オプションで排除のインターフェイス名を指定できます。

- **clear shun**

  すべての IP アドレスから排除を削除します。

脅威検出の履歴

機能名	プラットフォームリリース	説明
基本および拡張脅威検出統計情報、スキャン脅威検出	8.0(2)	基本および拡張脅威検出統計情報、スキャン脅威検出が導入されました。 次の画面が導入されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Traffic Overview]、[Home] > [Firewall Dashboard] > [Top 10 Access Rules]、[Home] > [Firewall Dashboard] > [Top Usage Status]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
排除期間	8.0(4)/8.1(2)	排除期間を設定できるようになりました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
TCP 代行受信の統計情報	8.0(4)/8.1(2)	TCP 代行受信の統計情報が導入されました。 次の画面が導入または変更されました。[Configuration] > [Firewall] > [Threat Detection]、[Home] > [Firewall Dashboard] > [Top 10 Protected Servers Under SYN Attack]。
ホスト統計情報レート間隔のカスタマイズ	8.1(2)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。

機能名	プラットフォームリリース	説明
バースト レート間隔が平均レートの 1/30 に変更されました。	8.2(1)	以前のリリースでは、平均レートの 1/60 でした。メモリを最大限に使用するため、サンプリング間隔が平均レートの間に 30 回に減らされました。
ポートおよびプロトコル統計情報レート間隔のカスタマイズ	8.3(1)	統計情報が収集されるレート間隔の数をカスタマイズできるようになりました。デフォルトのレート数は、3 から 1 に変更されました。 次の画面が変更されました。[Configuration] > [Firewall] > [Threat Detection]。
メモリ使用率の向上	8.3(1)	脅威検出のメモリ使用率が向上しました。
VPN サービスの脅威検出	9.20(3)	VPN サービスの脅威検出を設定して、IPv4 アドレスからの次のタイプの VPN 攻撃に対して保護できます。 • リモートアクセス VPN への過剰な認証失敗の試行（ユーザー名/パスワードをスキャンするブルートフォース攻撃など）。 • クライアント初期化攻撃。攻撃者は単一のホストからリモートアクセス VPN ヘッドエンドへの接続試行を繰り返し開始しますが、完了しません。 • 無効な VPN サービス、つまり内部専用サービスへのアクセス試行。 アクセスに失敗したとしても、これらの攻撃によってコンピューティングリソースを消費し、場合によってはサービス拒否（DoS）を引き起こす可能性があります。 **clear threat-detection service**、**show threat-detection service**、**shun**、**threat-detection service** の各コマンドが導入または変更されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。