ASA脅威の検出機能と設定の確認

内容

はじめに

このドキュメントでは、脅威検出機能と設定の3つの主要なコンポーネントについて説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス（ASA）の脅威検出機能の機能性および基本設定について説明します。脅威検出機能を使用することで、ファイアウォール管理者は、攻撃が内部ネットワーク インフラストラクチャに到達する前に攻撃を特定、認識および停止できます。そのため、この機能では、さまざまな多くのトリガおよび統計情報が使用されます。これらについては、このセクションの後半で詳しく説明します。

脅威検出機能は、ソフトウェア バージョン 8.0(2) 以降を実行する ASA ファイアウォールで使用できます。脅威検出は、専用 IDS/IPS ソリューションの代わりには使用できませんが、IPS が ASA のコア機能の保護を強化できない環境で使用できます。

脅威検出機能

脅威検出機能には、次の 3 つのメイン コンポーネントがあります。

1. 基本的な脅威の検出
2. 高度な脅威の検出
3. スキャン脅威の検出

これらの各コンポーネントは、このセクションで詳しく説明します。

基本的な脅威の検出（システム レベル レート）

基本的な脅威の検出は、8.0(2)以降を実行するすべてのASAでデフォルトで有効になっています。

基本的な脅威の検出は、さまざまな理由で ASA によりパケットがドロップされるレートを監視します。つまり、基本的な脅威の検出により生成される統計情報は、アプライアンス全体を対象とするだけで、一般的には、脅威の発信元または固有の性質に関する情報を提供するだけの詳細は含まれません。ただし、ASA は、次のイベントでドロップされるパケットを監視します。

- ACLドロップ(acl-drop)：パケットはアクセスリストによって拒否されます。
- Bad Pkts(bad-packet-drop):RFC標準に準拠していないL3およびL4ヘッダーを含む無効なパケット形式です。
- Conn Limit(conn-limit-drop)：設定された接続制限またはグローバル接続制限を超えたパケット。
- DoS攻撃(dos-drop)：サービス拒否(DoS)攻撃。
- ファイアウォール(fw-drop)：基本的なファイアウォールセキュリティチェック。

- ICMP攻撃(icmp-drop)：疑わしいICMPパケット。
- Inspect(inspect-drop)：アプリケーションインスペクションによる拒否。
- インターフェイス(interface-drop)：インターフェイスチェックによって廃棄されたパケット。
- スキャン（スキャン脅威）– ネットワーク/ホストスキャン攻撃。
- SYN攻撃(syn-attack):TCP SYN攻撃およびリターンデータを持たない単方向UDPセッションを含む、不完全なセッション攻撃。

これらの各イベントには、脅威の特定に使用されるトリガの特定のセットが含まれます。ほとんどのトリガは、特定の ASP ドロップの理由に関連付けられますが、特定の syslog および検査アクションも考慮されます。一部のトリガは、複数の脅威カテゴリで監視されます。次の表に示すトリガは、一般的なトリガのすべてではなく、一部のみです。

基本的な脅威	トリガ/ASP ドロップの理由
acl-drop	acl-drop
bad-packet-drop	invalid-tcp-hdr-length（無効なtcp-hdr-length） 無効なIPヘッダー inspect-dns-pak-too-long（オプション） inspect-dns-id-not-matched」というエラーメッセージが表示されます。
conn-limit-drop	conn制限
dos-drop	SPセキュリティが失敗しました
fw-drop	inspect-icmp-seq-num-not-matched」というエラーメッセージが表示されます。 inspect-dns-pak-too-long（オプション） inspect-dns-id-not-matched」というエラーメッセージが表示されます。 SPセキュリティが失敗しました acl-drop
icmp-drop	inspect-icmp-seq-num-not-matched」というエラーメッセージが表示されます。
inspect-drop	インスペクション エンジンでトリガされるフレーム ドロップ
interface-drop	SPセキュリティが失敗しました

	ルートなし
scanning-threat	TCP-3WHS失敗 TCP-NOT-SYN SPセキュリティが失敗しました acl-drop inspect-icmp-seq-num-not-matched」というエラーメッセージが表示されます。 inspect-dns-pak-too-long（オプション） inspect-dns-id-not-matched」というエラーメッセージが表示されます。
syn-attack	解放の理由が「SYN タイムアウト」である %ASA-6-302014 syslog

各イベントに対して、基本的な脅威の検出は、設定期間でドロップが発生するレートを測定します。この期間は、平均レート間隔（ARI）と呼ばれ、600 秒 ~ 30 日の範囲を指定できます。ARI 内で発生するイベント数が、設定されているレートしきい値を超えると、ASA は、これらのイベントを脅威と見なします。

基本的な脅威の検出には、イベントが脅威であると見なされるときのしきい値として、平均レートとバーストレートの2つのしきい値を設定できます。平均レートは、設定 ARI の期間内における 1 秒あたりの平均ドロップ数です。たとえば、ARI が 600 秒で、ACL ドロップの平均レートしきい値が 400 に設定されている場合、ASA は、最後の 600 秒で ACL によりドロップされた平均パケット数を計算します。この数値が 1 秒あたり 400 を超えると、ASA は脅威を記録します。

バースト レートも非常に似ていますが、バースト レート間隔（BRI）と呼ばれる、より短い期間のスナップショット データを使用します。BRI は常に ARI 未満です。たとえば、前述の例に基づき、ACL ドロップの ARI が 600 秒、バースト レートが 800 の場合について説明します。これらの値を使用して、ASAはACLによって廃棄されたパケットの平均数を20秒で計算します。ここで、20秒はBRIです。この計算された値が 1 秒あたり 800 ドロップを超えると、脅威が記録されます。使用される BRI については、ASA は、ARI の 30 分の 1 の値を使用します。そのため、前述の例では、600 秒の 30 分の 1 の 20 秒が使用されます。ただし、脅威検出の最小 BRI は 10 秒なので、ARI の 30 分の 1 の値が 10 未満の場合、ASA は BRI として 10 秒を使用します。また、8.2(1) よりも前のバージョンでは、この動作が異なるので注意してください。これらのバージョンでは、ARI の 30 分の 1 ではなく、60 分の 1 の値が使用されます。最小 BRI は、すべてのソフトウェア バージョンで 10 秒です。

基本的な脅威が検出されると、ASA は、syslog %ASA-4-733100 を生成し、潜在的な脅威が特定されたことを管理者に警告します。show threat-detection rate コマンドを使用すると、各脅威カテゴリのイベントの平均数、現在の数、合計数を表示できます。 累積イベントの合計数は、最後

の30個のBRIサンプルで見られたイベントの数の合計です。

syslogのバーストレートは、現在のBRIでこれまでに廃棄されたパケットの数に基づいて計算されます。BRIでは、計算は定期的に行われます。セキュリティ違反が発生すると、syslogが生成されます。 BRIで生成されるsyslogは1つだけに制限されます。「show threat-detection rate」のバーストレートは、最後のBRIで廃棄されたパケットの数に基づいて計算されます。この違いの設計では、syslogは時間の影響を受けやすいため、現在のBRIで違反が発生した場合にキャプチャされる可能性があります。「show threat-detection rate」は時間の影響を受けにくいため、最後のBRIからの番号が使用されます。

基本的な脅威の検出では、逸脱したトラフィックを停止したり、将来の攻撃を防止したりするためのアクションは実行されません。そのため、基本的な脅威の検出は、情報提供のみを目的として、監視またはレポート メカニズムとして使用できます。

高度な脅威の検出（オブジェクト レベルの統計情報と上位 N 個）

基本的な脅威の検出と同様、高度な脅威の検出は、より詳細なオブジェクトを対象とした統計情報の追跡に使用できます。ASA は、ホスト IP、ポート、プロトコル、ACL、および TCP インターセプトで保護されるサーバの統計情報追跡をサポートします。高度な脅威の検出は、デフォルトで、ACL 統計情報のみでイネーブルにされます。

ホスト、ポートおよびプロトコル オブジェクトについて、脅威検出は、特定期間内でオブジェクトにより送受信されたパケット数、バイト数、ドロップ数を追跡します。ACL に対して、脅威検出は、特定期間内で最も発生した上位 10 の ACE（許可と拒否の両方）を追跡します。

すべての状況における追跡期間は、20 分、1 時間、8 時間、24 時間です。これらの期間は設定できませんが、オブジェクトごとの追跡期間は、「number-of-rate」キーワードを使用して調整できます。詳細については、「コンフィギュレーション」セクションを参照してください。たとえば、「number-of-rate」が2に設定されている場合は、20分、1時間、8時間のすべての統計が表示されます。「number-of-rate」が1に設定されている場合は、20分、1時間のすべての統計が表示されます。20 分のレートは必ず表示されます。

TCP インターセプトがイネーブルの場合、脅威検出は、攻撃を受けていると見なされ、TCP インターセプトで保護される上位 10 のサーバを追跡できます。TCP インターセプトの統計情報は、測定レート間隔と特定の平均（ARI）およびバースト（BRI）レートを設定できるという点では、基本的な脅威の検出に似ています。TCP インターセプトの高度な脅威の検出統計情報は、ASA 8.0(4) 以降のみで使用できます。

高度な脅威の検出の統計情報は、show threat-detection statistics および show threat-detection statistics top コマンドを介して表示されます。これは、ASDMのファイアウォールダッシュボードの「上位」グラフを生成する機能でもあります。高度な脅威の検出により生成される syslog は、%ASA-4-733104 および %ASA-4-733105 のみです。これは、TCP インターセプトの統計情報で、それぞれ平均およびバースト レートを超えるとトリガされます。

基本的な脅威の検出と同様、高度な脅威の検出も情報を提供するだけです。高度な脅威の検出の統計情報に基づいてトラフィックをブロックすることはありません。

スキャン脅威の検出

スキャン脅威の検出は、サブネットの大量のホストまたはホスト/サブネットの大量のポートと接続する、疑わしい攻撃者を追跡するために使用されます。スキャン脅威の検出は、デフォルトでディセーブルです。

スキャン脅威の検出は、スキャン攻撃の脅威のカテゴリをすでに定義している、基本的な脅威の検出の概念に基づいています。そのため、レート間隔、平均レート（ARI）およびバースト レート（BRI）設定は、基本的な脅威の検出およびスキャン脅威の検出間で共有されます。これらの 2 つの機能間の違いは、基本的な脅威の検出は、平均またはバースト レートしきい値の情報を示すだけですが、スキャン脅威の検出は、スキャン対象のホストでより詳細な情報を提供できる攻撃者およびターゲット IP アドレスのデータベースを保守します。また、ターゲット ホスト/サブネットで実際に受信されるトラフィックだけが、スキャン脅威の検出と見なされます。基本的な脅威の検出は、トラフィックが ACL によりドロップされる場合でも、スキャン脅威をトリガできます。

スキャン脅威の検出は、オプションで、攻撃者 IP 排除により攻撃者に対応できます。このため、スキャン脅威の検出は、ASA を介した接続にアクティブに影響する脅威検出機能の唯一のサブセットです。

スキャン脅威の検出により攻撃が検出されると、攻撃者およびターゲット IP で %ASA-4-733101 が記録されます。攻撃者を排除するように設定されている場合、スキャン脅威の検出で排除が生成されると、%ASA-4-733102 が記録されます。%ASA-4-733103 は、排除が削除されると記録されます。show threat-detection scanning-threat コマンドは、スキャンの脅威のデータベース全体を表示するときに使用されます。

制限事項

- 脅威検出は、ASA 8.0(2) 以降のみで使用できます。これは、ASA 1000V プラットフォームではサポートされません。
- 脅威検出は、シングル コンテキスト モードのみでサポートされます。
- through-the-box 脅威のみが検出されます。ASA 自体に送信されるトラフィックは、脅威検出のみで考慮されます。
- ターゲットにされたサーバでリセットされる TCP 接続は、SYN 攻撃またはスキャン脅威としてカウントされません。

コンフィギュレーション

基本的な脅威の検出

基本的な脅威の検出は、threat-detection basic-threat コマンドを使用してイネーブルにされます。

<#root>

```
ciscoasa(config)#
```

threat-detection basic-threat

デフォルト レートは、show run all threat-detection コマンドを使用して表示できます。

```
<#root>

ciscoasa(config)#

show run all threat-detection


threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

カスタム値を使用してこれらのレートを調整するには、threat-detection rateコマンドを適切な脅威カテゴリに再設定します。

```
<#root>

ciscoasa(config)#

threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550
```

各脅威カテゴリには、最大 3 種類のレートを定義できます (レート ID、レート 1、レート 2、レート 3) 。超過した特定のレート ID は、%ASA-4-733100 syslog で参照されます。

前述の例では、脅威検出は、1200 秒間で 1 秒あたりの ACL ドロップ数が 250 を超える、または 40 秒間で 1 秒値のドロップ数が 550 を超える場合のみ syslog 733100 を作成します。

高度な脅威の検出

高度な脅威の検出をイネーブルにするには、threat-detection statistics コマンドを使用します。特定の機能キーワードを提供しない場合、すべての統計情報の追跡がイネーブルになります。

```
<#root>
```

```
ciscoasa(config)#
threat-detection statistics ?


configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

ホスト、ポート、プロトコルまたは ACL 統計情報で追跡されるレート間隔を設定するには、number-of-rate キーワードを使用します。

```
<#root>
ciscoasa(config)#
threat-detection statistics host number-of-rate 2
```

number-of-rate キーワードは、脅威追跡を設定して、間隔の最も短い n のみを追跡します。

TCP インターセプト統計情報をイネーブルにするには、threat-detection statistics tcp-intercept コマンドを使用します。

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept
```

TCP インターセプト統計情報のカスタム レートを設定するには、rate-interval、average-rate、burst-rate キーワードを使用します。

```
<#root>
ciscoasa(config)#
threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

スキャン脅威の検出

スキャン脅威の検出をイネーブルにするには、threat-detection scanning-threat コマンドを使用します。

<#root>

ciscoasa(config)#

threat-detection scanning-threat

スキャン脅威のレートを調整するには、基本的な脅威の検出により使用される threat-detection rate コマンドを使用します。

<#root>

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550

ASA でスキャン攻撃者 IP を排除できるようにするには、shun キーワードを threat-detection scanning-threat コマンドに追加します。

<#root>

ciscoasa(config)#

threat-detection scanning-threat shun

これにより、スキャン脅威の検出で、攻撃者を 1 時間排除できます。排除の期間を調整するには、threat-detection scanning-threat shun duration コマンドを使用します。

<#root>

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000

場合によっては、ASAが特定のIPを回避することを防ぐことができます。このようにするには、threat-detection scanning-threat shun except コマンドで例外を作成します。

<#root>

ciscoasa(config)#

threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255

ciscoasa(config)#

threat-detection scanning-threat shun except object-group no-shun

パフォーマンス

基本的な脅威の検出が ASA のパフォーマンスに与える影響はごくわずかです。高度な脅威の検出およびスキャン脅威の検出は、メモリでさまざまな統計情報を追跡する必要があるので、多くのリソースを消費します。許可されるトラフィックにアクティブに影響するのは、shun 機能をイネーブルにしたスキャン脅威の検出のみです。

ASA ソフトウェア バージョンが上がるにつれ、脅威検出のメモリ使用率は大幅に最適化されています。ただし、脅威検出を有効にする前と後では、ASAのメモリ使用率を監視するように注意する必要があります。場合によっては、特定の問題をアクティブにトラブルシューティングする際に、特定の統計情報（ホスト統計情報など）のみを一時的に有効にすることをお勧めします。

脅威検出のメモリ使用量の詳細を表示するには、show memory app-cache threat-detection [detail]コマンドを実行します。

推奨される対処法

次のセクションでは、さまざまな脅威検出関連のイベントが発生した場合に実行可能なアクションに関する一般的な推奨事項について説明します。

基本ドロップ レートを超えて %ASA-4-733100 が生成された場合

%ASA-4-733100 syslogに示されている特定の脅威カテゴリを判別し、これを show threat-detection rate を参照。この情報を使用して、 show asp drop トラフィックがドロップされる理由を判別します。

特定の理由でドロップされるトラフィックの詳細を表示するには、該当する理由を指定してASPドロップキャプチャを使用し、ドロップされるすべてのパケットを表示します。たとえば、ACLドロップの脅威がログに記録された場合は、ASPドロップの理由をキャプチャします。 acl-drop：

<#root>

ciscoasa#

capture drop type asp-drop acl-drop

ciscoasa#

show capture drop

1 packet captured

```
   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

このキャプチャは、ドロップされたパケットが10.10.10.10から192.168.1.100へのUDP/53パケットであることを示しています。

%ASA-4-733100 がスキャン脅威を報告する場合、一時的にスキャン脅威の検出をイネーブルにすることもできます。これにより、ASA は、攻撃に関連する送信元および宛先 IP を追跡できます。

基本的な脅威の検出は、主にASPによってすでにドロップされているトラフィックを監視するため、潜在的な脅威を阻止するための直接的なアクションは必要ありません。ただし、SYN攻撃とスキャン脅威は例外で、これらはASAを通過するトラフィックに関係します。

ASP ドロップ キャプチャに示されるドロップが、ネットワーク環境で許可または予測されている場合、基本レート間隔を適切な値に調整します。

ドロップが不正なトラフィックを示す場合、トラフィックがASAに到達する前に、トラフィックをブロックまたはレート制限するアクションを実行する必要があります。これにはアップストリーム デバイスの ACL や QoS が含まれます。

SYN 攻撃では、トラフィックは ASA の ACL でブロックできます。TCPインターセプトは、ターゲットサーバを保護するように設定することもできますが、その場合は単にConn Limit脅威が口グに記録されるだけです。

スキャン攻撃では、トラフィックは ASA の ACL でブロックできます。スキャン脅威の検出 shunオプションを有効にすると、ASAが一定期間、攻撃者からのすべてのパケットをプロアクティブにブロックできます。

スキャン脅威が検出されて %ASA-4-733101 が口グに記録された場合

%ASA-4-733101は、ターゲットホスト/サブネットまたは攻撃者のIPアドレスをリストする必要があります。ターゲットと攻撃者の完全なリストについては、 show threat-detection scanning-threatを参照。

攻撃者やターゲットに面するASAインターフェイスのパケットキャプチャも、攻撃の性質を明らかにするのに役立ちます。

検出されたスキャンが予期されていない場合は、トラフィックがASAに到達する前に、トラフィックをブロックまたはレート制限するアクションを実行する必要があります。これにはアップストリーム デバイスの ACL や QoS が含まれます。ユーザが shunオプションがスキャン脅威の検出設定に追加されました。これにより、ASAは一定期間、攻撃者IPからすべてのパケットをプロアクティブにドロップできます。最終的な手段として、ACL または TCP インターセプト ポリシーを介して ASA でトラフィックを手動でブロックすることもできます。

検出されたスキャンが誤検出の場合、ネットワーク環境に合わせてスキャン脅威のレート間隔を適切な値に調整します。

攻撃者が排除されて %ASA-4-733102 が口グに記録された場合

%ASA-4-733102 は、排除された攻撃者の IP アドレスをリストします。 show threat-detection shun コマ

ンドを発行して、脅威検出によって排除された攻撃者の完全なリストを表示します。 show shun コマンドを発行して、ASAによってアクティブに排除されているすべてのIPの完全なリストを表示します（脅威検出以外の送信元からのIPも含まれます）。

shun が正当な攻撃の一部である場合、処置は必要ありません。ただし、できるだけ送信元のアップストリームで、攻撃者のトラフィックを手動でブロックすることをお勧めします。これは ACL や QoS で実施できます。これにより、中間デバイスが不正なトラフィックにリソースを浪費する必要がなくなります。

shunをトリガーしたスキャンの脅威が誤検出の場合は、 clear threat-detection shun [IP_address] コマンドを使用して、アップグレードを実行します。

%ASA-4-733104 または %ASA-4-733105 が口グに記録された場合

%ASA-4-733104および%ASA-4-733105は、現在TCPインターセプトによって保護されている、攻撃の対象となるホストをリストします。攻撃レートと保護サーバの詳細については、次の出力を確認してください。 show threat-detection statistics top tcp-intercept を参照。

<#root>

```
ciscoasa#
```

```
show threat-detection statistics top tcp-intercept
```

```
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

高度な脅威の検出がこの種の攻撃を検出すると、ASAはすでにTCPインターセプトを介してターゲットサーバを保護しています。設定されている接続制限を参照して、攻撃の性質およびレートが適切に保護されているか確認します。また、できるだけ送信元のアップストリームで、攻撃者のトラフィックを手動でブロックすることをお勧めします。これは ACL や QoS で実施できます。これにより、中間デバイスが不正なトラフィックにリソースを浪費する必要がなくなります。

検出された攻撃が誤検出の場合は、TCPインターセプト攻撃のレートを適切な値に調整し、 threat-detection statistics tcp-interceptコマンドを使用して、アップグレードを実行します。

脅威を手動でトリガする方法

テストとトラブルシューティングを行うには、さまざまな脅威を手動でトリガーすると役立ちます。ここでは、いくつかの一般的な脅威タイプをトリガーする方法に関するヒントを示します。

基本的な脅威：ACLドロップ、ファイアウォール、およびスキャン

特定の基本的な脅威をトリガするには、前述の「機能」セクションの表を参照してください。特定の ASP ドロップの理由を選択して、適切な ASP ドロップの理由によりドロップされるトラフィックを ASA を介して送信します。

たとえば、ACLドロップ、ファイアウォール、およびスキャン脅威はすべて、acl-dropによってドロップされたパケットのレートを考慮します。これらの脅威を同時にトリガするには、次の手順を実行します。

1. ASA (10.11.11.11) 内部でターゲット サーバに送信されるすべての TCP パケットを明示的にドロップする ACL を ASA の外部インターフェイスで作成します。

```
access-list outside_in extended line 1 deny tcp any host 10.11.11.11
access-list outside_in extended permit ip any any
access-group outside_in in interface outside
```

2. ASA外部(10.10.10.10)の攻撃者から、nmapを使用してターゲットサーバのすべてのポートに対してTCP SYNスキャンを実行します。

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> 注:T5では、nmapができるだけ速くスキャンを実行するように設定されています。攻撃者のPCのリソースによると、これはまだ一部のデフォルトレートをトリガーするのに十分な速度ではありません。この場合は単純に確認したい脅威の設定されたレートを下げます。ARIおよびBRIを0に設定すると、基本的な脅威の検出は、レートに関係なく常に脅威をトリガーします。

3. ACLドロップ、ファイアウォール、およびスキャンの脅威に対して基本的な脅威が検出されていることに注意してください。

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

> 注：この例では、ACLドロップとファイアウォールARIおよびBRIが0に設定されているため、常に脅威をトリガーします。このため、最大設定レートが 0 としてリストされます。

高度な脅威 – TCPインターセプト

1. 外部インターフェイスで ACL を作成し、ASA (10.11.11.11) の内側にあるターゲット サーバへ送信されるすべての TCP パケットを許可します。

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. ターゲット サーバが実際には存在しない場合、または攻撃者からの接続の試みに対してリセットを行う場合は、ASA で偽装 ARP エントリを設定して内側のインターフェイスから送信される攻撃トラフィックを吸い込みます。

```
arp inside 10.11.11.11 dead.dead.dead
```

3. 単純な TCP インターセプト ポリシーを ASA で作成します。

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

ASA (10.10.10.10) の外側の攻撃者が nmap を使用してターゲット サーバのすべてのポートに対して TCP SYN スキャンを実行します。

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

脅威検出は、保護サーバを追跡します。

```
<#root>

ciscoasa(config)#

show threat-detection statistics top tcp-intercept


Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

---------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

スキャン脅威

1. 外部インターフェイスで ACL を作成し、ASA (10.11.11.11) の内側にあるターゲット サーバへ送信されるすべての TCP パケットを許可します。

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

> 注：スキャン脅威の検出でターゲットと攻撃者のIPを追跡するには、トラフィックがASAを通過することを許可する必要があります。

2. ターゲット サーバが実際には存在しない場合、または攻撃者からの接続の試みに対してリセットを行う場合は、ASA で偽装 ARP エントリを設定して内側のインターフェイスから送信される攻撃トラフィックを吸い込みます。

```
arp inside 10.11.11.11 dead.dead.dead
```

> 注：ターゲットサーバによってリセットされた接続は、脅威の一部としてカウントされません。

3. ASA (10.10.10.10) の外側の攻撃者が nmap を使用してターゲット サーバのすべてのポートに対して TCP SYN スキャンを実行します。

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

> 注:T5では、nmapができるだけ速くスキャンを実行するように設定されています。攻撃者のPCのリソースによると、これはまだ一部のデフォルトレートをトリガーするのに十分な速度ではありません。この場合は単純に確認したい脅威の設定されたレートを下げます。ARIおよびBRIを0に設定すると、基本的な脅威の検出は、レートに関係なく常に脅威をトリガーします。

4. スキャン脅威が検出され、攻撃者の IP が追跡され、攻撃者が排除されます。

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

関連情報

- ASA設定ガイド
- ASAコマンドリファレンス
- Cisco Secure Firewall ASAシリーズSyslogメッセージ
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。