セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したトラフィックのブロック

悪意のあるインターネットコンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティインテリジェンス機能があります。この機能により、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックすることができ、リソースを集中的に使用する詳細な分析が不要になります。セキュリティインテリジェンスのフィルタリングを行うには、Protection ライセンスが必要です。

セキュリティ インテリジェンスは、既知の好ましくないレピュテーションが含まれる IP アドレスを送信元/宛先とするトラフィックをブロックすることにより機能します。このトラフィック フィルタリングは、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも前に行われます。

IP アドレスでトラフィックを手動で制限することで、セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することができます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。

セキュリティインテリジェンスによってブロックされたトラフィックは直ちにブロックされるため、他のさらなる（侵入、エクスプロイト、マルウェアなどの）インスペクションの対象にはなりません。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされたであろう接続をシステムが分析できるだけでなく、ブロックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

便宜上、 シスコではインテリジェンス フィードを提供しています。インテリジェンス フィードは、VRT によってレピュテーションが低いと判断された、複数の定期的に更新される IP アドレスのコレクションで構成されます。インテリジェンス フィードは、オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）などを追跡します。この機能を組織の固有のニーズに適するようにカスタマイズできます。例を次に示します。

- サードパーティ フィード：インテリジェンス フィードをサードパーティのレピュテーション フィードで補足できます。それらのフィードはシスコのフィードと同様に自動的に更新できます。
- カスタムブロックリスト：ユーザのニーズに応じてさまざまな方法で特定の IP アドレスを手動でブロックできます。
- セキュリティゾーン別のブロックの適用：パフォーマンスを向上させるために、電子メールトラフィックを処理するゾーンにスパムのブロックを制限するなどして、適用対象を絞れます。
- ブロックに代わるモニタリング：特にパッシブ展開や、実装前にフィードをテストする場合に便利です。違反しているセッションをブロックする代わりにモニタするだけで、接続終了イベントを生成できます。
- 誤検出をなくすためのブロックなしリストの使用：ブロックリストの範囲が広すぎる場合、または（たとえば、重要なリソースに）許可するトラフィックを誤ってブロックした場合、ブロックリストをカスタムブロックなしリストでオーバーライドできます。

- セキュリティ インテリジェンス戦略の選択 （2 ページ）
- セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成 （4 ページ）

セキュリティ インテリジェンス戦略の選択

ライセンス：Protection

ブロックリストを作成する最も簡単な方法は、オープンリレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス（bogon）などを追跡するインテリジェンスフィードを使用することです。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムは最新の情報を使用してネットワーク トラフィックをフィルタ処理できます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

したがって、インテリジェンス フィードを補完するために、次の場合にサードパーティの IP アドレスのリストとフィードを使用してセキュリティ インテリジェンス フィルタリングを実行できるようになっています。

- リストとは、ASA FirePOWER モジュールにアップロードする IP アドレスの静的リストのことです。
- フィードとは、 ASA FirePOWER モジュールが定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。インテリジェンス フィードは特殊なタイプのフィードです。

インターネット アクセス要件を含め、セキュリティ インテリジェンスのリストとフィードを設定する方法の詳細については、セキュリティ インテリジェンス リストとフィードの操作を参照してください。

セキュリティ インテリジェンスのグローバルブロックリストの使用

分析中に、グローバルブロックリストを作成できます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気づいた場合、それらの IP アドレスをブロックリストに追加することができます。ASA FirePOWER モジュールは、すべてのアクセス コントロール ポリシーでこのグローバルブロックリスト（および関連するグローバルブロックなしリスト）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、グローバルブロックなしリストとブロックリストの操作を参照してください。

（注） グローバルブロックリスト（またはグローバルブロックなしリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他の変更には、アクセス コントロール ポリシーの再適用が必要になります。

ネットワーク オブジェクトの使用

さらに、ブロックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表すネットワークオブジェクトまたはネットワーク オブジェクト グループ を使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、ネットワーク オブジェクトの操作を参照してください。

セキュリティ インテリジェンスのブロックなしリストの使用

ブロックリストに加え、各アクセス コントロール ポリシーにはブロックなしリストが関連付けられます。これらには、セキュリティ インテリジェンス オブジェクトを取り込むことができます。ポリシーでは、ブロックなしリストがブロックリストをオーバーライドします。つまり、システムは、ブロックなしリストに登録されている送信元または宛先の IP アドレスを、その IPアドレスがブロックリストにも登録されているとしても、アクセス制御ルールを使用して評価します。通常、ブロックリストがまだ有用であっても、その適用範囲があまりにも広く、インスペクション対象のトラフィックを誤ってブロックする場合には、ブロックなしリストを使用してください。

たとえば、信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされても、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブロックリストから削除するのではなく、不適切に分類された IP アドレスのみをブロックなしリストに追加するという方法を取ることができます。

セキュリティ ゾーンを基準としたセキュリティ インテリジェンス フィルタリングの適用

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、セキュリティ インテリジェンス フィルタリングを適用することができます。

上述のブロックなしリストの例を拡張するには、不適切に分類された IP アドレスをブロックなしリストに追加した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティゾーンを使用して、オブジェクトを制限するという方法が考えられます。この方法では、ビジネスニーズを持つユーザだけが、それらの IP アドレスにアクセスできます。別の例として、サードパーティのスパムフィードを使用して、電子メールサーバのセキュリティゾーンのトラフィックをブロックすることができます。

接続のモニタリング（ブロッキングではなく）

特定の IP アドレスまたは一連のアドレスをブロックする必要があるかどうかわからない場合は、「モニタのみ」の設定を使用できます。この設定では、システムが一致する接続をアクセス制御ルールに渡せるだけでなく、ブロックリストと一致する接続がログに記録され、接続終了セキュリティインテリジェンスイベントが生成されます。注意点として、グローバルブロックリストをモニタのみに設定することはできません。

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

パッシブ展開環境では、パフォーマンスを最適化するために、Cisco では常にモニタ専用の設定を使用することを推奨しています。パッシブに展開されたデバイスはトラフィック フローに影響を与える可能性がないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成

ライセンス：Protection

ブロックリストとホワイトリストを作成するには、ネットワークオブジェクトとグループの任意の組み合わせに加え、セキュリティゾーン別に制約できるセキュリティインテリジェンスのフィードとリストを入力します。

デフォルトでは、アクセスコントロールポリシーは、任意のゾーンに適用する ASA FirePOWER モジュールのグローバルブロックしないリストおよびブロックリストを使用します。これらのリストは、アナリストによって入力されます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

（注） 入力したグローバル ブロックしないリストとブロックリストを使用するアクセス コントロール ポリシーは Protection ライセンスのないデバイスには適用できません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除**してからでないと**、ポリシーを適用できません。詳細については、グローバルブロックなしリストとブロックリストの操作を参照してください。

ブロックしないリストとブロックリストを作成した後は、ブロックした接続をログに記録できます。また、フィードとリストを含めてブロックした個々のオブジェクトをモニタのみに設定することもできます。これにより、システムはアクセス制御を使用してブロックした IP アドレスを含む接続を処理できるだけでなく、ブロックリストと一致する接続をログイに記録することもできます。

ブロックなしリスト、ブロックリスト、およびロギングのオプションを設定するには、アクセス コントロール ポリシーの [Security Intelligence] タブを使用します。このページには、ブロックなしリストまたはブロックリストのいずれかで使用できるオブジェクトのリスト（[Available Objects]）と、ブロックなしリストとブロックリストのオブジェクトの制約に使用できるゾーンのリスト（[Available Zones]）が表示されます。オブジェクトまたはゾーンのタイプは、異なるアイコンによって見分けられるようになっています。シスコのアイコンでマークされたオブジェクトは、インテリジェンス フィードの各種カテゴリを表します。

ブロックリストでは、ブロックするように設定されたオブジェクトはブロックアイコンでマークされ、モニタのみのオブジェクトはモニタアイコンでマークされます。ブロックなしリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブロックリストに登録されたオブジェクトに取り消し線が表示されます。

ブロックなしリストとブロックリストには、最大 255 個のオブジェクトを追加できます。つまり、ブロックなしリストのオブジェクトとブロックリストのオブジェクトを合計した数は 255 以下でなければなりません。

ネットマスク /0 のネットワークオブジェクトはブロックなしリストまたはブロックリストに追加できますが、ネットマスク /0 を使用したアドレスブロックは無視され、これらのアドレスに基づいたブロックなしリストおよびブロックリストフィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレスブロックも無視されます。すべてのトラフィックを監視またはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[Monitor] または [Block] ルール アクションでアクセス コントロール ルールを使用し、[Source Networks] および [Destination Networks] の [any] のデフォルト値をそれぞれ使用します。

アクセス コントロール ポリシーのセキュリティ インテリジェンスのブロックなしリストおよびブロックリストを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4 必要に応じて、ブロックされた接続をログに記録するには、ロギングアイコンをクリックします。

ロギングを有効にしてからでないと、ブロックされたオブジェクトをモニタのみに設定することはできません。詳細については、セキュリティ インテリジェンスによる判断のロギングを参照してください。

ステップ 5 1つ以上の使用可能なオブジェクトを選択して、ブロックなしリストとブロックリストの作成を開始します。

Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択し、右クリックして [Select All] を選択します。

ヒント リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、ブロックなしリストまたはブロックリストに追加するオブジェクトの検索 （7 ページ）を参照してください。

ステップ 6 オプションで、**使用可能なゾーン**を選択して、ゾーン別に選択したオブジェクトを制約します。

デフォルトでは、オブジェクトに制約はありません。つまり、オブジェクトのゾーンは [Any] に設定されます。[Any] を使用しない場合、制約の基準にできるゾーンは1つだけです。複数のゾーンでオブジェクトのセキュリティインテリジェンスフィルタリングを適用するには、ゾーンごとにオブジェクトをブロックなしリストまたはブロックリストに追加する必要があります。また、グローバルブロックなしリストまたはブロックリストをゾーンによって制約することはできません。

ステップ 7 **[Add to Do-Not-Block List]** または **[Add to Block List]** をクリックします。

また、オブジェクトをクリックして選択し、いずれかのリストにドラッグすることもできます。

選択したオブジェクトは、ブロックなしリストまたはブロックリストに追加されます。

ヒント オブジェクトをリストから削除するには、そのオブジェクトの削除アイコンをクリックします。Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択するか、または右クリックして [Select All]]を選択した後、右クリックして [Delete Selected] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ブロックなしリストまたはブロックリストからオブジェクトを削除しても、そのオブジェクトは ASA FirePOWER モジュールからは削除されません。

ステップ 8 オブジェクトをブロックなしリストまたはブロックリストに追加し終わるまで、ステップ ステップ 5 ～ ステップ 7 を繰り返します。

ステップ 9 必要に応じて、ブロックされたオブジェクトをモニタのみに設定するには、**[Add to Block List]** で該当するオブジェクトを右クリックし、[Monitor-only (do not block)] を選択します。

パッシブ展開環境の場合は、ブロックされたすべてのオブジェクトをモニタのみに設定することを推奨します。ただし、グローバルブロックリストをモニタのみに設定することはできません。

ステップ 10 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入を参照してください）。

ブロックなしリストまたはブロックリストに追加するオブジェクトの検索

ライセンス：Protection

複数のネットワークオブジェクト、グループ、フィード、およびリストを使用する場合は、検索機能を使用して、ブロックなしリストまたはブロックリストに追加するオブジェクトを絞り込むことができます。

リストに追加するオブジェクトを検索する方法：

[Search by name or value] フィールドにクエリを入力します。

入力すると、[Available Objects] リストが更新されて、一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上のリロードアイコンをクリックするか、検索フィールド内のクリアアイコンをクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば、Texas Office という名前で 192.168.3.0/24 という設定値を持つ個別ネットワーク オブジェクトがあり、そのオブジェクトが US Offices というグループ オブジェクトに含まれている場合、検索文字列の一部（Tex など）または全部を入力するか、3 などの値を入力することで、両方のオブジェクトを表示できます。