IPアドレスがCisco FireSIGHTシステムのセキュリティインテリジェンスによってブロックまたはブラックリストに登録される

内容

概要

セキュリティ インテリジェンス機能を使用すると、送信元または宛先 IP アドレスに基づいてネットワークをトラバースできるトラフィックを指定できます。これは、トラフィックがアクセス コントロール ルールによって分析される前に、特定の IP アドレスをブラックリストに入れる（トラフィックの送受信を拒否する）場合に特に役立ちます。このドキュメントでは、IP アドレスが Cisco FireSIGHT システムによってブロックされるかまたはブラックリストに登録される状況に対応する方法を説明します。

前提条件

要件

Cisco FireSIGHT Management Center に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco FireSIGHT Management Center
- Cisco FirePOWER アプライアンス

- Cisco ASA with Firepower（SFR）モジュール
- ソフトウェア バージョン 5.2 以降

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

インテリジェンス フィードとインテリジェンス リストの違い

FireSIGHT システムでセキュリティ インテリジェンス機能を使用する場合、次の 2 つの方法があります。

セキュリティ インテリジェンス フィード

セキュリティ インテリジェンス フィードは、Defense Center が、HTTP または HTTPS サーバからダウンロードする IP アドレスの動的なコレクションです。ブラックリストを作成するために、シスコは *セキュリティ インテリジェンス フィード*を提供しています。このフィードは Vulnerability Research Team（VRT）によってレピュテーションが低いと判断された IP アドレスを表しています。

セキュリティ インテリジェンス リスト

フィードとは対照的に、セキュリティ インテリジェンス リストは、手動で FireSIGHT Management Center にアップロードする IP アドレスの簡単な静的リストです。

正規 IP アドレスがブロックされるまたはブラックリストに登録される

IP アドレスがセキュリティ インテリジェンス フィードに含まれているかどうかの検証

IP アドレスがセキュリティ インテリジェンス フィード ブラックリストによりブロックされる場合は、次の手順に従って検証できます。

ステップ 1：FirePOWER アプライアンスまたはサービス モジュールの CLI にアクセスします。

ステップ 2：次のコマンドを実行します。<IP_Address> を、検索対象の IP アドレスに置き換えます。

```
admin@Firepower:~$ grep
```

たとえば、IP アドレス 198.51.100.1 を検索する場合は次のコマンドを実行します。

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```
このコマンドから指定した IP アドレスに一致するものが返される場合、その IP アドレスがセキュリティ インテリジェンス フィード ブラックリストに含まれています。

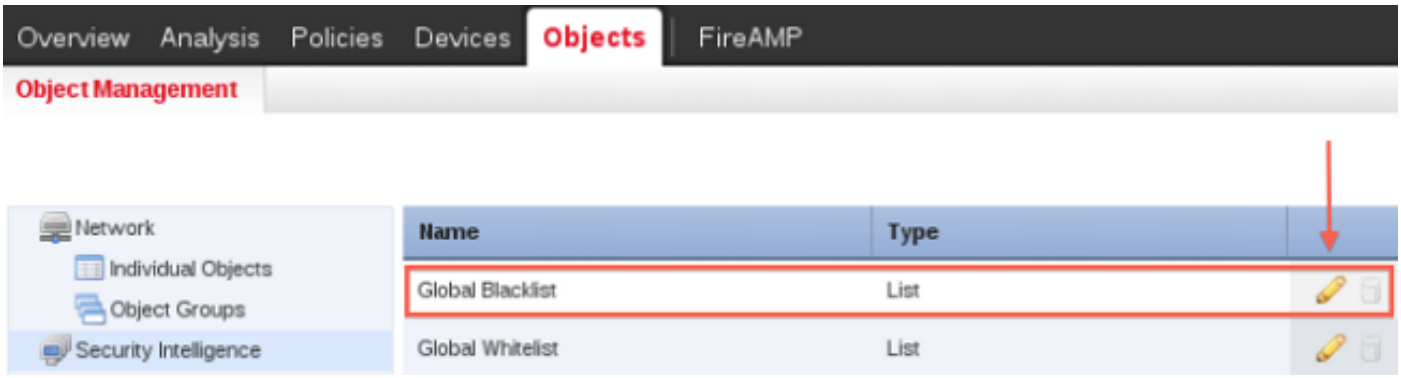
ブラックリストの確認

ブラックリストに登録されている IP アドレスのリストを見つけるには、次の手順を実行します。

ステップ 1：FireSIGHT Management Center の Web インターフェイスにアクセスします。

ステップ 2：[Objects] > [Object Management] > [Security Intelligence] に移動します。

ステップ 3：[鉛筆] アイコンをクリックして [Global Blacklist] **を開き、このブラックリストを編集します。**一連の IP アドレスがポップアップ ウィンドウに表示されます。



ブロックされた IP アドレスまたはブラックリストに登録された IP アドレスの処理

特定の IP アドレスがセキュリティ インテリジェンス フィードによってブロックされるかまたはブラックリストに登録されている場合、次のオプションを検討できます。

オプション 1：セキュリティ インテリジェンス ホワイトリスト

セキュリティ インテリジェンスによりブラックリストに登録された IP アドレスをホワイトリストに登録できます。ホワイトリストはブラックリストよりも優先されます。FireSIGHT システムは、送信元または宛先の IP アドレスがホワイトリストに登録されているトラフィックは、たとえそれらの IP アドレスがブラックリストにも登録されているとしても、そのトラフィックをアクセス コントロール ルールを使用して評価します。したがって、ブラ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、ホワイトリストを使用できます。

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たものの、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、そのフィード全体をブラ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 アドレスだけをホワイトリストに登録するという方法を取ることができます。

> **注意**：アクセス コントロール ポリシーを変更したら、ポリシーを管理対象デバイスに再適用する必要があります。

オプション 2：セキュリティ ゾーンに基づいてセキュリティ インテリジェンス フィルタを適用する

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。

上述のホワイトリストの例を拡張するとしたら、不適切に分類された IP アドレスをホワイトリストに登録した後、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、ホワイトリストの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、ホワイトリストに登録された 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ラックリスト登録することも考えられます。

オプション 3：ブラックリストへの登録ではなくモニタを行う

特定のIPアドレスまたはアドレスのセットをブラックリストに登録したいかどうか不明な場合は、「モニタ専用」設定を使用して、一致する接続をアクセスコントロールルールに渡し、ブラックリストへの一致も記録できます。注意する点として、グローバル ブラックリストをモニタ専用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。

「モニタ専用」設定を使用してセキュリティ インテリジェンスを設定する手順：

1. アクセス コントロール ポリシーの [Security Intelligence] **タブで、ロギング アイコンをクリックします。**[Blacklist Options] ダイアログボックスが表示されます。
2. トラフィックがセキュリティ インテリジェンスの条件に一致した場合に接続開始イベントをログに記録するには、[Log Connections] **チェックボックスをオンにします。**
3. 接続イベントの送信先を指定します。
4. [OK] をクリックしてロギング オプションを設定します。[Security Intelligence] タブが再表示されます。
5. [Save] をクリックします。変更を反映するには、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。

オプション 4：Cisco Technical Assistance Center へ問い合わせる

次に該当する場合は、いつでも Cisco Technical Assistance Center（TAC）に問い合わせることができます。

- 前述のオプション 1、2、3 に関して疑問点がある。
- セキュリティ インテリジェンスによりブラックリストに登録された IP アドレスについてさらに調査、分析を行いたい。
- セキュリティ インテリジェンスにより IP アドレスがブラックリストに登録された理由を確認したい。