セキュリティ インテリジェンス ブラックリスト

以下のトピックでは、セキュリティインテリジェンスの概要（トラフィックのブラックリストとホワイトリストの使用、基本設定など）を示します。

セキュリティ インテリジェンスについて

悪意のあるインターネットコンテンツに対する防御の前線として、セキュリティインテリジェンスは疑わしい IP アドレス、URL、ドメイン名が関連する接続をレピュテーション インテリジェンスを使用して迅速にブロックします。これは、セキュリティ インテリジェンス ブラックリスト登録と呼ばれます。

セキュリティインテリジェンスはアクセス制御の初期のフェーズであり、大量のリソースを消費する評価をシステムが実行する前に行われます。ブラックリスト登録により、インスペクションの必要がないトラフィックを迅速に除外することで、パフォーマンスが向上します。

（注） FastPath が適用されたトラフィックをブラックリストに登録することはできません。8000 シリーズの FastPath 適用およびプレフィルタ評価は、セキュリティインテリジェンスによるフィルタリングの前に行われます。FastPath が適用されたトラフィックは、セキュリティインテリジェンスを含め、以降のすべての評価をバイパスします。

カスタム ブラックリストを設定することはできますが、CIsco は定期的に更新されるインテリジェンスフィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。

セキュリティインテリジェンスのブラックリスト登録を改良するには、ホワイトリストとモニタ専用ブラックリストを併せて使用するという方法があります。これらのメカニズムは、トラフィックをブラックリストに登録しないようにしますが、一致するトラフィックを自動的に信頼したり FastPath を適用したりすることは**しません**。ホワイトリストに登録されたトラフィックや、セキュリティインテリジェンスの段階でモニタされるトラフィックは、意図的に残りのアクセス コントロールによる分析が適用されます。

関連トピック

セキュリティ インテリジェンスのリストとフィード
設定可能な接続ロギング
接続およびセキュリティ インテリジェンス イベント テーブルの使用

セキュリティ インテリジェンスのための要件

特定の IP アドレス、URL、ドメイン名をホワイトリストまたはブラックリストに登録したりモニタしたりするためには、カスタム オブジェクト、リスト、またはフィードを設定する必要があります。次の選択肢があります。

- ネットワーク、URL、DNS フィールドを設定するには、セキュリティ インテリジェンス フィードの作成を参照してください。
- ネットワーク、URL、DNS リストを設定するには、セキュリティ インテリジェンス リストの更新を参照してください。
- ネットワーク オブジェクトとオブジェクト グループを設定するには、ネットワーク オブジェクトの作成を参照してください。
- URL オブジェクトとオブジェクト グループを設定するには、URL オブジェクトの作成を参照してください。

DNS リストまたはフィードに基づくトラフィックのブラックリスト/ホワイトリスト登録あるいはモニタリングには、以下の条件もあります。

- DNS ポリシーを作成します。詳細については、基本 DNS ポリシーの作成を参照してください。
- DNS リストまたはフィードを参照する DNS ルールを設定します。詳細については、DNS ルールの作成および編集を参照してください。

DNS ポリシーはアクセス コントロール ポリシーの一部として展開するため、両方のポリシーを関連付ける必要があります。詳細については、DNS ポリシーの展開を参照してください。

セキュリティ インテリジェンスのガイドライン

セキュリティ インテリジェンス戦略では、次の要素を使用します。

- Cisco 提供のフィード：Cisco では、定期的に更新されるインテリジェンス フィードへのアクセスを提供しています。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表すサイトは目まぐるしく現れては消えるため、カスタム設定を更新して導入するのでは最新の状況に追いつきません。
- サードパーティのフィード：Cisco 提供のフィードをサードパーティのフィードで補完できます。これらのフィードは、Firepower Management Center が定期的にインターネットからダウンロードする動的リストです。
- グローバルおよびカスタム ブラックリスト：特定の IP アドレス、URL、ドメイン名をブラックリストに登録します。パフォーマンスを向上させるために、スパムのブラックリスト登録を電子メール トラフィックを処理するセキュリティ ゾーンに制限するなどして、適用対象を絞り込むこともできます。
- 誤検出をなくすためのホワイトリスト：ブラックリストの範囲が広すぎる場合、または残りのアクセス コントロールでさらに分析するトラフィックを前もってブロックしてしまう場合は、ブラックリストをカスタム ホワイトリストでオーバーライドできます。
- ブラックリスト登録に代わるモニタリング：特にパッシブ展開や、フィードを実装する前にテストする場合に有用です。違反しているセッションをブロックする代わりに単にモニタしてログに記録し、接続終了イベントを生成できます。

（注） 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、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管理対象デバイスはトラフィック フローに影響を与えることができないため、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。

例：ホワイトリスト登録

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は、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。

例：ゾーンを使用したセキュリティ インテリジェンス

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、組織内でそれらの 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 ゾーンにより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 URL にアクセスできます。あるいは、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という方法もあります。

例：モニタ専用のブラックリスト登録

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。

セキュリティ インテリジェンスの設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
脅威	保護	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

各アクセス コントロール ポリシーには、セキュリティ インテリジェンス オプションがあります。ネットワーク オブジェクト、URL オブジェクトとリスト、およびセキュリティ インテリジェンス フィードとリストをホワイトリストまたはブラックリストに追加でき、これらはすべてセキュリティ ゾーンによって制約できます。アクセス コントロール ポリシーに DNS ポリシーを関連付け、ドメイン名をホワイトリストまたはブラックリストに追加することもできます。

ホワイトリスト内のオブジェクトの数とブラックリスト内の数の合計が、255 個のネットワーク オブジェクトまたは 32767 個の URL オブジェクトとリストを超えることはできません。

（注） システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

注意 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（Security Intelligence）] タブからホワイトリストまたはブラックリストに複数のオブジェクトを追加したり、複数のオブジェクトを削除したりします。設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲット デバイスがトラフィックを処理する方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。Snort プロセスが再起動するかどうかは、インスペクションに使用できるメモリに応じて、デバイスごとに異なる場合があることに注意してください。

始める前に

パッシブ展開の場合、またはモニタのみにセキュリティ インテリジェンス フィルタリングを設定する場合は、ロギングを有効にします。セキュリティインテリジェンスによる接続のロギングを参照してください。

手順

ステップ 1 アクセス コントロール ポリシー エディタで、[セキュリティ インテリジェンス（Security Intelligence）] タブをクリックします。

コントロールが淡色表示されている場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。設定がロック解除されている場合は、[ベース ポリシーから継承する（Inherit from base policy）] をオフにして、編集を有効にします。

ステップ 2 次の選択肢があります。

- [ネットワーク（Networks）] タブをクリックして、ネットワーク オブジェクトを追加します。
- [URL（URLs）] タブをクリックして、URL オブジェクトを追加します。

ステップ 3 ホワイトリストまたはブラックリストに追加する利用可能なオブジェクトを探します。次の選択肢があります。

- [名前または値で検索（Search by name or value）] フィールドに入力して、利用可能なオブジェクトを検索します。[リロード（reload）]（）または [クリア（clear）]（）をクリックして、検索文字列をクリアします。
- 既存のリストまたはフィードがニーズを満たしていない場合は、追加アイコン（）をクリックし、[新規ネットワーク リスト（New Network List）] または [新規 URL リスト（New URL List）] を選択し、セキュリティ インテリジェンス フィードの作成または新しいセキュリティ インテリジェンス リストの Firepower Management Center へのアップロードの説明に従って続行します。

- 既存のオブジェクトがニーズを満たしていない場合は、追加アイコン（  ）をクリックし、[新規ネットワーク オブジェクト（New Network Object）] または [新規 URL オブジェクト（New URL Object）] を選択し、ネットワーク オブジェクトの作成の説明に従って続行します。

セキュリティ インテリジェンスは、/0 ネットマスクを使用して、IP アドレス ブロックを無視します。

ステップ 4 追加する 1 つ以上の**利用可能なオブジェクト**を選択します。

ステップ 5 （オプション）[利用可能なゾーン（Available Zone）] を選択して、選択したオブジェクトをゾーンごとに制約します。

システムが提供するセキュリティ インテリジェンス リストをゾーンで制約することはできません。

ステップ 6 [ホワイトリストに追加（Add to Whitelist）] または [ブラックリストに追加（Add to Blacklist）] をクリックするか、選択したオブジェクトをクリックしていずれかのリストにドラッグします。

ホワイトリストまたはブラックリストからオブジェクトを削除するには、その削除アイコン（  ）をクリックします。複数のオブジェクトを削除するには、オブジェクトを選択し、右クリックして [選択項目の削除（Delete Selected）] を選択します。

ステップ 7 （オプション）ブラックリスト登録されたオブジェクトをモニタ専用に設定するには、[ブラックリスト（Blacklist）] にリストされている該当するオブジェクトを右クリックし、[モニタ専用（ブロックしない）（Monitor-only (do not block)）] を選択します。

システムが提供するセキュリティ インテリジェンス リストをモニタ専用に設定することはできません。

ステップ 8 [DNS ポリシー（DNS Policy）] ドロップダウン リストから DNS ポリシーを選択します。DNS ポリシーの概要 を参照してください。

ステップ 9 [保存（Save）] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

関連トピック

セキュリティ インテリジェンスのリストとフィード

Snort® の再起動シナリオ

セキュリティ インテリジェンス オプション

アクセス制御ポリシーエディタのセキュリティインテリジェンスタブを使用して、ネットワーク（IP アドレス）と URL セキュリティ インテリジェンスを設定し、アクセス制御ポリシーを DNS ポリシーに関連付けます。

オブジェクト、ゾーン、ブラックリスト アイコン

アクセス制御ポリシー エディタのセキュリティ インテリジェンス タブで、オブジェクトまたはゾーンのそれぞれのタイプを別のアイコンと区別します。

ブラックリストでは、ブロックに設定したオブジェクトにはブロック アイコン（）を付け、監視対象のみのオブジェクトには、監視アイコン（）を付けます。監視のみの場合には、アクセス制御を使用して、ブラックリストの IP アドレスと URL を含む接続を処理し、ブラックリストに一致する接続をロギングします。

ホワイト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、ブラックリスト登録されたオブジェクトに取り消し線が表示されます。

ゾーンの制約

システムが提供したグローバル リスト以外、ゾーンごとにセキュリティ インテリジェンス フィルタリングを制約できます。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、ゾーンのそれぞれについて、オブジェクトをホワイトリストまたはブラックリストに追加する必要があります。

ログ

デフォルトで有効になっているセキュリティ インテリジェンス ロギングは、アクセス制御ポリシー対象のデバイスが処理するブロックされ、監視対象である接続はすべてロギングされます。ただし、システムはホワイトリストの一致はロギングしません。ホワイトリストに登録された接続のロギングは、その接続の最終的な傾向によって異なります。ブラックリストの接続については、ブラックリスト対象のオブジェクトを監視のみに設定する前にロギングを有効にする必要があります。

セキュリティ インテリジェンス カテゴリ

セキュリティ インテリジェンス カテゴリ	説明
Attacker	アクティブ スキャナと悪意のある発信アクティビティが知られているブラックリストのホスト。
Bogon	Bogon ネットワークおよび割り当てられていない IP アドレス
Bots	バイナリ マルウェア ドロッパを有するサイト
CnC	botnets 用のホスト C & C サーバを有するサイト

セキュリティインテリジェンス カテゴリ	説明
Dga	C＆Cサーバのランデブー ポイントとして機能するさまざまなドメイン名を生成するために使用されるマルウェア アルゴリズム
Exploitkit	クライアントのソフトウェアの脆弱性を特定するために設計されたソフトウェア キット
Malware	マルウェアバイナリまたはエクスプロイト キットを有するサイト
OpenProxy	匿名の web ブラウジングが可能な公開プロキシ
OpenRelay	スパム用に使用されることが既知のオープン メール リレー
Phishing	フィッシング ページを有するサイト
応答	悪意があるか疑わしいアクティブに積極的に参加している IP アドレスと URL
Spam	スパムを送信することが知られているメール ホスト
Suspicious	疑いがあり、既知のマルウェアと同様の特性を持つようなファイル
TorExitNode	Tor exit ノード

関連トピック

[今すぐブラックリストに登録（Blacklist Now）]、[今すぐホワイトリストに登録（Whitelist Now）]、およびグローバル リスト
セキュリティ インテリジェンス リストとマルチテナンシー

セキュリティインテリジェンスのトラブルシューティング

メモリ使用のトラブルシューティング

症状：セキュリティ インテリジェンスによってブラックリストに登録される必要がある接続が、代わりにアクセス コントロール ルールによって評価されます。セキュリティインテリジェンスのヘルス モジュールにより、メモリ不足であることが警告されています。

原因：メモリの制限です。シスコのインテリジェンス フィードは、Cisco Talos Security Intelligence and Research Group（Talos）の最新の脅威インテリジェンスに基づいています。このフィードは、時間が経つにつれてサイズが大きくなる傾向があります。FirePOWER デバイスがフィード更新を受信すると、セキュリティインテリジェンス用に割り当てられたメモリに可能な限り多くのエントリがロードされます。デバイスがすべてのエントリをロードできない場合は、想

定どおりにトラフィックがブロックされないことがあります。ブラックリストに登録する必要がある一部の接続は、代わりに引き続きアクセスコントロールルールによって評価されます。

影響を受けるプラットフォーム：低メモリ デバイスでは、特に多数のセキュリティ インテリジェンス カテゴリをブラックリストに登録している場合や、カテゴリおよびレピュテーションに基づいて URL をフィルタリングしている場合に、この問題が発生する可能性が高くなります。これらのデバイスには、Firepower 7010、7020、および 7030、ASA 5506-X、5508-X、5516-X、5512-X、5515-X、および 5525-X、NGIPSv が含まれます。

回避策：この問題が発生していると思われる場合は、影響を受けるデバイスに設定を再展開します。これにより、セキュリティインテリジェンスにより多くのメモリを割り当てることができます。問題が解決しない場合は、Cisco Technical Assistance Center（TAC）にお問い合わせください。問題の確認と、展開に適したソリューションの提案に役立つことができます。