ファイル ポリシーと高度なマルウェア防御

次のトピックでは、ファイル制御、ファイル ポリシー、ファイル ルール、AMP クラウド接続、および動的分析接続の概要を示します。

ファイル ポリシーと高度なマルウェア防御について

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減しやすくするため、高度なマルウェア防御（ネットワーク向け *AMP*、以前は *AMP for Firepower* と呼ばれていました）によって、ネットワーク トラフィックでのマルウェアの伝送を検出、追跡、保存、分析、および必要に応じてブロックできます。

ネットワーク向け AMPおよびファイル制御（ファイルにマルウェアが含まれているかどうかにかかわらず、特定のタイプのすべてのファイルを制御できます）をアクセス コントロール設定全体の一部として設定します。作成してアクセス コントロール ルールに関連付けたファイル ポリシーは、ルールに一致するネットワーク トラフィックを処理します。そのトラフィックで検出されたファイルをダウンロードし、ローカルマルウェア分析を実行して、ファイルにマルウェアが含まれているかどうかを判断できます。また、ファイルを動的分析のために AMP Threat Grid クラウドに送信して、そのファイルがマルウェアを表しているかどうかを判断できます。

アクティブ ファイル ポリシーのファイル イベント、マルウェア イベント、および取得されたファイル ロギングが自動的に有効になります。また、ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは関連する接続の終了を Firepower Management Center データベースに自動的に記録します。

（注） NetBIOS-ssn（SMB）トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワーク ファイル トラジェクトリ（network file trajectory）] ページを使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ヒント 組織で AMP for Endpoints を使用している場合は、システムで、ネットワーク向け AMP によって収集されたデータとともにエンドポイントベースのデータをインポートして表示できます。このデータのインポートには、ライセンスは必要ありません。

組織で追加のセキュリティが必要であるか、外部接続を制限する場合は、Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を使用します。AMPv は個別に AMP for Endpoints イベントを収集し、Firepower Management Center に転送します。

ファイル制御および Cisco AMP の基本

ネットワーク向け AMP

ネットワーク向け AMP では、インライン展開された管理対象デバイスを使用して、ネットワーク上のマルウェアを検出、保存、追跡、分析、およびブロックできます。ネットワーク向け AMP は、PDF、Microsoft Office ドキュメントを含め、多くのタイプのマルウェア ファイルをブロックできます。

ファイルの検出と保存

ネットワーク向け AMP により、管理対象デバイスは、特定のファイル タイプの送信のネットワーク トラフィックをモニタします。

デバイスが対象のファイルを検出すると、ファイルの SHA-256 ハッシュ値を Firepower Management Center に送信します。Firepower Management Center は、マルウェア クラウド ルックアップを実行し、AMP クラウドでファイルの性質をクエリします。デバイスは、ファイル ストレージ機能を使用して、ハードドライブまたはマルウェアのストレージ パックに対象ファイルを保存できます。キャプチャしたファイル情報は、[分析（Analysis）]>[ファイル（files）]>[キャプチャしたファイル（Captured Files）] で表示し、コピーをオフライン分析用にダウンロードすることができます。

ファイル分析

システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイルインスペクションと分析のいくつかの方法が適用されます。

（注） 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウドルックアップの結果を待機するか、または、クラウドルックアップの結果を待機せずにファイルを通過させることができます。

ファイルルールでオプションを有効にするかどうかに基づいて、システムは次の順序でファイルを検査します。

Spero 分析

ファイルが対象の実行可能ファイルの場合、デバイスはファイル構造を分析し、結果として得られた Spero シグネチャを AMP Threat Grid クラウドに送信できます。クラウドは、このシグネチャを使用して、ファイルにマルウェアが含まれるかを判断します。

ローカル マルウェア分析

ローカル マルウェア インスペクション エンジンを使用して、デバイスは対象ファイルを調べ、ファイルにマルウェアが含まれる場合、ファイルルールでそのように設定されていればこのファイルをブロックし、マルウェア イベントを生成します。

また、デバイスにより、ファイルプロパティ、組み込みオブジェクト、および可能性のあるマルウェアの詳細情報を含むファイル構成レポートが生成されます。

動的分析

デバイスが、マルウェアの可能性があるとしてファイルを事前分類している場合、デバイスがファイルを保存するかどうかに関係なく、これらのファイルを AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスに動的分析のために送信します。

AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスは、悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、クラウドが脅威スコアを割り当てた理由を詳細に説明する動的分析のサマリー レポートを表示できます。

ファイルとマルウェア イベント、およびキャプチャ ファイル

ファイル分析結果に基づいて、キャプチャされたファイル、生成されたマルウェアとファイルイベントを、[分析（Analysis）]>[ファイル（Files）]オプションで使用可能なページの表を使用して確認することができます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。また、ファイルがネットワークをどのように通過するか（ホストを通過するか）を示すマップ、およびさまざまなファイル プロパティを表示する、ネットワーク ファイル トラジェクトリにアクセスできます。

アーカイブ ファイル

システムは、ファイルがアーカイブ（.rar または .zip アーカイブ ファイルなど）の場合、一番外側のアーカイブ ファイル（レベル 0）の下の最大 3 レベルのネストされたファイルを検査できます。アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] と同じ大きさのアーカイブ ファイルまで検査できます。

ブロック アクションを含むファイル ルールにいずれかの個別ファイルが一致する場合は、その個別ファイルだけでなくアーカイブ全体がブロックされます。また、指定したネストのレベルを超えるアーカイブ、またはそのコンテンツが暗号化されているか検査できないアーカイブも、ブロックされることがあります。

ファイル トラッキング

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA-256 値をファイル リストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイル ポリシーに応じてクリーン リストまたはカスタム検出リストを使用できます。

（注） ファイル ポリシーで、マルウェア クラウド ルックアップを実行するか、一致ファイルでマルウェアをブロックしてファイルの SHA-256 値を計算するルールを設定する必要があります。

関連トピック

ファイル リスト

マルウェアの性質

システムは、AMP クラウドから返される性質に基づいてファイルの性質を決定します。パフォーマンスを改善するために、SHA-256 値に基づいてファイルの性質がシステムですでにわかっている場合、Firepower Management Center は AMP クラウドでクエリを行う代わりに、キャッシュ済みの性質を使用します。システムは、ファイルの性質に基づいてファイルをブロックすることもできます。アーカイブ ファイル内にネストされているファイルが 1 つでもブロックされる場合、システムはアーカイブ ファイル全体をブロックします。

ファイル リストへの追加操作の結果、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- マルウェア（Malware）：ファイルが AMP クラウドでマルウェアと分類されていること、ローカル マルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイル ポリシーに定義されたマルウェアのしきい値を超えたこと示します。

- [クリーン（Clean）]：AMPクラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明（Unknown）：システムはAMPクラウドでファイルの性質をクエリしましたが、ファイルには性質が割り当てられていませんでした。言い換えると、AMP クラウドがファイルを分類できませんでした。
- カスタム検出（Custom Detection）：ユーザがカスタム検出リストにファイルを追加したことを示します。
- 利用不可（Unavailable）：システムが AMP クラウドでクエリを行えなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。

アーカイブ ファイルの性質は、アーカイブ内部のファイルに割り当てられた性質に基づきます。識別されたマルウェア ファイルを含んでいる**すべて**のアーカイブは、マルウェア（Malware）の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブの場合、不明なファイルが 1 つでも含まれていれば 不明（Unknown）の性質、クリーン ファイルのみが含まれていれば クリーン（Clean）の性質になります。

表 *1*：内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
不明	1 つ以上	任意（Any）	[0]
クリーン（Clean）	[0]	1 つ以上	[0]
マルウェア（Malware）	任意（Any）	任意（Any）	1 つ以上

他のファイルと同様に、アーカイブ ファイルにも、該当する性質に関する条件が適用される場合はカスタム検出（Custom Detection）または利用不可（Unavailable）の性質が割り当てられます。

ヒント 短時間で利用不可（Unavailable）マルウェア イベントが連続して発生した場合は、Firepower Management Center が AMP クラウドに接続できることを確認してください。

ファイルの性質は変更される可能性があることに注意してください。たとえば、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。前の週にクエリを行ったファイルの性質が変更された場合、AMP クラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

AMP クラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカル マルウェア分析によって割り当てられた性質には、存続可能時間（TTL）が設定されます。性質

が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン：4 時間
- 不明：1 時間
- マルウェア：1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムは AMP クラウドに新しい性質を再びクエリします。

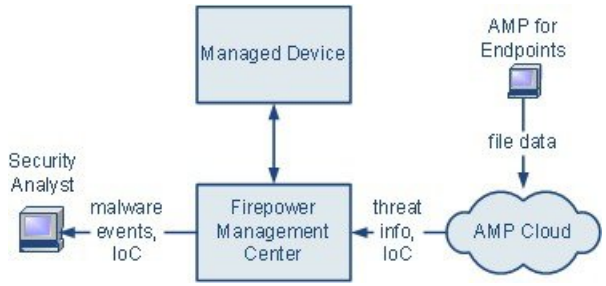
AMP for Networks を使用しないファイル制御

マルウェア ファイル伝送のブロックに加えて、（マルウェアを含むかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により防御網を広げることができます。AMP for Networks の場合と同様に、管理対象デバイスはネットワーク トラフィック内で特定のファイル タイプの伝送をモニタし、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御は AMP for Networks とは異なり、AMP クラウドへの照会を必要としないことに注意してください。

エンドポイント向け AMP

エンドポイント向け AMP は、シスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。次の図に、エンドポイント向け AMP を使用した場合の一般的な情報フローを示します。



所属部門がエンドポイント向け AMP を使用している場合、個々のユーザはエンドポイント（つまり、コンピュータやモバイル デバイス）に軽量コネクタをインストールします。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタは AMP クラウドと通信して、検査対象のファイルにマルウェアが含まれるかどうかを判断します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Center に送ります。さらに AMP クラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータを Firepower Management Center に送信することもできます。Firepower Management Center はこれらの情報をマルウェア イベントとしてログに記録します。

エンドポイント向け AMP は、ホストのセキュリティに感染の疑いがある場合、侵害の兆候（IOC）を生成することができます。Firepower システムでは、モニタ対象ホストの IOC 情報が表示できます。シスコでは折にふれて、エンドポイントベースのマルウェア イベントに対応する新しい IOC タイプの開発を行っており、システムにより自動的にダウンロードされます。

エンドポイント向け AMP では、マルウェア イベントに基づいて Management Center で開始される修復やアラートを設定できるだけでなく、エンドポイント向け AMP 管理コンソールを使ってマルウェアの影響を軽減することもできます。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け AMP 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。次の操作を実行できます。

- 部門全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイク コントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーション ブロッキング、除外リストなど
- カスタム保護の作成、グループ ポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成

ヒント エンドポイント向け AMP の詳細については『AMP for Endpoints management console』を参照してください。

AMP for Endpoints との統合を設定し、コンソールにアクセスするには、次を参照してください。

- AMP for Endpoints クラウド接続の設定 （26 ページ）
- AMP for Endpoints 管理コンソールへのアクセス （29 ページ）

ネットワーク向け AMP と AMP for Endpoints の比較

FirePOWER システムは、ネットワーク向け AMP および AMP for Endpoints のどちらのデータも使用できます。

管理対象デバイスはネットワーク トラフィックのマルウェアを検出しますが、エンドポイント向け AMP のマルウェア検出はダウンロード時または実行時にエンドポイントで行われるため、この 2 種類のマルウェア イベントの情報は異なります。たとえば、エンドポイント ベースの

マルウェア イベントには、ファイル パス、呼び出し元クライアント アプリケーションなどの情報が含まれるのに対して、ネットワーク トラフィックでのマルウェア検出には、ファイル伝送に使われた接続のポート、アプリケーション プロトコル、発信元 IP アドレス情報が含まれます。

別の例としては、ネットワークベースのマルウェア イベントの場合、ユーザ情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザを示すことが挙げられます。一方、エンドポイント向け AMP で報告されるユーザは、マルウェアが検出されたエンドポイントに現在ログインしているユーザを示します。

（注） 展開に応じて、AMP for Endpoints によってモニタされるエンドポイントは AMP for Networks でモニタされるものと同じホストにならない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、2 つの戦略の違いをまとめます。

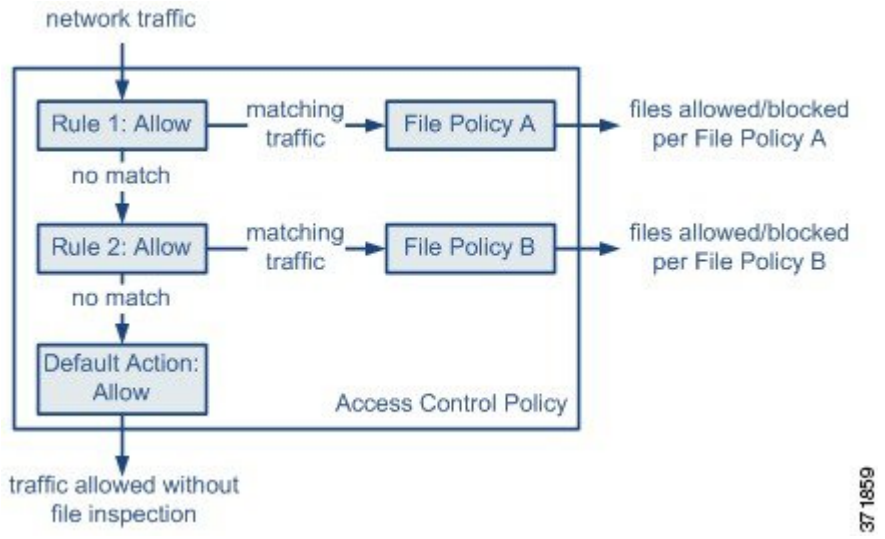
表 *2:* ネットワークベースとエンドポイントベースの高度なマルウェア防御戦略の比較

機能	ネットワーク向け AMP	エンドポイント向け AMP
ファイルタイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックで、アクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイントで、AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査する）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ
マルウェア分析の選択肢	Management Center ベース、および AMP クラウドでの分析	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロッキング、Management Center が開始する修復	エンドポイント向け AMP ベースの検疫およびアウトブレイク コントロール オプション、Management Center が開始する修復

機能	ネットワーク向け AMP	エンドポイント向け AMP
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェアイベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェアイベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	Management Center ベース	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
必要なライセンスまたはサブスクリプション	ファイル制御およびネットワーク向け AMP の実行に必要なライセンス	エンドポイント向け AMP サブスクリプション（ライセンスベースではありません）

ファイル ポリシー

ファイル ポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス コントロール 設定の一部としてこれを使用して、ネットワーク向け AMP とファイル制御を実行できます。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、インライン展開での単純なアクセス コントロール ポリシーがあるとします。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションも

また「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- ルール 1 に一致するトラフィックはファイル ポリシー A で検査されます。
- ルール 1 に一致しないトラフィックはルール 2 に照らして評価されます。ルール 2 に一致するトラフィックはファイル ポリシー B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

1 つのファイル ポリシーを、[許可（Allow）]、[インタラクティブ ブロック（Interactive Block）]、または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイルポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。

異なるファイルポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、アクセス コントロールのデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。

ファイル ポリシーの詳細設定

詳細なファイル インスペクションの設定に関する注意事項

ファイル ポリシーでは、詳細なオプションを設定して、カスタム検出リストのファイルのブロック、クリーン リストのファイルの許可、およびファイルがマルウェアと見なされる脅威スコアのしきい値の設定を行うことができます。

また、組織のニーズに合わせてアーカイブ ファイルを分析し、ブロックできるように、アーカイブ ファイルの内容を検査するようにファイルポリシーを設定できます。圧縮解除されたファイルに適用できるすべての機能（動的分析やファイル ストレージなど）は、アーカイブ ファイル内のネストされたファイルに使用可能です。

アーカイブ ファイルのインスペクションに関する注意事項

一部のアーカイブ ファイルには、追加のアーカイブ ファイル（など）が含まれています。ファイルがネストされるレベルは、そのアーカイブ ファイルの深さです。トップレベルのアーカイブ ファイルは深さの数で考慮されないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。

システムでは、ネストされたアーカイブ ファイルを最大 3 レベルまでしか検査できませんが、その深さ（または指定したそれより低い最大深さ）を超えるアーカイブ ファイルをブロックするようファイルポリシーを設定できます。ネストされたアーカイブをさらに制限する場合は、2 または 1 のより低い最大ファイル深さを設定するオプションがあります。

最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニタ対象のトラ

フィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

（注） アーカイブ ファイルを含むトラフィックがセキュリティ インテリジェンスによってブラックリスト登録またはホワイトリスト登録された場合、またはトップレベルのアーカイブ ファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブ ファイルの内容を検査しません。ネストされたファイルがブラックリスト登録された場合、アーカイブ全体がブロックされます。しかし、ネストされたファイルがホワイトリスト登録された場合、アーカイブは自動的に渡されません（他のネストされたファイルおよび特性による）。

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、[分析（Analysis）] > [ファイル（Files）] メニューのページにあるコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、アーカイブ ファイルがファイル イベント、マルウェア イベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイル コンテンツは表形式でリストされます。そのリストには、名前、SHA-256 ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワーク ファイル トラジェクトリ アイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] と同じ大きさのアーカイブ ファイルまでのみ検査できることに注意してください。

ファイル ポリシー設定に関する注意事項と制約事項

- 新しいポリシーの場合、ポリシーが使用中でないことが Web インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数が Web インターフェイスに示されます。どちらの場合も、テキストをクリックすると [アクセス コントロール ポリシー（Access Control Policies）] ページに移動できます。
- FTP に関する [マルウェア ブロック（Block Malware）] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ（Drop when Inline）] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイル転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[インライン時にドロップ（Drop when Inline）] を有効にした侵入ポリシーを選択する必要があります。

ファイル ポリシーの管理

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
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin/Access Admin

[ファイル ポリシー（File Policies）] ページには、既存のファイル ポリシーが最終更新日とともに表示されます。このページは、ファイル ポリシーの管理に使用できます。

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

（注） 動的分析の対象になるファイル タイプのリストが更新されたかどうか検査するために、システムは AMP クラウドをチェックします（多くても 1 日に 1 回）。対象になるファイル タイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに展開されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新したファイル ポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）]** を選択します。

ステップ 2 ファイル ポリシーを管理します。

- [比較（Compare）] : [ポリシーの比較（Compare Policies）] をクリックします（ポリシーの比較 を参照）。
- 作成：ファイル ポリシーを作成するには、[新規ファイル ポリシー（New File Policy）] をクリックし、ファイル ポリシーの作成 （13 ページ） で説明する手順を実行します。
- コピー：ファイルポリシーをコピーするには、コピーアイコン（  ）をクリックします。

  代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除：ファイル ポリシーを削除するには、削除アイコン（  ）をクリックし、プロンプトが表示されたら o と [OK] 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、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 展開：[展開（Deploy）] をクリックします（設定変更の展開 を参照）。
- 編集：既存のファイルポリシーを変更するには、編集アイコン（）をクリックします。
- [レポート（Report）]：レポート アイコン（）をクリックします（現在のポリシー レポートの生成 を参照）。

ファイル ポリシーの作成

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
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin/Access Admin

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）]** を選択します。

ヒント 既存のファイル ポリシーのコピーを作成するには、コピー アイコン（）をクリックして、表示されるダイアログボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ステップ 2 [新しいファイル ポリシー（New File Policy）] をクリックします。

ステップ 3 新しいポリシーの [名前（Name）] とオプションの [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ファイル ルールの作成 （23 ページ）の説明に従って、ファイル ポリシーに 1 つ以上のルールを追加します。

ステップ 6 必要に応じて、[詳細（Advanced）] タブを選択し、詳細オプションおよびアーカイブ ファイル検査オプション （14 ページ）の説明に従って詳細オプションを設定します。

ステップ 7 ファイル ポリシーを保存します。

次のタスク

- ファイル制御およびマルウェア保護のためのアクセス コントロール ルールの設定の説明に従って、アクセス コントロール ルールにファイル ポリシーを追加します。
- 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。

詳細オプションおよびアーカイブ ファイル検査オプション

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次の一般オプションがあります。

- [初回ファイル分析（First Time File Analysis）]：システムで初めて検出するファイル分析のためのファイルを送信します。ファイルは、マルウェア クラウドルックアップと Spero 分析、ローカルマルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。このオプションを無効にすると、初めて検出されたファイルの性質が「不明（Unknown）」になります。
- [カスタム検出リストを有効にする（Enable Custom Detection List）]：カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする（Enable Clean List）]：クリーン リストにあるファイルを許可します。
- [ダイナミック分析の脅威スコアに基づいてマルウェアとしてファイルをマークする（Mark files as malware based on dynamic analysis threat score）]：しきい値の脅威スコアを設定します。スコアがしきい値以上のファイルはマルウェアと見なされます。

  しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイルポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。

ファイル ポリシー エディターの [詳細設定（Advanced）] タブには、次のアーカイブ ファイル検査オプションがあります。

- [アーカイブを検査する（Inspect Archives）]：アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] と同じ大きさのアーカイブ ファイルまで、アーカイブ ファイルのコンテンツのインスペクションをできるようにします。

> ⚠ **注意** [アーカイブを検査する（Inspect Archives）] を有効化または無効化 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。

- [暗号化されたアーカイブをブロックする（Block Encrypted Archives）]：暗号化されたコンテンツを含むアーカイブ ファイルをブロックします。
- [検査不可能なアーカイブをブロックする（Block Uninspectable Archives）]：暗号化以外の理由でシステムが検査できないコンテンツを含むアーカイブ ファイルをブロックします。これは通常、破損したファイル、または指定した最大アーカイブ深度を超えるファイルに適用されます。
- **[最大アーカイブ深度（Max Archive Depth）]**：指定した深度を超えるネストされたアーカイブ ファイルをブロックします。トップレベルのアーカイブ ファイルはこの数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。

関連トピック

Snort® の再起動シナリオ

ファイル ポリシーの編集

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（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin/Access Admin

手順

ステップ 1 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [マルウェアとファイル（Malware & File）]** を選択します。

ステップ 2 編集するファイル ポリシーの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 3 次の選択肢があります。

- [ファイル ルールの追加（Add File Rule）] を選択して、ファイル ルールを追加します。詳細については、ファイル ルール （16 ページ）を参照してください。
- 既存のファイル ルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。
- 詳細オプションおよびアーカイブ ファイル検査オプション （14 ページ）の説明に従って詳細オプションを設定します。

（注） ファイル ポリシー エディタに、現在編集中のファイル ポリシーを使用しているアクセス コントロール ポリシーの数が表示されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [アクセス コントロール ポリシー（Access Control Policies）] ページに進むことができます。

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。

ファイル ルール

ファイルのポリシーには、その親であるアクセス コントロール ポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

ファイルがルールに一致すると、ルールは以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする
- キャプチャされたファイルをデバイスに保存する
- ローカル マルウェア分析、Spero 分析、または動的分析のために、キャプチャしたファイルを送信する。

さらに、ファイル ポリシーによって以下を実行できます。

- クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブ ファイル（`.zip` や `.rar` など）の内容を検査する
- アーカイブ ファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブ ファイルをブロックする

ファイル ルールのコンポーネント

表 *3:* ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意（Any）] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。 **ヒント** [任意（Any）] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ファイル ルールのコンポーネント	説明
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、ShockWave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 システムで検査可能なファイル タイプのリストについては、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択して、一時的な新しいファイル ポリシーを作成してから、[ルールの追加（Add Rule）] をクリックします。ファイル タイプ カテゴリを選択すると、システムが検査できるファイル タイプが [ファイルタイプ（File Types）] リストに表示されます。 （注） 頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。
ファイル ルール アクション	ファイル ルールのアクションによって、ルールの条件に一致したトラフィックをシステムが処理する方法が決定されます。 選択したアクションに応じて、システムでファイルを保存するか、ファイルに対して Spero 分析、ローカル マルウェア分析、または動的分析を実行するかを設定できます。[ブロック（Block）] アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。 （注） ファイル ルールは数値上の順番ではなく、ルール アクションの順番で評価されます。

ファイル ルール アクションと評価順序

効果を発揮するには、ファイル ポリシーに 1 つ以上のルールが含まれている必要があります。ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。

各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する 1 つのアクションが関連付けられます。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

複数のファイル ルール アクションは、以下のようなルール アクション順になります。

- [ファイル ブロック（Block Files）] ルールを使用すると、特定のファイル タイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェア ブロック（Block Malware）] ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、AMP クラウドを照会して、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。
- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [ファイル検出（Detect Files）] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をデータベースに記録できます。

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] を選択、[ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] または無効化、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除すると、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。

ファイル ルール アクションに応じて、ファイル転送がブロックされたときに接続をリセットするオプション、管理対象デバイスに取得したファイルを保存するオプション、ファイルでマ

ルウェアをローカルで分析するオプション、取得したファイルを動的分析および Spero 分析のために AMP クラウドに送信するオプション、および後で送信するためにクラウドに現在送信できないファイルを保存するオプションを設定できます。

表 *4:* ファイル ルール アクション

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
MSEXE 用の Spero 分析（Spero Analysis for MSEXE）	No	はい：実行可能ファイルを送信できます	No	はい：実行可能ファイルを送信できます
動的分析（Dynamic Analysis）	No	はい：不明なファイルの性質の実行可能ファイルを送信できます	No	はい：不明なファイルの性質の実行可能ファイルを送信できます
容量処理（Capacity Handling）	No	Yes	No	Yes
ローカル マルウェア分析（Local Malware Analysis）	No	Yes	No	Yes
接続のリセット（Reset Connection）	はい（推奨）	はい（推奨）	No	No
ファイルの保存（Store files）	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイル タイプを保存できます

ファイル ポリシーの注意事項と制約事項

ファイル ルール設定に関する注意事項と制約事項

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。

- [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、Firepower Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。
- シスコでは、[ファイル ブロック（Block Files）] アクションと [マルウェア ブロック（Block Malware）] アクションで [接続のリセット（Reset Connection）] を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。
- 大量のトラフィックをモニタしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したり**しないでください**。そのようにすると、システム パフォーマンスに悪影響が及ぶことがあります。
- システムで検出されるすべてのファイル タイプに対してマルウェア分析を実行できるわけではありません。[アプリケーション プロトコル（Application Protocol）]、[転送の方向（Direction of Transfer）]、および [アクション（Action）] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル検出に関する注意事項と制約事項

- アダプティブ プロファイリングが有効でなければ、アクセス コントロール ルールは、AMP を含め、ファイルの制御を実行できません。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーション プロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン タップ モードの展開では、FTP データ セッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、UNIX/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- ISO ファイルを検出するには、ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション の [ファイル タイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] オプションに関する情報を参照してください。

ファイル ブロックに関する注意事項と制約事項

- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは**マルウェア ブロック** ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。
- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイルイベントの生成を行いません。
- [ファイル ブロック（Block Files）] ルールでブロックされる NetBIOS-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送など）NetBIOS-ssn 経由で転送されるファイルを検出またはブロックするファイル ルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの展開前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。
- Firepower Threat Defense のハイ アベイラビリティを設定したときに、元のアクティブなデバイスがファイルを識別している間にフェイル オーバーが発生した場合、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

ファイル ルールの作成

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
脅威（ファイル制御） マルウェア（ネットワーク向けAMP）	Protection（ファイル制御） マルウェア（ネットワーク向けAMP）	任意（Any）	任意（Any）	Admin/Access Admin

注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] を選択した場合、[ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェア クラウド ルックアップ（Malware Cloud Lookup）] または [マルウェア ブロック（Block Malware）] ファイル ルール アクションを分析オプション（[Spero 分析または MSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカル マルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイル ルールを追加または最後のファイル ルールを削除した場合には、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。

手順

ステップ 1 ファイル ポリシー エディタで、[ファイル ルールの追加（Add File Rule）] をクリックします。

ステップ 2 ファイル ルールのコンポーネント （17 ページ）の説明に従って、[アプリケーション プロトコル（Application Protocol）] および [転送の宛先（Direction of Transfer）] を選択します。

ステップ 3 [ファイル タイプ（File Types）] を 1 つ以上選択します。

表示されるファイル タイプは、選択したアプリケーション プロトコル、転送の方向、およびアクションによって異なります。

ファイル タイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイル タイプ カテゴリ（File Type Categories）] を選択し、[選択したカテゴリのすべてのタイプ（All types in selected Categories）] をクリックします。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[名前および説明の検索（Search name and description）] フィールドに **Windows** と入力します。

ヒント　ファイル タイプの上にポインタを移動すると、説明が表示されます。

ステップ 4 ファイル ルール アクションと評価順序 （19 ページ）の説明に従って、ファイル ルールの [アクション（Action）] を選択します。

ステップ 5 選択したアクションに応じて、以下を実行するかどうかを設定します。

- ファイルのブロック後に接続をリセットする
- 一致するファイルを保存する
- Spero 分析を有効にする
- ローカル マルウェア分析を有効にする
- ダイナミック分析およびキャパシティの処理を有効にする

ファイル ルール アクションと評価順序 （19 ページ）の説明を参照してください。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [保存（Save）] をクリックしてポリシーを保存します。

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

Snort® の再起動シナリオ

クラウド接続

Firepower システムでは Cisco Advanced Malware Protection（AMP）を実施するため、次のパブリック クラウドベースのサーバへの接続を行います。

- AMP クラウド：ネットワーク向け AMP のマルウェア判定結果と更新、AMP for Endpoints のスキャン レコード、マルウェア検出、検疫、侵害の兆候（IOC）を取得できます。
- AMP Threat Grid クラウド：動的分析に利用可能なファイルの送信、脅威スコアや動的分析レポートの取得ができます。

部門のプライバシー、セキュリティ保護のニーズに応じて、プライベート クラウド サーバを導入することもできます。

- AMP プライベート クラウド仮想アプライアンス（AMPv）は、圧縮型、オンプレミス AMP クラウドおよびパブリック AMP クラウドに接続するための匿名プロキシとして機能します。

- AMP Threat Grid アプライアンスはパブリック AMP Threat Grid クラウドとは連絡しないオンプレミス AMP Threat Grid クラウドとして機能します。

AMP クラウド接続

高度なマルウェア防御（AMP）クラウドは、ビッグ データ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコ ホステッド サーバです。次の 2 つのシスコ AMP ソリューションはどちらも AMP クラウドを使用します。

- ネットワーク向け AMP は、管理対象デバイスがネットワーク トラフィックから検出した潜在的なマルウェアの性質を取得し、ローカルマルウェア分析とファイルの事前分類の更新を取得するために AMP クラウドを使用します。
- エンドポイント向け AMP は、シスコのエンタープライズクラスの AMP ソリューションです。ユーザはそれぞれ、AMP クラウドと通信するコンピュータやモバイル デバイスに軽量コネクタをインストールします。次に Firepower Management Center がスキャン、マルウェア検出、隔離、および侵害の兆候（IOC）のレコードをインポートします。

展開に応じて、AMP for Endpoints によってモニタされるエンドポイントは AMP for Networks でモニタされるものと同じホストにならない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる 2 つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

[AMP 管理（AMP Management）] ページ（**[AMP]** > **[AMP 管理（AMP Management）]**）で AMP クラウドとの接続を管理します。ネットワーク向け AMP では、デフォルトで米国（US）AMP パブリック クラウドへの接続が設定され、有効になっています。ネットワーク向け AMP クラウド接続の削除や無効化はできませんが、欧州連合（EU）および米国（US）AMP クラウドの切り替え、またはプライベート クラウド（AMPv）の接続の設定が可能です。

エンドポイントに独自の FireAMP 接続を追加するには、FireAMP ポータルのアカウントが必要です。ポータルに登録されていない AMP for Endpoints 接続では、ネットワーク向け AMP は無効になりません。

AMP クラウド接続要件

- AMP for Networks：パブリックまたはプライベートいずれの AMP クラウドを使用していても、ポート 443 を使って AMP for Networks のマルウェア クラウド ルックアップを行います。Firepower Management Center からの通信を行うため、このポートをアウトバウンドに開く必要があります。
- エンドポイント向け AMP：エンドポイントベースのマルウェア イベントを受信するために、システムはポート 443/HTTPS を使用してシスコ クラウド（パブリックまたはプライベート）に接続します。Firepower Management Center との通信を行うため、このポートを

インバウンドとアウトバウンドの両方に開く必要があります。また、Firepower Management Centerはインターネットに直接アクセスできる必要があります。デフォルトの正常性ポリシーに含まれる AMP ステータス モニタは、Firepower Management Center からクラウドへの最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

AMP の通信にレガシー ポートを使用するには集合型セキュリティ インテリジェンスの通信設定オプション （36 ページ） を参照してください。

AMP とハイ アベイラビリティ

ハイ アベイラビリティ ペアの Firepower Management Center はファイル ポリシーおよび関連する設定を共有しますが、クラウド接続、キャプチャされたファイル、ファイルイベント、マルウェアイベントを共有することはありません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firepower Management Center で同じであるようにするためには、アクティブとスタンバイ両方の Firepower Management Center がクラウドにアクセスできる必要があります。

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

これらの要件は、パブリック、プライベート両方の AMP クラウドに適用されます。

AMP クラウド接続とマルチテナンシー

マルチドメイン展開では、ネットワーク向け AMP 接続はグローバル レベルでのみ設定します。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。エンドポイント向け AMP 接続は、どのドメイン レベルでも設定可能です。ただし、各接続にそれぞれ個別のエンドポイント向け AMP アカウントを使用する必要があります。たとえば、MSSP の各クライアントは、それぞれ独自のエンドポイント向け AMP を展開している場合があります。

⚠

注意 特にリーフ ドメインに重複する IP スペースがある場合、エンドポイント向け AMP 接続はリーフ レベルのみで設定することを**強く**推奨します。複数のサブドメインに同じ IP-MAC アドレス ペアを持つホストが存在する場合、誤ったリーフ ドメインにエンドポイントベースのマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

AMP for Endpoints クラウド接続の設定

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
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

組織で AMP for Endpoints が展開されると、脅威の識別、侵害の兆候（IOC）、およびその他のマルウェア関連の情報を AMP クラウドからシステムにインポートできます。ネットワーク向け AMP 接続がすでに設定されている場合にも、AMP for Endpoints 接続を設定する必要があります。

注意 マルチドメイン展開では、特にリーフ ドメインに重複する IP スペースがある場合は、AMP for Endpoints 接続をリーフ レベルのみで設定することを**強く**お勧めします。複数のサブドメインに同じ IP-MAC アドレス ペアを持つホストがある場合、システムが誤ったリーフ ドメインにエンドポイントベースのマルウェア イベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

始める前に

- ネットワークで AMP for Endpoints が設定されていて、機能している必要があります。
- Firepower Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後に AMP クラウドに接続している場合は、AMP for Endpoints 管理コンソールを使用して以前の接続を削除します。

手順

ステップ 1 **[AMP]** > **[AMP 管理（AMP Management）]**を選択します。

ステップ 2 [AMP クラウド接続の作成（Create AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name）] ドロップダウン リストから、使用するクラウドを選択します。

- 欧州連合 AMP クラウドの場合、[EU クラウド（EU Cloud）] を選択します。
- 米国 AMP クラウドの場合、[US クラウド（US Cloud）] を選択します。
- AMPv の場合、[プライベート クラウド（Private Cloud）] を選択し、Cisco AMP プライベート クラウド （29 ページ）の説明に従って続行します。

ステップ 4 このクラウドを ネットワーク向け AMP と AMP for Endpoints に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

ステップ 5 [登録（Register）] をクリックします。

回転状態のアイコンは、たとえば、Firepower Management Center で接続を設定した後、AMP for Endpoints 管理コンソールの使用を許可する前に、接続が保留中であることを示します。失敗または拒否を示すアイコン（  ）は、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ステップ 6 AMP for Endpoints 管理コンソールを続行することを確認し、管理コンソールにログインします。

ステップ 7 管理コンソールを使用して、AMP for Endpoints データを Firepower Management Center に送信することを AMP クラウドに許可します。

ステップ 8 受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。

デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、AMP for Endpoints 管理コンソールで **[管理（Management）] > [グループ（Groups）]** を選択します。詳細については、管理コンソールのオンライン ヘルプを参照してください。

ステップ 9 [許可（Allow）] をクリックして接続を有効にして、データの転送を開始します。

[拒否（Deny）] をクリックすると Firepower Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま AMP for Endpoints 管理コンソールの [アプリケーション（Applications）] ページから別のページに移動した場合、Firepower Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルス モニタは失敗した接続のアラートを生成**しません**。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

AMP for Endpoints 接続の登録が未完了であっても、ネットワーク向け AMP 接続は無効になりません。

ステップ 10 接続が正しく設定されていることを確認するには、次の手順を実行します。

a) **[AMP] > [AMP 管理（AMP Management）]** ページで、[Cisco AMP ソリューション タイプ（Cisco AMP Solution Type）] 列に **`AMP for Endpoints`** が含まれている [クラウド名（Cloud Name）] をクリックします。

b) 表示される AMP for Endpoints コンソール ウィンドウで、[アカウント（Accounts）] > [アプリケーション（Applications）] を選択します。

c) Firepower Management Center が一覧に含まれていることを確認します。

次のタスク

- AMP for Endpoints コンソール ウィンドウで、必要に応じて設定を行います。たとえば、管理センターのグループ メンバーシップの定義や、ポリシーの割り当てを行います。詳細については、AMP for Endpoints のオンライン ヘルプまたはその他のドキュメントを参照してください。
- ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP for Endpoints 管理コンソールへのアクセス

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
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

ヒント AMP for Endpoints とそのコンソールの使用については、コンソールのオンライン ヘルプや、その他のドキュメンテーションを参照してください。 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html

Firepower Management Center から AMP for Endpoints コンソールにアクセスできます。

始める前に

AMP for Endpoints への接続が設定され（AMP for Endpoints クラウド接続の設定 （26 ページ）を参照してください）、Firepower Management Center が AMP クラウドに接続可能になっている必要があります。

手順

ステップ 1 **[AMP]** > **[AMP 管理（AMP Management）]**を選択します。

ステップ 2 テーブルでクラウド名をクリックします。

Cisco AMP プライベート クラウド

Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を構成することで、ネットワーク上の AMP エンドポイント データを収集することができます。AMPv は、AMP クラウドの圧縮型、オンプレミス バージョンとして機能する、シスコ独自の仮想マシンです。

エンドポイント向け AMP のすべてのコネクタが AMPv にデータを送信し、AMPv は Firepower Management Center にデータを転送します。AMPv は、エンドポイント データを外部接続では一切共有しません。Firepower Management Center は AMP クラウドに接続し、ネットワーク トラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブ マルウェア イベントを受信したりします。

部門のプライバシーやセキュリティ保護の観点から、モニタ対象ネットワークと AMP クラウドとの間で頻繁にあるいは直接接続することが困難、または不可能な場合があります。こうした状況で、Cisco AMP プライベート クラウド仮想アプライアンス（AMPv）を構成することができます。AMPv は、AMP クラウドの圧縮型、オンプレミス バージョンとして機能する、シスコ独自の仮想マシンであり、ユーザのネットワークと AMP クラウドの安全なメディエータです。Firepower Management Center を AMPv に接続すると、AMP クラウドとの既存の直接接続は無効化されます。

AMP クラウドとのすべての接続（ネットワーク向け AMP でも AMP for Endpoints でも）が AMPv に集約され、AMPv は、管理対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。ネットワーク トラフィックで検出されたファイルの判定結果のクエリ、レトロスペクティブ マルウェア イベントの受信、エンドポイント向け AMP データのインポートなどを行います。AMPv は、エンドポイント データを外部接続では一切共有しません。

各プライベート クラウドは、エンドポイント向け AMP コネクタを最大 10,000 までサポート可能で、複数のプライベート クラウドを設定できます。

[AMP 管理（AMP Management）] ページ（**[AMP]** > **[AMP 管理（AMP Management）]**）を使って、Firepower Management Center から AMPv との接続を制御します。

（注） ネットワーク向け AMP のコンポーネントであるダイナミック分析では、管理対象デバイスが、ポート 443 から AMP Threat Grid クラウドまたはオンプレミス AMP Threat Grid アプライアンスに、直接あるいはプロキシを介してアクセスできる必要があります。AMPv はダイナミック分析をサポート**していません**。また、シスコ集合型セキュリティ インテリジェンス (CSI) に依存するその他の機能（URL フィルタリングやセキュリティ インテリジェンス フィルタリングなど）のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMPv への接続

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
マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin

始める前に

- AMPv のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、後で Firepower Management Center で接続を設定するときに必要になります。
- Firepower Management Center が AMPv と通信できることを確認し、AMPv がインターネットにアクセスでき、AMP クラウドと通信できることを確認します。

手順

ステップ 1 **[AMP]** > **[AMP 管理（AMP Management）]**を選択します。

ステップ 2 [AMP クラウド接続の作成（Create AMP Cloud Connection）] をクリックします。

ステップ 3 [クラウド名（Cloud Name] ドロップダウン リストから [プライベート クラウド（Private Cloud）] を選択します。

ステップ 4 名前を入力します。

この情報は、AMPv によって生成または送信されるマルウェア イベントに表示されます。

ステップ 5 [ホスト（Host）] フィールドに、AMPv の設定時に設定したプライベート クラウドのホスト名を入力します。

ステップ 6 [証明書アップロード パス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、AMPv の有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMPv のマニュアルを参照してください。

ステップ 7 このプライベート クラウドを ネットワーク向け AMP と AMP for Endpoints に使用する場合は、[AMP for Firepower に使用（Use for AMP for Firepower）] チェックボックスをオンにします。

ネットワーク向け AMP 通信を処理する別のプライベート クラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMPv 接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

ステップ 8 プロキシを使用して AMPv と通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。

ステップ 9 [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMPv 管理コンソールを続行して登録を完了することを確認します。

ステップ 10 管理コンソールにログインして登録プロセスを完了します。手順の詳細については、AMPv のマニュアルを参照してください。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP クラウドおよび AMPv 接続の管理

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
マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin

クラウドからマルウェア関連の情報を受信する必要がなくなったら、Firepower Management Center を使用して AMP クラウドまたは AMPv 接続を削除します。AMP for Endpoints または AMPv管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Firepower Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。

⚠

注意 無効化された接続に対して、AMP クラウドおよびAMPvは、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firepower Management Center は、グローバル ドメインに属する ネットワーク向け AMP 接続を 1 つのみ保持できます。

手順

ステップ 1 **[AMP]** > **[AMP 管理（AMP Management）]** を選択します。

ステップ 2 AMP クラウド接続を管理します。

- 削除：削除アイコン（🗑）をクリックして、選択内容を確認します。
- 有効化または無効化：スライダをクリックして、選択内容を確認します。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

動的分析接続

AMP Threat Grid クラウドでは、ファイルがサンドボックス環境で実行されます。ネットワーク向け AMP ではクラウドを使用して、動的分析送信ファイルの脅威スコアと動的分析レポートを取得します。適切なライセンスを使用して、システムが自動的にクラウドにアクセスします。

組織のセキュリティ ポリシーが Firepower システムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスの AMP Threat Grid アプライアンスを設定できます。詳細については、『*Cisco AMP Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

Firepower Management Center の [ダイナミック分析接続（Dynamic Analysis Connections）] ページ（**[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]**）を使用して、AMP Threat Grid クラウドへのパブリック動的分析接続およびオンプレミスの AMP Threat Grid アプライアンスへのプライベート動的分析接続を管理します。

（注）

[AMP] > **[ダイナミック分析接続（Dynamic Analysis Connections）]** ページの ボタンの詳細については、パブリック クラウドでの動的分析の結果へのアクセスの有効化 （33 ページ）を参照してください。

デフォルトの動的分析接続の表示

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
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

デフォルトで、Firepower Management Center は、ファイルを送信したり、レポートを取得したりするために、パブリック AMP Threat Grid クラウドに接続できます。この接続は、設定したり、削除したりすることはできません。

手順

ステップ 1 **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。

ステップ 2 編集アイコン（）をクリックします。

パブリック クラウドでの動的分析の結果へのアクセスの有効化

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
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

Cisco AMP Threat Grid では、分析されたファイルに関して、Firepower Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Cisco AMP Threat Grid

パブリック クラウドのアカウントがあれば、Cisco AMP Threat Grid ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示することができます。ただし、プライバシー上の理由から、ファイル分析の詳細は、そのファイルを提出した組織だけが使用できます。そのため、この情報を表示するためには、Firepower Management Center を、管理対象デバイスによって提出されたファイルと関連付ける必要があります。

始める前に

Cisco AMP Threat Grid パブリック クラウドにアカウントがあること、およびアカウントのクレデンシャルを持っている必要があります。

手順

ステップ 1 [AMP] > [ダイナミック分析接続（Dynamic Analysis Connections）] を選択します。

ステップ 2 Cisco AMP Threat Grid パブリック クラウドに対応するテーブル行で、 をクリックします。

Cisco AMP Threat Grid ポータル ウィンドウが開きます。

ステップ 3 Cisco AMP Threat Grid パブリック クラウドにサインインします。

ステップ 4 [クエリの送信（Submit Query）] をクリックします。

（注） [デバイス（Devices）] フィールドのデフォルト値を変更しなでください。

このプロセスで問題が発生した場合は、Cisco TAC の Cisco AMP Threat Grid 担当者にお問い合わせください。

この変更が有効になるまでに最大で 24 時間かかることがあります。

次のタスク

関連付けが有効化された後、Cisco AMP Threat Grid パブリック クラウドの動的分析結果の表示 を参照してください。

Threat Grid のオンプレミス アプライアンス

組織にパブリックの AMP Threat Grid クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの AMP Threat Grid アプライアンスを展開することができます。このオンプレミス アプライアンスは、パブリック クラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを Firepower システムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

1 台のオンプレミス AMP Threat Grid アプライアンスを Firepower Management Center に接続できます。詳細については、『*Cisco AMP Threat Grid* アプライアンス セットアップおよび構成ガイド』を参照してください。

このオンプレミスアプライアンスへの動的分析接続を設定した場合、システムではパブリックの AMP クラウドを使用してマルウェア クラウドルックアップを実行し、またファイルが以前に動的分析用に送信されていないことを確認します。

システムでは、パブリック レポートの取得に AMP クラウドへのデフォルトのパブリック動的分析接続も使用します。オンプレミスアプライアンスがファイル用の動的分析レポートを生成しなかった場合、システムはこの動的分析レポートについてパブリックの AMP クラウドに問い合わせます。組織がファイルを送信していない限り、表示できるのは、限られたデータが含まれた、スクラビング処理が実行されたレポートだけです。

オンプレミスの動的分析接続の設定

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
マルウェア	マルウェア	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

ネットワークでオンプレミスの AMP Threat Grid アプライアンスをインストールする場合は、動的分析接続を設定して、ファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Firepower Management Center を登録します。

始める前に

- オンプレミスの AMP Threat Grid アプライアンスを設定します。『*Cisco AMP Threat Grid Appliance Setup and Configuration Guide*』を参照してください。
- ログインに使用する公開キー証明書を AMP Threat Grid アプライアンスからオンプレミスのアプライアンスにダウンロードします。『*Cisco AMP Threat Grid Appliance Administrator's Guide*』を参照してください。
- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。Firepower Management Center 管理インターフェイスの設定を参照してください。

手順

ステップ 1 **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]**を選択します。

ステップ 2 [新しい接続を追加（Add New Connection）] をクリックします。

ステップ 3 名前を入力します。

ステップ 4 [ホスト URL（Host URL）] を入力します。

ステップ 5 [証明書のアップロード（Certificate Upload）] の横にある [参照（Browse）] をクリックして、オンプレミスのアプライアンスとの接続を確立するために使用する公開キー証明書をアップロードします。

ステップ 6 設定されているプロキシを使用して接続を確立する場合は、[可能な場合はプロキシを使用（Use Proxy When Available）] を選択します。

ステップ 7 [登録（Register）] をクリックします。

ステップ 8 [はい（Yes）] をクリックして、オンプレミスの AMP Threat Grid アプライアンスのログインページを表示します。

ステップ 9 オンプレミスの AMP Threat Grid アプライアンスにユーザ名とパスワードを入力します。

ステップ 10 [サインイン（Sign in）] をクリックします。

ステップ 11 次の選択肢があります。

- 以前にオンプレミスのアプライアンスに Firepower Management Center を登録した場合は、[戻る（Return）] をクリックします。
- Firepower Management Center を登録していない場合は、[アクティブ化（Activate）] をクリックします。

集合型セキュリティ インテリジェンス通信の設定

Firepower システムは、レピュテーション、リスク、脅威インテリジェンスに関して、シスコ集合型セキュリティ インテリジェンス（CSI）を使用します。適正なライセンスがあれば、URL フィルタリングおよび ネットワーク向け AMP 機能の通信オプションを指定できます。

集合型セキュリティ インテリジェンスの通信設定オプション

- URL フィルタリング オプション （36 ページ）
- AMP for Networks のオプション （37 ページ）

URL フィルタリング オプション

Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URL フィルタリング ライセンスを追加すると、[URLフィルタンリングを有効にする（Enable URL Filtering）] が自動的に有効になります。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URL フィルタリングを有効にする場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、またはURL フィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco CSI から URL データをダウンロードします。このプロセスには、時間がかかる場合があります。

自動更新を有効にする（Enable Automatic Updates）

URL フィルタリング脅威データを更新するためのオプション。

- このページの [自動更新を有効にする（Enable Automatic Updates）] オプションを有効にすると、Firepower Management Center は 30 分ごとにクラウドの更新をチェックします。 このオプションは、URL フィルタリング ライセンスを追加すると、デフォルトで有効になります。
- システムが外部リソースに接触する時間を厳格に制御する必要がある場合、このページの自動更新を無効にし、代わりにスケジューラを使用して定期的なタスクを作成します。スケジュール設定されたタスクを使用した URL フィルタリング更新の自動化を参照してください。

[今すぐアップデート（Update Now）]

このダイアログ ボックスの上部にある [今すぐアップデート（Update Now）] ボタンをクリックすると、ワンタイムのオンデマンド更新を実行できますが、自動更新を有効にするか、スケジューラを使用して定期的なタスクを作成する必要があります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）

カテゴリとレピュテーションがローカル データセットにない Web サイトをユーザが閲覧するときに、脅威インテリジェンス評価のために URL がクラウドに送信されるようにします。プライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致**しません**。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

関連トピック

通信ポートの要件

AMP for Networks のオプション

ローカル マルウェア検出の自動更新を有効にする（Enable Automatic Local Malware Detection Updates）

ローカル マルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firepower Management Center が 30 分ごとに署名の更新を確認します。

マルウェア イベントの URL を Cisco と共有する（Share URI from Malware Events with Cisco）

ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関連する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

レガシー ポート 32137 を ネットワーク向け AMP に使用する（Use Legacy Port 32137 for AMP for Networks）

デフォルトでは、ネットワーク向け AMP はポート 443/HTTPS を使用して AMP クラウド（または AMPv）と通信します。このオプションは、ネットワーク向け AMP によるポート 32137 の使用を許可します。システムを以前のバージョンから更新する場合は、このオプションを有効にすることができます。

関連トピック

通信ポートの要件

集合型セキュリティ インテリジェンスでの通信の設定

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
URL フィルタリング（URL フィルタリング） マルウェア（ネットワーク向け AMP）	URL フィルタリング（URL フィルタリング） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin

始める前に

NGIPSvデバイスでカテゴリおよびレピュテーションベースのURLフィルタリングを使用する場合は、『*Firepower System Virtual Installation Guide*』を参照して、正しい量のメモリを割り当てる方法について確認してください。

手順

ステップ 1 **[システム（System）] > [統合（Integration）]**を選択します。

ステップ 2 [] タブをクリックします。

ステップ 3 集合型セキュリティ インテリジェンスの通信設定オプション （36 ページ）の説明に従って Cisco CSI 通信を設定します。

ステップ 4 [保存（Save）] をクリックします。