ファイルと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調整

次のトピックでは、ファイルと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を設定する方法について説明します。

ファイルおよびマルウェアのインスペクションのパフォーマンスとストレージの調整について

ファイル制御を実行するか、AMP for Firepower を使用する場合は、次の詳細設定ファイルとマルウェア インスペクション機能のオプションを設定できます。

- ファイル タイプを検出したときに検査されるバイト数を制限する。
- マルウェア ブロック ルールがキャッシュされた性質のないファイルと一致し、性質を取得せずに経過した時間が長すぎる場合は、ファイルの通過を許可する。
- 特定のサイズよりも大きい場合は、ファイルの保存、ファイルでのマルウェア クラウドルックアップの実行、またはカスタム検出リストでのファイルのブロックを回避する。
- 保存する最小ファイル サイズと最大ファイル サイズを指定する。
- 動的分析に送信する最小ファイル サイズと最大ファイル サイズを指定する。

これらのオプションはシステムパフォーマンスおよびファイルストレージに影響を与える可能性があります。

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

ファイル サイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。

注意 [ファイルおよびマルウェアの設定（File and Malware Settings）] でデフォルト以外の値を設定します 設定の変更を展開すると 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、管理対象デバイスのモデルおよびトラフィックの処理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。

表 *1*：アクセス コントロール ファイルおよび *AMP for Firepower* の詳細オプション

フィールド	説明	使用可能な値	注記（Notes）
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）	ファイル タイプを検出するときに検査するバイト数を指定します。	0 ～ 4294967295（4GB）	制限を取り除くには、0 を入力します。 デフォルト値は、TCP パケットの最大セグメント サイズです。ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
ファイルを許可するのにかかるマルウェア ブロックのクラウド ルックアップの制限時間（秒）（Allow file if cloud lookup for Block Malware takes longer than (seconds)）	マルウェア クラウド ルックアップの実行中に、システムが [マルウェア ブロック（Block Malware）] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ～ 30 秒	シスコは、接続の障害によってトラフィックのブロックを防ぐために、デフォルト値を使用することをお勧めします。サポートに連絡することなくこのオプションを 0 に設定**しない**でください。

フィールド	説明	使用可能な値	注記（**Notes**）
SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA--256 hash values for files larger than (in bytes)）	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェア クラウド ルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	`0` ～ `4294967295`（4GB）	制限を取り除くには、`0` を入力します。 この値は、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [動的分析テストの最大ファイルサイズ (バイト)（Maximum file size for dynamic analysis testing (bytes)）] の値以上に設定する必要があります。
保存する最小ファイル サイズ(バイト)（Minimum file size to store (bytes)）	システムがファイル ルールを使用して保管できるファイルの最小サイズを指定します。	`0` ～ `10485760`（10MB）	ファイル ストレージを無効にするには、`0` を入力します。 このフィールドは、[保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Maximum file size to store (bytes)）] の値以下に設定する必要があります。
保存する最大ファイルサイズ(バイト)（Maximum file size to store (bytes)）	システムがファイル ルールを使用して保管できるファイルの最大サイズを指定します。	`0` ～ `10485760`（10MB）	ファイル ストレージを無効にするには、`0` を入力します。 このフィールドは、[保存する最小ファイル サイズ(バイト)（Minimum file size to store (bytes)）] の値以上、および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。

フィールド	説明	使用可能な値	注記（**Notes**）
ダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）	システムがAMPクラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	0 ～ 104857600（100 MB）	このフィールドは、[動的分析テストの最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）] および [SHA-256 ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 バージョン 5.x の Firepower システムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは15360より小さい値をすべて15360に変更します。 システムはAMPクラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます（最大で1日1回）。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。

フィールド	説明	使用可能な値	注記（**Notes**）
ダイナミック分析の最大ファイルサイズ(バイト)（Maximum file size for dynamic analysis testing (bytes)）	システムがAMPクラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	0 ～ 104857600（100 MB）	このフィールドは、[Mダイナミック分析の最小ファイルサイズ（バイト）（Minimum file size for dynamic analysis testing (bytes)）] の値以上、[SHA-256ハッシュ値を計算するファイルの上限サイズ（バイト）（Do not calculate SHA-256 hash values for files larger than (in bytes)）] の値以下に設定する必要があります。 バージョン5.xのFirepowerシステムを実行するデバイスにアクセス コントロール ポリシーを展開した場合、システムは2097152より大きい値をすべて2097152に変更します。 システムはAMPクラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます（最大で1日1回）。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

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およびストレージの調整

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（AMP）	保護（ファイル制御） マルウェア（AMP）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

注意 [ファイルおよびマルウェアの設定（Files and Malware Settings）] にデフォルト以外の値を設定することによって、設定の変更を展開すると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、管理対象デバイスのモデルおよびトラフィックの処理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 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 2 [ファイルおよびマルウェアの設定（Files and Malware Settings）] 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 3 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，（2 ページ）で説明されている任意のオプションを設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。