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 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。

表 *1*: アクセス コントロール ファイルおよび ネットワーク向け ***AMP*** の詳細オプション

フィールド	説明	ガイドラインと制限
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（4 GB） 0 にすると制限が解除されます。 デフォルト値は、TCP パケットの最大セグメントサイズ（1460バイト）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。 ISO ファイルをブロックするには、36870 よりも大きい値を入力します。
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 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。 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。
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（4 GB） 0 にすると制限が解除されます。 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。

フィールド	説明	ガイドラインと制限
保存する最小ファイル サイズ(バイト)（Minimum file size to store (bytes)）	これらの設定は以下を指定します。 • 次のディテクタを使用してシステムが検査できるファイルサイズ： • Spero 分析 • サンドボクシングと事前分類 • ローカル マルウェア分析/ClamAV • アーカイブインスペクション • システムがファイルルールを使用して保存できるファイルサイズ。	0 ～ 10485760（10MB） 0にするとファイルストレージが無効になります。 [保存する最大ファイルサイズ（バイト）（Maximum file size to store (bytes)）] 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。
保存する最大ファイル サイズ（バイト）（Maximum file size to store (bytes)）		0 ～ 10485760（10MB） 0にするとファイルストレージが無効になります。 [保存する最小ファイルサイズ（バイト）（Minimum file size to store (bytes)）] 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。
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 ~ 10485760（10 MB） [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。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 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	ガイドラインと制限
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 ~ 10485760（10 MB） [動的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。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 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 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 （1 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

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