エレファントフローの検出

エレファントフローは（合計バイト数が）非常に大きい連続フローであり、ネットワークリンク上で測定されるTCP（または他のプロトコル）フローによって設定されます。デフォルトでは、エレファントフローとは1 GB/10 秒を超えるフローです。これらのフローは、Snort コアでのパフォーマンス拘束の原因となります。エレファントフローはそれほど多くありませんが、一定期間にわたって総帯域幅の不均衡な割合を占める可能性があります。これらのフローは、CPU 使用率の上昇やパケットドロップなどの問題につながる可能性があります。

Firewall Management Center 7.2.0 以降（Snort 3 デバイスのみ）では、エレファントフロー機能を使用して、エレファントフローを検出および修復できます。こうしたアクションはシステムストレスを軽減し、前述の問題を解決するために役立ちます。

エレファントフローの検出と修復について

エレファントフロー検出機能を使用して、エレファントフローを検出して修復できます。次の修復アクションを適用できます。

- **エレファントフローをバイパスする**：Snort インスペクションをバイパスするようにエレファントフローを設定できます。このアクションが設定されている場合、Snortはエレファントフローからパケットを受信しません。
- **エレファントフローをスロットルする**：フローにレート制限を適用して、フローの検査を続行できます。フローレートは動的に計算され、フローレートの 10% が削減されます。Snort は、判定結果（フローレートが 10% 少ない QoS フロー）をファイアウォールエンジンに送信します。識別されていないアプリケーションを含むすべてのアプリケーションをバイパスすることを選択した場合、いずれのフローに対してもスロットルアクション（レート制限）を設定できません。

（注） エレファントフロー検出を機能させるには、Snort 3 を検出エンジンにする必要があります。

インテリジェントアプリケーションバイパスからのエレファントフローのアップグレード

バージョン 7.2.0 以降の Snort 3 デバイスでは、インテリジェント アプリケーション バイパス（IAB）は廃止されました。

7.2.0 以降を実行しているデバイスの場合、AC ポリシー（[詳細設定（Advanced Settings）] タブ）の [エレファントフロー設定（Elephant Flow Settings）] セクションでエレファントフロー設定を構成する必要があります。

7.2.0（または以降）へのアップグレード後、Snort 3 デバイスを使用している場合、エレファントフロー構成設定は、[インテリジェントアプリケーションバイパス設定（Intelligent Application Bypass Settings ）] セクションからではなく、[エレファントフロー設定（Elephant Flow Settings ）] セクションから選択されて展開されるため、エレファントフロー構成設定に移行していない場合、次の展開時にデバイスのエレファントフロー構成は失われます。

次の表は、Snort 3 または Snort 2 エンジンを実行しているバージョン 7.2.0 以降およびバージョン 7.1.0 以前に適用できる IAB またはエレファントフロー構成を示しています。

Firewall Management Center	Firewall Threat Defense	エレファントフローまたは IAB 構成
Firewall Management Center 7.0 または 7.1	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス	IAB の構成が適用されます。
Firewall Management Center 7.2.0	Snort 2 デバイス	IAB の構成が適用されます。
	Snort 3 デバイス（7.1.0 以前）	IAB の構成が適用されます。
	Snort 3 デバイス（7.2.0 以降）	エレファントフローの構成が適用されます。

エレファントフローの設定

エレファントフローでアクションを実行するようにエレファントフローを設定できるため、システムの危機、高い CPU 使用率、パケットドロップなどの問題の解決に役立ちます。

注目 エレファントフロー検出は、Snortを介して処理されない、事前フィルタリングされたフロー、信頼されたフロー、または高速転送フローには適用できません。エレファントフローはSnortによって検出されるため、エレファントフロー検出は暗号化されたトラフィックには適用されません。

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、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[エレファントフロー設定（Elephant Flow Settings ）] の横にある **Edit** (✎) をクリックします。

代わりに **View** (👁) が表示される場合、設定は先祖ポリシーから継承されており、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、[Inherit from base policy] をオフにして、編集を有効にします。

図 *1*: エレファントフロー検出の設定

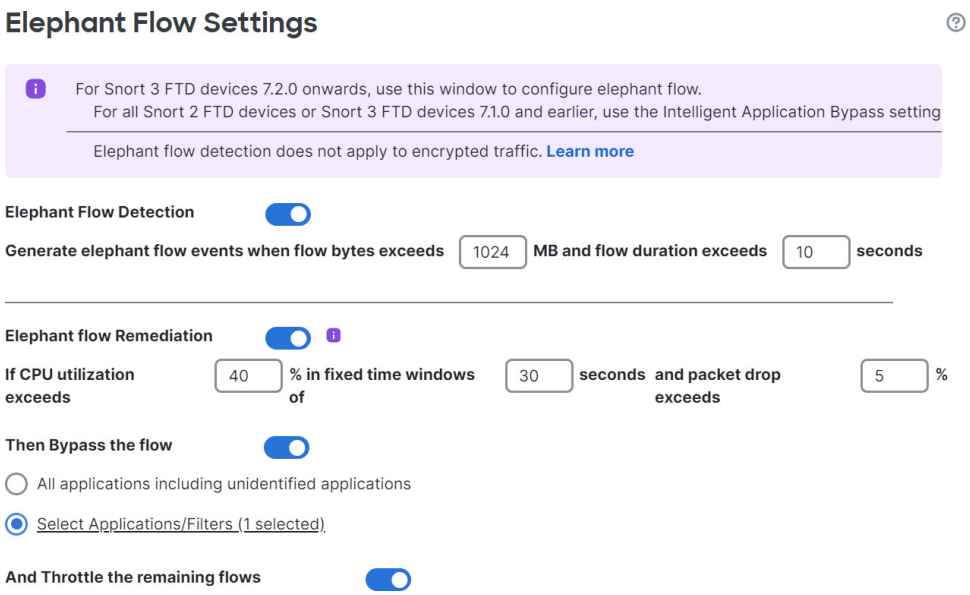

図 *2*: エレファントフロー検出の設定

ステップ2 [エレファントフロー検出（Elephant Flow Detection）] トグルボタンはデフォルトで有効になっています。フローバイトとフロー期間の値を設定できます。設定した値を超えると、エレファントフローイベントが生成されます。

ステップ3 エレファントフローを修復するには、[エレファントフローの修復（Elephant Flow Remediation）] トグルボタンを有効にします。

ステップ4 エレファントフローの修復基準を設定するには、CPU 使用率 %、固定時間ウィンドウの継続時間、およびパケットドロップ % の値を設定します。

CPU 使用率はエレファントフローごとに計算され、フロー遅延から導出されます。CPU 使用率が設定されたしきい値を超えて、固定時間枠やパケットドロップなどの他の設定も一致した場合、エレファントフロー修復アクションが適用されます。同様に、パケットドロップの計算は、CPU ごとのドロップされたパケット数に基づきます。パケットドロップ率が特定の CPU で設定された値を超えると、修復アクションが適用されます。たとえば、値がデフォルトに設定されているとします。つまり、CPU 使用率が 40%、固定時間枠が 30 秒、パケットドロップが 5% に設定されているとします。特定の CPU で、5% を超えるパケットドロップが検出され、フローごとの CPU 使用率が 30 秒の固定時間枠内で 40% を超えた場合、フローはバイパスまたはスロットリングされます。

ステップ 5 設定された基準を満たしている場合、エレファントフローの修復に対して次のアクションを実行できます。

1. [フローをバイパスする（Bypass the flow）]：選択したアプリケーションまたはフィルタの Snort インスペクションをバイパスするには、このボタンを有効にします。次から選択します。
   - [識別されていないアプリケーションを含むすべてのアプリケーション（All applications including unidentified applications）]：すべてのアプリケーション トラフィックをバイパスするには、このオプションを選択します。このオプションを設定すると、すべてのフローにスロットルアクション（レート制限）を設定できなくなります。
   - [アプリケーション/フィルタの選択（Select Applications/Filters）]：トラフィックをバイパスするアプリケーションまたはフィルタを選択するには、このオプションを選択します。『Cisco Secure Firewall Management Center デバイス設定ガイド』の「**アクセスコントロール ルール**」の章にある「**アプリケーション条件とフィルタの設定**」トピックを参照してください。
2. [フローをスロットルする（Throttle the flow）]：フローにレート制限を適用し、フローの検査を続行するには、このボタンを有効にします。Snort インスペクションをバイパスし、残りのフローをスロットルするアプリケーションまたはフィルタを選択できます。

（注）
スロットルされたエレファントフローからスロットルが自動的に削除されるのは、システムが危機を脱した場合、つまり、Snort パケットドロップのパーセンテージが設定されたしきい値よりも低い場合です。その結果、レート制限も削除されます。

次の Threat Defense コマンドを使用して、スロットルされたエレファントフローからスロットルを手動で削除することもできます。

- **clear efd-throttle <5-tuple/all> bypass**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snort インスペクションをバイパスします。
- **clear efd-throttle <5-tuple/all>**：このコマンドは、スロットルされたエレファントフローからスロットルを削除し、Snort インスペクションを続行します。このコマンドを使用すると、エレファントフローの修復はスキップされます。

  これらのコマンドの詳細については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 6 [修復除外ルール（Remediation Exemption Rule）] セクションで、[ルールの追加（Add Rule）] をクリックして、修復から除外する必要があるフローの L4 アクセス制御リスト（ACL）ルールを設定します。

ステップ 7 [ルールの追加（Add Rule）] ウィンドウで、[ネットワーク（Networks）] タブを使用してネットワークの詳細、つまり送信元ネットワークと宛先ネットワークを追加します。[ポート（Ports）] タブを使用して、送信元ポートと宛先ポートを追加します。

エレファントフローが検出され、定義されているルールに一致する場合、[接続イベント（Connection Events）] の [理由（Reason）] 列ヘッダーに理由として [エレファントフローの除外（Elephant Flow Exempted）] が表示されてイベントが生成されます。

ステップ 8 [修復除外ルール（Remediation Exemption Rule）] セクションで、修復アクションから除外されているフローを確認できます。

ステップ 9 [OK] をクリックして、エレファントフロー設定を保存します。

ステップ 10 [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。

エレファントフロー設定を構成した後、接続イベントをモニターして、フローが検出、バイパス、またはスロットリングされているかどうかを確認します。これは、接続イベントの [理由（Reason）] フィールドで確認できます。エレファントフロー接続の 3 つの理由は次のとおりです。

- エレファントフロー（Elephant Flow）
- エレファントフローがスロットリングされている（Elephant Flow Throttled）
- エレファントフローが信頼されている（Elephant Flow Trusted）

注目 エレファントフロー検出を有効にしただけでは、エレファントフローの接続イベントは生成されません。接続イベントが別の理由ですでにログに記録されており、フローもエレファントフローである場合、[理由（Reason）] フィールドにはこの情報が含まれます。ただし、すべてのエレファントフローを確実にロギングするには、該当するアクセス制御ルールで接続ロギングを有効にする必要があります。

詳細については、『Cisco Secure Firewall Elephant Flow Detection』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。