外部アラートの設定

ASA FirePOWER モジュールでは、モジュール インターフェイス内でイベントのさまざまなビューを提供していますが、重要なシステムの常時モニタリングを容易にするため、外部イベント通知の設定が求められる場合があります。次のいずれかが発生した場合にアラートを生成して、電子メール、SNMP トラップまたは syslog により通知するように、モジュールを設定できます。

- ネットワークベースのマルウェア イベントまたはレトロスペクティブ マルウェア イベント
- 特定のアクセス コントロール ルールによってトリガーとして使用される接続イベント

ASA FirePOWER モジュールでこれらのアラートが送信されるようにするには、まず*アラート応答*を作成する必要があります。アラート応答とは、アラートの送信先とする予定の外部システムとモジュールが連携できるようにするための一連の設定です。それらの設定では、たとえば、SNMP アラート パラメータ、または syslog ファシリティおよびプライオリティを指定する場合があります。

アラート応答を作成した後、アラートをトリガーとして使用するために使用するイベントに関連付けます。アラート応答とイベントを関連付けるための処理は、次のように、イベントのタイプによって異なることに注意してください。

- アラート応答をマルウェア イベントと関連付ける場合は、それぞれの設定ページを使用します。
- SNMP および syslog アラート応答を接続のログ記録と関連付ける場合は、アクセス コントロール ルールとポリシーを使用します。

ASA FirePOWER モジュールには、実行可能なもう 1 つのタイプのアラートがあります。この場合は、個々の侵入イベントに対して、SNMP および syslog による侵入イベント通知を設定します。これらの通知は侵入ポリシーで設定します。侵入ルールの外部アラートの設定（39-1 ページ）および SNMP アラートの追加（27-38 ページ）を参照してください。次の表では、アラート生成に必要なライセンスについて説明します。

表 38-1　アラートを生成するためのライセンス要件

アラートを生成する条件	必要なライセンス
侵入イベント	Protection
ネットワークベースのマルウェア イベント	Malware
接続イベント	接続をログに記録するために必要なライセンス

詳細については、以下を参照してください。

- アラート応答の使用（38-2 ページ）
- ネットワーク トラフィックの接続のロギング（36-1 ページ）

アラート応答の使用

ライセンス：任意（Any）

外部アラートを設定する際の最初の手順は、アラート応答を作成することです。アラート応答とは、アラートの送信先とする予定の外部システムとASA FirePOWER モジュールが連携できるようにするための一連の設定です。アラート応答を作成して、電子メール、Simple Network Management Protocol（SNMP）トラップ、またはシステム ログ（syslog）によりアラートを送信できます。

アラートで受け取る情報は、アラートをトリガーしたイベントのタイプによって異なります。

作成したアラート応答は自動的に有効になります。有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。

アラート応答の管理は、[アラート（Alerts）] ページ（[ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）]）で行います。各アラート応答の横のスライダは有効かどうかを示します。有効なアラート応答のみがアラートを生成できます。このページは、たとえば、アクセス コントロール ルールの接続をログに記録するための設定でアラート応答が使用されているかどうかも示します。該当する列見出しをクリックして、名前、タイプ、使用中ステータス、および有効または無効のステータスでアラート応答をソートできます。列見出しを再度クリックすると、順序が反転します。

詳細については、以下を参照してください。

- SNMP アラート応答の作成（38-2 ページ）
- Syslog アラート応答の作成（38-3 ページ）
- アラート応答の変更（38-6 ページ）
- アラート応答の削除（38-6 ページ）
- アラート応答の有効化と無効化（38-7 ページ）

SNMP アラート応答の作成

ライセンス：任意（Any）

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注）　SNMP で 64 ビット値をモニタする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

SNMP アラート応答を作成する方法：

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。

手順 2　[アラートの作成（Create Alert）] ドロップダウン メニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

[SNMP アラート作成の設定（Create SNMP Alert Configuration）] ポップアップ ウィンドウが表示されます。

手順 3　[名前(Name)] フィールドに、SNMP 応答を識別するために使用する名前を入力します。

手順 4　[トラップサーバ(Trap Server)] フィールドに、英数字を使用して SNMP トラップ サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス(192.169.1.456 など)を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

手順 5　[バージョン(Version)] ドロップダウンリストから、使用する SNMP バージョンを選択します。

SNMP v3 がデフォルトです。SNMP v1 または SNMP v2 を選択すると、異なるオプションが表示されます。

手順 6　どのバージョンの SNMP を選択したかに応じて、以下のようにします。

- SNMP v1 または SNMP v2 の場合、英数字または特殊文字(`*` または `$`)を使用して、[コミュニティ ストリング(Community String)] フィールドに SNMP コミュニティの名前を入力し、ステップ 12 に進みます。
- SNMP v3 の場合、[ユーザ名(User Name)] フィールドに SNMP サーバで認証するユーザの名前を入力し、次のステップに進みます。

手順 7　[認証プロトコル(Authentication Protocol)] ドロップダウンリストから、認証に使用するプロトコルを選択します。

手順 8　[認証パスワード(Authentication Password)] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

手順 9　[プライバシー プロトコル(Privacy Protocol)] リストから、[なし(None)] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

手順 10　[プライバシー パスワード(Privacy Password)] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

手順 11　[エンジン ID(Engine ID)] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化には エンジン ID 値が使用されます。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。

Cisco は、ASA FirePOWER モジュールの IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、ASA FirePOWER モジュールの IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

手順 12　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

アラート応答が保存され、自動的に有効になります。

Syslog アラート応答の作成

ライセンス:任意(Any)

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント　syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、syslog および syslog.conf の man ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、syslog.conf ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

次の表に、選択可能な syslog ファシリティを示します。

表 38-2　使用可能な syslog ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 38-3　syslog 重大度レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

syslog アラートの送信を開始する前に、syslog サーバがリモート メッセージを受信できることを確認してください。

syslog アラートを作成する方法:

手順 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [アクション アラート(Actions Alerts)] の順に選択します。

[アラート(Alerts)] ページが表示されます。[アラートの作成(Create Alert)] ドロップダウン メニューから、[Syslog アラートの作成(Create Syslog Alert)] を選択します。

[Syslog アラート作成の設定(Create Syslog Alert Configuration)] ポップアップ ウィンドウが表示されます。

手順 2　[名前(Name)] フィールドに、保存される応答を識別するために使用する名前を入力します。

手順 3　[ホスト(Host)] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス(192.168.1.456 など)を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

手順 4　[ポート(Port)] フィールドに、サーバが syslog メッセージに使用するポートを入力します。

この値はデフォルトで 514 です。

手順 5　[ファシリティ(Facility)] リストから、ファシリティを選択します。

使用可能なファシリティの一覧については、使用可能な syslog ファシリティの表を参照してください。

手順 6　[重大度(Severity)] リストから、重大度を選択します。

使用可能な重大度の一覧については、syslog 重大度レベルの表を参照してください。

手順 7　[タグ(Tag)] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

タグ名には英数字のみを使用します。スペースまたは下線は使用**できません**。

例として、syslog に送信されるすべてのメッセージの前に `FromMC` を付ける場合、フィールドに `FromMC` と入力します。

手順 8　[ASA FirePOWER の変更の保存(Store ASA FirePOWER Changes)] をクリックします。

アラート応答が保存され、自動的に有効になります。

アラート応答の変更

ライセンス:任意（Any）

ほとんどのタイプのアラートについて、アラート応答が有効で使用中の場合、アラート応答への変更はすぐに反映されます。ただし、接続イベントをログに記録するアクセス コントロール ルールで使用されるアラート応答の場合、アクセス コントロール ポリシーを再適用するまで変更は有効になりません。

アラート応答を編集する方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。

手順 2　編集するアラート応答の横にある編集アイコン（ ）をクリックします。

そのアラート応答の設定ポップアップ ウィンドウが表示されます。

手順 3　必要に応じて変更を加えます。

手順 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

アラート応答が保存されます。

アラート応答の削除

ライセンス:任意（Any）

使用中でない任意のアラート応答を削除できます。

アラート応答を削除する方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。

手順 2　削除するアラート応答の横にある削除アイコン（ ）をクリックします。

手順 3　アラート応答を削除することを確認します。

アラート応答が削除されます。

アラート応答の有効化と無効化

ライセンス:任意（Any）

有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。無効化するときにアラートが使用中の場合は、無効にしても使用中とみなされることに注意してください。

アラート応答を有効または無効にする方法:

手順 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクション アラート（Actions Alerts）] の順に選択します。

[アラート（Alerts）] ページが表示されます。

手順 2　有効または無効にするアラート応答の横の有効または無効のスライダをクリックします。

アラート応答が有効だった場合は、無効になります。無効だった場合は、有効になります。