



侵入イベントに関する外部アラート

次のトピックでは、侵入イベントに関する外部アラートを設定する方法について説明します。

- [侵入イベントの外部アラートについて, 1 ページ](#)
- [侵入イベントの SNMP アラートの設定, 2 ページ](#)
- [侵入イベントの Syslog アラートの設定, 4 ページ](#)
- [侵入イベントに対する電子メールアラートの設定, 6 ページ](#)

侵入イベントの外部アラートについて

外部侵入イベント通知は、クリティカルなシステム モニタリングに役立ちます。

- **SNMP** : 侵入ポリシーごとに設定し、管理対象デバイスが送信します。SNMP アラートは侵入ルールごとに有効にすることができます。
- **syslog** : 侵入ポリシーごとに設定し、管理対象デバイスが送信します。1つの侵入ポリシーの syslog アラートを有効にすると、ポリシーに含まれるすべてのルールに適用されます。
- **電子メール** : すべての侵入ポリシーに設定され、Firepower Management Center が送信します。電子メールアラートは侵入ルールごとに有効にすることができ、長さや頻度を制限することもできます。

侵入イベントの抑制やしきい値を設定すると、システムは、ルールがトリガーされるたびに侵入イベントを生成しなくなる（したがってアラートを送信しなくなる）場合があるのでご注意ください。

マルチドメイン導入環境では、どのドメインでも外部アラートを設定できます。先祖ドメインでは、システムは子孫ドメインの侵入イベントの通知を生成します。



(注) Firepower Management Center も SNMP、syslog、および電子メールアラート応答を使って種々の外部アラートを送信します。[Firepower Management Center アラート応答](#)を参照してください。システムは、個々の侵入イベントに対するアラートを送信するためにアラート応答を使用しません。

関連トピック

[侵入ポリシーの侵入イベント通知のフィルタ](#)

侵入イベントの SNMP アラートの設定

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 (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーで外部 SNMP アラートを有効にした後、トリガー時に SNMP アラートを送信する個々のルールを設定できます。これらのアラートは管理対象デバイスから送信されます。

手順

- ステップ 1 侵入ポリシーエディタのナビゲーションウィンドウで、[詳細設定 (Advanced Settings)] をクリックします。
- ステップ 2 [SNMP アラート (SNMP Alerting)] が有効になっていることを確認し、[編集 (Edit)] をクリックします。
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。
- ステップ 3 SNMP バージョンを選択し、[侵入 SNMP アラートのオプション](#)、(3 ページ) の説明に従って構成オプションを指定します。
- ステップ 4 ナビゲーションウィンドウで [ルール (Rules)] をクリックします。
- ステップ 5 [ルール (rules)] ペインで、SNMP アラートを設定するルールを選択し、[アラート (Alerting)] > [SNMP アラートの追加 (Add SNMP Alert)] を選択します。
- ステップ 6 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。
変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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。

侵入 SNMP アラートのオプション

ネットワーク管理システムで Management Information Base (MIB) ファイルが必要な場合は、Firepower Management Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして (as Binary)] を選択します。それ以外の場合は、[文字列として (as String)] を選択します。たとえば、HP OpenView では [文字列として (as String)] が必要になります。
トラップ サーバ (Trap Server)	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティストリング (Community String)	コミュニティ名。

SNMP v3 オプション

管理対象デバイスは、エンジン ID の値を使用して SNMPv3 アラートをエンコードします。アラートをデコードするには、SNMP サーバにこの値が必要です。この値は、送信デバイスの管理インターフェイスの IP アドレスの 16 進数のバージョンで、「01」が付加されています。

たとえば、SNMP アラートを送信するデバイスの管理インターフェイスの IP アドレスが 172.16.1.50 である場合、エンジン ID の値は 0xAC10013201 です。

オプション	説明
トラップ タイプ	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして (as Binary)] を選択します。それ以外の場合は、[文字列として (as String)] を選択します。たとえば、HP OpenView では [文字列として (as String)] が必要になります。
トラップ サーバ (Trap Server)	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。

オプション	説明
認証パスワード (Authentication Password)	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5 (MD5) ハッシュ関数またはセキュア ハッシュ アルゴリズム (SHA) ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
プライベートパスワード (Private Password)	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard (DES) ブロック暗号を使用して、このパスワードを暗号化します。SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーンテキストで表示されますが、暗号化形式で保存されます。 プライベートパスワードを指定すると、プライバシーが有効になり、認証パスワードも指定する必要があります。
ユーザ名 (UserName)	SNMP ユーザ名。

侵入イベントの Syslog アラートの設定

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 (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入ポリシーで syslog アラートを有効にすると、管理対象デバイス自体または外部ホスト上の syslog にすべての侵入イベントが送信されます。外部ホストを指定した場合、syslog アラートは管理対象デバイスから送信されます。

手順

- ステップ 1 侵入ポリシーエディタのナビゲーションウィンドウで、[詳細設定 (Advanced Settings)] をクリックします。
- ステップ 2 [Syslog アラート (Syslog Alerting)] が有効になっていることを確認し、[編集 (Edit)] をクリックします。
ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。
- ステップ 3 syslog アラートを送信するロギングホストの IP アドレスを入力します。
このフィールドを空のままにすると、管理対象デバイスは、独自の syslog 機能を使用して侵入イベントをログに記録します。

システムは、各リーフドメインに個別のネットワークマップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ます。上書き対応オブジェクトを使用すると、子孫ドメインの管理者は、グローバル コンフィギュレーションを自分のローカル環境に調整できます。

ステップ 4 侵入 **syslog** アラートのファシリティとプライオリティ、(5 ページ) の説明に従って、ファシリティと優先度レベルを選択します。

ステップ 5 最後のポリシー確定後にこのポリシーで行った変更を保存するには、[ポリシー情報 (Policy Information)] を選択して、[変更を確定 (Commit Changes)] をクリックします。変更を確定せずにポリシーをそのままにした場合は、別のポリシーを編集すると、最後の確定後の変更は破棄されます。

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。

侵入 **syslog** アラートのファシリティとプライオリティ

管理対象デバイスは、特定のファシリティとプライオリティを使用して、侵入イベントを **syslog** アラートとして送信できるため、ロギング ホストがアラートを分類できます。ファシリティには、それを生成したサブシステムを指定します。プライオリティには、その重大度を指定します。これらのファシリティとプライオリティの値は、実際の **syslog** メッセージには表示されません。

ご使用の環境に基づいて意味のある値を選択します。ローカル設定ファイル (UNIX ベースのロギングホストの **syslog.conf** など) では、どのログファイルにどのファシリティを保存するかを示すことができます。

Syslog アラート ファシリティ

ファシリティ	説明
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。
CRON	クロック デーモンによって生成されるメッセージ。
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。

ファシリティ	説明
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。
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。

Syslog アラートのプライオリティ

水準器	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

侵入イベントに対する電子メールアラートの設定

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 (Access)
脅威 (Threat)	Protection	任意 (Any)	任意 (Any)	Admin/Intrusion Admin

侵入の電子メールアラートを有効にした場合、どの管理対象デバイスまたは侵入ポリシーが侵入を検出したかに関係なく、システムは侵入イベントの生成時に電子メールを送信できます。これらのアラートは Firepower Management Center から送信されます。

はじめる前に

- 電子メールアラートを受信するようにメールホストを設定します。[メールリレーホストおよび通知アドレスの設定](#)を参照してください。
- Firepower Management Center が独自の IP アドレスを逆解決できることを確認します。

手順

-
- ステップ 1 [ポリシー (Policies)] > [アクション (Actions)] > [アラート (Alerts)] を選択します。
 - ステップ 2 [侵入電子メール (Intrusion Email)] タブをクリックします。
 - ステップ 3 [侵入電子メールアラートのオプション, \(7 ページ\)](#) の説明に従って、アラートを生成する侵入ルールや侵入グループを含むアラートオプションを選択します。
 - ステップ 4 [保存 (Save)] をクリックします。
-

侵入電子メールアラートのオプション

On/Off

侵入電子メールアラートを有効または無効にします。

アドレス送信元/宛先 (From/To Addresses)

電子メールの送信者と受信者。受信者のカンマ区切りリストを指定できます。

最大アラート数と頻度 (Max Alerts and Frequency)

Firepower Management Center が時間間隔 ([頻度 (Frequency)]) ごとに送信する電子メールアラートの最大数 ([最大アラート数 (Max Alerts)]) 。

合同アラート (Coalesce Alerts)

同じ送信元 IP とルール ID を持つアラートをグループ化することによって送信されるアラートの数を減らします。

サマリー出力 (Summary Output)

テキスト制限されたデバイスに適した短いアラートを有効にします。短いアラートには、以下の情報が含まれています。

- Timestamp

- プロトコル
- 送信元と宛先の IP とポート
- メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

例 : 2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0
snort_decoder: Unknown Datagram decoding problem! (116:108)

[サマリー出力 (Summary Output)] を有効にする場合は、[合同アラート (Coalesce Alerts)] も有効にすることを検討してください。テキストメッセージの制限を超えないように、[最大アラート数 (Max Alerts)] を下げることができます。

タイムゾーン

アラート タイムスタンプのタイムゾーン。

特定のルール設定に基づく電子メール警告 (Email Alerting on Specific Rules Configuration)

電子メールアラートを設定するルールを選択できます。