侵入ルールの外部アラートの設定

ASA FirePOWER モジュールでは、ユーザ インターフェイスで侵入イベントのさまざまな側面を表示できますが、重要なシステムを継続的にモニタリングできるように、外部侵入イベント通知を定義することを望んでいる企業もあります。syslog ファシリティへのロギングを有効にしたり、SNMP トラップ サーバにイベント データを送信したりできます。

各侵入ポリシー内では、侵入イベントの通知制限を指定し、外部ロギング ファシリティへの侵入イベント通知をセットアップし、侵入イベントへの外部応答を設定できます。

ヒント

アナリストによっては、同じ侵入イベントに対して複数のアラートを受信することは望まないものの、特定の侵入イベントの発生については、頻度を制限したうえで通知を受信したいと考えています。詳細については、ポリシー単位の侵入イベント通知のフィルタリング（24-23 ページ）を参照してください。

侵入ポリシー以外にも、ASA FirePOWER モジュールで実行可能な別のタイプのアラートがあります。特定のアクセス コントロール ルールによって記録された接続イベントなど、他のタイプのイベントに対して SNMP、syslog アラートによる応答を設定できます。詳細については、外部アラートの設定（35-1 ページ）を参照してください。

外部侵入イベント通知の詳細情報については、次の項を参照してください。

- SNMP 応答の使用（36-1 ページ）では、指定された SNMP トラップ サーバにイベント データを送信する場合に設定可能なオプションや、SNMP アラート オプションを指定する手順について説明します。
- Syslog 応答の使用（36-4 ページ）では、外部 syslog にイベント データを送信する場合に設定可能なオプションや、syslog アラート オプションを指定する手順について説明します。

SNMP 応答の使用

ライセンス：Protection

*SNMP トラップ*は、ネットワーク管理に関する通知です。侵入イベントに関する通知を SNMP トラップ（*SNMP アラート*とも呼ばれる）として送信するようにデバイスを設定できます。各 SNMP アラートには次のものが含まれます。

- トラップを生成するサーバの名前
- アラートを検出したデバイスの IP アドレス
- アラートを検出したデバイスの名前
- イベント データ

さまざまな SNMP アラート パラメータを設定できます。使用可能なパラメータは、使用する SNMP のバージョンによって異なります。SNMP アラートを有効化および無効化する方法の詳細については、侵入ポリシーの詳細設定の設定（23-7 ページ）を参照してください。

ヒント　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、ASA FirePOWER モジュールの `/etc/sf/DCEALERT.MIB` から取得できます。

SNMPv2 のオプション

SNMPv2 の場合は、次の表で説明しているオプションを指定できます。

表 36-1　SNMPv2 のオプション

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）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
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。

（注）　SNMPv2 は、読み込み専用コミュニティのみをサポートしています。

SNMPv3 のオプション

SNMPv3 の場合は、次の表で説明しているオプションを指定できます。

（注）　SNMPv3 を使用する場合、アプライアンスは Engine ID 値を使用してメッセージをエンコードします。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。現在、この Engine ID 値は常に、文字列の末尾に `01` が付く、アプライアンスの IP アドレスの 16 進数バージョンになります。たとえば、SNMP アラートを送信するアプライアンスの IP アドレスが `172.16.1.50` である場合、Engine ID は `0xAC10013201` になります。また、アプライアンスの IP アドレスが `10.1.1.77` である場合、Engine ID `0x0a01014D01` が使用されます。

表 36-2　SNMPv3 のオプション

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）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
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。

表 36-2　SNMPv3 のオプション(続き)

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。SNMPv3 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。SNMPv3 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。 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ます。プライベート パスワードを指定する場合は、認証パスワードも指定する必要があります。
ユーザ名（User Name）	SNMP ユーザ名。

(注)　SNMPv3 は、読み取り専用ユーザと AES128 による暗号化のみをサポートしています。

SNMP アラートの設定の詳細については、SNMP 応答の設定（36-3 ページ）を参照してください。

SNMP 応答の設定

ライセンス：Protection

侵入ポリシーで SNMP アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは SNMP トラップで検出した侵入イベントをすべて通知するようになります。SNMP アラートの詳細については、SNMP 応答の使用（36-1 ページ）を参照してください。

SNMP アラート オプションの設定方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 4　外部応答の [SNMP アラート（SNMP Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SNMP アラート（SNMP Alerting）] ページが表示されます。

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。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　IP アドレスに使用するトラップ タイプの形式を [バイナリとして（as Binary）] または [文字列として（as String）] のいずれかに指定します。

（注）　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）] オプションを使用できます。正常にレンダリングされなかった場合は、[文字列として（as String）] オプションを使用します。たとえば、HP OpenView では [文字列として（as String）] オプションが必要になります。

ステップ 6　SNMPv2 または SNMPv3 を選択します。

- SNMPv2 を設定するには、使用するトラップ サーバの IP アドレスとコミュニティ名を対応するフィールドに入力します。SNMPv2 のオプション（36-2 ページ）を参照してください。
- SNMPv3 を設定するには、使用するトラップ サーバの IP アドレス、認証パスワード、プライベート パスワード、およびユーザ名を対応するフィールドに入力します。詳細については、SNMPv3 のオプション（36-2 ページ）を参照してください。

（注）　SNMPv2 **または** SNMPv3 を選択する必要があります。SNMPv2 は読み取り専用コミュニティのみをサポートし、SNMPv3 は読み取り専用ユーザのみをサポートしています。

（注）　SNMPv3 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。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

Syslog 応答の使用

ライセンス：Protection

システム ログ、つまり *syslog* は、ネットワーク イベント ロギングの標準ロギング メカニズムです。侵入イベントの通知である *syslog アラート*をアプライアンスの syslog に送信できます。syslog では、syslog 内の情報を優先度別およびファシリティ別に分類することができます。*優先度*はアラートの重大度を反映し、*ファシリティ*はアラートを生成したサブシステムを示します。ファシリティおよび優先度は syslog の実際のメッセージに表示されませんが、その代わりに、syslog メッセージを受信するシステムにそれを分類する方法を指示するために使用されます。

syslog アラートには次の情報が含まれます。

- アラート生成の日時
- イベント メッセージ
- イベント データ
- トリガー イベントのジェネレータ ID
- トリガー イベントの Snort ID
- 改訂

侵入ポリシーでは、syslog アラートを有効にして、syslog の侵入イベントの通知に関連付けられている syslog の優先度およびファシリティを指定できます。アクセス コントロール ポリシーの一部として侵入ポリシーを適用した場合、システムは、検出した侵入イベントの syslog アラートをローカル ホストまたはポリシーで指定されたロギング ホストの syslog ファシリティに送信します。アラートを受信したホストは、syslog アラートの設定時に設定されたファシリティおよび優先度に関する情報を使用して、アラートを分類します。

次の表には、syslog アラートを設定する場合に選択できるファシリティを示します。使用するリモート syslog サーバの設定に基づいて、効果のあるファシリティの設定を行ってください。リモート システムにある `syslog.conf` ファイル（UNIX または Linux ベースのシステムに syslog メッセージをロギングしている場合）は、サーバのどのログ ファイルにどのファシリティが保存されるかを示します。

表 36-3　使用可能な syslog 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。
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。

このアラートで生成されるすべての通知を表示するには、次の標準的な syslog の優先度レベルのいずれかを選択します。

表 36-4　syslog の優先度レベル

レベル	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

syslog の動作とその設定方法の詳細については、システムに付属の資料を参照してください。UNIX または Linux ベースのシステムの syslog にログインしている場合、`syslog.conf` man ファイル（コマンドラインで `man syslog.conf` と入力）および syslog man ファイル（コマンドラインで `man syslog` と入力）に、syslog の動作とその設定方法に関する情報が示されます。

syslog 応答の設定

ライセンス：Protection

侵入ポリシーで syslog アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは syslog で検出した侵入イベントをすべて通知するようになります。syslog アラートの詳細については、Syslog 応答の使用（36-4 ページ）を参照してください。

syslog アラート オプションの設定方法：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

ステップ 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

ステップ 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

ステップ 4　外部応答の [Syslog アラート（Syslog Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Syslog アラート（Syslog Alerting）] ページが表示されます。

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。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（16-1 ページ）を参照してください。

ステップ 5　オプションで、[ロギング ホスト（Logging Hosts）] フィールドに、ロギング ホストとして指定するリモート アクセス IP アドレスを入力します。複数のホストを指定する場合は、カンマで区切ります。

ステップ 6　ドロップダウン リストからファシリティおよび優先度のレベルを選択します。

ファシリティおよび優先度オプションの詳細については、Syslog 応答の使用（36-4 ページ）を参照してください。

ステップ 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（15-15 ページ）を参照してください。