侵入ルールに関する外部アラートの設定

ASA FirePOWER モジュールのユーザ インターフェイスには侵入イベントに関するさまざまなビューがありますが、企業によっては、重要なシステムの継続的なモニタリングを容易にするために、外部侵入イベントの通知を定義したいという要望があります。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処理」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 および 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」セクションでは、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が説明されています。
- 「Syslog 応答の使用」セクションでは、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が説明されています。

- SNMP 応答の使用 （2 ページ）
- Syslog 応答の使用 （5 ページ）

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（/etc/sf/DCEALERT.MIB）から入手できます。

SNMP v2 オプション

SNMP v2 の場合、次の表で説明されているオプションを指定できます。

表 *1 : SNMP v2* オプション

オプション	説明
Trap Type	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、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
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。
Community String	コミュニティ名。
Sensor ID	侵入イベントを SNMP トラップとして送信する管理対象デバイスを表す、ユーザ定義の整数。

SNMP v3 オプション

SNMP v3 の場合、次の表で説明されているオプションを指定できます。

（注） SNMP v3 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、メッセージを復号化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 の場合、Engine ID は 0xAC10013201 です。また、アプライアンスの IP アドレスが 10.1.1.77 の場合、Engine ID として 0x0a01014D01 が使用されます。

オプション	説明
Trap Type	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、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
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。
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 Secure Hash Algorithm（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。
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。 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。
User Name	SNMP ユーザ名。

SNMP アラートの設定の詳細については、SNMP 応答の使用 （2 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 応答の設定 （3 ページ）を参照してください。

SNMP アラート オプションを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[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を参照してください。

[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 パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4 外部応答の [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、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[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 レイヤでのレイヤの使用」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 [as Binary] または [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、[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、[as String] オプションを使用します。たとえば、HP OpenView では [as String] オプションが必要になります。

ステップ 6 [SNMP v2] または [SNMP v3] を選択します。

- SNMP v2 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。SNMP v2 オプション （2 ページ） を参照してください。
- SNMP v3 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、「SNMP v3 オプション （3 ページ）」を参照してください。

（注） [SNMP v2] または [SNMP v3] を選択する必要があります。

（注） 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。

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」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 内の情報を優先順位別およびファシリティ別に分類することができます。優先順位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順位は 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
- リビジョン

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 の優先順位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順位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 *2*：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。

ファシリティ	説明
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の優先順位レベルのいずれかを選択します。

表 *3 : syslog* の優先順位レベル

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 （5 ページ）を参照してください。

syslog アラート オプションを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[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を参照してください。

[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 パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4 外部応答の [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、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[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 レイヤでのレイヤの使用」を参照してください。

ステップ 5 オプションで、[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順位のレベルを選択します。

ファシリティおよび優先順位オプションの詳細については、Syslog 応答の使用 （5 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」を参照してください。