侵入イベントの外部アラート

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）
- 侵入イベントに関する外部アラートのライセンス要件 （2 ページ）
- 侵入イベントに関する外部アラートの要件と前提条件 （2 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、Secure Firewall 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、長さと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。

（注） Secure Firewall 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。Secure Firewall 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フィルタ

侵入イベントに関する外部アラートのライセンス要件

Threat Defense ライセンス

IPS

従来のライセンス

保護

侵入イベントに関する外部アラートの要件と前提条件

モデルのサポート

任意

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

侵入イベントの SNMP アラートの設定

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。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイド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、Secure Firewall 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 サーバー（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 サーバー（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。
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。
ユーザー名（User Name）	SNMP ユーザー名。

侵入イベントの Syslog アラートの設定

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。[Syslogアラート（Syslog Alerting）] ページが [詳細設定（Advanced Settings）] ページの下に追加されます。

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。

[ロギングホスト（Logging Hosts）] フィールドを空白のままにした場合、ロギングホストの詳細は関連付けられているアクセス制御ポリシーの [ロギング（Logging）] から取得されます。

ステップ 4 侵入 syslog アラートの機能と重大度 （5 ページ）の説明に従って、[ファシリティ（Facility）] と **[重大度（Severity）]** の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。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

侵入 syslog アラートの機能と重大度

管理対象デバイスは、特定のファシリティと [重大度（Severity）] 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。これらのファシリティと [重大度（Severity）] 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。
CONSOLE	アラート メッセージ。
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。

ファシリティ	説明
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	ユーザー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 アラートの重大度

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

侵入イベントに対する電子メール アラートの設定

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 Secure Firewall Management Center から送信されます。

始める前に

- 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。
- Secure Firewall 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）] 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。

（注） 有効にすると、個々のルールが選択されていない限り、すべてのルールのアラートが有効になります。

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）

Secure Firewall 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）] を下げることもできます。

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。

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。