

ASDM (On-box Management) を使用した FirePOWER モジュールでのシステム/トラフィック イベントのロギングの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[出力先の設定](#)

[手順 1 : Syslog サーバの構成](#)

[ステップ 2 : SNMP サーバの構成](#)

[トラフィックのイベントを送信するための設定](#)

[接続イベントに外部ロギング](#)

[侵入イベントに外部ロギング](#)

[IP Security Intelligence/DNSセキュリティIntelligence/URL Security Intelligenceの外部ロギングを有効にします](#)

[SSLのイベントに外部ロギング](#)

[システム イベントを送信するための設定](#)

[システム イベントに外部ロギング](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

[関連するシスコ サポート コミュニティ ディスカッション](#)

概要

このドキュメントでは、FirePOWERモジュールの外部ロギング サーバでのイベントを送信するトラフィックのシステム イベントとさまざまな方法を説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA (適応型セキュリティ アプライアンス) ファイアウォール、ASDM (Adaptive Security Device Manager (ASDM)) の知識。
- FirePOWER アプライアンス。

- Syslog、SNMPプロトコル知識。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA Firepower モジュール (ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X)、ソフトウェア バージョン 5.4.1 以降を実行。
- ASAのFirePOWERモジュール (ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X) で、ソフトウェア バージョン6.0.0以上。
- ASDM 7.5(1) 以降。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

イベントのタイプ

Firepowerモジュールのイベントは、次の2種類に分類できます。

1. トラフィックのイベント (接続イベント/侵入イベント/セキュリティ インテリジェンス Events/SSLイベント/マルウェア/ファイル イベント) 。
2. システム イベント (FirePOWERのオペレーティング システム (OS) のイベント) 。

設定

出力先の設定

手順 1 : Syslog サーバの構成

トラフィックのイベントのSyslogサーバを、動きが設定> ASA FirePOWER設定>ポリシー>操作のアラートに設定し、作成のアラートのドロップダウン メニューをクリックし、選択肢を選ぶにSyslogアラートを作成します。Syslog サーバの値を入力します。

[Name] : Syslogサーバを示す名前を指定します。

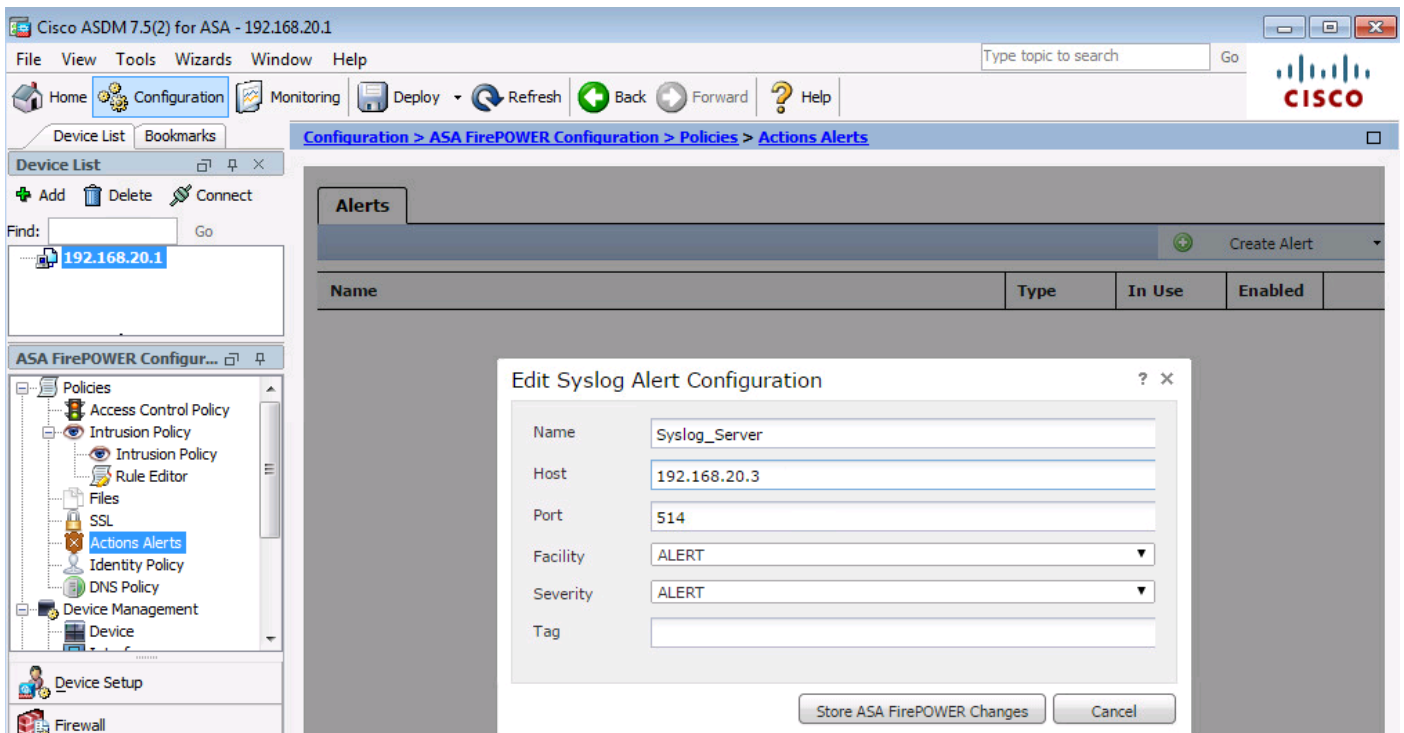
ホスト : SyslogサーバのIPアドレス/ホスト名を指定します。

[Port] : Syslog サーバのポート番号を指定します。

Facility : Syslogサーバに設定された機能を選択します。

Severity : syslogサーバで設定された重大度を選択します。

タグ : syslogメッセージを表示することタグ名を指定します。



ステップ 2 : SNMPサーバの設定

トラフィックのイベントのSNMPトラップサーバを設定するには、ASDM > ASA FirePOWER設定 > ポリシー > 操作のアラートに移動し、**作成のアラートのドロップダウンメニュー**をクリックして、オプションを作成するSNMPのアラートを選択します。

[Name] : SNMPトラップサーバを示す名前を指定します。

Trap Server : SNMPトラップサーバのIPアドレス/ホスト名を指定します。

バージョン FirepowerモジュールはSNMP v1/v2/v3をサポートしています。ドロップダウンメニューからSNMPバージョンを選択してください。

Community string : バージョンv1とv2のオプションを選択すると、SNMPコミュニティ名を指定します。

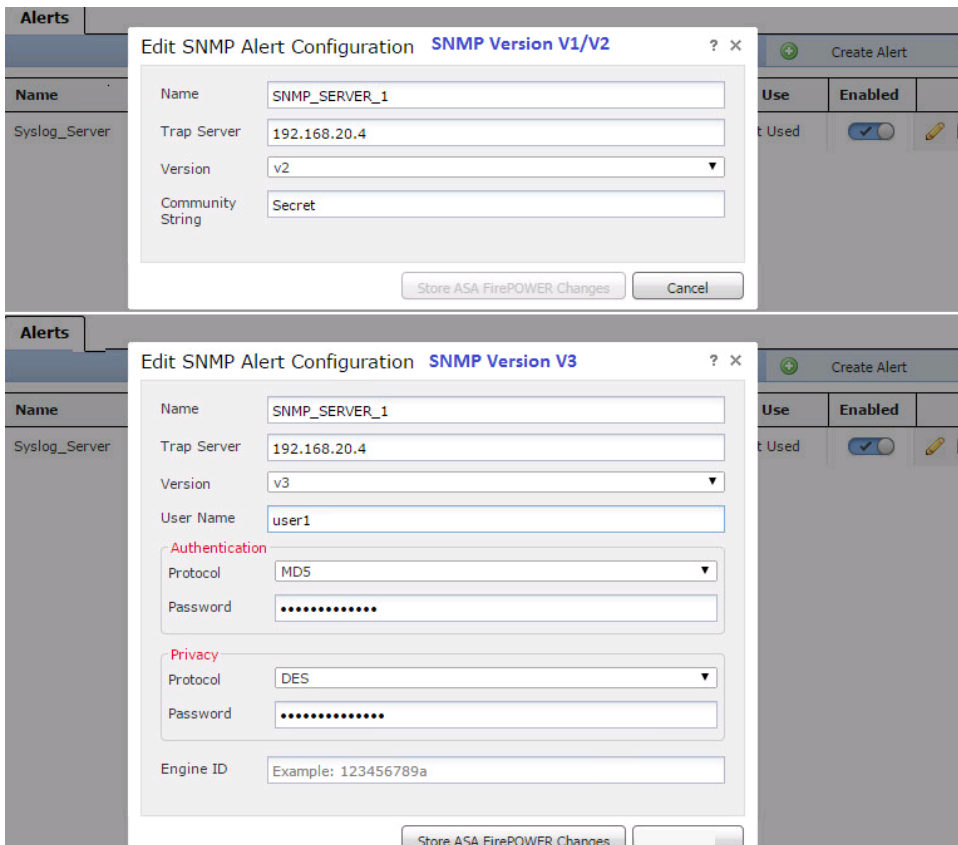
ユーザ名: バージョンv3のオプションを選択し、ユーザ名フィールドをサポートします。ユーザ名を指定します。

認証 : このオプションはSNMP v3設定の一部です。次のアルゴリズムに基づく認証が行われます : ハッシュアルゴリズム。

MD5またはSHAアルゴリズムを使用するアルゴリズム。プロトコルで**メニュー**を選択または入力ハッシュアルゴリズムを選択します

パスワード オプションのパスワード。この機能を使用するのでない限りNone)]オプションを選択します。

プライバシー (Privacy) : このオプションはSNMP v3設定の一部です。これはDESアルゴリズムを使用して暗号化を提供します。ProtocolドロップダウンメニューでDESがPasswordフィールドにパスワードを入力するオプションを選択します。データ暗号化機能を使用するのでない限りなしオプション選択しないでください。



トラフィックのイベントを送信するための設定

接続イベントに外部ロギング

接続イベントはトラフィックが有効なロギング アクセス ルールに一致すると生成されます。接続イベントの外部ロギングを有効にするには、[(ASDM > ASA FirePOWER設定>ポリシー>アクセス制御ポリシー) アクセス ルールを編集し、ログ オプションに移動します。

接続の端末の**接続の始まりと終わりにログ オプションlogまたはログ**を選択します。接続イベントを送信し、**オプション**で指定するイベントの送信先を移動します。

イベントを外部syslogサーバに[Syslogに**送信して**ドロップダウン リストからSyslogアラートの応答を選択します。オプションで、Syslog アラート応答を追加するには、追加アイコンをクリックします。

接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。オプションで、追加アイコンをクリックして SNMP アラート応答を追加することもできます。

Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

ASA ASA FirePOWER

Editing Rule - WebsiteBlock

Name: WebsiteBlock Enabled [Move](#)

Action: Block with reset IPS: no policies Variables: n/a Files: no inspection Logging: connections: Event Viewer, syslog, s

Zones Networks Users Applications Ports **URLs** ISE Attributes Inspection Logging

Log at Beginning and End of Connection
 Log at End of Connection
 No Logging at Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog (Connection Event only)
 SNMP Trap

[Save](#)

侵入イベントに外部ロギング

シグニチャ (Snortルール) が悪意のあるトラフィックと一致すると、侵入イベントが生成されます。侵入イベントの外部ロギングを有効にするには、[ASDM Configuration] > [ASA Firepower Configuration] > [Policies] > [Intrusion Policy] > [Intrusion Policy]に移動します。新しい侵入ポリシーを作成するか、既存の侵入ポリシーを編集します。「拡張設定」>「外部応答」に移動します。

侵入イベント、警告するSNMPの[Enabledオプションを外部SNMPサーバに送信して編集オプションをクリックします。

Trap Type : トラップ タイプはアラートに表示される IP アドレスに使用されます。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、[Binary]を選択できます。そうでない場合は、[String]を選択します。

SNMP Version : 次のいずれかを選択します バージョン 2 または バージョン 3 オプションボタンを選択します。

SNMP v2 オプション

Trap Server : このイメージに示すように、SNMP トラップ サーバの IP アドレス/ホスト名を指定します。

Community String : コミュニティ名を指定します。

SNMP v3 オプション

Trap Server : このイメージに示すように、SNMP トラップ サーバの IP アドレス/ホスト名を指定します。

Authentication Password : このインスタンスのパスワードが必要です。SNMP v3はパスワードの

認証にハッシュ関数を使用します。

プライベートパスワード：暗号化のパスワードを指定します。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。

ユーザ名：ユーザ名を指定します。

Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

The screenshot shows the 'SNMP Alerting' configuration page for an intrusion policy. The left sidebar contains a navigation menu with 'Policy Information', 'Rules', 'Advanced Settings', 'Global Rule Thresholding', 'SNMP Alerting', and 'Policy Layers'. The main content area is titled 'SNMP Alerting' and includes a '< Back' link. Under the 'Settings' section, 'Trap Type' is set to 'as Binary' and 'SNMP Version' is set to 'Version 2'. The 'SNMP v2' section contains a 'Trap Server' field with the value '192.168.20.3' and a 'Community String' field with the value 'Secret'.

Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy

The screenshot shows the 'SNMP Alerting' configuration page for an intrusion policy, similar to the previous one but with 'SNMP Version' set to 'Version 3'. The 'SNMP v3' section contains a 'Trap Server' field with the value '192.168.20.3', an 'Authentication Password' field with masked characters, a 'Private Password' field with masked characters and a note '(SNMP v3 passwords must be 8 or more characters)', and a 'Username' field with the value 'user3'. A 'Revert to Defaults' button is located at the bottom right of the configuration area.

外部Syslogサーバに侵入イベントを送信するには、オプションを選択します **有効 syslog内 アラート** 次に、 **編集** オプションを選択します。

Logging Host：Syslog サーバの IP アドレス/ホスト名を指定します。

Facility：任意のファシリティを選択 syslogサーバに設定されます。

Severity：syslogサーバで設定された重大度を選択します。



IP Security Intelligence/DNSセキュリティIntelligence/URL Security Intelligenceの外部ロギングを有効にします

IP Security Intelligence/DNSセキュリティIntelligence/URLセキュリティ インテリジェンス イベントはトラフィックがIPアドレス/ドメイン名/URL Security Intelligenceのデータベースに一致したときに生成されます。IP/URL/DNSセキュリティ インテリジェンス イベントの外部ロギングを有効にするには、移動 (ASDM > ASA FirePOWER設定>ポリシー>アクセス制御ポリシー>セキュリティ インテリジェンス)、

IP/DNS/URL Security Intelligenceの記録を有効にするには、図に示すようにアイコンをクリックします。アイコンをクリックすると、外部サーバにイベントを送信するとロギング オプションを有効にする)]ダイアログボックスが表示されます。

イベントを外部syslogサーバに[Syslogに送信してドロップダウン リストからSyslogアラートの応答を選択します。オプションで、Syslog アラート応答を追加するには、追加アイコンをクリックします。

接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。オプションで、追加アイコンをクリックして SNMP アラート応答を追加することもできます。

Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy

ASA ASA FirePOWER

Default Allow All Traffic Show Warnings

Enter a description

Status: Access Control policy out-of-date on device

Identity Policy: None SSL Policy: None

Rules Security Intelligence HTTP Responses Advanced

Available Objects Available Zones

Search for a URL

Networks URLs

Global-Blacklist-for-URL
Global-Whitelist-for-URL
URL Attackers
URL Bogon
URL Bots
URL CnC
URL Malware
URL Open_proxy

Any

Add to Whitelist
Add to Blacklist

DNS Policy: Default DNS Policy

Whitelist (2)

Networks
Global-Whitelist (Any Zone)

URLs
Global-Whitelist-for-URL (Any)

Enable logging for DNS blacklisting Events

Blacklist (2)

Networks
Global-Blacklist (Any Zone)

URLs
Global-Blacklist-for-URL (Any)

Enable logging for IP SI Events

Enable logging for URL SI Events

SSLのイベントに外部ロギング

SSLのイベントはトラフィックの録音が有効なSSLポリシー ルールに一致すると生成されます。SSLトラフィックの外部ロギングを有効にするには、[ASDM Configuration] > [ASA Firepower Configuration] > [Policies] > [SSL]に移動します。既存のルールを編集するか、新しいルールを作成し、[log at End of Connection]オプションを選択します。

接続イベントを送信して指定するイベントの送信先を移動します。

イベントを外部 Syslog サーバに送信するには、[Syslog] を選択してからドロップダウン リストから Syslog アラート応答を選択します。オプションで、Syslog アラート応答を追加するには、追加アイコンをクリックします。

接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。オプションで、追加アイコンをクリックして SNMP アラート応答を追加することもできます。

Default SSL Policy

SSL Policy

Editing Rule - SSL_Re_Sign

Name: Enabled Move:

Action: with Replace Key

Zones	Networks	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
-------	----------	-------	--------------	-------	----------	-------------	----	-------------	--------------	---------

Log at End of Connection

Send Connection Events to:

Event Viewer

Syslog

SNMP Trap

システム イベントを送信するための設定

システム イベントに外部ロギング

システム イベントがFirePOWERのオペレーティング システムのステータスを示します。SNMPマネージャはこれらのシステム イベントのポーリングに使用できます。

FirePOWERモジュールからのシステム イベントをポーリングするためのSNMPサーバを設定するには情報をSNMPサーバからポーリングできるFirePOWER Management Information Base (MIB) で行うシステム ポリシーを設定する必要があります。

ASDM > ASA FirePOWER設定>ローカル システム> Policies]に移動し、**SNMP**をクリックします。

SNMP Version : FirepowerモジュールはSNMP v1/v2/v3をサポートしています。SNMPバージョンを指定してください。

Community string : SNMPバージョン オプションのv1/v2を選択したら、コミュニティ スtring フィールドのSNMPコミュニティ名を入力します。

ユーザ名: オプションのバージョンv3オプションを選択します。ユーザの追加]ボタンをクリックし、[ユーザ名]フィールドにユーザ名を指定します。

認証 : このオプションはSNMP v3設定の一部です。MD5 または SHA アルゴリズムを使用する、ハッシュ メッセージ認証コードに基づく認証を提供します。ハッシュ アルゴリズムの protocols を選択するとパスワードを入力します

([Password] フィールド)。認証機能を使用すると思わなかつたりNone)]オプションを選択します。

プライバシー (Privacy) : このオプションはSNMP v3設定の一部です。これはDES/AESアルゴリズムを使用して暗号化を提供します。プロトコルの暗号化を選択すると、[Password]フィールドにパスワードを入力します。データ暗号化機能を必要と思わなかつたりなしオプション選択しないでください。

Policy Name	Default
Policy Description	Default System Policy
Status: System policy out-of-date on device	
SNMP Version V1/V2	
Access List	
Email Notification	
▶ SNMP	
STIG Compliance	
Time Synchronization	
SNMP Version	Version 2 ▼
Community String	Secret
Save Policy and Exit	Cancel

Policy Name	Default
Policy Description	Default System Policy
Status: System policy out-of-date on device	
SNMP Version V3	
Access List	
Email Notification	
▶ SNMP	
STIG Compliance	
Time Synchronization	
Username	user2
Authentication Protocol	SHA ▼
Authentication Password
Verify Password
Privacy Protocol	DES ▼
Privacy Password
Verify Password
	Add
Save Policy and Exit	Cancel

(MIB)FirepowerMIB(DCEALERT.MIB)(etc/sf/DCEALERT.MIB)

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)