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

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。

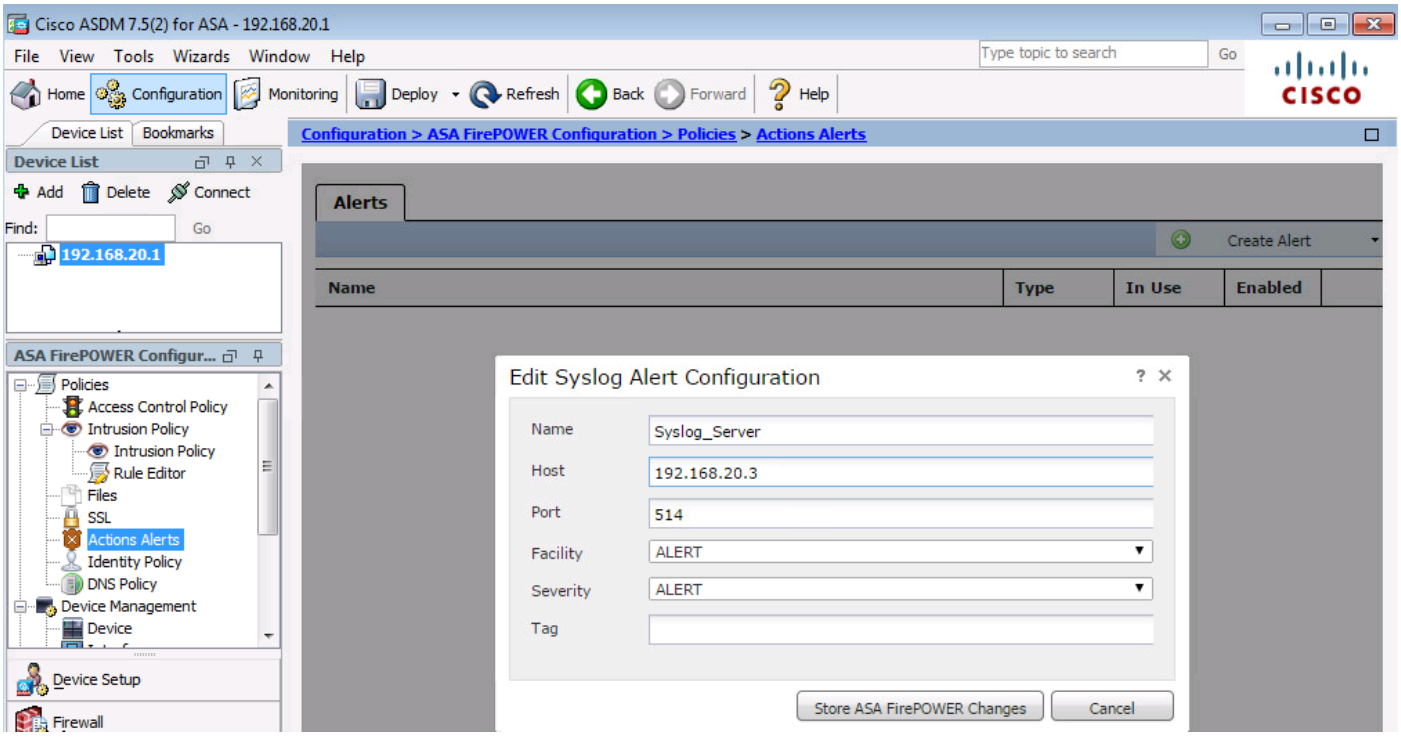
ホスト：SyslogサーバのIPアドレス/ホスト名を指定します。

[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。**

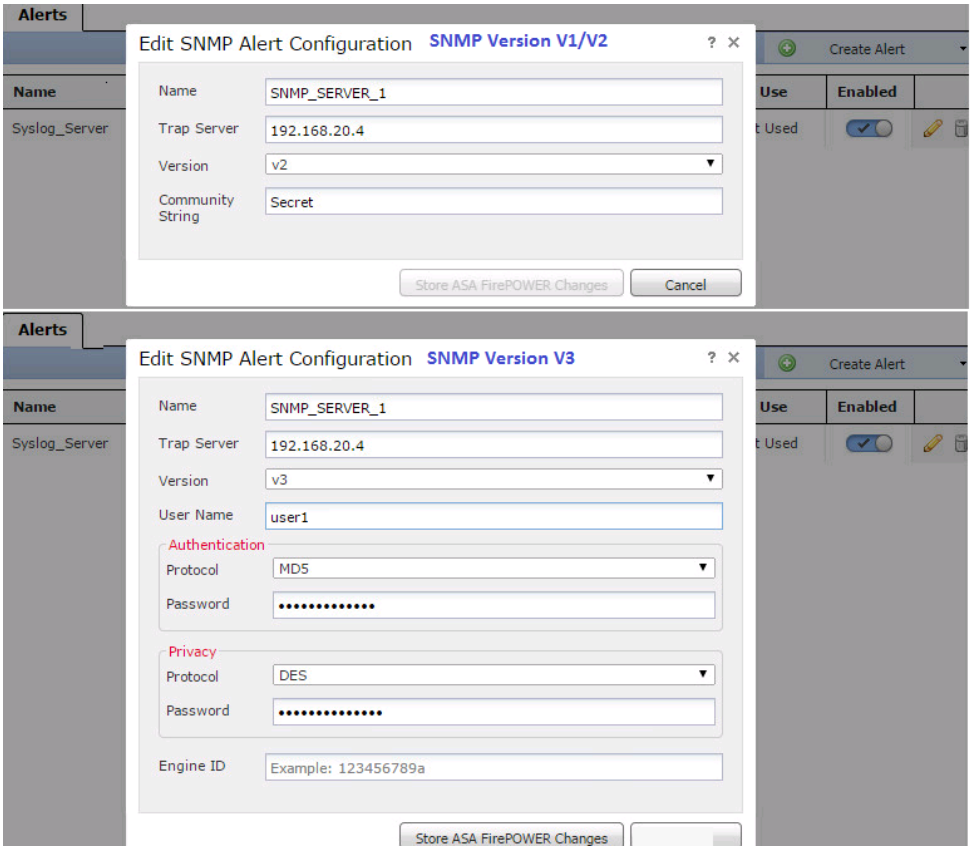
ユーザ名: バージョンv3のオプションを**選択し、ユーザ名フィールドをサポートします。**ユーザ名を指定します。

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

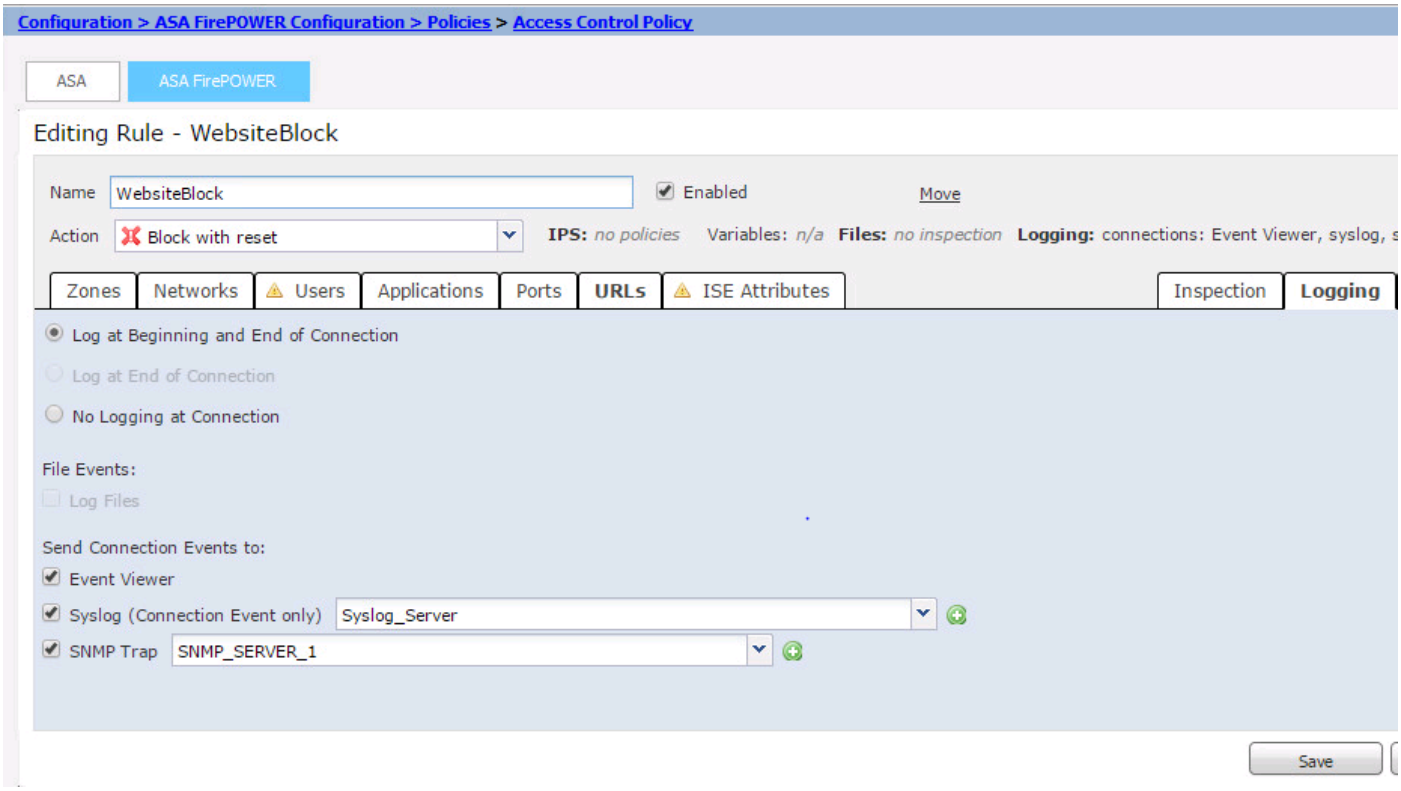
接続イベントに外部ロギング

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。



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

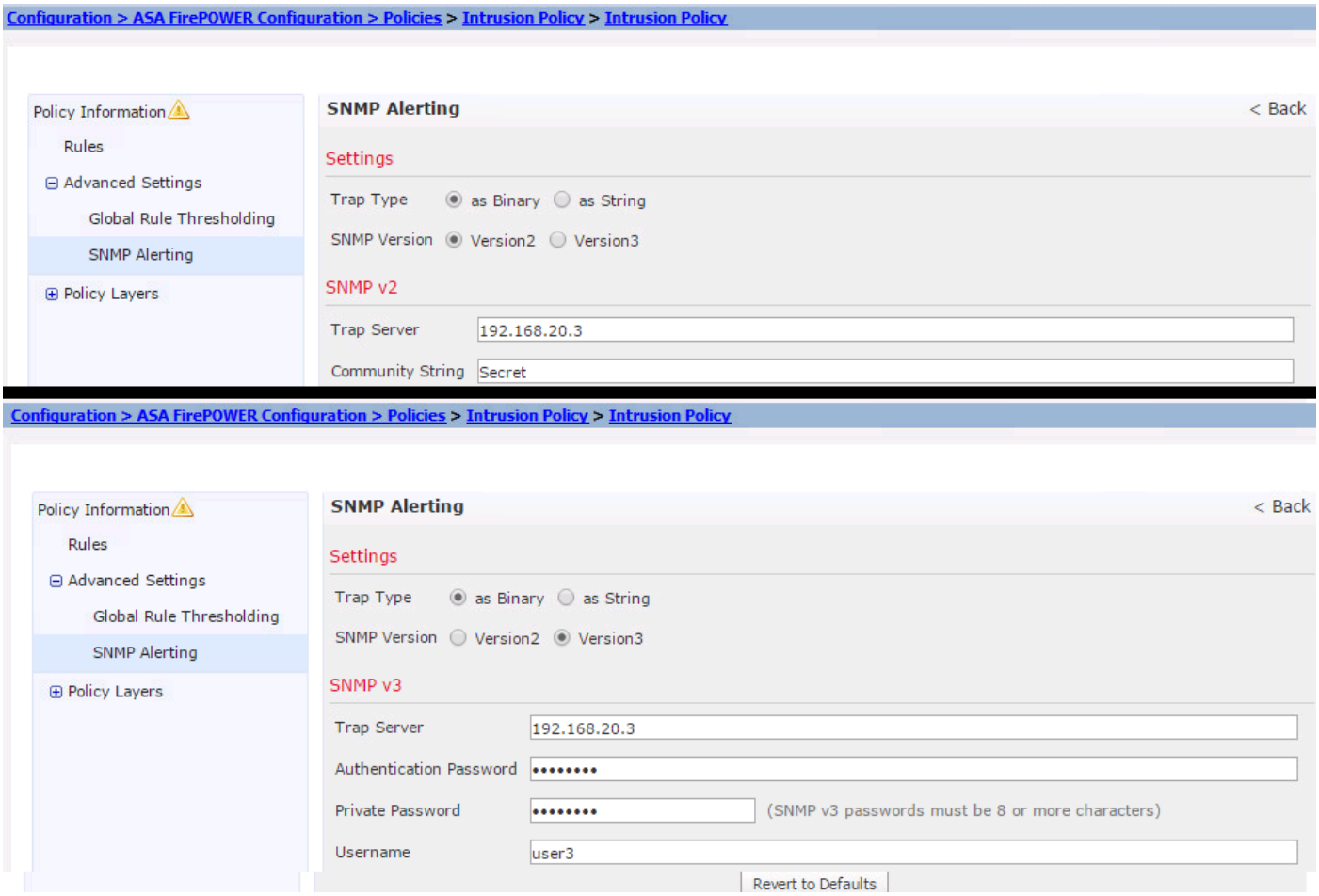
Trap Server：このイメージに示すように、SNMP トラップ サーバの IP アドレス/ホスト名を指定します。

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。



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。

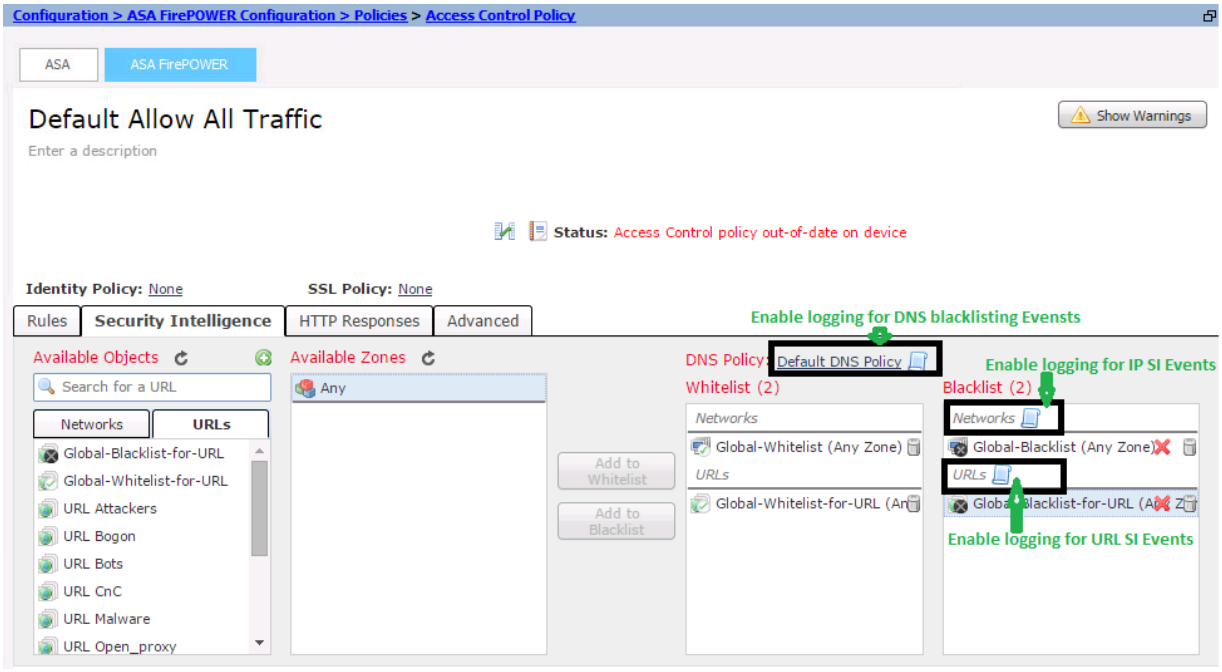
IP Security Intelligence/DNSセキュリティIntelligence/URL Security Intelligenceの外部ロギングを有効にします

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。



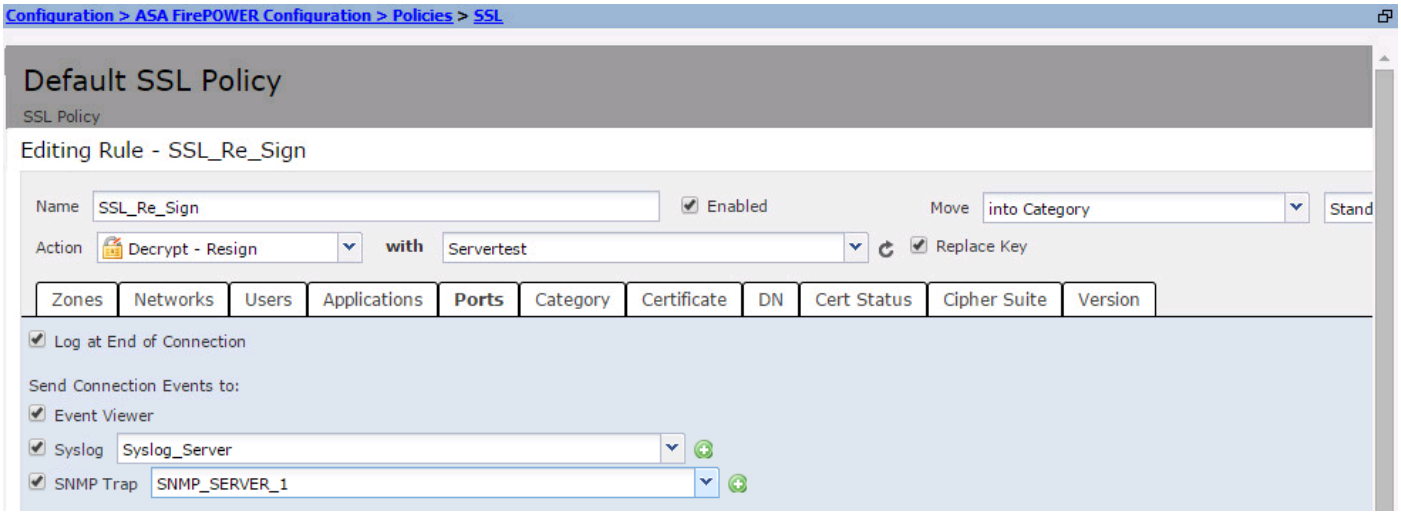
SSLのイベントに外部ロギング

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。



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。

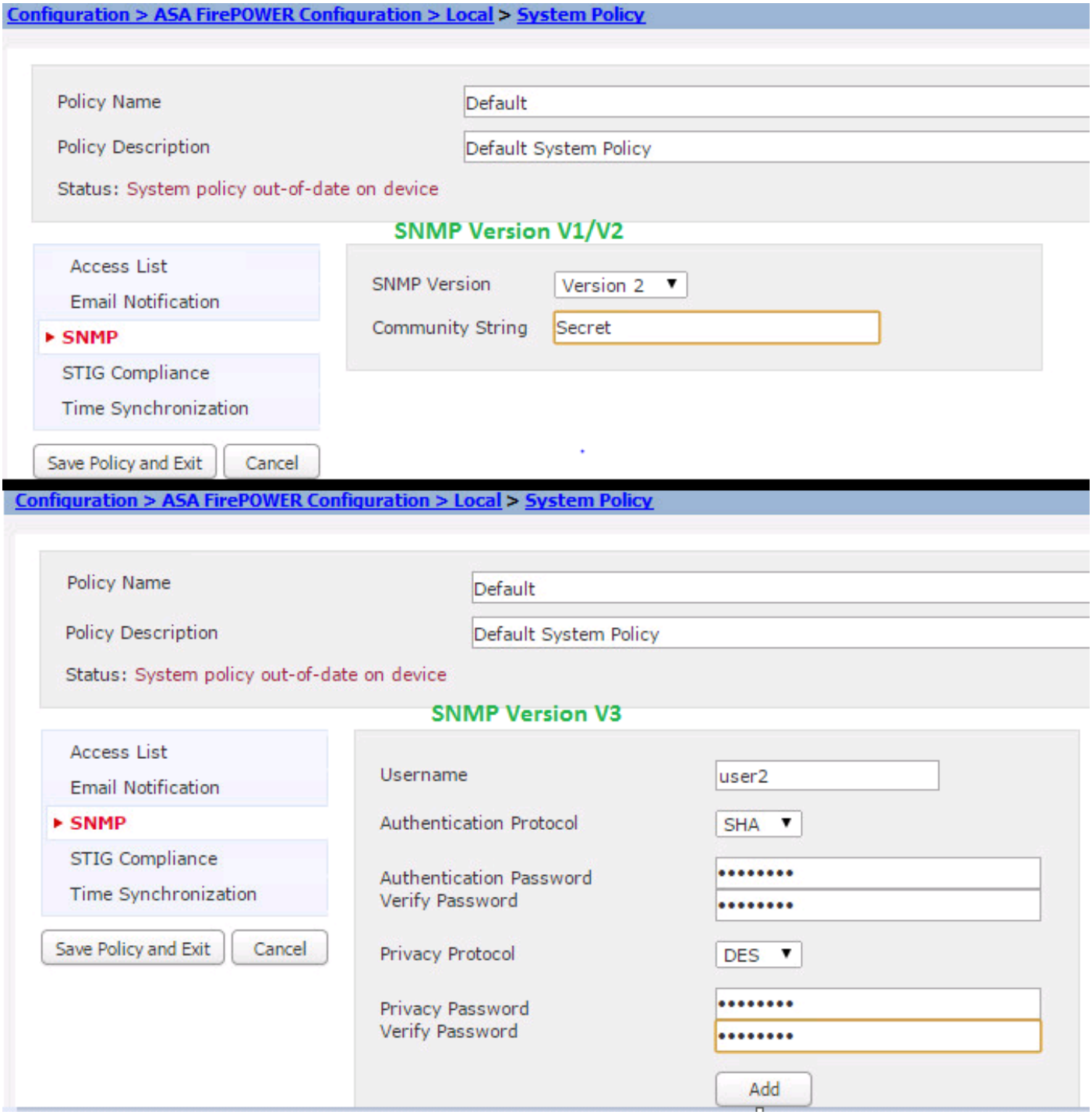
Community string： SNMPバージョン オプションのv1/v2を選択したら、コミュニティ ストリング フィールドのSNMPコミュニティ名を入力します。

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 **アルゴリズムのプロトコル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ったり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ったりなしオプション選択しないでください。



(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。

トラブルシュート

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