

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

目次

[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に外部ロギング](#)

[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](#)

[Cisco サポート コミュニティ - 特集対話](#)

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アプライアンスの知識。
- 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くものです。

- ASAのFirePOWERモジュール (ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X) で、ソフトウェア バージョン5.4.1以上。
- 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。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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つのタイプに分類できます: -

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。

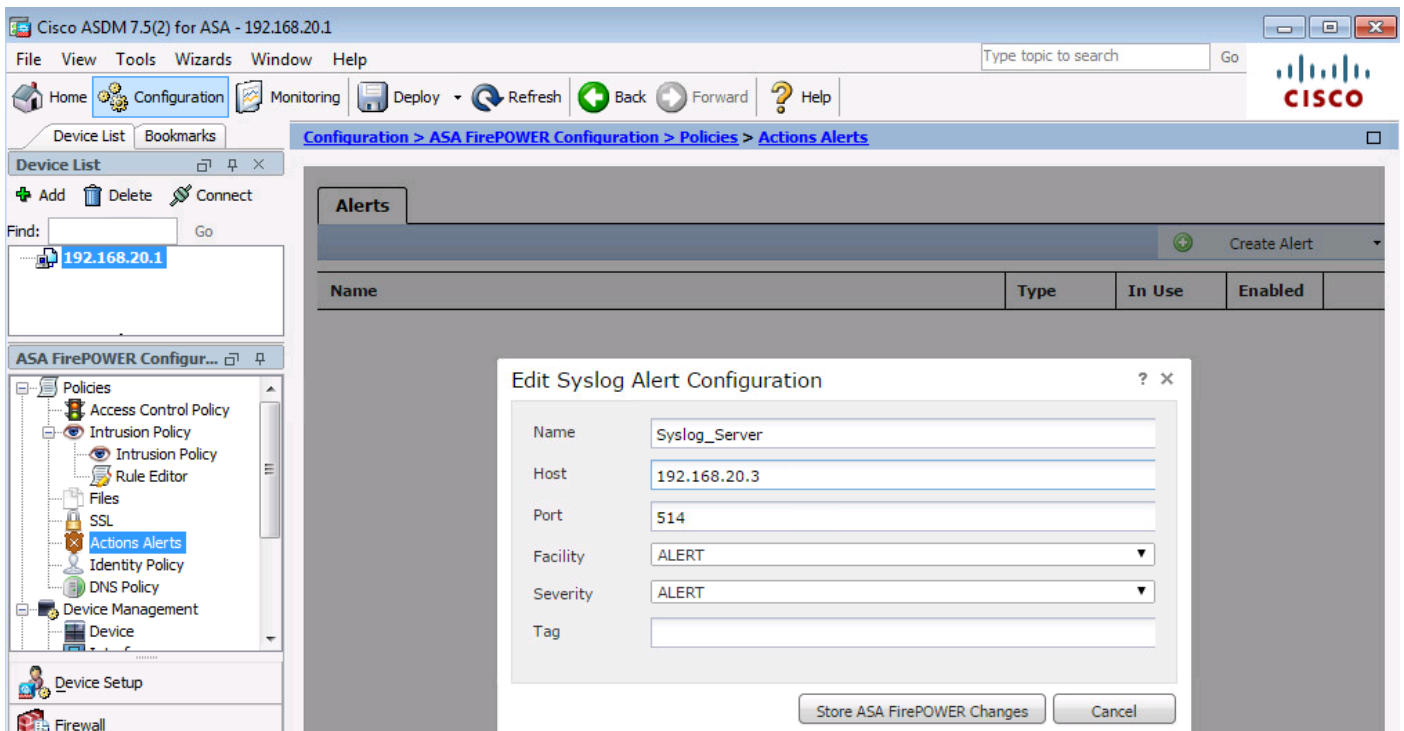
Host : Syslog サーバの IP アドレス/ホスト名を指定します。

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。

Tag : 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 サーバの構成

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。

Version : FirePOWERモジュールはSNMP v1/v2/v3をサポートします。ドロップダウンメニューからSNMPバージョンを選択します。

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。

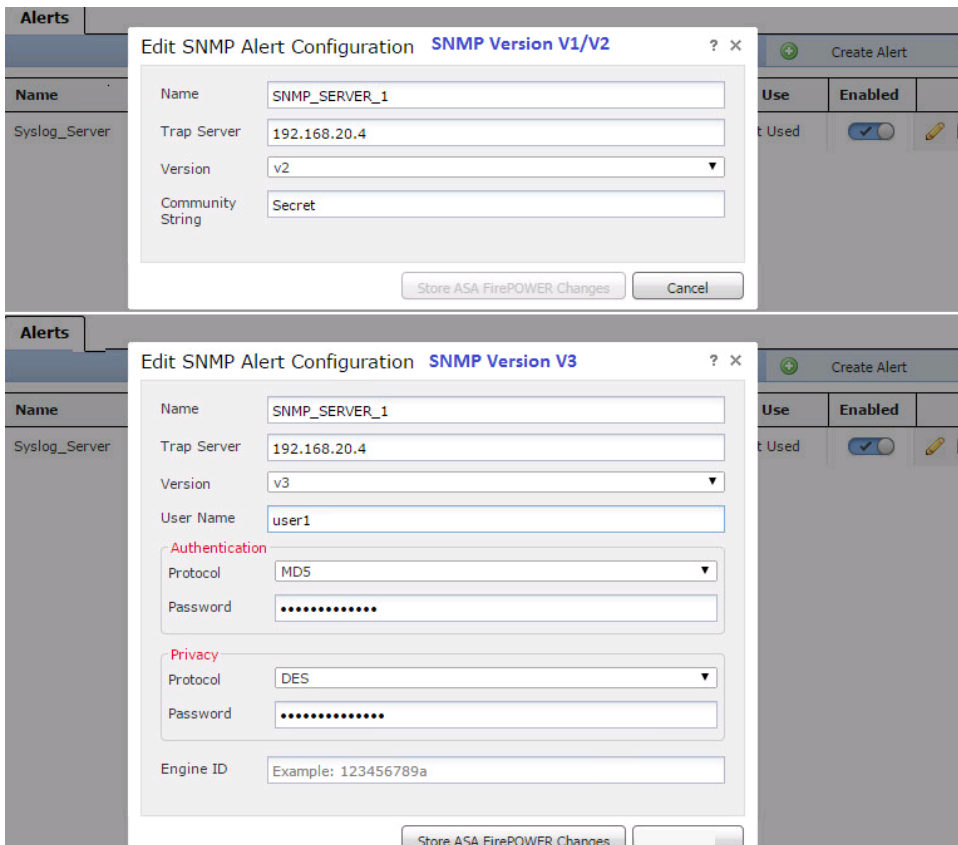
Username : バージョンv3のオプションを選択し、ユーザ名フィールドをサポートします。ユーザ名を指定します。

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 [v](#) 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) Syslog_Server [v](#) [+](#)
 SNMP Trap SNMP_SERVER_1 [v](#) [+](#)

[Save](#)

侵入イベントに外部ロギング

侵入イベントはシグニチャ (Snort Rule) が悪意のあるトラフィックに一致すると生成されます。侵入イベントの外部ロギングも移行ASDM > ASA FirePOWER設定> Policies> Intrusion Policy >侵入ポリシーを有効にします。新しい侵入ポリシーを作成または詳細設定に既存の侵入 Policy.Navigate >外部応答を編集します。

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 : バージョン バージョン2または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 : Specifypasswordは認証のために必要です。SNMP v3はパスワードの認証にハッシュ関数を使用します。

Private Password : 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

Policy Information 

- Rules
- Advanced Settings
 - Global Rule Thresholding
 - SNMP Alerting**
- Policy Layers

SNMP Alerting

< Back

Settings

Trap Type as Binary as String

SNMP Version Version2 Version3

SNMP v2

Trap Server

Community String

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

Policy Information 

- Rules
- Advanced Settings
 - Global Rule Thresholding
 - SNMP Alerting**
- Policy Layers

SNMP Alerting

< Back

Settings

Trap Type as Binary as String

SNMP Version Version2 Version3

SNMP v3

Trap Server

Authentication Password

Private Password (SNMP v3 passwords must be 8 or more characters)

Username

[Revert to Defaults](#)


外部syslogサーバに侵入イベントを送信するには、[警告するsyslogで有効になる選択オプション]では、次に示すように[Edit Options]をクリックします。

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

Facility : 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。

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

Policy Information 

- Rules
- Advanced Settings
 - Global Rule Thresholding
 - SNMP Alerting
 - Syslog Alerting**
- Policy Layers

Syslog Alerting

< Back

Settings

Logging Hosts (Single IP address or comma-separated list)

Facility

Priority

[Revert to Defaults](#)

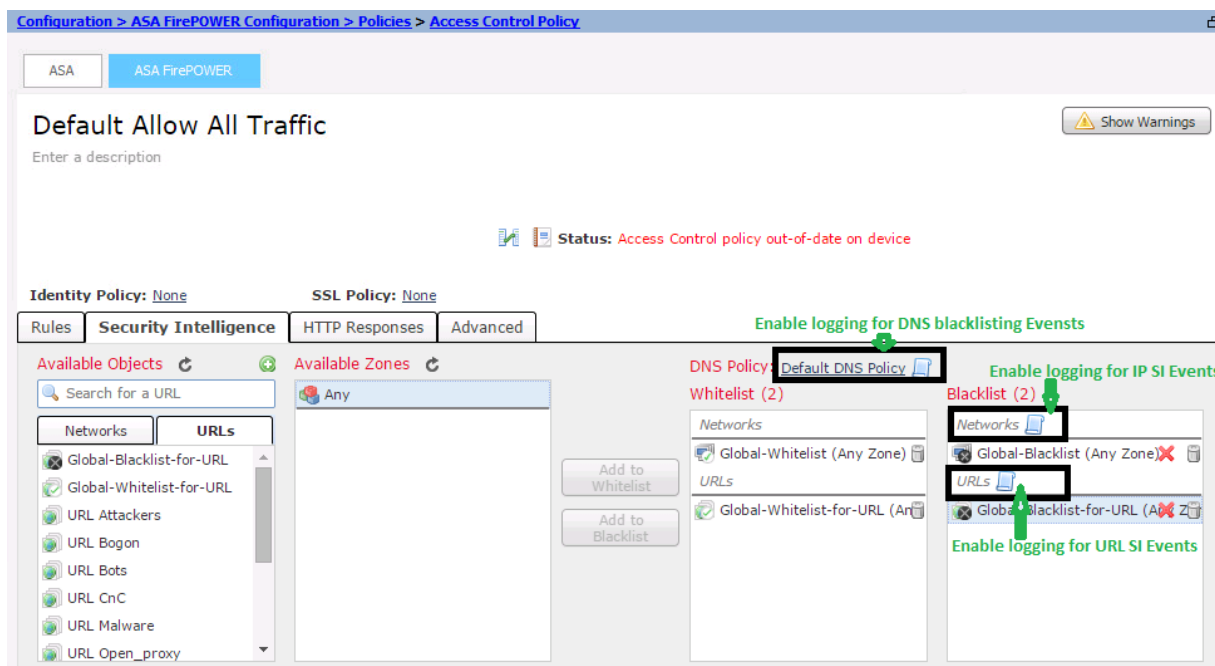
IP Security Intelligence/DNSセキュリティIntelligence/URL Security Intelligenceの外部ロギングを有効にします

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。



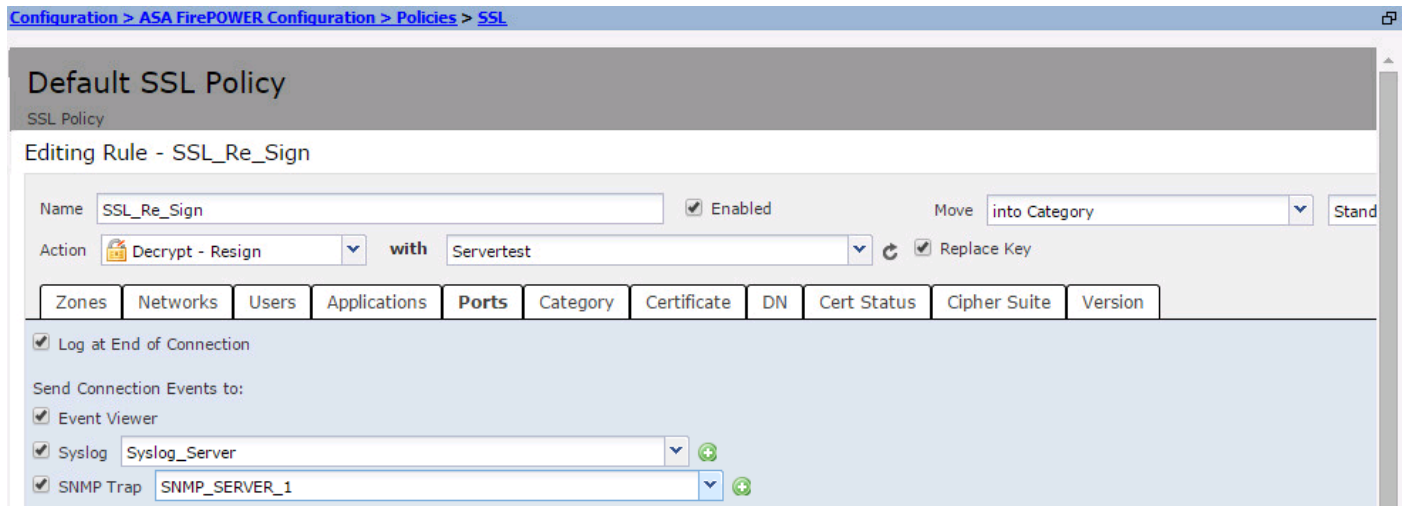
SSLのイベントに外部ロギング

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トラフィック用の外部ロギングも移行ASDM > ASA FirePOWER設定>ポリシー> SSLを有効にする。プレゼンスを編集または新しいルールを作成し、ログ オプションに移動します。接続オプションの最後にlog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 をサポートします。SNMP バージョンを指定します。

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。

Username : 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。

[Configuration](#) > [ASA FirePOWER Configuration](#) > [Local](#) > [System Policy](#)

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

[Configuration](#) > [ASA FirePOWER Configuration](#) > [Local](#) > [System Policy](#)

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

: MIB FirePOWERMIBDCEALERT.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

現在のところ、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](#)