**Document ID**: 118735

**Updated**: 2015 年 2 月 10 日

Sumit Bist によって貢献される、Cisco TAC エンジニア。



### 関連製品

- セキュリティ
- Cisco Catalyst 6500 シリーズ ファイアウォール サービス モジュール

# 目次



# 概要

この資料はリリース 4.1.11 またはそれ以降にソフトウェアアップグレードの後で Firewall Services Module（FWSM）の断続的なトラフィック ドロップにおける特定の問題を記述したものです。

# 前提条件

### 要件

このドキュメントに関する固有の要件はありません。

### 使用するコンポーネント

この文書に記載されている情報はソフトウェア リリース 4.1(11) または それ 以降との FWSM に基づいています。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 背景説明

FWSM 動作によって、syslog サーバにメッセージを送るために口ギング転送 プロトコルとして TCP を使用すればそれはセキュリティ対策として FWSM が syslog サーバに達することができない場合新しい接続を否定します。 この制約事項を **logging permit-hostdown** 取除くためにコマンドを使用できます。

## 問題

リリース 4.1.11 またはそれ以降へアップグレードの後に FWSM に断続的なトラフィック ドロップする問題があります。 FWSM はすべての新しい接続を否定し始めます。

最も顕著なトラフィック ドロップするはインターネット制御メッセージ プロトコル （ICMP）のため各 ICMP工コー要求が新しい接続として扱われるので、です。 接続は syslog サーバへの TCP 接続が正常なら復元する。

FWSM リリース 4.1.11 またはそれ以降に関しては、TCP ベースの syslog サーバが「許可 hostdown」ポリシーと到達可能でなければ、FWSM はすべての新しい接続を否定します。「口ギング許可hostdown」機能はリリース 4.1.11 またはそれ以降にもはや後 FWSM アップグレード動作しませんでした。

FWSM はタイム サーバーが稼働しているまで Tcp syslog にサーバを毎分再接続し続けます。 従って、単一 TCP ハンドシェイク失敗はすべての**新しい接続**のための最小分停止 1 つという結果に 1 分の後やっと FWSM が Tcp syslog サーバを再度接続することを試みるので終ります。

### 条件

- FWSM はリリース 4.1.11 またはそれ以降を実行します。
- FWSM はシングル モードにあるはずです。
- Tcp syslog サーバは FWSM から到達不能である必要があります。

### 確認

この動作を確認するために、遅いパス（NP3）統計情報をチェックして下さい。 拒否 Conns

（Conn 状態）カウンターは TCP ベースの syslog サーバが到達可能でなければ、増えます「許可hostdown」ポリシーと。

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014

pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
------------------

Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <------Counter to monitor

pri/act# show clock
09:32:06.020 GMT Thu May 15 2014

pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
------------------

Egress Discards : 46634
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 46235 <------Counter seen increasing
```

# 解決策

問題はこの問題をトラッキングするためにファイルされましたが FWSM がソフトウェアメンテナンスリリース日付の端に達したので固定ではないです。

[ファイアウォールサービス モジュールのための終りの販売およびサポート終了（EOL）速報]

この問題を解決するために、UDP 転送するに口グ収集サーバ 設定を変更して下さい。

```
pri/act# show clock
09:31:55.070 GMT Thu May 15 2014

pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
------------------

Egress Discards : 34412
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 34013 <------Counter to monitor

pri/act# show clock
09:32:06.020 GMT Thu May 15 2014

pri/act# show np3 stats | ex : 0
<<NP 3 stats>>
Discard Statistics
```

```
------------------

Egress Discards : 46634
ACL Denied Packets : 157
Rev Route Lkup Fail : 202
Self Route Packets : 40
Deny Conns (Conn State): 46235 <------Counter seen increasing
```

## 関連情報

- コマンド リファレンス： 許可hostdown の記録
- コマンド リファレンス： logging host
- テクニカルサポートとドキュメント - Cisco Systems



## Cisco サポート コミュニティ - 特集対話

Cisco サポート コミュニティでは、フォーラムに参加して情報交換することができます。



Updated: 2015 年 2 月 10 日
Document ID: 118735