



ID de document : 118735

Mis à jour : FÉV 10, 2015

Contribué par Sumit Bist, ingénieur TAC Cisco.



[PDF de téléchargement](#)



[Copie](#)

[\[+\] Feedback](#)

## Produits connexes

- [Sécurité](#)
- [Module de services pare-feu de la gamme Cisco Catalyst 6500](#)

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Conditions](#)

[Vérifiez](#)

[Solution](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

## Introduction

Ce document décrit un problème spécifique avec des baisses intermittentes du trafic sur le Module de services de Pare-feu (FWSM) après une mise à niveau de logiciel pour libérer 4.1.11 ou plus tard.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

## Composants utilisés

Les informations dans ce document sont basées sur le FWSM avec la version de logiciel 4.1(11) ou ultérieures.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Informations générales

Selon le comportement FWSM, si vous utilisez le TCP pendant que le protocole de transport se connectant afin d'envoyer message à un serveur de Syslog, il refuse de nouvelles connexions comme mesure de sécurité si le FWSM ne peut pas atteindre le serveur de Syslog. Vous pouvez employer **logging permit-hostdown** la commande afin de retirer cette restriction.

## Problème

Il y a une question intermittente de baisse du trafic sur le FWSM après une mise à jour pour libérer 4.1.11 ou plus tard. Les débuts FWSM pour refuser toutes les nouvelles connexions.

La baisse du trafic la plus apparente est pour le Protocole ICMP (Internet Control Message Protocol), puisque chaque requête d'écho d'ICMP est traitée comme nouvelle connexion. La Connectivité est restaurée une fois que la connexion TCP au serveur de Syslog est réussie.

Pour FWSM libérez 4.1.11 ou plus tard, si le serveur basé sur TCP de Syslog n'est pas accessible même avec la stratégie de « autorisation-hostdown », le FWSM refuse toutes les nouvelles connexions. La caractéristique « se connectant autorisation-hostdown » ne fonctionne plus après qu'une mise à jour FWSM pour relâcher 4.1.11 ou plus tard.

Le FWSM continue à rebrancher au serveur de Syslog de TCP chaque minute jusqu'à ce que le Serveur de synchronisation soit en fonctionnement. Ainsi, une panne simple de prise de contact de TCP a comme conséquence une panne minute minimum pour toutes les **nouvelles** connexions, parce que les essais FWSM pour contacter le serveur de Syslog de TCP de nouveau, seulement après qu'une minute.

## Conditions

- La version 4.1.11 de passages FWSM ou plus tard.
- Le FWSM devrait être dans le mode unique.
- Le serveur de Syslog de TCP doit être inaccessible du FWSM.

## Vérifiez

Afin d'identifier ce comportement, vérifiez les statistiques lentes du chemin (NP3). Le compteur de Conns de refuser (état conn.) augmente si le serveur basé sur TCP de Syslog n'est pas accessible, même avec la stratégie de « autorisation-hostdown ».

```
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
```

## Solution

Un défaut a été classé pour dépister cette question, mais il ne sera pas réparé puisque le FW5600 a atteint l'extrémité de la date de sortie de maintenance logicielle.

[Annonce de fin de commercialisation et de fin de vie pour des Modules de services de Pare-feu](#)

Afin de réparer cette question, changez la configuration du serveur se connectante au transport d'UDP.

```
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

## [Informations connexes](#)

- [Référence de commandes : se connecter l'autorisation-hostdown](#)
- [Référence de commandes : hôte de journalisation](#)
- [Support et documentation techniques - Cisco Systems](#)

Ce document était-il utile ? [Oui aucun](#)

Merci de votre feedback.

[Ouvrez une valise de support](#) (exige un [contrat de service Cisco](#).)

## **Cisco relatif prennent en charge des discussions de la Communauté**

[Cisco prennent en charge la Communauté](#) est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au [Conventions relatives aux conseils techniques Cisco](#) pour les informations sur des conventions utilisées dans ce document.

Mis à jour : FÉV 10, 2015

ID de document : 118735