

# Panne automatique de mise à jour de téléchargement à un centre de Gestion de puissance de feu

## Contenu

[Introduction](#)

[Possibles raison pour la panne](#)

[Incidence](#)

[Vérification](#)

[Vérifiez les configurations de DN](#)

[Vérifiez la connexion](#)

[Dépannez](#)

[Documents connexes](#)

## Introduction

Ce document discute des raisons une tâche programmée de mettre à jour un centre de Gestion de puissance de feu de Cisco pourrait échouer. Vous pouvez mettre à jour un centre de Gestion de puissance de feu de Cisco manuellement ou automatiquement. Afin d'exécuter une mise à jour logicielle automatique, vous pouvez créer une tâche de programme à votre centre de Gestion de s'exécuter à un futur temps.

## Possibles raison pour la panne

Un centre de Gestion de puissance de feu pourrait pour télécharger un fichier de mise à jour de l'infrastructure de mise à jour de téléchargement de Cisco quand une de ces actions se produit dans votre réseau :

- Stratégie de sécurité de votre trafic de Système de noms de domaine (DNS) de blocs de société.
- Configuration en dehors de votre téléchargement d'incidences de centre de Gestion. Par exemple, une règle de Pare-feu pourrait permettre seulement une adresse IP pour `support.sourcefire.com`.

**Attention** : Cisco utilise des DN de recherche séquentielle pour l'Équilibrage de charge, la tolérance aux pannes, et la disponibilité. Par conséquent, les adresses IP du mgih de serveurs DNS changent.

## Incidence

Si vous utilisez cette méthode...

Configuration de paramètres systèmes par défaut pour le téléchargement automatique

Action à  
entreprendre  
Aucune action

Téléchargez le fichier de mise à jour manuellement et téléchargez-le au centre de Gestion de puissance de feu

Les règles de Pare-feu de filtrer l'accès à Cisco ont géré l'infrastructure de mise à jour de téléchargement

requis

Aucune action

requis

Suivez la so

- Des pannes sont partiellement atténuées par les trois relances et le prochain passage programmé. Les pannes répétées sont probables une indication d'un facteur externe tel que des Pare-feu ou une panne avec l'infrastructure.
- Pendant que les DN de recherche séquentielle est sur le nom de domaine, vous devez prendre des mesures afin de s'assurer qu'il n'y a aucune panne intermittente de téléchargement.

## Vérification

### Vérifiez les configurations de DN

Assurez-vous que votre centre de Gestion de puissance de feu est configuré pour utiliser votre serveur DNS.

**Attention** : Cisco recommande vivement que vous gardiez les valeurs par défaut.

- Information
- HTTPS Certificate
- Database
- **Network**
- Management Interface
- Process
- Time
- Remote Storage Device
- Change Reconciliation
- Console Configuration
- Cloud Services

### Network Settings

**IPv4**

Configuration

IPv4 Management IP  Netmask

Default Network Gateway

**IPv6**

Configuration

**Shared Settings**

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

MTU

Remote Management Port

### Configure Proxies to Access the Internet

**Direct connection**

Connected directly to the Internet.

**Manual proxy configuration**

HTTP Proxy

Port

Use Proxy Authentication

User Name

Password

Confirm Password

Vous pouvez configurer les configurations de DN dans le **système > les gens du pays > la configuration**, sous la section de **réseau**. Sous les **configurations partagées** section, vous pouvez spécifier jusqu'à trois serveurs DNS.

Remarque: Si vous sélectionnez le **DHCP** dans la liste déroulante de **configuration**, vous ne pouvez pas manuellement spécifier les **configurations partagées**.

## Vérifiez la connexion

Vous pouvez employer de diverses commandes, telles que le `telnet`, le `nslookup`, ou la `fouille` afin de déterminer l'état du serveur DNS, et les configurations de DN à votre centre de Gestion de puissance de feu. Exemple :

```
telnet support.sourcefire.com 443nslookup support.sourcefire.comdig support.sourcefire.com
```

Remarque: Le ping à `support.sourcefire.com` ne fonctionne pas. Par conséquent il ne devrait pas être utilisé comme test de Connectivité.

Connexion de test au site du support technique d'une appliance (pour télécharger des mises à jour, et ainsi de suite), vous pouvez se connecter dans votre appliance par l'intermédiaire de l'accès de SSH ou de direct-console, et utilisez cette commande :

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

Le cette commande montre la négociation de certificat, aussi bien que te fournit un équivalent d'une session de telnet à un web server du port 80. Voici un exemple de la sortie de commande :

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

Il ne devrait y avoir aucune demande en ce moment. Cependant, car la session attend l'entrée, vous pouvez alors sélectionner la commande :

```
GET /
```

Vous devriez recevoir le HTML cru qui est la page de connexion de site du support technique.

## Dépannez

**Option 1 :** Remplacez l'adresse IP statique par le nom de domaine `support.sourcefire.com` sur des Pare-feu. Si vous devez utiliser une adresse IP statique, assurez-vous que c'est correct. Voici les informations détaillées du serveur de téléchargement utilisé par un système de puissance de feu :

- **Domaine :** `support.sourcefire.com`
- **Port :** `443/tcp` (bidirectionnel)
- **Adresse IP :** `50.19.123.95`, `50.16.210.129`

Les adresses IP supplémentaires qui sont également utilisées par `support.sourcefire.com` (dans la méthode de recherche séquentielle) sont :

```
54.221.210.248
54.221.211.1
54.221.212.60
54.221.212.170
54.221.212.241
54.221.213.96
54.221.213.209
54.221.214.25
54.221.214.81
```

**Option 2 :** Vous pouvez télécharger des mises à jour manuellement avec un navigateur Web, et puis l'installez manuellement pendant votre fenêtre de maintenance.

**Option 3 :** Ajoutez un enregistrement A pour `support.sourcefire.com` sur votre serveur DNS.

## Documents connexes

- [Tape des mises à jour qui peuvent être installées sur un système de puissance de feu](#)
- [Adresses du serveur requises pour des exécutions avancées de protection de malware \(AMPÈRE\)](#)
- [Ports de transmission requis pour l'exploitation du système de puissance de feu](#)
- [Support et documentation techniques - Cisco Systems](#)