Foire aux questions de tunnel de Techsupport de sécurité du contenu

Contenu

Introduction

Ce document apporte des réponses aux forums aux questions au sujet de l'utilisation des tunnels de Techsupport sur des appliances de sécurité du contenu de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurité du courrier électronique de Cisco (ESA)
- Appliance de sécurité Web de Cisco (WSA)
- Appliance de Gestion de sécurité Cisco (SMA)
- AsyncOS

Composants utilisés

Les informations dans ce document sont basées sur les appliances de sécurité du contenu de Cisco qui exécutent n'importe quelle version d'AsyncOS.

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.

Quels sont des tunnels de Techsupport ?

Les tunnels de Techsupport sont des connexions de Protocole Secure Shell (SSH) qui sont créées d'une appliance de sécurité du contenu de Cisco à un bastion host aux sièges sociaux de sécurité du contenu de Cisco. Les tunnels permettent au support technique de Cisco et aux ingénieurs technico-commerciaux pour analyser un système et pour dépanner.

Comment les tunnels de Techsupport fonctionnent-ils ?

Le tunnel de Techsupport fonctionne par la plupart des Pare-feu sans modification. Quand les initiés de connexion en tunnel, l'appliance établit une connexion SSH à partir d'une haute-source aléatoire mettre en communication au port spécifié d'un de ces serveurs sécurisés par Cisco :

- **63.251.108.107 -** pour des constructions plus anciennes d'AsyncOS
- **upgrades.ironport.com -** pour des constructions plus anciennes d'AsyncOS
- **c.tunnels.ironport.com -** pour la série C appliances/ESA
- **x.tunnels.ironport.com -** pour la X-gamme appliances/ESA
- **m.tunnels.ironport.com -** pour la M-gamme appliances/SMA
- **s.tunnels.ironport.com -** pour la série S appliances/WSA

Les ports qui sont disponibles sur les serveurs de sécuriser-tunnel de Cisco sont 22, 25, 53, 80, 443, et 4766. Puisque le rapport est établi à l'adresse Internet plutôt qu'une adresse IP dur-codée, un Domain Name Server actif (DN) est exigé afin d'établir le tunnel.

Quelques périphériques Protocol-avertis bloquent la connexion due au protocole/à non-concordance de port et à un certain protocole SMTP (SMTP) - les périphériques avertis interrompent la connexion. Dans les cas où il y a des périphériques Protocol-avertis ou des connexions sortantes qui sont bloqués, l'utilisation d'un port autre que le par défaut (25) pourrait être exigée. Access à l'extrémité distante du tunnel est limité seulement au support technique de Cisco et aux ingénieurs technico-commerciaux.

> Remarque: Quand Cisco les prennent en charge ou ingénieur technico-commercial est connectés au tunnel, le système invite sur l'appliance inclut **(SERVICE)**.

> **Conseil** : Les tunnels tentent automatiquement de se rétablir, comme quand une panne de réseau se produit ou quand l'appliance est redémarrée.

Comment est-ce que j'établis un tunnel de Techsupport ?

Afin d'établir une connexion en tunnel de Techsupport par l'intermédiaire de l'appliance CLI en tant qu'utilisateur d'admin, terminez-vous ces étapes :

1. Sélectionnez la commande de **techsupport**.

2. Choisissez le **tunnel**.

3. Terminez-vous les demandes.

   Remarque: Quand vous activez un tunnel, vous devez entrer un mot de passe provisoire et le fournir à l'ingénieur d'assistance clientèle de Cisco. Ce mot de passe n'est pas utilisé directement, mais est utilisé afin de générer un mot de passe propre à une machine.

Afin d'établir un tunnel du GUI d'admin d'appareils, terminez-vous ces étapes :

1. Naviguez vers l'**administration système > l'Accès à distance**.

2. Assurez-vous que vous vérifiez l'**Accès à distance d'autoriser à cette appliance** et **initiez la connexion par l'intermédiaire de sécurisez des** cases de **tunnel**.

3. Soumettez la forme.

Il est important de noter que n'importe quel Pare-feu doit être configuré afin de permettre les connexions sortantes à **upgrades.ironport.com**. Si votre Pare-feu a l'inspection de protocole SMTP activée, le tunnel n'établit pas. Dans ces situations, vous devez spécifier un port alternatif. Choisissez le port le plus approprié de cette liste :

- 22
- 53
- 80
- 443
- 4766

Remarque: Le port 25 est utilisé comme destination port par défaut.

Conseil : Afin de désactiver le tunnel quand on ne l'exige plus, sélectionnez la commande de **techsupport** et choisissez le **débronchement**.

Comment est-ce que je peux tester le tunnel de Techsupport pour la Connectivité ?

Employez cet exemple afin de réaliser un premier essai pour la Connectivité par votre Pare-feu :

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

Pourquoi le tunnel de Techsupport ne travaille-t-il pas à l'appliance de Gestion de la sécurité (SMA) ?

Cela ne fonctionne pas dans les exemples où le SMA est placé dans le réseau local sans accès direct à l'Internet, cependant les ports mentionnés répertoriés avant que le tunnel de Techsupport n'établisse pas. Dans ce cas le tunnel de Techsupport peut être activé sur un ESA à la place et l'accès de SSH peut être activé sur le SMA. Ceci permet le support de Cisco à d'abord se connectent par l'intermédiaire du tunnel de Techsupport à l'ESA et de l'ESA au SSH au SMA, qui exige qu'il y a de Connectivité entre l'ESA et le SMA sur le port 22.

Établissez le SSH Access par l'intermédiaire du SMA CLI en tant qu'utilisateur d'admin

1. Sélectionnez la commande de **techsupport**.
2. Choisissez **SSHACCESS**.
3. Terminez-vous les demandes.

   Remarque: Une fois qu'activé, fournissez le support de Cisco le numéro de série de l'ESA et le SMA aussi bien que le mot de passe de service.