Technote sur la Foire aux questions pour l'Accès à distance sur Cisco ESA/WSA/SMA

Contenu

Introduction

Ce document apporte des réponses aux forums aux questions au sujet de l'utilisation de l'Accès à distance par le support technique de Cisco sur des appliances de sécurité du contenu de Cisco. Ceci inclut l'appliance de sécurité du courrier électronique de Cisco (ESA), l'appliance de sécurité Web de Cisco (WSA), et l'appliance de Gestion de sécurité Cisco (SMA).

Conditions préalables

Composants utilisés

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

Quel est Accès à distance ?

L'Accès à distance est une connexion de Protocole Secure Shell (SSH) qui est activée d'une appliance de sécurité du contenu de Cisco à un hôte sécurisé à Cisco. Seulement l'assistance de client de Cisco peut accéder à l'appliance une fois qu'une session distante est activée. L'Accès à distance permet au support technique de Cisco pour analyser une appliance. Le support accède

à l'appliance par un tunnel de SSH que cette procédure crée entre l'appliance et le serveur d'upgrades.ironport.com.

Comment l'Accès à distance fonctionne

Quand les initiés d'une connexion d'Accès à distance, l'appliance ouvre un sécurisé, aléatoire, port de haute-source par l'intermédiaire d'une connexion SSH sur l'appliance à port 1 configuré/sélectionné des serveurs suivants de sécurité du contenu de Cisco :

Adresse IP	Nom de l'hôte	Utilisation
63.251.108.107	upgrades.ironport.com	Toutes les appliances de sécurité du contenu
63.251.108.107	c.tunnels.ironport.com	Appliances de série C (ESA)
63.251.108.107	x.tunnels.ironport.com	Appliances de X-gamme (ESA)
63.251.108.107	m.tunnels.ironport.com	Appliances de M-gamme (SMA)
63.251.108.107	s.tunnels.ironport.com	Appliances de série S (WSA)

Il est important de noter qu'un Pare-feu de client peut devoir être configuré pour permettre les connexions sortantes à un des serveurs ci-dessus répertoriés. Si votre Pare-feu a l'inspection de protocole SMTP activée, le tunnel n'établira pas. Les ports que Cisco recevra des connexions de l'appliance pour l'Accès à distance sont :

- 22
- 25 (par défaut)
- 53
- 80
- 443
- 4766

Le rapport d'Accès à distance est établi à un nom d'hôte et pas à une adresse IP dur-codée. Ceci exige du Domain Name Server (DN) d'être configuré sur l'appliance afin d'établir la connexion sortante.

Sur un réseau client, quelques périphériques Protocol-avertis de réseau peuvent bloquer cette connexion due au protocole/à non-concordance de port. Un certain protocole SMTP (SMTP) - les périphériques avertis peut également interrompre 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) peut être exigée. Access à l'extrémité distante du tunnel est limité seulement au support technique de Cisco. Veuillez être sûr que vous passez en revue votre Pare-feu/réseau pour les connexions sortantes en essayant d'établir ou dépanner des connexions d'Accès à distance pour votre appliance.

> **Note**: Quand un ingénieur d'assistance clientèle de Cisco est connecté à l'appliance par l'intermédiaire de l'Accès à distance le système invite sur l'appliance affiche *(SERVICE)*.

Comment activer l'Accès à distance

> **Note**: Veuillez être sûr de passer en revue le guide utilisateur de votre appliance et la version d'AsyncOS pour des instructions sur « activer l'Accès à distance pour le personnel de support technique de Cisco ».

> **Note**: Les connexions envoyées par l'intermédiaire de l'email à attach@cisco.com peuvent ne pas être sécurisées en transit. Le gestionnaire de cas de support est l'option sécurisée préférée de Cisco de télécharger les informations dans votre cas. Pour se renseigner plus sur les limites de Sécurité et de taille d'autres options de téléchargement de fichier : Téléchargements de fichier de client au centre d'assistance technique Cisco

Identifiez un port qui peut être atteint de l'Internet. Le par défaut est le port 25, qui fonctionnera dans la plupart des environnements parce que le système exige également de l'accès général au-dessus de ce port afin d'envoyer des messages électroniques. On permet des connexions au-dessus de ce port dans la plupart des configurations de Pare-feu.

CLI

Afin d'établir une connexion d'Accès à distance par l'intermédiaire du CLI, comme un utilisateur d'admin, se terminent ces étapes :

1. Sélectionnez la commande de **techsupport**
2. Choisissez le **TUNNEL**
3. Choisissez de générer ou *écrire une* chaîne aléatoire de graine
4. Spécifiez le numéro de port pour la connexion
5. Répondez « **Y** » pour activer l'accès de service

L'Accès à distance sera activé à ce moment. L'appliance fonctionnent maintenant pour établir la connexion sécurisée au bastion host sécurisé à Cisco. Fournissez le numéro de série d'appareils et la chaîne de graine qui est générée à l'ingénieur TAC prenant en charge votre cas.

GUI

Afin d'établir une connexion d'Accès à distance par l'intermédiaire du GUI, comme un utilisateur d'admin, se terminent ces étapes :

1. Naviguez **pour aider et le support > l'Accès à distance** (pour l'ESA, le SMA), **les prennent en charge et aide > Accès à distance** (pour WSA)
2. **Enable de** clic
3. Choisissez la méthode pour la chaîne de graine
4. Assurez-vous que vous cochez la *connexion initiée par l'intermédiaire de sécurisez la* case de *tunnel* et spécifiez le numéro de port pour la connexion
5. Cliquez sur Submit

L'Accès à distance sera activé à ce moment. L'appliance fonctionnent maintenant pour établir la connexion sécurisée au bastion host sécurisé à Cisco. Fournissez le numéro de série d'appareils et la chaîne de graine qui est générée à l'ingénieur TAC prenant en charge votre cas.

Comment désactiver l'Accès à distance

CLI

1. Sélectionnez la commande de **techsupport**
2. Choisissez le **DÉBRONCHEMENT**
3. Répondez « **Y** » une fois incité « êtes vous sure que vous voulez désactiver l'accès de

service ? »

GUI

1. Naviguez **pour aider et le support > l'Accès à distance** (pour l'ESA, le SMA), **les prennent en charge et aide > Accès à distance** (pour WSA).
2. **Débronchement de** clic
3. La sortie GUI affichera le « succès — l'Accès à distance a été désactivé »

Comment tester la Connectivité d'Accès à distance

Employez cet exemple afin de réaliser un premier essai pour la Connectivité de votre appliance à Cisco :

```
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
```

La Connectivité peut être testée pour les ports l'uns des répertoriés ci-dessus : 22, 25, 53, 80, 443, ou 4766. Si la Connectivité échoue, vous pouvez devoir exécuter une capture de paquet pour voir où la connexion manque de votre appliance/réseau.

Pourquoi l'Accès à distance ne travaille-t-il pas au SMA ?

L'Accès à distance peut ne pas activer sur un SMA si le SMA est placé dans le réseau local sans accès direct à l'Internet. Pour cet exemple, l'Accès à distance peut être activé sur un ESA ou un WSA, 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 de l'Accès à distance à l'ESA/WSA, et puis de l'ESA/WSA au SMA par l'intermédiaire du SSH. Ceci exigera la Connectivité entre l'ESA/WSA et le SMA sur le port 22.

> **Note**: Veuillez être sûr de passer en revue le guide utilisateur de votre appliance et la version d'AsyncOS pour des instructions sur « activer l'Accès à distance aux appliances sans connexion Internet directe ».

CLI

Afin d'établir une connexion d'Accès à distance par l'intermédiaire du CLI, comme un utilisateur d'admin, se terminent ces étapes :

1. Sélectionnez la commande de **techsupport**
2. Choisissez **SSHACCESS**
3. Choisissez de générer ou *écrire une* chaîne aléatoire de graine
4. Répondez « **Y** » pour activer l'accès de service

L'Accès à distance sera activé à ce moment. La sortie CLI affichera la chaîne de graine. Veuillez

fournir ceci à l'ingénieur d'assistance clientèle de Cisco. La sortie CLI affichera également les détails d'état de la connexion et d'Accès à distance, y compris le numéro de série d'appareils. Veuillez fournir ce numéro de série à l'ingénieur d'assistance clientèle de client.

GUI

Afin d'établir une connexion d'Accès à distance par l'intermédiaire du GUI, comme un utilisateur d'admin, se terminent ces étapes :

1. Naviguez **pour aider et le support > l'Accès à distance** (pour l'ESA, le SMA), **les prennent en charge et aide > Accès à distance** (pour WSA)
2. **Enable de** clic
3. Choisissez la méthode pour la chaîne de graine
4. Ne cochez pas la *connexion initiée par l'intermédiaire de sécurisent la* case de *tunnel*
5. Cliquez sur Submit

L'Accès à distance sera activé à ce moment. La sortie GUI t'affichera un message de succès et la chaîne de la graine des appareils. Veuillez fournir ceci à l'ingénieur d'assistance clientèle de Cisco. La sortie GUI affichera également l'état de la connexion et les détails d'Accès à distance, y compris le numéro de série d'appareils. Veuillez fournir ce numéro de série à l'ingénieur d'assistance clientèle de client.

Comment désactiver l'Accès à distance une fois activé pour SSHACCESS

Désactiver l'Accès à distance pour SSHACCESS est les mêmes étapes de la manière prévue en haut.

Dépannage

Si l'appliance n'est pas Accès à distance activé capable et se connecte à upgrades.ironport.com par l'intermédiaire d'un des ports répertoriés, vous devrez exécuter une capture de paquet directement de l'appliance pour passer en revue ce qui fait échouer la connexion sortante.

> **Note**: Veuillez être sûr de passer en revue le guide utilisateur de votre appliance et la version d'AsyncOS pour des instructions sur « exécuter une capture de paquet ».

L'ingénieur d'assistance clientèle de Cisco peut demander de faire fournir le fichier .pcap afin de passer en revue et assister le dépannage.

Informations connexes

- FOIRE AUX QUESTIONS ESA : Quels sont les niveaux de l'accès administratif disponibles sur l'ESA ?
- Support produit d'appareils de sécurité du courrier électronique de Cisco
- Support produit de sécurité Web de Cisco
- Support produit d'appareils de Gestion de sécurité du contenu de Cisco
- Support et documentation techniques - Cisco Systems