Contenu

Question

Comment est-ce que je fournis à Cisco TAC l'Accès à distance ou prends en charge le tunnel à une appliance d'email ou de sécurité Web de Cisco ?

Environnement

Appliance de sécurité du courrier électronique de Cisco (ESA), sécurité Web Appliance(WSA) de Cisco

Cisco des appliances envoient/sécurités Web peut utiliser un tunnel sécurisé de SSH afin de permettre à Cisco TAC pour accéder aux appliances du système d'exploitation. Par défaut, l'appliance ne permet pas ce type de connexion (l'Accès à distance de signification est désactivé par défaut).

Vous pouvez activer ceci par l'intermédiaire du CLI ou du GUI. Veuillez voir les instructions ci-dessous :

Du CLI

```
ESA.example.com> techsupport

Service Access currently disabled.
Serial Number: <S/N of the appliance>

Choose the operation you want to perform:
```

- SSHACCESS - Permettez à un représentant de service client pour accéder à distance votre système,
  sans établir un tunnel.
- TUNNEL - Permettez à un représentant de service client pour accéder à distance votre système,
  et établissez un tunnel sécurisé pour la transmission.
- ÉTAT - Affichez l'état en cours de techsupport.
  [] > tunnel

Entrez un mot de passe provisoire pour le support technique pour l'utiliser. Ce mot de passe ne pourra pas être utilisé pour accéder à directement votre système.

- Le mot de passe doit être entre 6 et 128 caractères longs.
- Il ne peut pas être blanc ou consister seulement en espaces.
- Il doit être différent du mot de passe de l'administrateur.

[] > ***<supportpassword>***

```
Enter the port number for tunnel connection:
[25]> <Specify port or press Enter>

Are you sure you want to enable service access? [N]> Y

Service access has been ENABLED. Please provide your temporary password to your
Cisco Customer Support representative.

Waiting for ssh tunnel to connect, Ctrl-C to cancel...
```

Du GUI

Allez **« aider et le prendre en charge »** *(le coin supérieur droit)* --> **« Accès à distance** sous « le Soutien technique ».

1. Cliquez sur le bouton **« éditent d'Accès à distance configurations »**.
2. Entrez un mot de passe dans le domaine **« de mot de passe de support technique »**.
3. Vérifiez « sécurisent le (recommandé) de tunnel : la » option et introduisent un numéro de port. Le par défaut est 25.
4. Cliquez sur « **soumettent** » le bouton.
5. Fournissez le mot de passe choisi à Cisco TAC.

Cisco TAC pourra prendre le contrôle de l'appliance après que vous leur ayez fourni votre numéro de série et mot de passe provisoire. Toutes les données sont transférées sécurisé (utilisant le cryptage) et ne peuvent pas être lues par n'importe quel interlocuteur l'autre puis personnel de Cisco TAC. Si Cisco l'appliance envoient/sécurités Web ne peut pas se connecter au-dessus du SMTP (port TCP 25), alors les autres ports disponibles sont 22, 80, 443, et 4766.

Remarque: Dans les dernières versions d'AsyncOS, nous avons apporté les modifications ci-dessous dans la section de « Accès à distance » pour les raisons de sécurité supplémentaires :

- Le mot de passe désigné maintenant sous le nom de la ***« chaîne de graine »***.
- Il y a une option de générer une chaîne aléatoire de graine : Ceci créera la clé plus élevée aléatoire de bit qui sera utilisée comme mot de passe pour la connexion d'Accès à distance.
- Longueur du mot de passe/de chaîne de graine : Le mot de passe doit être entre 12 et 128 caractères longs.