Protection de la sécurité du réseau lors de l'attribution de l'accès à des tiers

Contenu

Introduction

Pendant cette demande de service, vous pouvez vouloir que les ingénieurs de Cisco accèdent au réseau de votre organisation. L'octroi d'un tel accès permettra souvent votre demande de service d'être résolu plus rapidement. En pareil cas, Cisco mettent en boîte, et seulement, accéder à votre réseau avec votre autorisation.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Meilleures pratiques

Cisco recommande que vous suiviez ces instructions afin de vous aider à protéger la Sécurité de votre réseau quand vous accordez l'accès à n'importe quel technicien de support ou personne en dehors de votre société ou organisation.

- Si possible, employez le Cisco Unified MeetingPlace afin de partager les informations avec des techniciens de support. Cisco recommande que vous utilisiez le Cisco Unified MeetingPlace pour ces raisons :Le Cisco Unified MeetingPlace utilise le protocole de Protocole SSL (Secure Socket Layer), qui est plus sécurisé que le Protocole Secure Shell (SSH) ou le telnet dans certains cas.Le Cisco Unified MeetingPlace n'exige pas de vous de fournir des mots de passe à n'importe qui en dehors de votre société ou organisation.**Remarque:** Toutes les fois que vous accordez l'accès au réseau aux personnes en dehors de votre société ou organisation, tous les mots de passe que vous fournissez doivent être des mots de passe provisoires qui sont valides seulement tant que le tiers a besoin de l'accès à votre réseau.Typiquement, le Cisco Unified MeetingPlace n'exige pas de vous de changer votre stratégie de Pare-feu parce que la plupart des Pare-feu d'entreprise permettent l'accès sortant HTTPS.Pour en savoir plus de Cisco Unified MeetingPlace de visite.
- Si vous ne pouvez pas utiliser le Cisco Unified MeetingPlace et si vous choisissez de permettre le tiers accès par une autre application, telle que le SSH, assurez que le mot de passe est provisoire et disponible pour l'usage une fois seulement. En outre, vous devez immédiatement changer ou infirmer le mot de passe après que le tiers accès ne soit plus nécessaire. Si vous utilisez une application autre que le Cisco Unified MeetingPlace, vous pouvez suivre ces procédures et instructions :Afin de créer un compte provisoire sur des routeurs Cisco IOS, utilisez cette commande :`Router(config)#`**`username tempaccount secret QWE!@#`** Afin de créer un compte provisoire sur PIX/ASA, utilisez cette commande :`PIX(config)#`**`username tempaccount password QWE!@#`** Afin de retirer le compte provisoire, utilisez cette commande :`Router (config)#`**`no username tempaccount`** Générez aléatoirement le mot de passe provisoire. Le mot de passe provisoire ne doit pas être lié à la demande de service ou au fournisseur particulière des services de support technique. Par exemple, n'utilisez pas les mots de passe tels que *Cisco*, *cisco123*, ou *ciscotac*.Ne donnez jamais votre propre nom d'utilisateur ou mot de passe.N'utilisez pas le telnet au-dessus de l'Internet. Il n'est pas sécurisé.
- Si le périphérique de Cisco qui exige le support se trouve derrière un Pare-feu entreprise et une modification aux stratégies de Pare-feu est exigé pour un technicien de support au SSH dans le périphérique de Cisco, assurez-vous que le changement de politique est spécifique au technicien de support assigné à la question. Ne rendez jamais l'exception de stratégie ouverte d'Internet dans son ensemble ou de plus grande plage des hôtes que nécessaire.Pour modifier une stratégie de Pare-feu sur un Pare-feu Cisco IOS, ajoutez ces lignes à la liste d'accès en entrée sous l'Internet faisant face à l'interface :`Router(config)#`**`ip access-list ext inbound`** `Router(config-ext-nacl)#`**`1 permit tcp host <`***`IP address for TAC engineer`***`> host <`***`Cisco device address`***`> eq 22`** **Remarque:** Dans cet exemple, le `routeur (config-ext.-NaCl) #` configuration est affiché sur deux lignes afin d'économiser l'espace. Cependant, quand vous ajoutez cette commande à la liste d'accès en entrée, la configuration doit apparaître sur une ligne.Pour modifier une stratégie de Pare-feu sur un Pare-feu de Cisco PIX/ASA, ajoutez cette ligne à l'access-group d'arrivée :`ASA(config)#`**`access-list inbound line 1 permit tcp host <`***`IP address for TAC engineer`***`> host <`***`Cisco device address`***`> eq 22`** **Remarque:** Dans cet exemple, la configuration d'`ASA(config)#` est affichée sur deux lignes afin d'économiser l'espace. Cependant, quand vous ajoutez cette commande à l'access-group d'arrivée, la configuration doit apparaître sur une ligne.Pour permettre l'accès de SSH sur des routeurs Cisco IOS, ajoutez cette ligne à l'access-class :`Router(config)#`**`access-list 2 permit host <`***`IP address for TAC engineer`***`>`** `Router(config)#`**`line vty 0 4`** `Router(config-line)#`**`access-class 2`** Pour permettre l'accès de SSH sur Cisco PIX/ASA, ajoutez cette configuration :`ASA(config)#`**`ssh <`***`IP address`*

```
for TAC engineer> 255.255.255.255 outside
```

Si ayez les questions environ ou ayez besoin de l'assistance supplémentaire avec les informations décrites dans ce document, entrez en contact avec le centre d'assistance technique Cisco (TAC).

Cette page Web est à des fins d'information seulement et est fournie sur « de même que » la base sans n'importe quelle garantie ou garantie. Les pratiques recommandées ci-dessus ne sont pas destinées pour être complètes, mais sont suggérées pour compléter les procédures de sécurité en cours des clients. L'efficacité de n'importe quelle pratique de sécurité dépend de la situation spécifique de chaque client ; et des clients sont encouragés à considérer tous les facteurs appropriés en déterminant des procédures de sécurité les plus appropriées pour leurs réseaux.

Informations connexes

- Cisco Unified MeetingPlace
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Centre d'assistance technique Cisco (TAC)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems