Protection de la sécurité du réseau et octroi de l'accès à des tiers

Contenu

Introduction

Au cours de cette demande de service, vous pouvez demander aux ingénieurs Cisco d'accéder au réseau de votre entreprise. L'octroi d'un tel accès permet souvent de résoudre plus rapidement votre demande de service. Dans de tels cas, Cisco peut et ne peut accéder à votre réseau qu'avec votre autorisation.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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 vous recommande de suivre ces directives afin de vous aider à protéger la sécurité de votre réseau lorsque vous accordez l'accès à tout ingénieur d'assistance ou personne en dehors de votre entreprise ou organisation.

- Si possible, utilisez Cisco Unified MeetingPlace afin de partager des informations avec les ingénieurs du support technique. Cisco vous recommande d'utiliser Cisco Unified MeetingPlace pour les raisons suivantes :Cisco Unified MeetingPlace utilise le protocole SSL (Secure Socket Layer), qui est plus sécurisé que SSH (Secure Shell) ou Telnet dans certains cas.Cisco Unified MeetingPlace n'exige pas que vous fournissiez des mots de passe à quiconque se trouve en dehors de votre entreprise ou de votre organisation.**Remarque :** Lorsque vous accordez un accès réseau à des personnes extérieures à votre entreprise ou organisation, les mots de passe que vous fournissez doivent être des mots de passe temporaires valides uniquement tant que le tiers requiert un accès à votre réseau.En règle générale, Cisco Unified MeetingPlace ne nécessite pas de modification de votre stratégie de pare-feu, car la plupart des pare-feu d'entreprise autorisent l'accès HTTPS sortant.Visitez Cisco Unified MeetingPlace pour plus d'informations.
- Si vous ne pouvez pas utiliser Cisco Unified MeetingPlace et si vous choisissez d'autoriser un accès tiers via une autre application, telle que SSH, assurez-vous que le mot de passe est temporaire et disponible pour une utilisation unique uniquement. En outre, vous devez immédiatement modifier ou invalider le mot de passe après que l'accès tiers n'est plus nécessaire. Si vous utilisez une application autre que Cisco Unified MeetingPlace, vous pouvez suivre les procédures et directives suivantes :Afin de créer un compte temporaire sur les routeurs Cisco IOS, utilisez cette commande :
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Afin de créer un compte temporaire sur PIX/ASA, utilisez cette commande :
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Afin de supprimer le compte temporaire, utilisez cette commande :
  ```
  Router (config)#no username tempaccount
  ```

  Générer aléatoirement le mot de passe temporaire. Le mot de passe temporaire ne doit pas être lié à la demande de service ou au fournisseur de services de support. Par exemple, n'utilisez pas de mots de passe tels que *cisco*, *cisco123* ou *ciscotac*.Ne donnez jamais votre nom d'utilisateur ou votre mot de passe.N’utilisez pas Telnet sur Internet. Ce n'est pas sûr.
- Si le périphérique Cisco nécessitant une assistance se trouve derrière un pare-feu d'entreprise et qu'une modification des stratégies de pare-feu est nécessaire pour qu'un ingénieur d'assistance puisse SSH sur le périphérique Cisco, assurez-vous que la modification de la stratégie est spécifique à l'ingénieur d'assistance affecté au problème. Ne rouvrez jamais l'exception de stratégie ouverte à l'ensemble d'Internet ou à une plage d'hôtes plus large que nécessaire.Pour modifier une stratégie de pare-feu sur un pare-feu Cisco IOS Firewall, ajoutez ces lignes à la liste d'accès entrante sous l'interface Internet :
  ```
  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, la configuration `Router(config-ext-nacl)#` s'affiche sur deux lignes afin de conserver de l'espace. Cependant, lorsque vous ajoutez cette commande à la liste d'accès entrante, la configuration doit apparaître sur une ligne.Pour modifier une stratégie de pare-feu sur un pare-feu Cisco PIX/ASA, ajoutez cette ligne au groupe d'accès entrant :
  ```
  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 `ASA(config)#` s'affiche sur deux lignes afin de

conserver de l'espace. Cependant, lorsque vous ajoutez cette commande au groupe d'accès entrant, la configuration doit apparaître sur une ligne.Pour autoriser l’accès SSH sur les routeurs Cisco IOS, ajoutez cette ligne à la classe d’accès :

```
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 autoriser l'accès SSH sur Cisco PIX/ASA, ajoutez cette configuration :

```
ASA(config)#ssh <IP address for TAC engineer> 255.255.255.255 outside
```

Si vous avez des questions ou avez besoin d'une assistance supplémentaire avec les informations décrites dans ce document, contactez le centre d'assistance technique Cisco (TAC).

Cette page Web est fournie à titre informatif seulement et est fournie « telle quelle » sans garantie ni garantie. Les meilleures pratiques ci-dessus ne sont pas destinées à être complètes, mais sont proposées pour compléter les procédures de sécurité actuelles des clients. L'efficacité de toute pratique de sécurité dépend de la situation spécifique de chaque client ; et les clients sont encouragés à tenir compte de tous les facteurs pertinents lors de la détermination 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