Proteger a segurança da rede e conceder acesso a terceiros

Contents

Introduction

Durante a solicitação de serviço, talvez você queira que os engenheiros da Cisco acessem a rede da sua organização. A concessão desse acesso frequentemente permitirá que sua solicitação de serviço seja resolvida mais rapidamente. Nesses casos, a Cisco pode e acessará sua rede com sua permissão.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter informações sobre convenções de documentos.

Melhores práticas

A Cisco recomenda que você siga estas diretrizes para ajudá-lo a proteger a segurança da sua rede ao conceder acesso a qualquer engenheiro de suporte ou pessoa fora da sua empresa ou organização.

- Se possível, use o Cisco Unified MeetingPlace para compartilhar informações com engenheiros de suporte. A Cisco recomenda que você use o Cisco Unified MeetingPlace pelos seguintes motivos:O Cisco Unified MeetingPlace usa o protocolo SSL (Secure Socket Layer), que é mais seguro que o shell seguro (SSH) ou o Telnet em alguns casos.O Cisco Unified MeetingPlace não exige que você forneça senhas a ninguém fora da sua empresa ou organização.**Observação:** sempre que você conceder acesso à rede a pessoas fora da sua empresa ou organização, quaisquer senhas fornecidas devem ser senhas temporárias válidas apenas enquanto o terceiro exigir acesso à sua rede.Geralmente, o Cisco Unified MeetingPlace não exige que você altere sua política de firewall porque a maioria dos firewalls corporativos permite acesso HTTPS de saída.Visite o Cisco Unified MeetingPlace para obter mais informações.
- Se você não puder usar o Cisco Unified MeetingPlace e optar por permitir o acesso de terceiros por meio de outro aplicativo, como o SSH, verifique se a senha é temporária e está disponível somente para uso único. Além disso, você deve alterar ou invalidar imediatamente a senha depois que o acesso de terceiros não for mais necessário. Se você usar um aplicativo diferente do Cisco Unified MeetingPlace, poderá seguir estes procedimentos e diretrizes:Para criar uma conta temporária nos roteadores Cisco IOS, use este comando:
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Para criar uma conta temporária no PIX/ASA, use este comando:
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Para remover a conta temporária, use este comando:
  ```
  Router (config)#no username tempaccount
  ```

  Gerar aleatoriamente a senha temporária. A senha temporária não deve estar relacionada à solicitação de serviço específica ou ao provedor de serviços de suporte. Por exemplo, não use senhas como *cisco*, *cisco123* ou *ciscotac*.Nunca forneça seu próprio nome de usuário ou senha.Não use Telnet na Internet. Não é seguro.
- Se o dispositivo Cisco que requer suporte estiver localizado atrás de um firewall corporativo e for necessária uma alteração nas políticas de firewall para que um engenheiro de suporte faça SSH no dispositivo Cisco, certifique-se de que a alteração de política seja específica para o engenheiro de suporte atribuído ao problema. Nunca torne a exceção de política aberta para toda a Internet ou para uma maior variedade de hosts do que o necessário.Para modificar uma política de firewall em um Cisco IOS Firewall, adicione estas linhas à lista de acesso de entrada na interface para 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
  ```

  Observação: neste exemplo, a configuração `Router(config-ext-nacl)#` é exibida em duas linhas para conservar espaço. No entanto, quando você adiciona esse comando à lista de acesso de entrada, a configuração deve aparecer em uma linha.Para modificar uma política de firewall em um firewall Cisco PIX/ASA, adicione esta linha ao grupo de acesso de entrada:
  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  Observação: neste exemplo, a configuração do `ASA(config)#` é exibida em duas linhas para conservar espaço. No entanto, quando você adiciona esse comando ao grupo de acesso de entrada, a configuração deve aparecer em uma linha.Para permitir o acesso SSH nos

roteadores Cisco IOS, adicione esta linha à classe de acesso:

```
Router(config)#access-list 2 permit host <IP address for TAC engineer>
Router(config)#line vty 0 4
Router(config-line)#access-class 2
```

Para permitir acesso SSH no Cisco PIX/ASA, adicione esta configuração:

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

Se tiver dúvidas ou precisar de assistência adicional com as informações descritas neste documento, entre em contato com o Cisco Technical Assistance Center (TAC).

Esta página da Web tem apenas fins informativos e é fornecida "no estado em que se encontra" sem qualquer garantia ou garantia. As melhores práticas acima não se destinam a ser abrangentes, mas são sugeridas para complementar os procedimentos de segurança atuais dos clientes. A eficácia de qualquer prática de segurança depende da situação específica de cada cliente; e os clientes são incentivados a considerar todos os fatores relevantes ao determinar os procedimentos de segurança mais apropriados para suas redes.

Informações Relacionadas

- Cisco Unified MeetingPlace
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Cisco Technical Assistance Center (TAC)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems