

# Segurança de rede de proteção ao conceder o acesso às terceiras partes

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Melhores práticas](#)

[Informações Relacionadas](#)

## [Introdução](#)

Durante este pedido do serviço, você pode querer engenheiros da Cisco alcançar a rede da sua organização. Conceder tal acesso permitirá frequentemente que seu pedido do serviço seja resolvido mais rapidamente. Nesses casos, Cisco enlata, e somente, para alcançar sua rede com sua permissão.

## [Pré-requisitos](#)

### [Requisitos](#)

Não existem requisitos específicos para este documento.

### [Componentes Utilizados](#)

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

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter informações sobre convenções de documentos.

## [Melhores práticas](#)

Cisco recomenda que você segue estas diretrizes a fim o ajudar a proteger a Segurança de sua rede quando você concede o acesso a todo o engenheiro de suporte ou pessoa fora de sua empresa ou organização.

- Se possível, use o Cisco Unified MeetingPlace a fim compartilhar da informação com os engenheiros de suporte. Cisco recomenda que você use o Cisco Unified MeetingPlace por estas razões: O Cisco Unified MeetingPlace usa o protocolo do Secure Socket Layer (SSL), que é mais seguro do que o Shell Seguro (ssh) ou o telnet em alguns casos. O Cisco Unified MeetingPlace não o exige fornecer senhas a qualquer um fora de sua empresa ou organização. **Note:** Sempre que você concede o acesso de rede às pessoas fora de sua empresa ou organização, todas as senhas que você fornecer devem ser as senhas provisórias que são válidas somente enquanto a terceira parte exige o acesso a sua rede. Tipicamente, o Cisco Unified MeetingPlace não o exige mudar sua política de firewall porque a maioria de Firewall da empresa permitem o acesso de partida HTTPS. [Cisco Unified MeetingPlace da](#) visita para mais informação.
- Se você não pode usar o Cisco Unified MeetingPlace e se você escolhe permitir o acesso da terceira com um outro aplicativo, tal como o SSH, assegure-se de que a senha esteja provisória e disponível para o único uso somente. Além, você deve imediatamente mudar ou invalidar a senha depois que o acesso da terceira é já não necessário. Se você usa um aplicativo a não ser o Cisco Unified MeetingPlace, você pode seguir estes procedimentos e diretrizes: A fim criar uma conta provisória no Roteadores do Cisco IOS, use este comando:  
Router(config)#username tempaccount secret QWE!@#

A fim criar uma conta provisória no PIX/ASA, use este comando:

```
PIX(config)#username tempaccount password QWE!@#
```

A fim remover a conta provisória, use este comando:

```
Router (config)#no username tempaccount
```

Gerencia aleatoriamente a senha provisória. A senha provisória não deve ser relacionada ao pedido do serviço particular ou ao fornecedor dos serviços de assistência. Por exemplo, não use senhas tais como *Cisco*, *cisco123*, ou *ciscotac*. Nunca dê sua própria nome de usuário ou senha. Não use o telnet sobre o Internet. Não é seguro.

- Se o dispositivo Cisco que exige o apoio é ficado situado atrás de um firewall corporativa e de uma mudança às políticas de firewall é exigido para um engenheiro de suporte ao SSH no dispositivo Cisco, assegure-se de que a alteração de política esteja específica ao engenheiro de suporte atribuído à edição. Nunca faça a exceção da política aberta às todas a internet ou a uma escala mais larga dos anfitriões do que necessária. Para alterar uma política de firewall em um Cisco IOS Firewall, adicionar estas linhas à lista de acessos de entrada sob o Internet que enfrenta a relação:

```
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
```

**Note:** Neste exemplo, o roteador (configuração-ext-nacl) # configuração é indicado em duas linhas a fim conservar o espaço. Contudo, quando você adiciona este comando à lista de acessos de entrada, a configuração deve aparecer em uma linha. Para alterar uma política de firewall em um Firewall de Cisco PIX/ASA, adicionar esta linha ao acesso-grupo de entrada:

```
ASA(config)#access-list inbound line 1 permit tcp host
    <IP address for TAC engineer> host <Cisco device address> eq 22
```

**Note:** Neste exemplo, a configuração de ASA(config)# é indicada em duas linhas a fim conservar o espaço. Contudo, quando você adiciona este comando ao acesso-grupo de entrada, a configuração deve aparecer em uma linha. Para permitir o SSH alcance no

Roteadores do Cisco IOS, adicionam esta linha à acesso-classe:

```
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 o SSH alcance em Cisco PIX/ASA, adicionam esta configuração:

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

Se tenha perguntas aproximadamente ou exija o auxílio adicional com a informação descrita neste documento, contacte o [centro de assistência técnica da Cisco \(TAC\)](#).

Esta página da web é apenas para fins informativos e é fornecido no “como é” a base sem nenhuma garantia ou garantia. Os melhores prática acima não são pretendidos ser detalhados, mas são sugeridos para complementar os procedimentos de segurança atuais dos clientes. A eficácia de toda a prática da Segurança é dependente da situação específica de cada cliente; e os clientes são incentivados considerar todos os fatores relevantes ao determinar os procedimentos de segurança os 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 \(incluindo PIX\)](#)
- [Centro de Assistência Técnica \(TAC\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)