保护网络安全并授予第三方访问权限

目录

简介

在此服务请求过程中，您可能希望思科工程师访问您组织的网络。授予此类访问权限通常可以更快地解决您的服务请求。在这种情况下，思科可以且只会在您允许的情况下访问您的网络。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

最佳实践

思科建议您遵循这些准则，以便在授予任何支持工程师或公司或组织外部人员访问权限时，帮助您保护网络安全。

- 如果可能，请使用Cisco Unified MeetingPlace与支持工程师共享信息。思科建议您使用Cisco Unified MeetingPlace，原因如下：Cisco Unified MeetingPlace使用安全套接字层(SSL)协议，在某些情况下，该协议比安全外壳(SSH)或Telnet更安全。Cisco Unified MeetingPlace不要求您为公司或组织之外的任何人提供密码。**注意：**无论何时您向公司或组织外的人员授予网络访问权限，您提供的任何密码都必须是临时密码，只要第三方需要访问您的网络，该临时密码才有效。通常，Cisco Unified MeetingPlace不要求您更改防火墙策略，因为大多数企业防火墙

都允许出站HTTPS访问。有关详细信息，请访问Cisco Unified MeetingPlace。

- 如果无法使用Cisco Unified MeetingPlace，并且选择允许通过其他应用（如SSH）进行第三方访问，请确保密码为临时密码且仅可一次性使用。此外，在不再需要第三方访问后，您必须立即更改或使密码失效。如果您使用的应用不是Cisco Unified MeetingPlace，则可以遵循以下程序和指南：要在Cisco IOS路由器上创建临时帐户，请使用以下命令：

```
Router(config)#username tempaccount secret QWE!@#
```

要在PIX/ASA上创建临时帐户，请使用以下命令：

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

要删除临时帐户，请使用以下命令：

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

随机生成临时密码。临时密码不得与特定服务请求或支持服务提供商相关。例如，请勿使用口令，如*cisco*、*cisco123*或*ciscotac*。切勿提供您自己的用户名或密码。请勿在Internet上使用Telnet。它不安全。

- 如果需要支持的思科设备位于公司防火墙后，且支持工程师需要更改防火墙策略才能SSH到思科设备，请确保策略更改特定于分配给该问题的支持工程师。切勿将策略例外开放到整个Internet或范围更广的主机，而不必这样做。要修改Cisco IOS防火墙上的防火墙策略，请将以下行添加到面向互联网的接口下的入站访问列表：

```
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
```

注意：在本示例中，Router(config-ext-nacl)#配置显示在两行上。但是，当您将此命令添加到入站访问列表时，配置必须显示在一行上。要修改Cisco PIX/ASA防火墙上的防火墙策略，请将此行添加到入站访问组：

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

注意：在本示例中，ASA(config)#配置显示在两行上以节省空间。但是，当您将此命令添加到入站访问组时，配置必须显示在一行上。要允许在Cisco IOS路由器上进行SSH访问，请将此行添加到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
```

要允许Cisco PIX/ASA上的SSH访问，请添加以下配置：

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

如果对本文档中描述的信息有任何疑问或需要其他帮助，请联系思科技术支持中心(TAC)。

此网页仅供参考，按“原样”提供，不提供任何保证或保证。上述最佳实践不是旨在全面的，而是建议补充客户当前的安全程序。任何安全实践的有效性取决于每个客户的具体情况；我们鼓励客户在确定最适合其网络的安全程序时考虑所有相关因素。

相关信息

- Cisco Unified MeetingPlace
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考

- 安全产品 Field Notices (包括 PIX)
- Cisco 技术 支持 中心 (TAC)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems