当准许第三方访问时保护网络安全

目录

简介

在此服务请求期间，您可以Cisco工程师访问您的组织网络。授权这样访问经常将允许您的服务请求迅速被解决。在这类情况下，思科能，并且只，请访问您的与您的权限的网络。

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

思科建议您遵从这些指南为了帮助您保护您的网络安全，当您准许对所有技术支持工程师或人的访问在您的公司或组织外面时。

- 若可能，请使用Cisco Unified MeetingPlace为了共享与技术支持工程师的信息。思科建议您使用Cisco Unified MeetingPlace对于这些原因：Cisco Unified MeetingPlace使用安全套接字层SSL协议，比安全壳SSH或Telnet在某些情况下是安全的更多。Cisco Unified MeetingPlace不要求您提供密码给任何人在您的公司或组织外面。**注意：** 每当您准许对人的网络访问您的公司或组织的外部，您提供的所有密码必须是有效的临时密码，只有只要第三方需要对您的网络的访问。一般，因为多数企业防火墙允许出站HTTPS访问， Cisco Unified MeetingPlace不要求

您更改您的防火墙策略。访问Cisco Unified MeetingPlace欲知更多信息。

- 如果不能使用Cisco Unified MeetingPlace，并且，如果选择通过另一应用程序允许第三方访问，例如SSH，请保证密码是临时和可用的为仅一次性使用。另外，在第三方访问不再是必要的后，您必须立即更改或无效密码。除Cisco Unified MeetingPlace之外，如果使用一应用程序，您可以遵从这些步骤和指南：为了创建在Cisco IOS路由器的一个临时帐户，请使用此命令：

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

为了创建在PIX/ASA的一个临时帐户，请使用此命令：

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

为了删除临时帐户，请使用此命令：

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

请随机地生成临时密码。不能与支持服务的特定服务请求或服务商涉及临时密码。例如，请勿使用密码例如*cisco*、*cisco123*或者*ciscotac*。请勿给您自己的用户名或密码。请勿使用在互联网的Telnet。它不安全。

- 如果要求支持的Cisco设备在公司防火墙和一更改后查找对防火墙策略为一位技术支持工程师要求SSH的到Cisco设备，请保证策略变更是特定对技术支持工程师分配到问题。比必要请勿做策略例外开放对整个互联网或对各种各样的主机。要修改在Cisco IOS防火墙的一项防火墙策略，请添加这些线路到进入访问控制列表在面对接口的互联网下：

```
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： 在本例中，(config-ext-nacl) #配置在两条线路显示为了保存空间。然而，当您添加此命令到进入访问控制列表时，配置必须出现在一条线路。要修改在思科PIX/ASA防火墙的一项防火墙策略，请添加此线路到入站访问组：

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

注意： 在本例中，ASA(config)-配置在两条线路显示为了保存空间。然而，当您添加此命令到入站访问组时，配置必须出现在一条线路。要允许在Cisco IOS路由器的SSH访问，请添加此线路到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
```

要允许在思科PIX/ASA的SSH访问，请添加此配置：

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

如果请有问题或要求与在本文描述的信息的其他帮助，请与Cisco技术支持中心(TAC)联系。

没有任何保证或质保，此网页只是作为提供情报的目的和现状提供根据一个基本类型。以上的最佳实践没有打算全面，然而被建议补全客户的当前安全步骤。所有安全实践的效果依靠每客户的特殊的例子;当确定安全程序适当为他们的网络时，并且客户被鼓励设想所有相关要素。

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