保護網路安全並向第三方授予訪問許可權

目錄

簡介

在此服務請求過程中，您可能希望思科工程師訪問您組織的網路。授予此類訪問許可權通常會使您的服務請求得到更快的解決。在此類情況下，思科可以而且將只會在您允許的情況下訪問您的網路。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需檔案慣例的相關資訊，請參閱思科技術提示慣例。

最佳實踐

思科建議您遵循以下准則，以便在授予貴公司或組織之外的任何支援工程師或人員的訪問許可權時幫助您保護網路安全。

- 如有可能，請使用Cisco Unified MeetingPlace與支援工程師共用資訊。出於以下原因，思科建議您使用Cisco Unified MeetingPlace:Cisco Unified MeetingPlace使用安全套接字層(SSL)協定，該協定在某些情況下比安全外殼(SSH)或Telnet更安全。Cisco Unified MeetingPlace不要求您向公司或組織之外的任何人提供密碼。**注意：**當您向公司或組織外部人員授予網路訪問許可權時，您提供的任何密碼都必須是臨時密碼，並且僅在第三方要求訪問您的網路時才有效。通

常，Cisco Unified MeetingPlace不需要您更改防火牆策略，因為大多數企業防火牆都允許出站HTTPS訪問。有關詳細資訊，請訪問Cisco Unified MeetingPlace。

- 如果不能使用Cisco Unified MeetingPlace並選擇允許第三方通過其他應用程式（如SSH）訪問，請確保密碼是臨時的，且只能一次性使用。此外，在不再需要第三方訪問之後，您必須立即更改密碼或使密碼無效。如果您使用Cisco Unified MeetingPlace以外的應用程式，可以遵循以下步驟和准則：要在Cisco IOS路由器上建立臨時帳戶，請使用以下命令：

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

要在PIX/ASA上建立臨時帳戶，請使用以下命令：

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

若要移除臨時帳戶，請使用以下命令：

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

隨機生成臨時密碼。臨時密碼不得與特定服務請求或支援服務提供商相關。例如，請勿使用*cisco*、*cisco123*或*ciscotac*等密碼。切勿提供自己的使用者名稱或密碼。請勿通過Internet使用Telnet。這不安全。

- 如果需要支援的思科裝置位於公司防火牆後面，並且需要更改防火牆策略才能使支援工程師通過SSH連線到思科裝置，請確保策略更改特定於分配給問題的支援工程師。切勿將策略例外開啟到整個Internet或所需的主機範圍更廣。要在Cisco IOS防火牆上修改防火牆策略，請將這些行新增到面向網際網路的介面下的入站訪問清單中：

```
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，Router(config-ext-nacl)#configuration顯示在兩行上以節省空間。但是，將此命令新增到入站訪問清單時，配置必須顯示在一行上。要修改Cisco PIX/ASA防火牆上的防火牆策略，請將此行新增到入站訪問組：

```
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)#配置顯示在兩行上以節省空間。但是，將此命令新增到入站訪問組時，配置必須顯示在一行上。要在Cisco IOS路由器上允許SSH訪問，請將此行新增到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
```

要在Cisco PIX/ASA上允許SSH訪問，請新增以下配置：

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

如果您對本檔案中描述的資訊有疑問或需要其他幫助，請聯絡思科技術協助中心(TAC)。

此網頁僅供參考，按「原樣」提供，沒有任何保證或擔保。上述最佳實踐不是為了全面，而是為了補充客戶當前的安全程式。任何安全慣例的效力取決於每個客戶的具體情況；鼓勵客戶在確定最適合其網路的安全程式時考慮所有相關因素。

相關資訊

- Cisco Unified MeetingPlace
- Cisco PIX防火牆軟體

- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 思科技術支援中心(TAC)
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems