Proteja la seguridad de la red y conceda acceso a terceros

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Mejores medidas](#)
[Información Relacionada](#)

Introducción

Durante esta solicitud de servicio, es posible que desee que los ingenieros de Cisco accedan a la red de su organización. Al conceder dicho acceso, a menudo su solicitud de servicio se resolverá más rápidamente. En estos casos, Cisco puede acceder a su red con su permiso, y solo lo hará.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener información sobre las convenciones sobre documentos.

Mejores medidas

Cisco recomienda que siga estas directrices para ayudarle a proteger la seguridad de su red cuando conceda acceso a cualquier ingeniero de soporte o persona fuera de su empresa u organización.

- Si es posible, utilice Cisco Unified MeetingPlace para compartir información con los ingenieros de soporte. Cisco recomienda utilizar Cisco Unified MeetingPlace por estos motivos:Cisco Unified MeetingPlace utiliza el protocolo Secure Socket Layer (SSL), que en algunos casos es más seguro que Secure Shell (SSH) o Telnet.Cisco Unified MeetingPlace no requiere que proporcione contraseñas a nadie fuera de su empresa u organización.**Nota:** Siempre que conceda acceso a la red a personas ajenas a su empresa u organización, cualquier contraseña que proporcione debe ser una contraseña temporal que sólo sea válida mientras el tercero requiera acceso a su red.Normalmente, Cisco Unified MeetingPlace no requiere que cambie la política de firewall porque la mayoría de los firewalls empresariales permiten el acceso HTTPS saliente.Visite Cisco Unified MeetingPlace para obtener más información.
- Si no puede utilizar Cisco Unified MeetingPlace y si decide permitir el acceso de terceros a través de otra aplicación, como SSH, asegúrese de que la contraseña es temporal y está disponible sólo para uso único. Además, debe cambiar o invalidar inmediatamente la contraseña después de que el acceso de terceros ya no sea necesario. Si utiliza una aplicación distinta de Cisco Unified MeetingPlace, puede seguir estos procedimientos y directrices:Para crear una cuenta temporal en los routers Cisco IOS, utilice este comando:
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Para crear una cuenta temporal en PIX/ASA, utilice este comando:
  ```
  PIX(config)#username tempaccount password QWE!@#
  ```

  Para quitar la cuenta temporal, utilice este comando:
  ```
  Router (config)#no username tempaccount
  ```

  Genere aleatoriamente la contraseña temporal. La contraseña temporal no debe estar relacionada con la solicitud de servicio específica o con el proveedor de servicios de soporte. Por ejemplo, no utilice contraseñas como *cisco*, *cisco123* o *ciscotac.*Nunca dé su propio nombre de usuario o contraseña.No utilice Telnet a través de Internet. No es seguro.
- Si el dispositivo de Cisco que requiere soporte se encuentra detrás de un firewall corporativo y se requiere un cambio en las políticas de firewall para que un ingeniero de soporte inicie SSH en el dispositivo de Cisco, asegúrese de que el cambio de política sea específico para el ingeniero de soporte asignado al problema. Nunca abra la excepción de política a todo Internet o a un rango más amplio de hosts de lo necesario.Para modificar una política de firewall en un Cisco IOS Firewall, añada estas líneas a la lista de acceso entrante en la interfaz orientada a 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
  ```

  Nota: En este ejemplo, la configuración `Router(config-ext-nacl)#` se muestra en dos líneas para conservar espacio. Sin embargo, cuando agrega este comando a la lista de acceso entrante, la configuración debe aparecer en una línea.Para modificar una política de firewall en un firewall Cisco PIX/ASA, agregue esta línea al grupo de acceso entrante:
  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

  Nota: En este ejemplo, la `configuración ASA(config)#` se muestra en dos líneas para conservar espacio. Sin embargo, cuando agrega este comando al grupo de acceso entrante, la configuración debe aparecer en una línea.Para permitir el acceso SSH en los routers Cisco

IOS, agregue esta línea a la clase de acceso:

```
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 el acceso SSH en Cisco PIX/ASA, agregue esta configuración:

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

Si tiene preguntas sobre la información descrita en este documento o necesita asistencia adicional, póngase en contacto con el Centro de asistencia técnica de Cisco (TAC).

Información Relacionada

- Cisco Unified MeetingPlace
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Centro de la asistencia técnica de Cisco (TAC)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems