Seguridad de la red de protección al conceder el acceso a los otros vendedores

Contenido

Introducción

Durante el curso de esta solicitud de servicio, usted puede quisiera que los ingenieros de Cisco accedieran la red de su organización. La concesión de tal acceso permitirá a menudo que su solicitud de servicio sea resuelta más rápidamente. En estos casos, Cisco puede, y solamente, acceder su red con su permiso.

prerrequisitos

Requisitos

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 usted sigue estas guías de consulta para ayudarle a proteger la Seguridad de su red cuando usted concede el acceso a cualquier ingeniero de servicio técnico o persona fuera de su compañía u organización.

- Si es posible, utilice el Cisco Unified MeetingPlace para compartir la información con los ingenieros de servicio técnico. Cisco recomienda que usted utiliza el Cisco Unified MeetingPlace por estas razones:El Cisco Unified MeetingPlace utiliza el protocolo del Secure Socket Layer (SSL), que es más seguro que el Secure Shell (SSH) o Telnet en algunos casos.El Cisco Unified MeetingPlace no le requiere proporcionar las contraseñas a cualquier persona fuera de su compañía u organización.**Note**: Siempre que usted conceda el acceso a la red a las personas fuera de su compañía u organización, cualquier contraseña que usted proporcione debe ser las contraseñas temporales que son válidas solamente mientras el otro vendedor requiere el acceso a su red.Típicamente, el Cisco Unified MeetingPlace no le requiere cambiar sus políticas del firewall porque la mayoría de los Firewall de la empresa permiten el acceso saliente HTTPS.Cisco Unified MeetingPlace de la visita para más información.
- Si usted no puede utilizar el Cisco Unified MeetingPlace y si usted elige permitir el acceso de tercera persona con otra aplicación, tal como SSH, asegúrese que la contraseña esté temporal y disponible para el uso de una sola vez solamente. Además, usted debe cambiar o invalidar inmediatamente la contraseña después de que el acceso de tercera persona sea no más necesario. Si usted utiliza una aplicación con excepción del Cisco Unified MeetingPlace, usted puede seguir estos procedimientos y guías de consulta:Para crear una cuenta temporal en el Routers del Cisco IOS, utilice este comando:
  ```
  Router(config)#username tempaccount secret QWE!@#
  ```

  Para crear una cuenta temporal en el 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 se debe relacionar con la petición del servicio determinado o el proveedor de los servicios del soporte. Por ejemplo, no utilice las contraseñas tales como *Cisco*, *cisco123*, o *ciscotac*.Nunca dé su propio Nombre de usuario o contraseña.No utilice Telnet sobre Internet. No es seguro.
- Si el dispositivo de Cisco que requiere el soporte está situado detrás de un escurdo de protección corporativo y de un cambio a las políticas del firewall se requiere para un ingeniero de servicio técnico a SSH en el dispositivo de Cisco, asegúrese de que el cambio de política sea específico al ingeniero de servicio técnico asignado al problema. Nunca haga la excepción de la directiva abierta al toda la Internet o a una gama más amplia de los host que necesaria.Para modificar las políticas del firewall en un Firewall Cisco IOS, agregue estas líneas a la lista de acceso de entrada bajo Internet que hace frente a la interfaz:
  ```
  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: En este ejemplo, visualizan al `router (config-extensión-nacl) #` configuración en dos líneas para conservar el espacio. Sin embargo, cuando usted agrega este comando a la lista de acceso de entrada, la configuración debe aparecer en una línea.Para modificar las políticas del firewall en un Firewall del PIX/ASA de Cisco, agregue esta línea al acceso-grupo entrante:
  ```
  ASA(config)#access-list inbound line 1 permit tcp host
      <IP address for TAC engineer> host <Cisco device address> eq 22
  ```

Note: En este ejemplo, la configuración de `ASA(config)#` se visualiza en dos líneas para conservar el espacio. Sin embargo, cuando usted agrega este comando al acceso-grupo entrante, la configuración debe aparecer en una línea.Para permitir el acceso de SSH en el Routers del Cisco IOS, agregue esta línea a la acceso-clase:

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

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

Si tenga preguntas alrededor o requiera la ayuda adicional con la información descrita en este documento, entre en contacto 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