Nota Técnica en el FAQ para el Acceso Remoto en Cisco ESA/WSA/SMA

Contenido

Introducción

Este documento proporciona las respuestas a las preguntas frecuentes sobre el uso del Acceso Remoto por el Soporte técnico de Cisco en los dispositivos de seguridad del contenido de Cisco. Esto incluye el dispositivo de seguridad del correo electrónico de Cisco (ESA), el dispositivo de seguridad de la red de Cisco (WSA), y el dispositivo de la Administración del Cisco Security (S A).

Prerrequisitos

Componentes Utilizados

La información en este documento se basa en los dispositivos de seguridad del contenido de Cisco que funcionan con cualquier versión de AsyncOS.

¿Cuál es Acceso Remoto?

El Acceso Remoto es una conexión del Secure Shell (SSH) que se habilita de un dispositivo de seguridad del contenido de Cisco a un host seguro en Cisco. Solamente la ayuda del cliente de Cisco puede acceder el dispositivo una vez que habilitan a una sesión remota. El Acceso Remoto

permite que el soporte de cliente de Cisco analice un dispositivo. El soporte accede el dispositivo a través de un túnel de SSH que este procedimiento cree entre el dispositivo y el servidor de upgrades.ironport.com.

Cómo el Acceso Remoto trabaja

Cuando los iniciados de una conexión de acceso remoto, el dispositivo abren un seguro, al azar, puerto de la alto-fuente vía una conexión SSH en el dispositivo al configurado/el puerto seleccionado uno de los servidores de seguridad siguientes del contenido de Cisco:

DIRECCIÓN IP	Nombre del host	Utilice
63.251.108.107	upgrades.ironport.com	Todos contentan los dispositivos de seguridad
184.94.240.126	c.tunnels.ironport.com	utilizado para la serie C appliances/ESA
184.94.240.126	x.tunnels.ironport.com	utilizado para las X-series appliances/ESA
184.94.240.126	m.tunnels.ironport.com	utilizado para las M-series appliances/SMA
184.94.240.126	s.tunnels.ironport.com	utilizado para la serie S appliances/WSA

Es importante observar que un Firewall del cliente puede necesitar ser configurado para permitir las conexiones salientes a uno arriba de los servidores mencionados. Si su Firewall tiene examen del protocolo S TP habilitado, el túnel no establecerá. Los puertos que Cisco validará las conexiones del dispositivo para el Acceso Remoto son:

- 22
- 25 (valor por defecto)
- 53
- 80
- 443
- 4766

La conexión de acceso remoto se hace a un nombre del host y no a una dirección IP codificada por hardware. Esto requiere el Domain Name Server (DNS) ser configurada en el dispositivo para establecer la conexión saliente.

En una red del cliente, algunos dispositivos de red protocolo-enterados pueden bloquear esta conexión debido a la discordancía del /port del protocolo. Un cierto protocolo simple mail transport (S TP) - los dispositivos enterados puede también interrumpir la conexión. En caso de que haya los dispositivos o las conexiones salientes protocolo-enterados se bloquean que, el uso de un puerto con excepción del valor por defecto (25) puede ser requerido. El acceso al extremo remoto del túnel se restringe solamente al soporte de cliente de Cisco. Esté por favor seguro que usted revisa su Firewall/red para las conexiones salientes al intentar establecer o resolver problemas las conexiones de acceso remoto para su dispositivo.

> Nota: Cuando un ingeniero de servicio técnico del cliente de Cisco está conectado con el dispositivo vía el Acceso Remoto el prompt del sistema en el dispositivo muestra *(SERVICIO)*.

Cómo habilitar el Acceso Remoto

> Nota: Esté por favor seguro de revisar el guía del usuario de su dispositivo y la versión de AsyncOS para las instrucciones en “habilitar el Acceso Remoto para el personal de soporte

técnico de Cisco".

Nota: Las conexiones enviadas vía el email a attach@cisco.com pueden no ser seguras adentro transitan. El administrador del caso de soporte es la opción segura preferida de Cisco de cargar la información a su caso. Para aprender más sobre la Seguridad y las limitaciones de espacio de otras File Upload (Subir archivo) opciones: Cargas del archivo de cliente al Centro de Asistencia Técnica de Cisco

Identifique un puerto que se pueda alcanzar de Internet. El valor por defecto es el puerto 25, que trabajará en la mayoría de los entornos porque el sistema también requiere el acceso general sobre ese puerto para enviar los correos electrónicos. Las conexiones sobre este puerto se permiten en la mayoría de las configuraciones de escudo de protección.

CLI

Para establecer una conexión de acceso remoto vía el CLI, como Usuario administrador, completa estos pasos:

1. Ingrese el comando del **techsupport**
2. Elija el **TÚNEL**
3. Elija generar o *ingresar una* cadena al azar del germen
4. Especifique el número del puerto para la conexión
5. Conteste "**Y**" para habilitar el acceso del servicio

El Acceso Remoto será habilitado ahora. El dispositivo ahora trabaja para establecer la conexión segura al bastion host seguro en Cisco. Proporcione el número de serie del dispositivo y la cadena del germen que se genera al ingeniero de TAC que soporta su caso.

GUI

Para establecer una conexión de acceso remoto vía el GUI, como Usuario administrador, completa estos pasos:

1. Navegue **para ayudar y el soporte > el Acceso Remoto** (para el ESA, el S A), **soportan y ayuda > Acceso Remoto** (para WSA)
2. **Permiso del** tecleo
3. Elija el método para la cadena del germen
4. Asegúrese de que usted marque la *conexión iniciado vía la* casilla de verificación del *túnel seguro* y especifique el número del puerto para la conexión
5. El tecleo **somete**

El Acceso Remoto será habilitado ahora. El dispositivo ahora trabaja para establecer la conexión segura al bastion host seguro en Cisco. Proporcione el número de serie del dispositivo y la cadena del germen que se genera al ingeniero de TAC que soporta su caso.

Cómo inhabilitar el Acceso Remoto

CLI

1. Ingrese el comando del **techsupport**

2. Elija la **NEUTRALIZACIÓN**
3. Conteste "**Y**" cuando está indicado "es usted seguro que usted quiere inhabilitar el acceso del servicio?"

GUI

1. Navegue **para ayudar y el soporte > el Acceso Remoto** (para el ESA, el S A), **soportan y ayuda > Acceso Remoto** (para WSA).
2. **Neutralización del** tecleo
3. La salida GUI mostrará el "éxito — se ha inhabilitado el Acceso Remoto"

Cómo probar la Conectividad del Acceso Remoto

Utilice este ejemplo para realizar una prueba inicial para la Conectividad de su dispositivo a Cisco:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

La Conectividad se puede probar para los puertos uces de los enumerados arriba: 22, 25, 53, 80, 443, o 4766. Si la Conectividad falla, usted puede necesitar funcionar con a una captura de paquetes para ver donde la conexión está fallando de su dispositivo/red.

¿Por qué el Acceso Remoto no trabaja en el S A?

El Acceso Remoto puede no habilitar en un S A si el S A se coloca en la red local sin el acceso directo a Internet. Para este caso, el Acceso Remoto se puede habilitar en un ESA o un WSA, y el acceso de SSH se puede habilitar en el S A. Esto permite el soporte de Cisco a primero conecta vía el Acceso Remoto al ESA/WSA, y entonces del ESA/WSA al S A vía SSH. Esto requerirá la Conectividad entre el ESA/WSA y el S A en el puerto 22.

> Nota: Esté por favor seguro de revisar el guía del usuario de su dispositivo y la versión de AsyncOS para las instrucciones en "habilitar el Acceso Remoto a los dispositivos sin una conexión de Internet directa".

CLI

Para establecer una conexión de acceso remoto vía el CLI, como Usuario administrador, completa estos pasos:

1. Ingrese el comando del **techsupport**
2. Elija **SSHACCESS**
3. Elija generar o *ingresar una* cadena al azar del germen
4. Conteste "**Y**" para habilitar el acceso del servicio

El Acceso Remoto será habilitado ahora. La salida CLI mostrará la cadena del germen.

Proporcione por favor esto al ingeniero de servicio técnico del cliente de Cisco. La salida CLI también mostrará a los detalles del estado de la conexión y del Acceso Remoto, incluyendo el número de serie del dispositivo. Proporcione por favor este número de serie al ingeniero de asistencia técnica al cliente del cliente.

GUI

Para establecer una conexión de acceso remoto vía el GUI, como Usuario administrador, completa estos pasos:

1. Navegue **para ayudar y el soporte > el Acceso Remoto** (para el ESA, el S A), **soportan y ayuda > Acceso Remoto** (para WSA)
2. **Permiso del** tecleo
3. Elija el método para la cadena del germen
4. No marque la *conexión iniciado vía la* casilla de verificación del *túnel seguro*
5. El tecleo **somete**

El Acceso Remoto será habilitado ahora. La salida GUI le mostrará un Mensaje de éxito y la cadena del germen del dispositivo. Proporcione por favor esto al ingeniero de servicio técnico del cliente de Cisco. La salida GUI también mostrará el estado de la conexión y a los detalles del Acceso Remoto, incluyendo el número de serie del dispositivo. Proporcione por favor este número de serie al ingeniero de asistencia técnica al cliente del cliente.

Cómo inhabilitar el Acceso Remoto cuando está habilitado para SSHACCESS

Inhabilitar el Acceso Remoto para SSHACCESS es los mismos pasos como está previsto arriba.

Resolución de problemas

Si el dispositivo no es Acceso Remoto habilitado capaz y conecta con upgrades.ironport.com vía uno de los puertos enumerados, usted necesitará funcionar con a una captura de paquetes directamente del dispositivo para revisar qué está haciendo la conexión saliente fallar.

> Nota: Esté por favor seguro de revisar el guía del usuario de su dispositivo y la versión de AsyncOS para las instrucciones en “funcionar con a una captura de paquetes”.

El ingeniero de servicio técnico del cliente de Cisco puede pedir para hacer el archivo .pcap proporcionar para revisar y ayudar con el troubleshooting.

Información Relacionada

- ESA FAQ: ¿Cuáles son los niveles de acceso administrativo disponibles en el ESA?
- Soporte de productos del dispositivo de seguridad del correo electrónico de Cisco
- Soporte de producto de seguridad de la red de Cisco
- Soporte de productos del dispositivo de la Administración de seguridad del contenido de Cisco
- Soporte Técnico y Documentación - Cisco Systems