

Direcciones de Destino de Acceso Seguro para la Configuración de Ruteo Dividido

Contenido

Problema

Al implementar Cisco Secure Access (CSA) con Cisco Secure Client (CSC) en terminales Windows en una arquitectura de red de hub-radio, lo más probable es que las organizaciones necesiten configurar el routing dividido para permitir que el tráfico del sitio de Spoke se conecte directamente a CSA a través del circuito de Internet local de Spoke en lugar de pasar por el concentrador. Esta configuración requiere conocer todas las direcciones de destino de Cisco utilizadas al establecer el túnel CSA, de modo que las excepciones de routing (routing de ruptura/división) se puedan definir en los dispositivos de red, como los firewalls de Fortigate.

El requisito específico es identificar toda la información de destino (direcciones IP o URL) para los terminales CSA utilizados por CSC al establecer los túneles TLS/DTLS, lo que permite una configuración adecuada de las políticas de routing que omiten el túnel VPN de hub-radio para el tráfico CSA.

Entorno

- Implementación de Cisco Secure Access (CSA)
- Cisco Secure Client (CSC) en terminales Windows
- Topología de red de hub-radio con firewalls Fortigate
- Conectividad de túnel TLS/DTLS con CSA

Resolución

Para configurar el routing dividido para las conexiones de Cisco Secure Access, la información de destino descrita en las siguientes secciones debe configurarse en el dispositivo Fortigate para permitir la conectividad directa con los terminales CSA.

Puertos y dominio de destino de CSA

Dominio principal

`*.vpn.sse.cisco.com`

Puertos y protocolos necesarios

- TCP/UDP 443: Se utiliza para el establecimiento de túneles TLS/DTLS
- UDP 500/4500: Se utiliza para establecer túneles IPsec
- TCP 80: Se utiliza para comprobaciones de revocación de certificados VPN

Enfoque de configuración de Fortigate

Configure las políticas de routing en el dispositivo Fortigate para dirigir el tráfico destinado al dominio CSA (`*.vpn.sse.cisco.com`) y los puertos especificados a través del circuito de Internet de radio local en lugar de a través del túnel VPN de hub-radio. Esto habilita el flujo de tráfico descrito en los siguientes fragmentos de código.

Flujo de tráfico deseado

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

En lugar del flujo de tráfico a través del sitio del hub

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

Consideraciones importantes

Los destinos de conexión CSA se determinan dinámicamente durante el tiempo de ejecución, lo que significa que las direcciones IP específicas no se pueden predeterminar para la configuración de ruteo estático. El enfoque basado en dominios que utiliza *.vpn.sse.cisco.com proporciona el método más fiable para configurar las políticas de routing dividido.

Consulte la documentación oficial de Cisco Secure Access para conocer los requisitos de puerto y destino más actuales, ya que es muy probable que se actualicen con nuevas versiones de software.

Causa

En las topologías de red Hub-Spoke, todo el tráfico de Internet procedente de los sitios Spoke se dirige normalmente a través del sitio Hub de forma predeterminada. Al implementar CSA con CSC, este comportamiento de routing predeterminado hace que el tráfico del túnel CSA pase por el sitio del hub antes de llegar a los terminales CSA, lo que puede introducir latencia e ineficiencias en el ancho de banda. La naturaleza dinámica de la selección de terminales CSA requiere políticas de routing basadas en dominios en lugar de reglas estáticas basadas en IP para garantizar una funcionalidad de routing dividido adecuada.

Contenido relacionado

- [Documentación de Cisco Secure Access - Requisitos de conexión](#)
- [Documentación de Cisco Secure Access - Configuración de red](#)

- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).