VPN de acceso seguro: no se puede acceder a Jabber

Contenido

Problema

Los usuarios de Secure Client no pudieron acceder a las aplicaciones internas y privadas, como Jabber y Epic, a través del túnel VPN de Secure Access cuando utilizaban una política de acceso privado. Los usuarios experimentaron errores de conectividad al intentar acceder a estas aplicaciones empresariales críticas a través de la conexión VPN. Durante la resolución de problemas, se observó tráfico unidireccional para los recursos Epic, donde el tráfico SYN de TCP y ping se observó egresando del túnel VPN de acceso seguro, pero se identificaron problemas de validación de tráfico de retorno en el firewall de Palo Alto. Además, se documentaron problemas de disponibilidad de Jabber en los que los FQDN de CUCM se resolvían a través de DNS interno mientras el direccionamiento del tráfico se configuraba para el routing basado en IP, lo que provocaba una discordancia en el flujo de tráfico.

Entorno

- Cisco Secure Access con configuración de túnel VPN
- Secure Client para conectividad VPN
- Implementación de políticas de acceso privado
- Cisco Unified Communications Manager (CUCM) para servicios Jabber
- Recursos de aplicaciones épicos
- Firewall de Palo Alto para la seguridad de la red
- Resolución DNS interna para FQDN de CUCM

Resolución

La resolución implicó varios cambios de configuración y pasos de resolución de problemas para restaurar la conectividad a las aplicaciones internas a través del túnel VPN de acceso seguro:

Configuración de Subred y Modificaciones de Túnel

Paso 1: Agregar subredes adicionales al túnel VPN

Se agregaron subredes adicionales a la configuración del túnel VPN para los recursos afectados. Después de implementar este cambio, los recursos que antes eran inaccesibles comenzaron a cargarse correctamente.

Configuración de dirección de direcciones IP de CUCM

Paso 2: Configuración de la dirección IP de CUCM

Para resolver el problema de conectividad de Jabber en el que los FQDN de CUCM se resolvían a través de DNS interno mientras el direccionamiento del tráfico se basaba en IP, las direcciones IP de CUCM se dirigían a Secure Client. Este cambio de configuración alineó la resolución DNS con el mecanismo de dirección del tráfico.

Paso 3: Crear regla de directiva de acceso

Se creó una regla de política de acceso para permitir el acceso a las direcciones IP de CUCM. Esta regla restauró la conectividad correcta a la infraestructura de CUCM, habilitando la funcionalidad de Jabber en el túnel VPN.

Configuración de Ruteo Estático

Paso 4: Configuración del enrutamiento estático para la subred de CUCM

Asegúrese de que las direcciones IP de CUCM y la subred general de CUCM estén incluidas en la tabla de routing estático para el túnel de red. Esta configuración garantiza un routing adecuado del tráfico entre el grupo de usuarios de Secure Client y la infraestructura de CUCM.

Validación de tráfico de devoluciones

Paso 5: Validar el flujo de paquetes y el tráfico de retorno

Valide la configuración del flujo de paquetes para confirmar que el tráfico de retorno puede alcanzar el grupo de usuarios de Secure Client. Esto incluye la revisión de la configuración del firewall de Palo Alto para garantizar una validación adecuada de la ruta de retorno para todos los

recursos internos, especialmente para la conectividad Epic, donde se observó tráfico unidireccional.

Causa

Los problemas de conectividad fueron causados por varias brechas de configuración en la implementación de VPN de acceso seguro:

- La falta de configuraciones de subred en el túnel VPN impidió el enrutamiento correcto a los recursos internos de la aplicación
- La discordancia entre la resolución de DNS (basada en FQDN) y la configuración de la dirección del tráfico (basada en IP) para los servicios de CUCM provocó errores de conectividad de Jabber
- Reglas de política de acceso incompletas que no permitían el tráfico a las direcciones IP de CUCM
- Faltan entradas de routing estático para subredes de CUCM en la configuración del túnel de red
- Problemas de validación de la ruta de tráfico de retorno en el firewall de Palo Alto que afectan a la comunicación bidireccional

Contenido relacionado

- 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).