Problemas de conectividad FQDN alojada en Azure mediante acceso seguro con integración de Meraki

Contenido

Problema

Los FQDN alojados en Azure específicos se vuelven inalcanzables cuando el tráfico de usuario se enruta a través de Meraki a Cisco Secure Access, a pesar de que los registros de Secure Access muestran el tráfico como "permitido". El problema afecta principalmente a la conectividad RDP usando puertos no estándar para estos FQDN.

Al buscar registros por FQDN en el portal de acceso seguro, solo se muestran los registros de seguridad DNS con el estado "permitido". Sin embargo, la conectividad RDP a los mismos destinos en los puertos no estándar falla. Cuando el FQDN se resuelve en una dirección IP y la búsqueda de actividad utiliza la IP de destino, se muestran los registros de Cloud Firewall que han estado bloqueando el tráfico.

Entorno

- Cisco Secure Access (SSE) con integración con Meraki
- Panel de Meraki con capacidad de ruptura local
- Recursos de desarrollo alojados en Azure que requieren acceso RDP en puertos no estándar
- Routing del tráfico a través del túnel Meraki para un acceso seguro

Resolución

Solución alternativa inmediata

Agregue los FQDN afectados a las reglas de ruptura locales de Meraki para omitir el acceso seguro para los destinos específicos detallados en las siguientes secciones.

Paso 1: Acceder al panel de Meraki

Navegue hasta el panel de Meraki y localice la sección de configuración de la ruptura local.

Paso 2: Configurar reglas de separación local

Agregue los FQDN problemáticos a las reglas de desconexión locales para omitir el routing de acceso seguro. Este cambio de configuración restablece inmediatamente el acceso de los usuarios afectados enrutando el tráfico directamente desde Meraki a Internet, sin pasar por el túnel de acceso seguro.

Resolución de problemas y análisis

Paso 1: Análisis de registro por FQDN

Busque los registros de actividad de acceso seguro mediante el FQDN. Esto muestra principalmente los registros de seguridad DNS y puede mostrar el estado "permitido" para el tráfico web en el puerto 443.

Paso 2: Análisis de registro por IP de destino

Resuelva el FQDN en su dirección IP y busque los registros de actividad utilizando la IP de destino en lugar del FQDN. Esto muestra los registros de Cloud Firewall que muestran el tráfico

bloqueado, proporcionando la disposición real del tráfico.

Paso 3: Verificar flujo de tráfico

Confirme que el problema ocurre solamente cuando el tráfico sigue la trayectoria: Usuario → Túnel Meraki → → Acceso Seguro → Internet. La prueba de omisión a través de una ruptura local resuelve el problema de conectividad.

Resolución a largo plazo

El comportamiento observado se ha identificado como la funcionalidad esperada dentro de la implementación actual de Secure Access. Se ha abierto una solicitud de características (FR CSE-I-5543) para abordar las preocupaciones funcionales y de visibilidad relacionadas con:

- Discrepancia entre búsquedas de registro basadas en FQDN y basadas en IP
- Informes de disposición de tráfico incoherentes entre los registros de Seguridad DNS y Firewall de nube
- Visibilidad mejorada para el tráfico RDP en puertos no estándar

Causa

El problema surge de una discrepancia en cómo Secure Access procesa y notifica el tráfico para los FQDN alojados en Azure cuando se accede a través de RDP en puertos no estándar. Al buscar registros por FQDN, el sistema muestra principalmente registros de seguridad DNS que muestran el estado "permitido" para el tráfico web (normalmente el puerto 443). Sin embargo, el tráfico RDP real en los puertos no estándar está siendo procesado por las reglas de Cloud Firewall, que solo son visibles cuando se realiza una búsqueda por la dirección IP de destino resuelta en lugar del FQDN.

Esto crea una brecha de visibilidad en la que los administradores ven el tráfico "permitido" en las búsquedas basadas en FQDN mientras las conexiones RDP reales están siendo bloqueadas por las políticas de firewall que solo son evidentes en las búsquedas de registro basadas en IP. El comportamiento se considera actualmente una funcionalidad esperada, pero se ha enviado una

solicitud de función para mejorar la visibilidad y la coherencia de los informes de tráfico a través de los diferentes métodos de búsqueda.

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).