El bloqueo del protocolo de aplicaciones de acceso seguro impide la conectividad a Internet

Contenido

- Problema
- Entorno
- Resolución
  - Paso 1: Identificación de la regla de bloqueo
  - Paso 2: Modificar configuración de aplicación
  - Paso 3: Aplicar y verificar cambios
- Causa
- Contenido relacionado

Problema

Tras la migración a Cisco Secure Access, los usuarios experimentaron un bloqueo de la conectividad a Internet al intentar acceder a los servicios web. El síntoma específico consistía en que la política de seguridad bloqueaba el tráfico HTTP, lo que impedía el acceso a aplicaciones y sitios web legítimos.

Los detalles del evento de bloqueo mostraron estas características:

- Acción: Bloqueado
- Motivo del bloqueo de eventos: AC_RULE_MATCH_BLOCK
- Destino: http://www.bing.com/api/shopping/v1/user/shoppingsettings

- Puerto de Destino: 443
- Categorías: Sin categoría
- Categoría de aplicación: Buscar
- Protocolo de aplicación: Protocolo de transferencia de hipertexto
- Protocolo: TCP

Entorno

- Implementación de Cisco Secure Access
- Política de seguridad activa con restricciones de protocolo de aplicación

Resolución

La resolución implica la modificación de la configuración de la regla de seguridad para permitir el tráfico del protocolo de aplicación HTTP y, al mismo tiempo, mantener el estado de seguridad de las aplicaciones que realmente no son de confianza.

Paso 1: Identificación de la regla de bloqueo

Localice la regla específica que causa el bloqueo en la interfaz de administración de Secure Access:

- ‘Nombre de la regla Prueba
- Configuración actual Uso del bloque Configuración de la aplicación como destino.

Paso 2: Modificar configuración de aplicación

Acceda a la configuración de la regla y compruebe el nombre de la configuración de la aplicación en Destino:

- Vaya a Recursos > Recursos de Internet y SaaS > Listas de aplicaciones. A continuación, haga clic en la aplicación.
- Busque la configuración de Application Protocol.
- Desactive o elimine HTTP de la lista de protocolos de aplicación bloqueados.
- Asegúrese de que se mantienen otros controles de seguridad para las aplicaciones reales no fiables.

Paso 3: Aplicar y verificar cambios

Guarde las modificaciones de reglas y pruebe la conectividad:

1.- Aplicar los cambios de configuración a la política activa.

2.- Probar la conectividad a internet a destinos previamente bloqueados.

3.- Supervisar los registros de seguridad para garantizar que se permite el tráfico HTTP legítimo.

4.- Verificar que otras protecciones de seguridad sigan siendo efectivas.

Causa

La causa raíz fue una configuración de reglas de seguridad excesivamente restrictiva en Cisco Secure Access. La regla se configuró para bloquear todo el tráfico del protocolo de aplicación HTTP, lo que impedía la exploración Web y el acceso a las aplicaciones legítimos. La amplia aplicación del bloqueo del protocolo HTTP afectó a la conectividad normal de Internet para los usuarios que acceden a servicios web legítimos y aplicaciones que utilizan protocolos HTTP/HTTPS.

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).