

Configuración de descarga de archivo ZIP protegido por contraseña de acceso seguro

Contenido

Problema

Después de migrar a Cisco Secure Access, los usuarios no pueden descargar archivos ZIP protegidos mediante contraseña (cifrados). Las descargas fallan constantemente cuando se intenta acceder al contenido de archivos cifrados a través del servicio de acceso seguro. Este problema se produce a pesar de haber configurado las políticas de tráfico enlazado a Internet en un dispositivo C8200 con varias reglas de seguridad, entre las que se incluyen el bloqueo por categorías, los controles de inspección SSL y la funcionalidad de sandbox.

Los usuarios experimentan errores de descarga completos al intentar acceder a archivos ZIP protegidos mediante contraseña a los que se podía acceder anteriormente antes de la migración de Secure Access. El problema persiste en varios grupos de túnel y afecta a las 15 ubicaciones configuradas.

Entorno

- Cisco Secure Access (ID de organización de acceso seguro: 8320925)
- Dispositivo C8200 que gestiona las políticas de tráfico de Internet
- Varios grupos de túneles en 15 ubicaciones (TK-TG y otros)
- Políticas de inspección SSL con configuraciones activadas y desactivadas
- Perfiles de seguridad de sandbox habilitados en determinadas políticas
- Perfiles IPS configurados en reglas de acceso específicas

Resolución

La resolución para permitir descargas de archivos ZIP protegidos con contraseña en Cisco Secure Access implica configurar la opción Permitir el acceso a archivos cifrados e implementar soluciones alternativas apropiadas cuando sea necesario.

Método de configuración principal

Paso 1: Acceso a la configuración de Cisco Secure Access Policy

Desplácese hasta la política de acceso específica que gestiona el tráfico afectado en su panel de Cisco Secure Access.

Paso 2: Habilitar el acceso a archivos cifrados

En la directiva Configuración avanzada, busque y habilite la opción Permitir acceso a archivos cifrados. Esta opción se configura por regla y controla si se puede acceder al contenido cifrado a través de esa directiva específica.

Paso 3: Aplicación de la configuración

Guarde y aplique los cambios de directiva para activarlos para el tráfico de usuarios.

Método alternativo

Si el método principal no resuelve el problema, implemente la solución alternativa descrita en las siguientes secciones.

Paso 1: Identificar las URL afectadas

Determine las URL o dominios específicos donde se alojan los archivos ZIP protegidos por contraseña y que provocan errores de descarga.

Paso 2: Configurar lista de no descifrado

Agregue las URL identificadas a la lista No descifrar en su configuración de Cisco Secure Access. Esto evita la inspección SSL en estas URL específicas.

Paso 3: Crear directiva de omisión de inspección SSL

Asegúrese de que una política de acceso con la inspección SSL desactivada esté configurada para manejar el tráfico a estas URL.

Esta política debe tener:

- Inspección de SSL deshabilitada
- Todos los perfiles de seguridad desactivados
- Mayor prioridad que las políticas habilitadas para inspección SSL

Referencia de configuración de políticas

El orden de políticas descrito en las subsecciones siguientes y sus respectivas configuraciones se pueden utilizar como referencia para el manejo adecuado del tráfico.

Política 1: Regla de bloqueo basada en categorías

- Nombre de la política: IA-To-InternetContentBlock
- Perfil IPS: Ninguno

- Propósito: Bloquear categorías de contenido específicas
- Objetivo: Todos los grupos de túnel

Política 2: Regla de inspección de SSL desactivada

- Nombre de la política: IA-SSL-Inspection-MUKOU
- Perfil IPS: Inhabilitado
- Perfiles de seguridad: Todos los inhabilitados
- Objetivo: Todos los grupos de túnel

Política 3: Regla habilitada para inspección de SSL

- Nombre de la política: IA-SSL-Inspección
- Perfil IPS: Habilitado
- Perfiles de seguridad: Funcionalidad de sandbox habilitada
- Objetivo: Todos los grupos de túnel

Notas de configuración importantes

No existe una configuración global equivalente para la funcionalidad Permitir acceso a archivos cifrados. Este parámetro debe configurarse en políticas de acceso individuales según sea necesario. Cada directiva que requiera acceso a archivos cifrados debe tener esta opción habilitada explícitamente en su configuración de configuración avanzada.

Al probar los cambios de configuración, deje tiempo suficiente para que la política se propague por la infraestructura de Cisco Secure Access antes de validar la funcionalidad. Los incidentes de servicio o las ventanas de mantenimiento pueden afectar a los resultados de las pruebas y deben tenerse en cuenta al resolver problemas.

Causa

El problema se produce porque Cisco Secure Access, de forma predeterminada, bloquea el acceso a los archivos cifrados como medida de seguridad. Cuando la inspección SSL está habilitada y encuentra contenido cifrado o protegido mediante contraseña, el servicio impide la descarga a menos que se configure explícitamente para permitir dicho acceso. La opción Permitir el acceso a archivos cifrados de la Configuración avanzada de las directivas de acceso controla este comportamiento y, sin esta opción habilitada, los archivos ZIP cifrados y el contenido similar se bloquean durante el proceso de descarga.

Además, las políticas de inspección de SSL pueden interferir con las descargas de archivos cifrados cuando el proceso de inspección no puede gestionar correctamente el contenido cifrado, lo que requiere la configuración de acceso a archivos cifrados o la omisión de inspección de SSL para las URL afectadas.

Contenido relacionado

- [Controles de seguridad avanzados](#)
- [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).