Errores de autenticación de comprobación de estado de inspección de certificado de acceso seguro

Contenido

Problema

Cuando se intenta implementar Secure Access con el perfil de estado del terminal mediante la función de inspección de certificados, todos los intentos de inicio de sesión fallan a pesar de que no se pueden identificar las causas específicas del fallo en los registros del paquete DART. Los usuarios están intentando utilizar la autenticación SAML IDP y también desean aplicar la validación de certificados a través del mecanismo de comprobación de estado, pero esta configuración da como resultado fallos de autenticación coherentes incluso cuando las coincidencias de certificados backend son correctas.

Entorno

- Cisco Secure Access - Acceso remoto seguro del cliente (VPN, estado, recurso privado)
- Integración de autenticación IDP de SAML
- Perfil de estado del terminal con la función de inspección de certificados habilitada
- Certificados de usuario con el campo UPN en las direcciones de correo electrónico SAN coincidentes
- Configuración de arrendatarios de acceso seguro con usuarios, grupos y dispositivos de terminales

Resolución

Las comprobaciones del extremo del certificado en estado sólo se aplican cuando se utiliza la autenticación de varios certificados, que requiere la validación del certificado de usuario y del certificado de equipo. Dado que el escenario de implementación implica usuarios con solo certificados de usuario que necesitan utilizar un único perfil VPN, la solución implica la implementación de la autenticación de certificado único + SAML en lugar de confiar en la verificación de certificados de estado.

Pasos de configuración de autenticación

Paso 1: Configuración de SAML + Autenticación de certificado único

Configure el método de autenticación para utilizar la autenticación SAML combinada con la autenticación de certificado único en lugar de intentar forzar la validación de certificados mediante comprobaciones de estado.

Paso 2: Configurar coincidencia de UPN de certificado

Asegúrese de que el campo UPN del nombre alternativo de asunto (SAN) del certificado contenga la dirección de correo electrónico del usuario que coincida con la propiedad auth configurada para el usuario en Acceso seguro en Usuarios, grupos y dispositivos de terminales.

Paso 3: Establecer campo de autenticación principal

Configure el campo principal para que se autentique utilizando el UPN del certificado, asegurándose de que se corresponde con la dirección de correo electrónico del usuario en la base de datos de usuarios de Secure Access.

Requisitos de estructura de certificados

La estructura del certificado debe configurarse de modo que el UPN o el valor secundario del certificado coincida con la propiedad auth del usuario en Secure Access. Si un usuario presenta un certificado que tiene un UPN o un valor secundario que no coincide con la propiedad de autenticación configurada para ese usuario en Secure Access, se rechazará la autenticación.

Notas de configuración importantes

Se requeriría autenticación de varios certificados (IDP SAML + Multi-Cert Auth) si se necesita la aplicación de la comprobación de certificados de estado, pero esto requiere certificados de usuario y de equipo. Para las implementaciones en las que los usuarios solo tienen certificados de usuario y necesitan utilizar un único perfil VPN, la autenticación de certificado único + SAML proporciona la solución adecuada al tiempo que se mantienen los controles de seguridad basados en certificados.

Causa

Las comprobaciones del extremo del certificado en estado sólo se aplican cuando se configura la autenticación de varios certificados. Cuando se utiliza la autenticación SAML con la comprobación de certificados de estado, el sistema espera que los certificados de usuario y de equipo estén presentes para la validación. Dado que la implementación sólo utilizaba certificados de usuario con autenticación SAML, la función de inspección de certificados de estado no superaba sistemáticamente los intentos de autenticación a pesar de que la coincidencia de certificados backend era satisfactoria, ya que el mecanismo de estado no estaba diseñado para funcionar con escenarios de autenticación de certificados únicos.

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).