La validación del estado de Identity Services Engine (ISE) 3.3 falla tras la migración del firewall de ASA a FTD

Contenido

Problema

El problema notificado puede aparecer como el terminal que permanece en un estado de cumplimiento de estado "Desconocido". Además, el portal de aprovisionamiento de estado no se puede mostrar al usuario.

En algunos casos, los clientes han informado de que, tras migrar de ASA a FTD, reutilizaron la misma configuración; sin embargo, FTD requiere ajustes adicionales y específicos para que Posture VPN funcione correctamente.

Entorno

- Cisco Identity Services Engine (ISE) versión 3.3
- Implementación de ISE con dos nodos
- Cisco Secure Client versión 5.1.7.80
- Firepower Threat Defence (FTD) versión 7.4.1.1
- Terminales que se conectan mediante VPN
- Dirección IP pertinente para la validación del estado: 72.163.1.80 (enroll.cisco.com)

Resolución

Estos pasos detallan el flujo de trabajo para identificar, diagnosticar y resolver el problema de validación del estado de ISE después de la migración a FTD. Cada paso se explica para mayor claridad, con referencias directas a los registros e indicadores de configuración, tal y como se observa en el entorno.

Paso 1: Recopile un paquete DART para verificar las sondas

Compruebe el estado de los terminales que intentan la conectividad VPN en busca de errores o estados atascados. Revise los registros del agente de estado de ISE (ISEPosture.txt) para ver si hay mensajes de error que indiquen que los servidores del servidor no son válidos o que el estado no se puede recuperar.

Ejemplo de extracto de registro que indica el problema:

2026/01/05 15:38:26 [Advertencia] csc_iseagent Función: Target::parsePostureStatusResponseThread Id: 0x32D0 Archivo: Target.cpp Línea: 370 Nivel: warn Headend está vacío. Posiblemente, el contenido no tiene el formato 'X-ISE-PDP'.

2026/01/05 15:38:26 [Información] csc_iseagent Función: Target::Probe Thread Id: 0x32D0 Archivo: Target.cpp Línea: 212 Nivel: debug Estado del destino de redirección 192.168.1.254 es 5 <Servidor no válido.>.

2026/01/05 15:38:28 [Información] csc_iseagent Función: SwiftHttpRunner::http_discovery_callback Thread Id: 0x1AD8 Archivo: SwiftHttpRunner.cpp Línea: 519 Nivel: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [Información] csc_iseagent Función: SwiftHttpRunner::http_discovery_callback Thread Id: 0x1AD8 Archivo: SwiftHttpRunner.cpp Línea: 580 Nivel: info Activación del siguiente temporizador de ronda.

2026/01/05 15:38:28 [Información] csc_iseagent Función: GetCurrentUserName Thread Id: 0x1AD8 Archivo: ImpersonateUser.cpp Línea: 60 Nivel: info Nombre de usuario del usuario actualmente conectado es basheer.mohamed.

2026/01/05 15:38:29 [Información] csc_iseagent Función: hs_transport_winhttp_get Thread Id: 0x698C Archivo: hs_transport_winhttp.c Línea: 4912 Nivel: debug La solicitud ha agotado el tiempo de espera.

2026/01/05 15:38:29 [Información] csc_iseagent Función: Target::probeDiscoveryUrl Thread Id: 0x698C Archivo: Target.cpp Línea: 269 Nivel: debug GET request to URL (http://enroll.cisco.com/auth/discovery?architecture=9), devolvió el estado -1 <Operation Failed.>.

2026/01/05 15:38:29 [Información] csc_iseagent Función: Target::Probe Thread Id: 0x698C Archivo: Target.cpp Línea: 212 Nivel: debug Status of Redirection target enroll.cisco.com is 6 <No disponible.>.

En este caso, enroll.cisco.com no es accesible, lo que hace que el proceso de detección falle.

Paso 2: Confirmar el perfil de autorización de ISE y los registros en directo

Compruebe que el registro de vida de RADIUS se envía correctamente al extremo. Debe incluir los parámetros de aceptación de acceso y redirección URL para la validación de estado.

Ejemplo:

Tipo de acceso = ACCESS_ACCEPT

cisco-av-pair = url-redirect-acl=redirect

cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp

Para este ejemplo específico, hemos confirmado que la redirección funciona según lo esperado; sin embargo, el proceso de detección falla porque se informa que el gateway es un servidor no válido. Este comportamiento se puede esperar en un escenario de integración VPN, ya que el extremo no depende del gateway VPN para la detección. En su
lugar, the endpoint attempts to reach the ISE node using enroll.cisco.com.

Paso 3. Verifique la configuración de ACL en el FTD

Verifique que enroll.cisco.com esté explícitamente permitido en la ACL de redirección, así como en la ACL configurada para el túnel dividido.

Para comprobar ambas ACL, en el FMC puede navegar hastaObjeto > Administración de objetos > Lista de acceso > Extendida.

Para verificar si el túnel dividido está configurado en la VPN, navegue hasta Dispositivos > VPN > Acceso remoto > Elija la configuración de VPN y perfil de conexión > Editar política de grupo > Túnel dividido.

Nota: Si el túnel dividido no está configurado en la política VPN, esta validación no es necesaria, por lo tanto, la ACL del túnel dividido no es necesaria en este escenario.

Causa

La causa principal del problema fue la ausencia de la dirección IP de detección necesaria (72.163.1.80, enroll.cisco.com) en la política de red tras la migración a Firepower Threat Defence (FTD).

Sin esta IP, Cisco Secure Client no pudo detectar el nodo de ISE Policy Service al conectarse a través de VPN, lo que dio como resultado que el estado de estado permaneciera en un estado pendiente. Además, los servicios de ubicación deshabilitados en los terminales contribuyeron a una validación de estado incompleta.

Contenido relacionado

- Soporte 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).