A validação de postura do Identity Services Engine (ISE) 3.3 falha após a migração do firewall do ASA para o FTD

Contents

Problema

O problema relatado pode ser apresentado como o ponto de extremidade que permanece em um status de conformidade de postura "Desconhecido". Além disso, o Portal de Provisionamento de Postura não pode ser exibido para o usuário.

Em alguns cenários, os clientes relataram que, após a migração do ASA para o FTD, reutilizaram a mesma configuração; no entanto, o FTD requer configurações adicionais e específicas para que a VPN de postura funcione corretamente.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.3
- Implantação do ISE com dois nós
- Cisco Secure Client versão 5.1.7.80
- Firepower Threat Defense (FTD) versão 7.4.1.1
- Endpoints conectados via VPN
- Endereço IP relevante para validação da postura: 72.163.1.80 (enroll.cisco.com)

Resolução

Estas etapas detalham o workflow para identificar, diagnosticar e resolver o problema de validação da postura do ISE após a migração para o FTD. Cada etapa é explicada para fins de clareza, com referências diretas a logs e indicadores de configuração conforme observado no ambiente.

Etapa 1: Colete um pacote DART para verificar os testes

Verifique o status de postura dos pontos de extremidade que estão tentando conectividade VPN em busca de erros ou estados de travamento. Verifique os logs do agente de postura do ISE (ISEPosture.txt) em busca de mensagens de erro que indicam servidores de servidor inválidos ou status não acessível.

Exemplo de trecho de registro indicando o problema:

2026/01/05 15:38:26 [Aviso] csc_iseagent Função: Target::parsePostureStatusResponse Thread Id: 0x32D0 Arquivo: Target.cpp Linha: 370 Nível: warn Headend está vazio. Possivelmente, o conteúdo não está no formato 'X-ISE-PDP'.

2026/01/05 15:38:26 [Information] csc_iseagent Função: Target::Probe Thread Id: 0x32D0 Arquivo: Target.cpp Linha: 212 Nível: Status de depuração Redirection target 192.168.1.254 is 5 <Servidor inválido.>.

2026/01/05 15:38:28 [Informações] csc_iseagent Função: SwiftHttpRunner::http_discovery_callback Id do Thread: 0x1AD8 Arquivo: SwiftHttpRunner.cpp Linha: 519 Nível: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [Informações] csc_iseagent Função: SwiftHttpRunner::http_discovery_callback Id do Thread: 0x1AD8 Arquivo: SwiftHttpRunner.cpp Linha: 580 Nível: info Habilitando o próximo temporizador round.

2026/01/05 15:38:28 [Informações] csc_iseagent Função: GetCurrentUserName Id do Thread: 0x1AD8 Arquivo: ImpersonateUser.cpp Linha: 60 Nível: info O nome de usuário do usuário atualmente conectado é basheer.mohamed.

2026/01/05 15:38:29 [Informações] csc_iseagent Função: hs_transport_winhttp_get Id do Thread: 0x698C Arquivo: hs_transport_winhttp.c Linha: 4912 Nível: debug A solicitação expirou.

2026/01/05 15:38:29 [Information] csc_iseagent Função: Target::probeDiscoveryUrl Thread Id: 0x698C Arquivo: Target.cpp Linha: 269 Nível: depurar solicitação GET para URL (http://enroll.cisco.com/auth/discovery?architecture=9), status retornado -1 <Operation Failed.>.

2026/01/05 15:38:29 [Information] csc_iseagent Função: Target::Probe Thread Id: 0x698C Arquivo: Target.cpp Linha: 212 Nível: debug Status of Redirection target enroll.cisco.com is 6 <Not Reachable.>.

Nesse caso, enroll.cisco.com não está acessível, o que faz com que o processo de descoberta falhe.

Etapa 2: Confirmar o perfil de autorização do ISE e os registros em tempo real

Verifique se o log de vida RADIUS foi enviado corretamente para o ponto de extremidade. Ele deve incluir os parâmetros Access Accept e URL redirect para validação de postura.

Exemplo:

Tipo de acesso = 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 exemplo específico, confirmamos que o redirecionamento está funcionando conforme esperado; no entanto, o processo de descoberta falha porque o gateway é relatado como um servidor inválido. Esse comportamento pode ser esperado em um cenário de integração de VPN, pois o ponto de extremidade não depende do gateway de VPN para descoberta. Em vez disso, the endpoint attempts to reach the ISE node using enroll.cisco.com.

Etapa 3. Verificar as configurações das ACLs no FTD

Verifique se enroll.cisco.com é permitido explicitamente na ACL de redirecionamento, bem como na ACL configurada para o túnel dividido.

Para verificar as duas ACLs, no FMC você pode navegar paraObjeto > Gerenciamento de objeto > Lista de acesso > Estendida.

Para verificar se o túnel dividido está configurado na VPN, navegue para Devices > VPN > Remote Access > Choose the VPN and Connection Profile settings > Edit Group Policy > Split Tunnel.

Observação: se o Túnel dividido não estiver configurado na política de VPN, essa validação não será necessária, portanto, a ACL do Túnel dividido não é necessária nesse cenário.

Causa

A causa principal do problema foi a ausência do endereço IP de descoberta necessário (72.163.1.80, enroll.cisco.com) na política de rede após a migração para o Firepower Threat Defense (FTD).

Sem esse IP, o Cisco Secure Client não conseguiu descobrir o Nó de Serviço de Política do ISE ao se conectar via VPN, resultando no status de postura restante em um estado pendente. Além disso, os serviços de localização desabilitados nos pontos de extremidade contribuíram para a validação de postura incompleta.

Conteúdo relacionado

- Suporte da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.