Identity Services Engine (ISE) 3.3 Houding validatie mislukt na Firewall migratie van ASA naar FTD

Inhoud

uitgeven

Het gemelde probleem kan zich voordoen als het eindpunt dat in een "Onbekende" houding blijft. Bovendien kan het Posture Provisioning Portal niet worden weergegeven aan de gebruiker.

In sommige scenario's hebben klanten gemeld dat ze na de migratie van ASA naar FTD dezelfde configuratie hebben hergebruikt; FTD vereist echter extra en specifieke instellingen voor Posture VPN om correct te functioneren.

milieu

- Cisco Identity Services Engine (ISE) versie 3.3
- ISE-implementatie met twee knooppunten
- Cisco Secure Client versie 5.1.7.80
- Firepower Threat Defense (FTD) versie 7.4.1.1
- Eindpunten die verbinding maken via VPN
- Relevante IP-adres voor posture validatie: 72.163.1.80 (enroll.cisco.com)

resolutie

Deze stappen beschrijven de workflow voor het identificeren, diagnosticeren en oplossen van het ISE-posture validatieprobleem na migratie naar FTD. Elke stap wordt uitgelegd voor duidelijkheid, met directe verwijzingen naar logs en configuratie-indicatoren zoals waargenomen in de omgeving.

Stap 1: Verzamel een DART-bundel om sondes te verifiëren

Controleer de status van de positie van eindpunten die proberen een VPN-verbinding te maken op fouten of vastgelopen toestanden. Controleer de logs van de ISE Posture Agent (ISEPosture.txt) op foutmeldingen die aangeven dat de server ongeldig is of niet kan worden hersteld.

Voorbeeld van een uittreksel uit het logboek dat het probleem aangeeft:

2026/01/05 15:38:26 [Waarschuwing] csc_iseagent Functie: Doel::parsePostureStatusResponse Thread ID: 0x32D0 Bestand: Target.cpp Lijn: 370 Niveau: waarschuwing Headend is

leeg. Mogelijk is de inhoud niet in de vorm 'X-ISE-PDP'.

2026/01/05 15:38:26 [Informatie] csc_iseagent Functie: Doel::Probe Thread Id: 0x32D0 Bestand: Target.cpp Lijn: 212 Niveau: debug Status van omleiding doel 192.168.1.254 is 5 <Ongeldige server.>.

2026/01/05 15:38:28 [Informatie] csc_iseagent Functie: SwiftHttpRunner::http_discovery_callback Thread Id: 0x1AD8 Bestand: SwiftHttpRunner.cpp Lijn: 519 Niveau: info Time-out voor omleidingsdoel enroll.cisco.com.

2026/01/05 15:38:28 [Informatie] csc_iseagent Functie: SwiftHttpRunner::http_discovery_callback Thread Id: 0x1AD8 Bestand: SwiftHttpRunner.cpp Lijn: 580 Niveau: info Volgende ronde timer inschakelen.

2026/01/05 15:38:28 [Informatie] csc_iseagent Functie: GetCurrentUserName Thread Id: 0x1AD8 Bestand: ImpersonateUser.cpp Lijn: 60 Niveau: info Gebruikersnaam van de momenteel ingelogde gebruiker is basheer.mohamed.

2026/01/05 15:38:29 [Informatie] csc_iseagent Functie: hs_transport_winhttp_get Thread Id: 0x698C Bestand: hs_transport_winhttp.c Lijn: 4912 Niveau: foutopsporing De aanvraag is verlopen.

2026/01/05 15:38:29 [Informatie] csc_iseagent Functie: Doel::probeDiscoveryUrl Thread Id: 0x698C Bestand: Target.cpp Lijn: 269 Niveau: debug GET-verzoek naar URL (http://enroll.cisco.com/auth/discovery?architecture=9), geretourneerde status -1 <Bewerking mislukt.>.

2026/01/05 15:38:29 [Informatie] csc_iseagent Functie: Doel::Probe Thread Id: 0x698C Bestand: Target.cpp Lijn: 212 Niveau: debug Status van Redirection doel enroll.cisco.com is 6 <Niet Bereikbaar.>.

In dit geval is enroll.cisco.com niet bereikbaar, waardoor het detectieproces mislukt.

Stap 2: Bevestig het ISE-autorisatieprofiel en de livelogs

Controleer of het RADIUS-livelog correct naar het eindpunt is geduwd. Het moet toegangs- en URL-omleidingsparameters bevatten voor positievalidatie.

Voorbeeld:

Toegangstype = ACCESS_ACCEPT

Cisco-AV-Paar = URL-Redirect-ACL=Redirect

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

Voor dit specifieke voorbeeld hebben we bevestigd dat de omleiding werkt zoals verwacht; het

detectieproces mislukt echter omdat de gateway wordt gerapporteerd als een ongeldige server. Dit gedrag kan worden verwacht in een VPN-integratiescenario, omdat het eindpunt niet afhankelijk is van de VPN-gateway voor detectie. In plaats daarvan probeert het eindpunt de ISE-node te bereiken met behulp van enroll.cisco.com.

Stap 3. Controleer de instellingen van de ACL's in de FTD

Controleer of enroll.cisco.com expliciet is toegestaan in de omleiding ACL en in de ACL geconfigureerd voor de Split Tunnel.

Als u beide ACL's wilt controleren, kunt u in de FMC navigeren naar Object > Objectbeheer > Toegangslijst > Uitgebreid.

Om te controleren of Split Tunnel is geconfigureerd in de VPN, navigeert u naar Apparaten > VPN > Externe toegang > Kies de instellingen voor VPN en verbindingsprofiel > Groepsbeleid bewerken > Splittunnel.

Opmerking: Als Split Tunnel niet is geconfigureerd in het VPN-beleid, is deze validatie niet vereist, dus is de Split Tunnel ACL niet nodig in dit scenario.

Oorzaak

De hoofdoorzaak van het probleem was het ontbreken van het vereiste IP-adres voor detectie (72.163.1.80, enroll.cisco.com) in het netwerkbeleid na migratie naar Firepower Threat Defense (FTD).

Zonder dit IP-adres kon Cisco Secure Client de ISE Policy Service Node niet detecteren bij het maken van een verbinding via VPN, waardoor de status van de houding in de wachtstand bleef. Bovendien droegen de locatiediensten op eindpunten bij tot de onvolledige validatie van de houding.

Verwante inhoud

- Cisco-ondersteuning

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.