

Échec de la validation de la position ISE (Identity Services Engine) 3.3 après la migration du pare-feu de ASA vers FTD

Table des matières

Problème

Le problème signalé peut se présenter comme le point de terminaison restant dans un état de conformité de position « Inconnu ». En outre, le Portail d'approvisionnement de position ne peut pas être affiché pour l'utilisateur.

Dans certains scénarios, les clients ont signalé qu'après avoir migré d'ASA vers FTD, ils ont réutilisé la même configuration ; cependant, FTD nécessite des paramètres supplémentaires et spécifiques pour que Posture VPN fonctionne correctement.

Environnement

- Cisco Identity Services Engine (ISE) version 3.3
- Déploiement ISE avec deux noeuds
- Client sécurisé Cisco version 5.1.7.80
- Firepower Threat Defense (FTD) version 7.4.1.1
- Terminaux se connectant via VPN
- Adresse IP appropriée pour la validation de position : 72.163.1.80 (enroll.cisco.com)

Résolution

Ces étapes détaillent le workflow permettant d'identifier, de diagnostiquer et de résoudre le problème de validation de la position ISE après la migration vers FTD. Chaque étape est expliquée pour plus de clarté, avec des références directes aux journaux et aux indicateurs de configuration observés dans l'environnement.

Étape 1 : collectez un ensemble DART pour vérifier les sondes

Vérifiez l'état de posture des points d'extrémité qui tentent une connectivité VPN pour détecter les erreurs ou les états bloqués. Consultez les journaux d'agent de posture ISE (ISEPosture.txt) pour les messages d'erreur indiquant des serveurs non valides ou un état d'impossibilité d'accès.

Exemple d'extrait de journal indiquant le problème :

```
2026/01/05 15:38:26 [Avertissement] csc_iseagent Fonction :
```

Target::parsePostureStatusResponse ID de thread : 0x32D0 Fichier : Target.cpp Ligne : 370
Niveau : warn Headend est vide. Le contenu n'est peut-être pas au format 'X-ISE-PDP'.

2026/01/05 15:38:26 [Information] csc_iseagent Fonction: Target::Probe Thread Id: 0x32D0
Fichier: Target.cpp Ligne: 212 Niveau: debug Status of Redirection target 192.168.1.254 is 5
<Invalid server.>.

2026/01/05 15:38:28 [Information] csc_iseagent Fonction :
SwiftHttpRunner::http_discovery_callback Id De Thread: 0x1AD8 Fichier : SwiftHttpRunner.cpp
Ligne: 519 Niveau: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [Information] csc_iseagent Fonction :
SwiftHttpRunner::http_discovery_callback ID de thread : 0x1AD8 Fichier : SwiftHttpRunner.cpp
Ligne : 580 Niveau : info Activation du minuteur du tour suivant.

2026/01/05 15:38:28 [Information] csc_iseagent Fonction : GetCurrentUserUsername ID de thread :
0x1AD8 Fichier : ImpersonateUser.cpp Ligne : 60 Niveau : info Le nom d'utilisateur de l'utilisateur
actuellement connecté est basheer.mohamed.

2026/01/05 15:38:29 [Information] csc_iseagent Fonction : hs_transport_winhttp_get ID de thread :
0x698C Fichier : hs_transport_winhttp.c Ligne : 4912 Niveau : debug La requête a expiré.

2026/01/05 15:38:29 [Information] csc_iseagent Function: Target::probeDiscoveryUrl Thread Id:
0x698C File: Target.cpp Line: 269 Level: debug GET request to URL
(http://enroll.cisco.com/auth/discovery?architecture=9), return status -1 <Operation Failed.>

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

Dans ce cas, enroll.cisco.com n'est pas accessible, ce qui entraîne l'échec du processus de
découverte.

Étape 2 : Confirmez le profil d'autorisation ISE et les journaux actifs

Vérifiez que le journal en direct RADIUS est correctement envoyé au point de terminaison. Il doit
inclure les paramètres d'acceptation d'accès et de redirection d'URL pour la validation de la
position.

Exemple :

Type d'accès = 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

Pour cet exemple spécifique, nous avons confirmé que la redirection fonctionne comme prévu. Cependant, le processus de détection échoue car la passerelle est signalée comme un serveur non valide. Ce comportement peut être attendu dans un scénario d'intégration VPN, car le point d'extrémité ne dépend pas de la passerelle VPN pour la détection. À la place, the endpoint attempts to reach the ISE node using enroll.cisco.com.

Étape 3. Vérification des paramètres des listes de contrôle d'accès dans le FTD

Vérifiez que enroll.cisco.com est explicitement autorisé dans la liste de contrôle d'accès de redirection ainsi que dans la liste de contrôle d'accès configurée pour le tunnel partagé.

Pour vérifier les deux listes de contrôle d'accès, dans le FMC, vous pouvez accéder à Object > Object Management > Access List > Extended.

Pour vérifier si le tunnel partagé est configuré dans le VPN, accédez à Devices > VPN > Remote Access > Choose the VPN and Connection Profile settings > Edit Group Policy > Split Tunnel.

Remarque : si le split tunnel n'est pas configuré sur la stratégie VPN, cette validation n'est pas requise, par conséquent la liste de contrôle d'accès du split tunnel n'est pas nécessaire dans ce scénario.

Motif

La cause principale du problème était l'absence de l'adresse IP de détection requise (72.163.1.80, enroll.cisco.com) dans la stratégie réseau après la migration vers Firepower Threat Defense (FTD).

Sans cette adresse IP, Cisco Secure Client n'a pas pu détecter le noeud de service de stratégie ISE lors de la connexion sur VPN, ce qui a pour conséquence que l'état de la position reste en attente. En outre, les services de localisation désactivés sur les terminaux ont contribué à une validation incomplète de la position.

Autres informations utiles

- [Assistance Cisco](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.