

La convalida della postura di Identity Services Engine (ISE) 3.3 non riesce dopo la migrazione del firewall da ASA a FTD

Sommario

Problema

Il problema segnalato può essere presente come endpoint con stato di conformità della postura "Sconosciuto". Inoltre, non è possibile visualizzare il portale di provisioning della postura per l'utente.

In alcuni scenari, i clienti hanno segnalato che dopo la migrazione da ASA a FTD, hanno riutilizzato la stessa configurazione; tuttavia, FTD richiede impostazioni aggiuntive e specifiche per il corretto funzionamento della VPN per postura.

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.3
- Implementazione ISE con due nodi
- Cisco Secure Client versione 5.1.7.80
- Firepower Threat Defense (FTD) versione 7.4.1.1
- Endpoint che si connettono tramite VPN
- Indirizzo IP pertinente per la convalida della postura: 72.163.1.80 (enroll.cisco.com)

Risoluzione

Questi passaggi descrivono in dettaglio il flusso di lavoro per l'identificazione, la diagnosi e la risoluzione del problema di convalida della postura ISE dopo la migrazione a FTD. Ogni passaggio viene spiegato per chiarezza, con riferimenti diretti ai registri e agli indicatori di configurazione osservati nell'ambiente.

Passaggio 1: raccogliere un pacchetto DART per verificare le sonde

Verificare lo stato di postura degli endpoint che tentano la connettività VPN per individuare eventuali errori o stati bloccati. Esaminare i log degli agenti di postura ISE (ISEPosture.txt) per individuare i messaggi di errore che indicano server non validi o lo stato non raggiungibile.

Esempio di estratto di registro che indica il problema:

```
2026/01/05 15:38:26 [Warning] csc_iseagent Funzione: Target::parsePostureStatusResponse
```

Thread Id: 0x32D0 File: Target.cpp Riga: 370 Livello: l'headend di avviso è vuoto. Il contenuto potrebbe non essere nel formato 'X-ISE-PDP'.

2026/01/05 15:38:26 [Informazioni] csc_iseagent Funzione: Target::Probe Thread Id: 0x32D0 File: Target.cpp Riga: 212 Livello: debug Status of Redirection target 192.168.1.254 is 5 <Server non valido.>.

2026/01/05 15:38:28 [Informazioni] csc_iseagent Funzione: SwiftHttpRunner::http_discovery_callback ID thread: 0x1AD8 File: SwiftHttpRunner.cpp Riga: 519 Livello: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [Informazioni] csc_iseagent Funzione: SwiftHttpRunner::http_discovery_callback ID thread: 0x1AD8 File: SwiftHttpRunner.cpp Linea: 580 Livello: info Abilitazione del timer di ciclo successivo.

2026/01/05 15:38:28 [Informazioni] csc_iseagent Funzione: GetCurrentUserName ID thread: 0x1AD8 File: ImpersonateUser.cpp Riga: 60 Livello: info Il nome utente dell'utente attualmente connesso è basheer.mohamed.

2026/01/05 15:38:29 [Informazioni] csc_iseagent Funzione: hs_transport_winhttp_get Thread Id: 0x698C File: hs_transport_winhttp.c Riga: 4912 Livello: debug Timeout della richiesta.

2026/01/05 15:38:29 [Informazioni] csc_iseagent Funzione: Target::probeDiscoveryUrl ID thread: 0x698C File: Target.cpp Riga: 269 Livello: debug GET richiesta all'URL (http://enroll.cisco.com/auth/discovery?architecture=9), restituito stato -1 <Operazione non riuscita.>.

2026/01/05 15:38:29 [Informazioni] csc_iseagent Funzione: Target::Probe Thread Id: 0x698C File: Target.cpp Riga: 212 Livello: debug Status of Redirection target enroll.cisco.com is 6 <Non raggiungibile.>.

In questo caso, enroll.cisco.com non è raggiungibile e il processo di rilevamento ha esito negativo.

Fase 2: Conferma del profilo di autorizzazione ISE e dei Live Log

Verificare che il livelog RADIUS sia stato inserito correttamente nell'endpoint. Deve includere i parametri Access Accept e URL redirect per la convalida della postura.

Esempio:

Tipo di accesso = 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

Per questo esempio specifico, è stato confermato che il reindirizzamento funziona come previsto. Tuttavia, il processo di individuazione ha esito negativo perché il gateway è segnalato come server non valido. Questo comportamento può essere previsto in uno scenario di integrazione VPN, in quanto l'endpoint non si basa sul gateway VPN per l'individuazione. Al contrario, the endpoint attempts to reach the ISE node using enroll.cisco.com.

Passaggio 3. Verificare le impostazioni degli ACL nell'FTD

Verificare che enroll.cisco.com sia autorizzato esplicitamente nell'ACL di reindirizzamento e nell'ACL configurato per il tunnel suddiviso.

Per controllare entrambi gli ACL, nel FMC è possibile selezionare Oggetto > Gestione oggetti > Elenco accessi > Esteso.

Per verificare se è configurato il tunnel diviso nella VPN, selezionare Dispositivi > VPN > Accesso remoto > Scegliere le impostazioni VPN e del profilo di connessione > Modifica Criteri di gruppo > Tunnel diviso.

Nota: se il criterio VPN non prevede la configurazione del tunnel suddiviso, questa convalida non è necessaria, pertanto in questo scenario non è necessario l'ACL del tunnel suddiviso.

Causa

La causa principale del problema è stata l'assenza dell'indirizzo IP di individuazione richiesto (72.163.1.80, enroll.cisco.com) nei criteri di rete dopo la migrazione a Firepower Threat Defense (FTD).

Senza questo IP, Cisco Secure Client non è stato in grado di individuare il nodo del servizio criteri ISE durante la connessione tramite VPN. Di conseguenza, lo stato della postura rimane in sospeso. Inoltre, la disabilitazione dei servizi di posizione sugli endpoint ha contribuito a una convalida della postura incompleta.

Contenuto correlato

- [Supporto Cisco](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).