Comportamento errore distribuzione georilevazione con rilevamento minacce abilitato su FTD firewall protetto

Sommario

Problema

Durante il tentativo di configurare il filtro del traffico basato sulla posizione geografica su un Cisco Secure Firewall FTD 3105, sono stati riscontrati diversi problemi:

- I criteri di controllo dell'accesso basati su area geografica e le regole di prefiltro non bloccano i tentativi di connessione VPN ad accesso remoto HTTPS (RA-VPN) che bloccano le aree all'interfaccia esterna FTD.
- Dopo l'aggiornamento alla versione 7.7.11, la configurazione dell'accesso al servizio basato su Geo-VPN RSA non è riuscita a essere distribuita quando i paesi dei Paesi Bassi o delle Antille Olandesi sono stati inclusi nel criterio.
- Distribuzione FMC non riuscita all'83% con questo messaggio di errore:

```
FMC >> object-group geolocation FMC_GEOLOCATION_184683596782_116848397
FMC >> location "Netherlands"
device >> [error] :
location "Netherlands"
^
ERROR: % Invalid input detected at '^' marker.
Config Error -- location "Netherlands"
```

Ambiente

- Cisco Secure Firewall Firepower Threat Defense (FTD) 3105 gestito da FMC
- Versione software aggiornata: 7.7.11-1061

- Configurazione RSA-VPN che richiede restrizioni di accesso basate su paese

Risoluzione

La risoluzione ha richiesto più passaggi per convalidare correttamente un controllo degli accessi basato sulla posizione geografica. Inoltre, è stata individuata una limitazione con il rilevamento delle minacce abilitato, che ha portato a nuove linee guida relative al comportamento di corrispondenza del traffico.

1: Aggiornare FMC e FTD alla versione 7.7.11-1061 per abilitare la funzionalità di accesso al servizio basato su rete geografica RA-VPN, poiché questa funzionalità è supportata solo dalla versione 7.7.0 e successive.

2: Configurare l'accesso al servizio basato su rete geografica RA-VPN in base alla documentazione Cisco e associarlo ai criteri RA-VPN.

3: Per risolvere il problema di implementazione causato dall'ID bug Cisco CSCwq15499 quando si aggiungono paesi specifici come le Antille olandesi o olandesi, applicare la seguente soluzione:

1. Creare un oggetto di accesso al servizio RA-VPN vuoto senza paesi configurati.
2. Applicare l'oggetto di accesso al servizio vuoto al criterio RA-VPN e distribuire correttamente.
3. Modificare lo stesso oggetto di accesso al servizio e aggiungere le regole del paese richieste.
4. Distribuire di nuovo la configurazione. La distribuzione ora ha esito positivo ed è attivo il filtro della posizione geografica.

4: Verificare che la distribuzione venga completata correttamente e che l'accesso e i registri RSA-VPN riflettano le restrizioni previste per il paese. Monitorare il sistema per verificare il corretto funzionamento delle limitazioni di geolocalizzazione.

5: Determinare se una funzione di rilevamento minacce è già abilitata sull'FTD e corrisponde al traffico prima che possa raggiungere i criteri di accesso. Queste configurazioni determinano l'omissione delle regole di geolocalizzazione man mano che il rilevamento delle minacce subentra prima dell'applicazione delle policy.

<#root>

```
device# show run threat-detection
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept

threat-detection service invalid-vpn-access
threat-detection service remote-access-authentication hold-down 1440 threshold 5
threat-detection service remote-access-client-initiations hold-down 1440 threshold 5
```

6: Correlare tutti gli ID di syslog relativi alle corrispondenze e agli shun di rilevamento delle minacce per confermare che il traffico sta violando il rilevamento delle minacce anziché la geolocalizzazione.

- %FTD-4-401002 Shun aggiunge: Indirizzo_IP Indirizzo_IP porta
- %FTD-4-401003 Shun eliminato: Indirizzo_IP
- %FTD-4-401004 Pacchetto ignorato: Indirizzo_IP ==> Indirizzo_IP sull'interfaccia nome_interfaccia
- %FTD-4-73102: Il rilevamento delle minacce aggiunge l'host all'elenco di esclusione
- %FTD-4-73103: Il rilevamento delle minacce rimuove l'host dall'elenco di esclusione
- %FTD-4-73201: Rilevamento delle minacce: Service[remote-access-client-initiations] Peer[peer-ip]: soglia di errore del valore superato: aggiunta di shun all'interfaccia. SSL: Numero eccessivo di richieste di avvio client da parte dell'Autorità registrazione.
- %FTD-4-73201: Rilevamento delle minacce: Service[remote-access-client-initiations] Peer[peer-ip]: soglia di errore superata: aggiunta di shun all'interfaccia. IKEv2:RA_exceeded_client_initiation_Requests

```
<164>Feb 26 2026 23:05:45: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:07:36: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:12:25: %FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] P
<164>Feb 26 2026 23:00:00: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
<164>Feb 26 2026 23:00:01: %FTD-4-401004: Shunned packet: SRCIPADDRESS ==> DSTIPADDRESS on interface Ou
---
device# show shun
```

Causa

I problemi riscontrati hanno due cause principali distinte:

- Limitazione di corrispondenza regola di georilevazione: Il controllo degli accessi basato su Geo RSA-VPN è supportato solo a partire dalla versione software 7.7.0 e successive. Inoltre, il rilevamento delle minacce RAVPN configurate può influire sul traffico, impedendo la corrispondenza con le regole basate su area geografica.
- ID bug Cisco CSCwq1549: Nella versione 7.7.11, gli errori di distribuzione si verificano quando si aggiungono determinati paesi ai criteri di accesso ai servizi basati su Geo RSA-VPN a causa di un bug software noto nel meccanismo di gestione dell'accesso al servizio Geo RSA-VPN.

Contenuto correlato

- Supporto tecnico Cisco e download

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).