# Configurazione di criteri basati sulla georilevazione per la VPN ad accesso remoto su Secure Firewall Threat Defense

## Sommario



## Introduzione

In questo documento viene descritto il processo per autorizzare o negare le connessioni VPN in base a geolocalizzazioni specifiche in Secure Firewall Threat Defense (FTD).

## Prerequisiti

### Requisiti e limitazioni

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Centro gestione firewall protetto (FMC)
- RAVPN (Remote Access VPN)
- Configurazione geolocalizzazione di base

I requisiti e i limiti attuali per le politiche basate sulla geolocalizzazione sono i seguenti:

- Supportato solo su FTD versione 7.7.0+, gestito da FMC versione 7.7.0+.
- Non supportato su FTD gestito da Secure Firewall Device Manager (FDM).

- Non supportato in modalità cluster
- Gli indirizzi IP non classificati basati sulla georilevazione non sono classificati in base all'origine geografica. Per questi casi, il CCP applica l'azione predefinita del criterio di accesso ai servizi.
- I criteri di accesso ai servizi basati sulla georilevazione non si applicano alle pagine WebLaunch, consentendo di scaricare Secure Client senza restrizioni.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Secure Firewall versione 7.7.0
- Secure Firewall Management Center versione 7.7.0

Per informazioni dettagliate su questa funzionalità, vedere la sezione Gestione dell'accesso VPN di utenti remoti in base alla geolocalizzazione nella guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center 7.7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

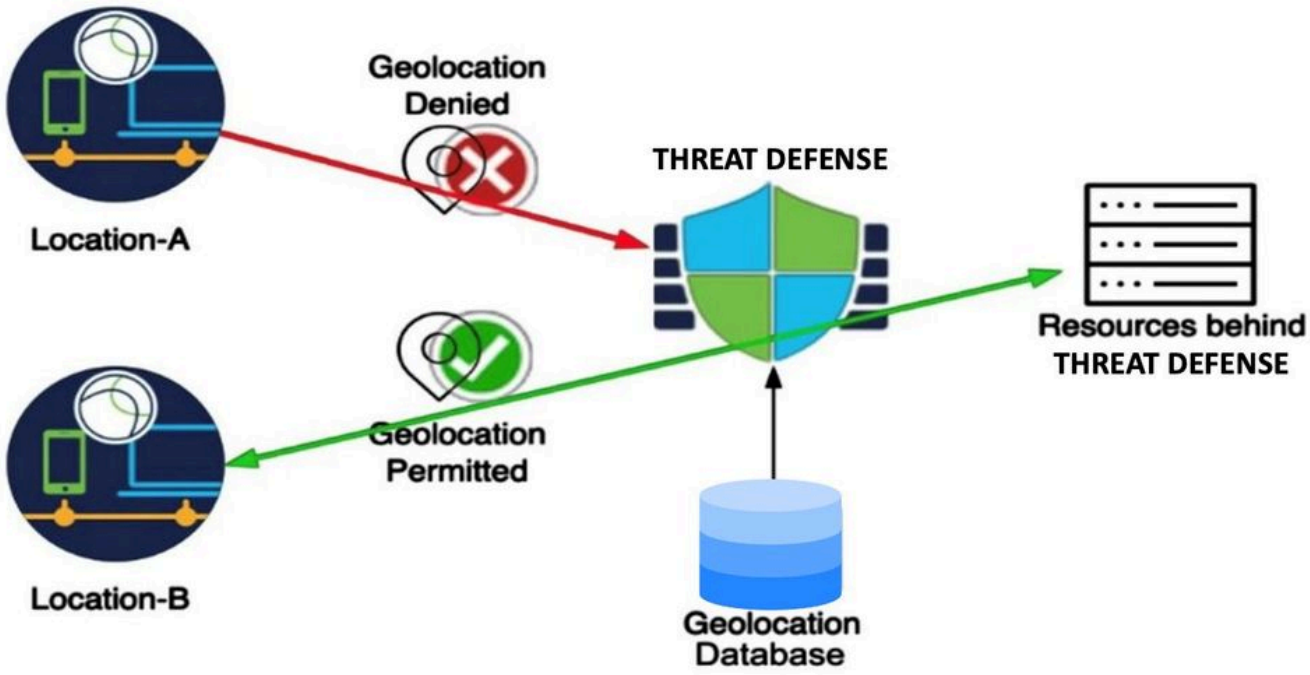
Le policy di accesso basate sulla geolocalizzazione offrono oggi un valore significativo nella sicurezza della rete, consentendo di bloccare il traffico in base alla sua origine geografica. In genere, le organizzazioni possono definire policy di accesso al traffico per il traffico di rete generale che attraversa il firewall. Ora, con l'introduzione di questa funzione, è possibile applicare il controllo dell'accesso basato sulla georilevazione per le richieste di sessioni VPN ad accesso remoto.

Questa funzione offre i seguenti vantaggi:

- Regole basate sulla georilevazione: I clienti possono creare regole per autorizzare o negare le richieste RAVPN in base a geolocalizzazioni specifiche, ad esempio paesi o continenti. Ciò consente un controllo preciso su quali posizioni geografiche possono avviare sessioni VPN.
- Blocco preautenticazione: Le sessioni identificate da queste regole per un'azione di negazione vengono bloccate prima dell'autenticazione e questi tentativi vengono registrati correttamente per motivi di sicurezza. Questa azione preventiva consente di ridurre i tentativi di accesso non autorizzato.
- Conformità e sicurezza: Questa funzione aiuta a garantire l'aderenza alle politiche organizzative e di governance locali, riducendo al contempo la superficie di attacco del

server VPN.

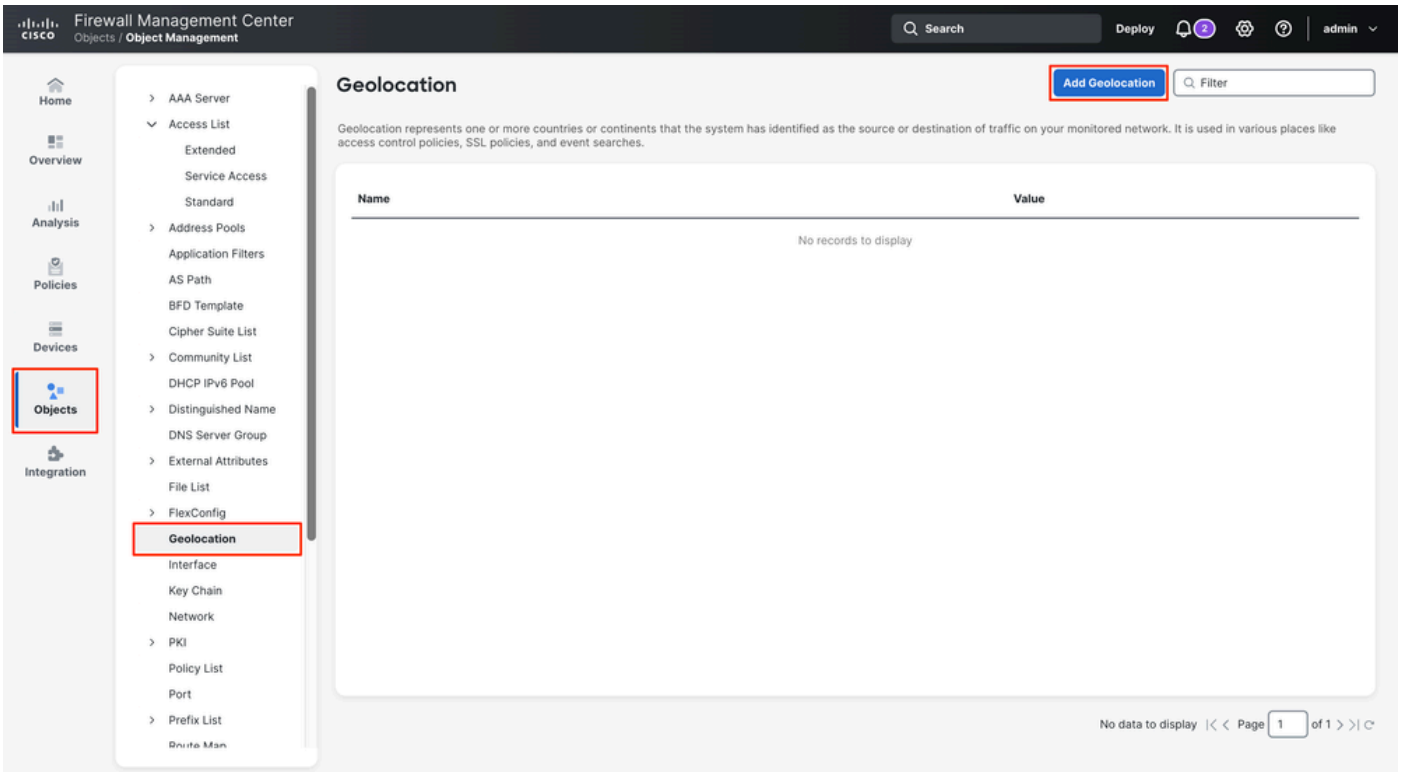
Dato che i server VPN dispongono di indirizzi IP pubblici accessibili via Internet, l'introduzione di regole basate sulla geolocalizzazione consente alle organizzazioni di limitare in modo efficace le richieste degli utenti da specifiche geolocalizzazioni, riducendo in tal modo la vulnerabilità agli attacchi di forza bruta.



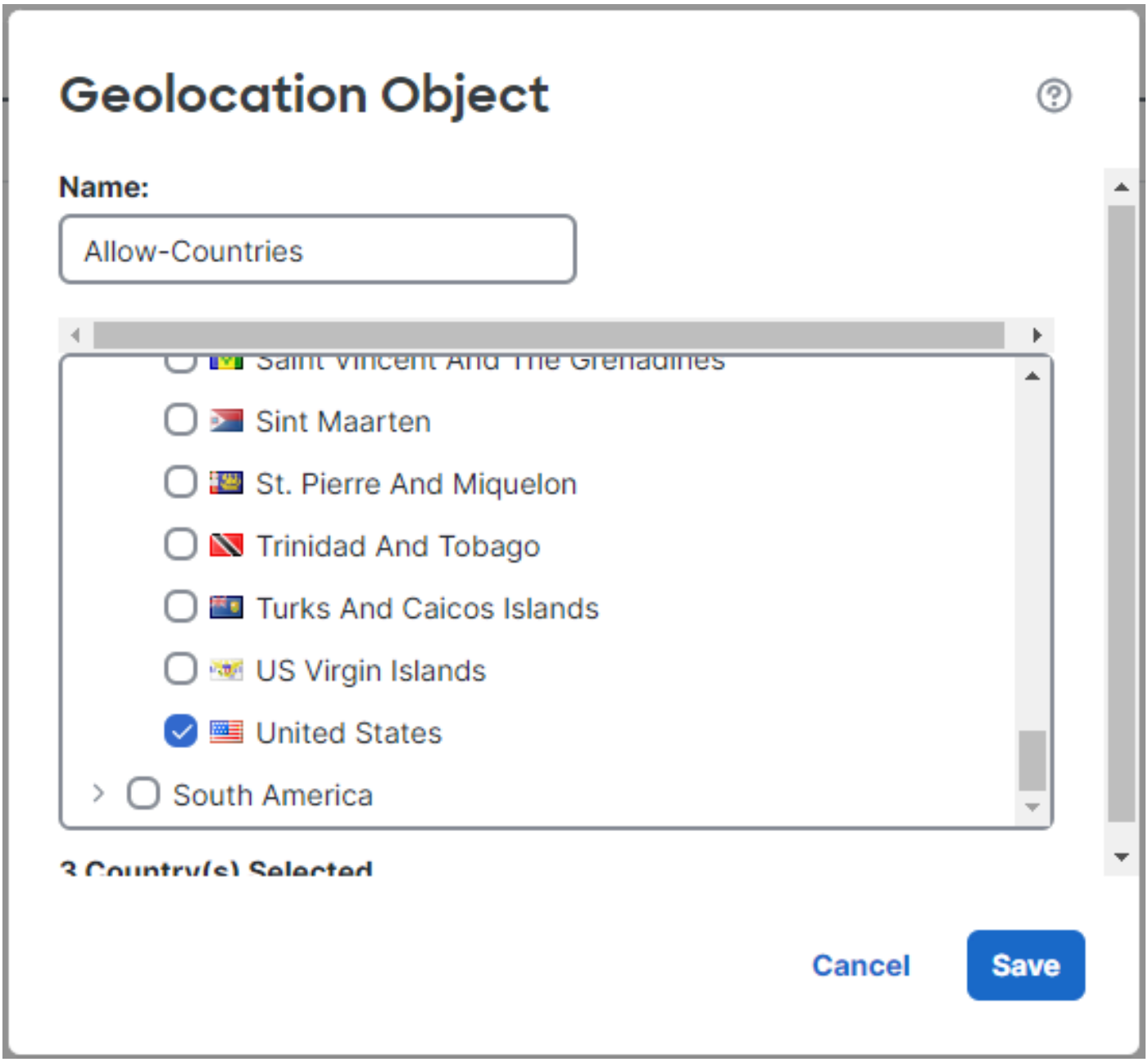

# Configurazione

## Passaggio 1. Creare un oggetto di accesso al servizio

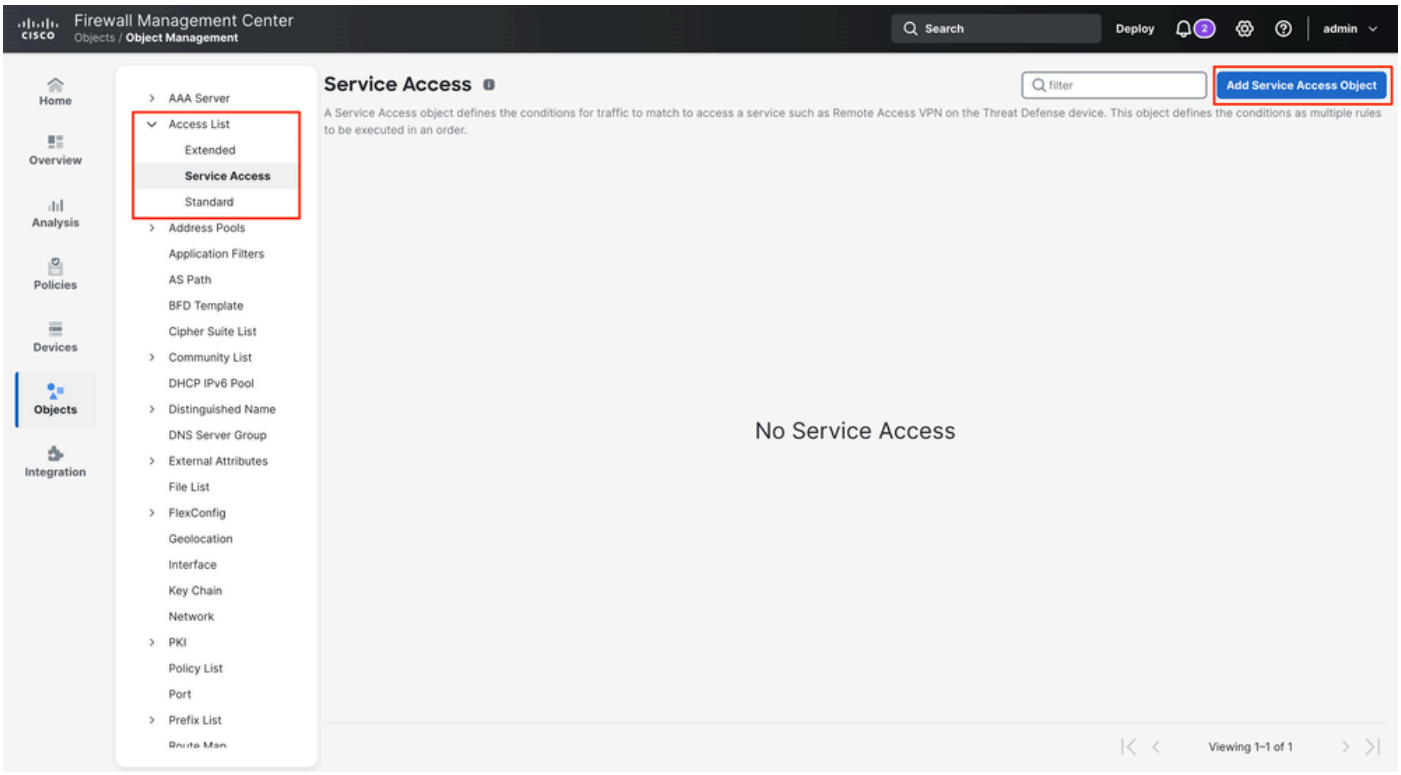
1. Accedere al centro di gestione Secure Firewall.
2. Passare a Oggetti > Gestione oggetti > Geolocazione e fare clic su Aggiungi geolocazione per creare un oggetto di geolocazione.



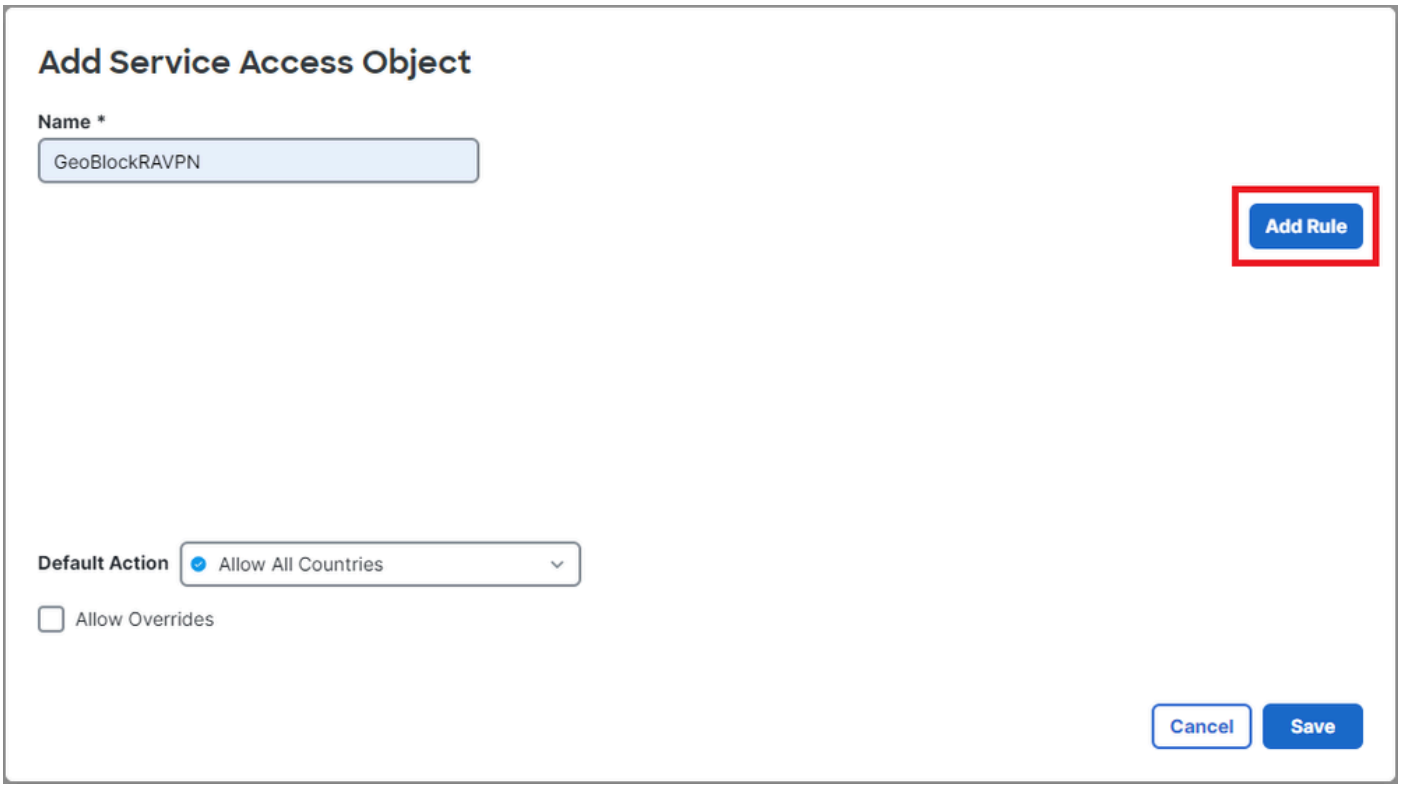

3. Creare l'oggetto selezionando i flag di paese appropriati per ogni gruppo, a seconda che siano consentiti o meno.




4. Dopo aver creato gli oggetti di georilevazione, selezionare Oggetti > Gestione oggetti > Elenco accessi > Accesso servizio e fare clic su Aggiungi oggetto di accesso al servizio.




5. Definire il nome della regola, quindi fare clic su Aggiungi regola.

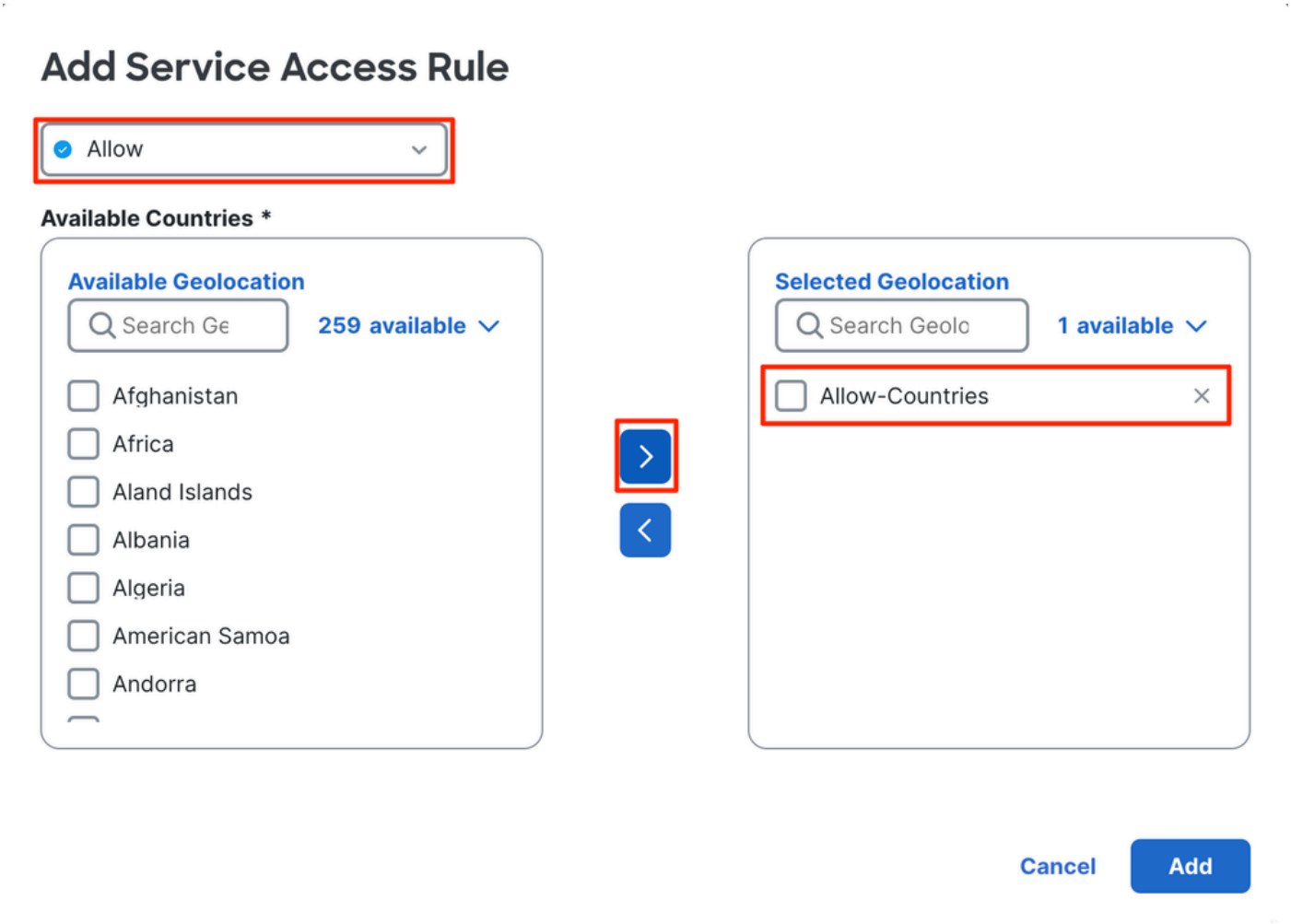



6. Selezionare l'azione della regola (Consenti o Nega), individuare l'oggetto Geolocation creato in

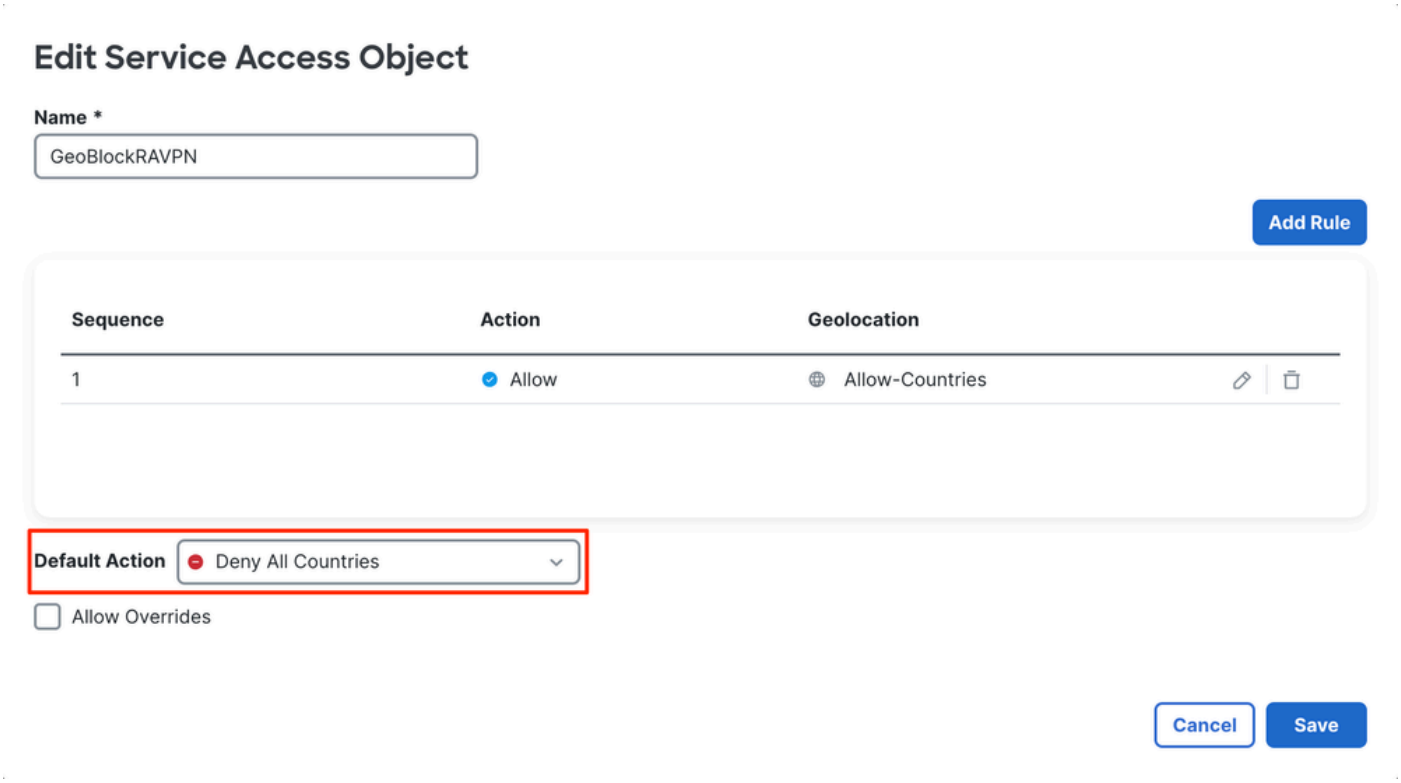
precedenza e aggiungerlo alla regola facendo clic sulla freccia destra. Quindi, fare clic su Add (Aggiungi) per creare la regola.

Nota: In un oggetto di accesso al servizio, un oggetto di geolocalizzazione (paese, continente o geolocalizzazione personalizzata) può essere utilizzato solo in una regola.

Nota: assicurarsi di configurare le regole di accesso al servizio nell'ordine corretto, poiché non è possibile riordinarle.



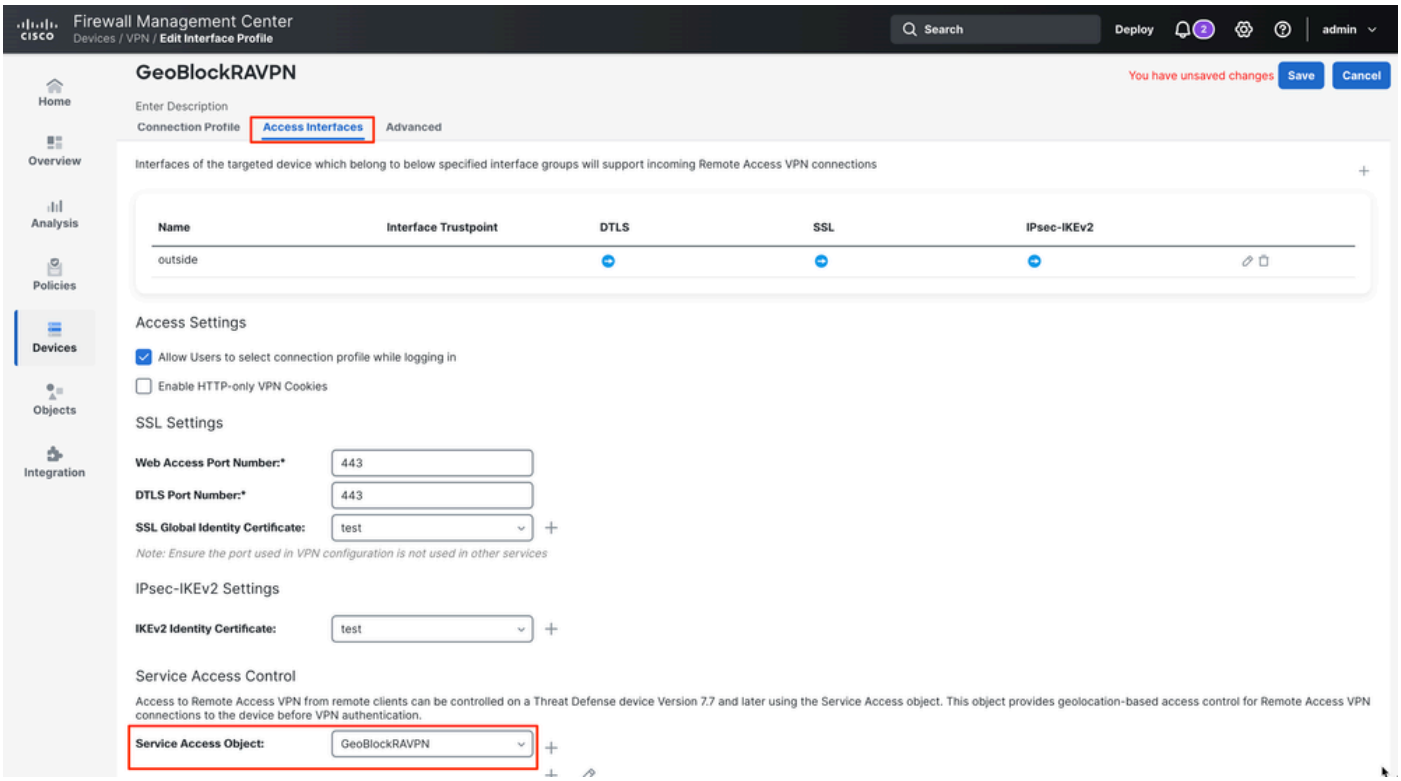

7. Modificare l'azione predefinita in Nega tutti i paesi per rifiutare le richieste di sessione provenienti da altri paesi.




Passaggio 2. Applicare la configurazione dell'oggetto assistenza in RAVPN.

1. Passare alla configurazione RAVPN in Dispositivi > Accesso remoto > Oggetto configurazione RAVPN > Interfaccia di accesso.

2. Nella sezione Controllo accesso servizio, selezionare l'oggetto Accesso servizio creato in precedenza.

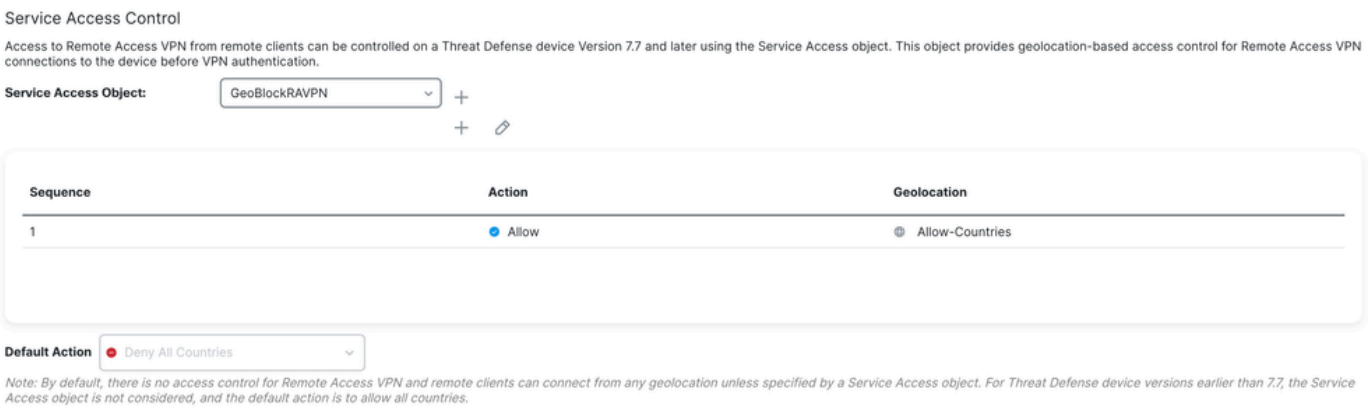



3. L'oggetto Accesso al servizio selezionato visualizza il sintetico delle regole e l'azione predefinita.

4. Infine, salvare le modifiche e distribuire la configurazione.

# Verifica

Una volta salvata la configurazione, le regole vengono visualizzate nella sezione Controllo di accesso ai servizi, consentendo di verificare quali gruppi e paesi sono bloccati o autorizzati.



Eseguire il show running-config service-access per assicurarsi che le regole di accesso al servizio siano disponibili dalla CLI FTD.

<#root>

```
firepower#
```

**show running-config service-access**

```
service-access permit ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_418243765
service-access deny ra-ssl-client ra-ikev2 geolocation FMC_GEOLOCATION_8589938211_487190092
service-access permit ra-ssl-client ra-ikev2 geolocation any
```

# Syslog e monitoraggio

Secure Firewall introduce nuovi ID syslog per acquisire gli eventi relativi alle connessioni RAVPN bloccate dai criteri basati sulla geolocalizzazione:

- 761031: indica quando una connessione IKEv2 viene negata da un criterio basato sulla geolocalizzazione. Questo syslog fa parte della classe di registrazione VPN esistente.

%FTD-6-751031: Sessione di accesso remoto IKEv2 negata per faddr <ip_client> laddr <ip_dispositivo> da una regola geografica (geo=<nome_paese>, id=<codice_paese>)

- 751031: indica quando una connessione SSL viene negata da un criterio basato sulla geolocalizzazione. Questo syslog fa parte della classe di registrazione WebVPN esistente.

%FTD-6-71616: Sessione di accesso remoto SSL negata per faddr <ip_client> da una regola geografica (geo=<nome_paese>, id=<codice_paese>)

---

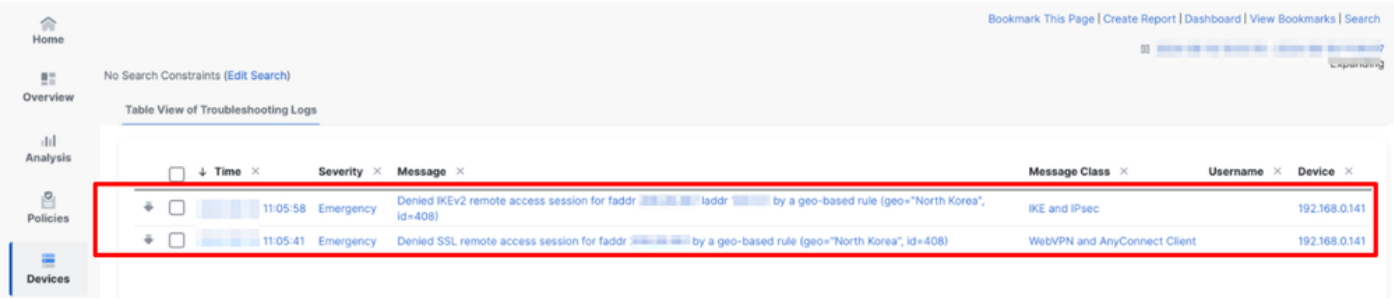
Nota: Il livello di gravità predefinito per questi nuovi syslog è informativo se abilitato dalle rispettive classi di log. Tuttavia, è possibile abilitare questi ID syslog singolarmente e personalizzarne la gravità.

---

## Monitoraggio connessioni bloccate

Per convalidare le connessioni bloccate, selezionare Dispositivi > Risoluzione dei problemi > Log per la risoluzione dei problemi. In questa pagina vengono visualizzati i log relativi alle connessioni bloccate, incluse le informazioni sulle regole che influiscono sulla connessione e sul tipo di sessione.

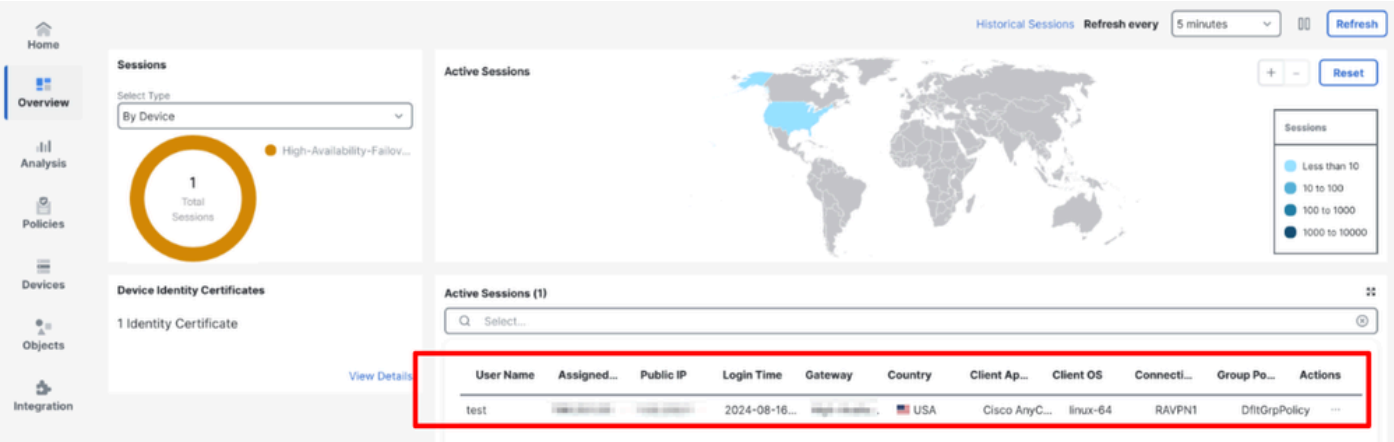
Nota: Syslog deve essere configurato per raccogliere queste informazioni nei log di risoluzione dei problemi.




### Monitora connessioni consentite

Le sessioni consentite vengono monitorate in Panoramica > Dashboard VPN ad accesso remoto, in cui vengono visualizzate le informazioni sulla sessione, incluso il paese di origine.

Nota: In questo dashboard vengono visualizzate solo le connessioni dai paesi consentiti e dagli utenti a cui è consentita la connessione. Le connessioni rifiutate non vengono visualizzate in questo dashboard.




## Risoluzione dei problemi

Per la risoluzione dei problemi, eseguire la procedura seguente:

1. Verificare che le regole siano configurate correttamente nell'oggetto Accesso al servizio.
2. Controllare se nella sezione Log di risoluzione dei problemi viene visualizzato un syslog di

negazione quando una georilevazione consentita richiede una sessione.
3. Verificare che la configurazione mostrata nel FMC corrisponda a quella presente nella CLI del FTD.
4. Utilizzare i comandi successivi per raccogliere ulteriori dettagli utili per la risoluzione dei problemi:

- debug geolocation <1-255>
- show service-access
- mostra dettagli di accesso al servizio
- show service-access interface
- mostra percorso di accesso al servizio
- show service-access service
- mostra contesto geodb
- mostra contatori geodb
- show geodb ipv4
- show geodb ipv6

## Informazioni correlate

- Per ulteriore assistenza, contattare TAC. È necessario un contratto di supporto valido:Contatti del supporto Cisco internazionali.
- In questa sezione puoi anche visitare la Cisco VPN Community.

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).