Configurazione del blocco del traffico basato sulla georilevazione su FTD per il filtro del traffico in entrata e in uscita

Sommario

Problema

- Descrivere il modo migliore per bloccare il traffico in base alla geolocalizzazione con Cisco Secure Firewall Threat Defense (FTD), sia per il traffico proveniente da una regione che per il traffico destinato a una regione.
- Vengono sollevate domande relative alla necessità di regole di controllo dell'accesso separate per il filtro del traffico in entrata e in uscita e alla necessità di creare oggetti di geolocalizzazione aggiuntivi quando le voci di geolocalizzazione sono già disponibili nella scheda Geolocation della scheda Reti delle regole di controllo dell'accesso.

Ambiente

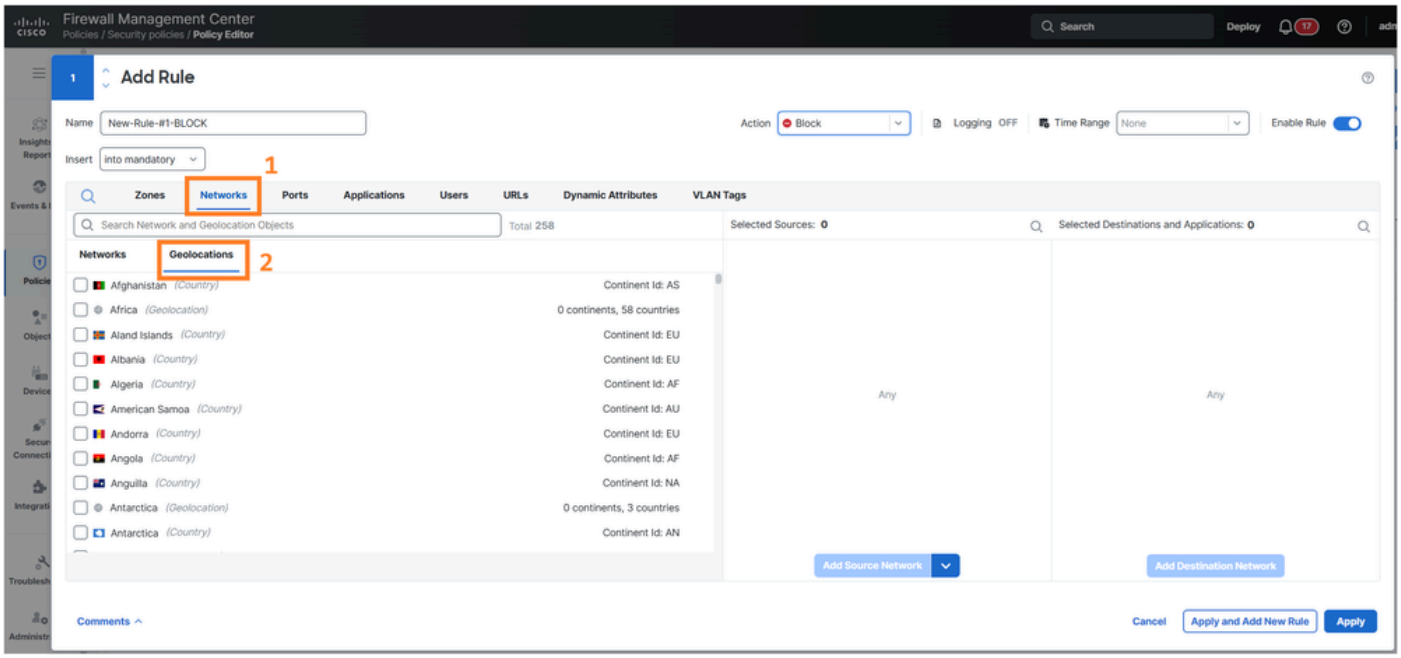
- Software FTD versione 7.1. Sono interessate anche altre versioni software.
- Software Cisco Secure Firewall Management Center (FMC) versione 7.1. Il problema interessa anche altre versioni software.

Risoluzione

Il filtro del traffico basato sulla georilevazione su Cisco FTD può essere gestito in modo efficace utilizzando la funzionalità di georilevazione esistente disponibile nella scheda Reti, sezione Regola dei criteri di controllo dell'accesso dell'interfaccia utente di FMC. L'approccio della configurazione dipende dalla direzione del traffico e dai requisiti delle policy.

Accesso alla configurazione di georilevazione

Passare a Criteri > Criteri di protezione > Editor criteri, modificare una regola e selezionare Reti > Geolocation scheda nell'interfaccia utente di FMC. Le voci di geolocalizzazione esistenti disponibili in questa sezione possono essere utilizzate direttamente per la creazione di policy di controllo dell'accesso senza richiedere oggetti di geolocalizzazione separati.



Strategia di creazione delle regole

L'approccio adottato per la creazione delle regole varia in base alla direzionalità del traffico e agli obiettivi strategici.

Per bloccare il traffico in entrata da geolocalizzazioni specifiche

Creare regole di controllo d'accesso che identifichino il traffico di origine proveniente da aree geografiche specifiche e applichino azioni di blocco. Queste regole devono essere posizionate in modo appropriato all'interno della regola per garantire un'adeguata applicazione delle politiche.

Per il controllo del traffico in uscita verso geolocalizzazioni specifiche

Configurare le regole di controllo d'accesso che identificano il traffico di destinazione diretto ad aree geografiche specifiche. A seconda dei criteri di sicurezza, questi possono essere configurati per consentire o bloccare il traffico verso tali destinazioni.

Requisiti regola separata

Regole di controllo dell'accesso separate sono necessarie quando si implementa il filtro di geolocalizzazione bidirezionale perché:

- Il filtro in ingresso richiede regole che valutino gli attributi di geolocalizzazione di origine.
- Il filtro in uscita richiede regole che valutino gli attributi di geolocalizzazione di destinazione.
- La direzionalità del traffico determina quale campo di geolocalizzazione (origine o destinazione) viene valutato dal modulo di controllo dell'accesso.

La configurazione della regola specifica dipende dalla topologia di rete, dai requisiti di sicurezza e dagli obiettivi di controllo del flusso di traffico desiderati per ogni area geografica.

Causa

La necessità di un chiarimento deriva dalla complessità dell'implementazione del controllo dell'accesso basato sulla geolocalizzazione, in cui sono richiesti diversi tipi di regole e configurazioni in base alla direzione del traffico. La disponibilità di voci di geolocalizzazione preesistenti nella scheda Reti delle regole di controllo di accesso dei criteri di sicurezza può creare confusione sulla necessità o meno di creare oggetti aggiuntivi per l'implementazione dei criteri.

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).