Op geolocatie gebaseerde verkeersblokkering configureren op FTD voor inkomende en uitgaande verkeersfiltering

Inhoud

uitgeven

- Beschrijf wat de beste manier is om verkeer te blokkeren op basis van geolocatie op Cisco Secure Firewall Threat Defense (FTD), zowel voor verkeer afkomstig uit een regio als verkeer bestemd voor een regio.
- Er rijzen vragen over de vraag of afzonderlijke toegangscontroleregels vereist zijn voor inkomende en uitgaande verkeersfiltering en of er extra geolocatieobjecten moeten worden gemaakt wanneer geolocatiegegevens al beschikbaar zijn op het tabblad Geolocaties onder toegangscontroleregels Netwerken.

milieu

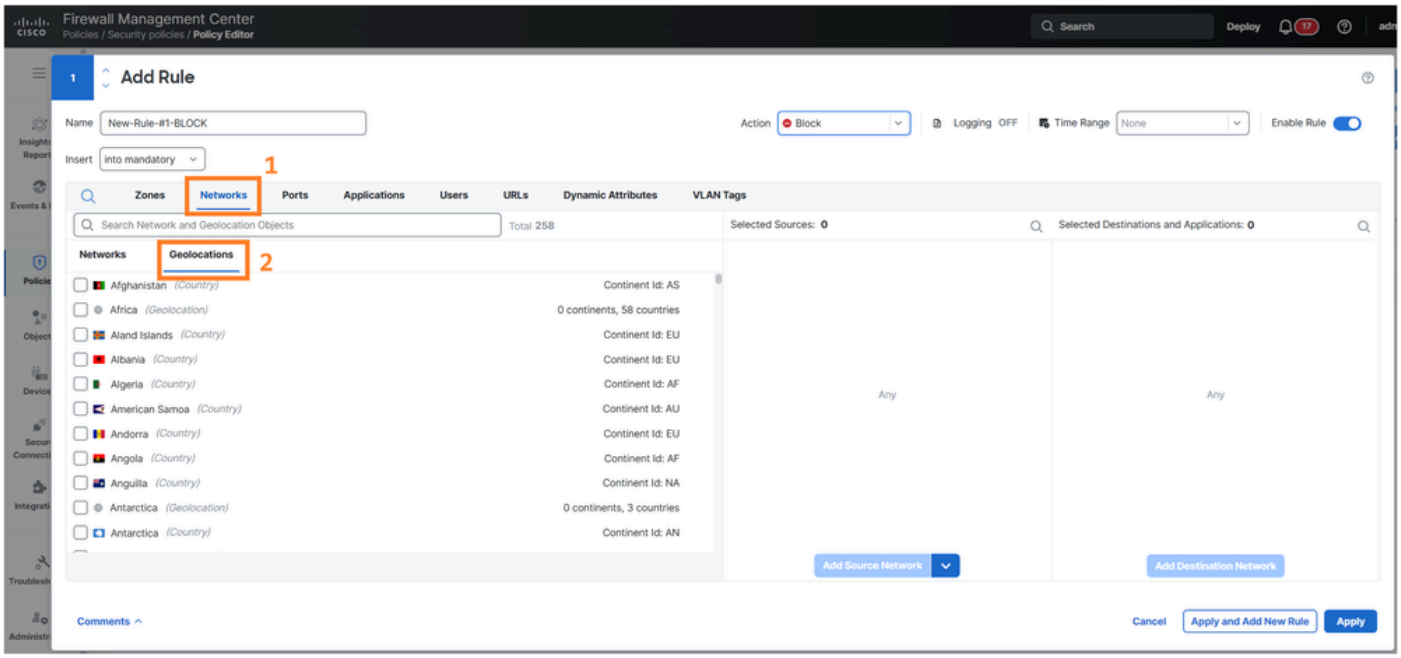
- FTD-softwareversie 7.1. Ook andere software versies zijn hierbij betrokken.
- Cisco Secure Firewall Management Center (FMC)-software versie 7.1. Ook andere software versies zijn hierbij betrokken.

resolutie

Op geolocatie gebaseerde verkeersfiltering op Cisco FTD kan effectief worden beheerd met behulp van de bestaande geolocaties-functionaliteit die beschikbaar is op het tabblad Netwerken, sectie Access Control Policy Rule van de FMC-gebruikersinterface (UI). De configuratiebenadering is afhankelijk van de specifieke verkeersrichting en beleidsvereisten.

Toegang tot geolocatieconfiguratie

Navigeer naar Beleid > Beveiligingsbeleid > Beleidseditor, bewerk een regel en selecteer Netwerken > Geolocaties tabblad in de FMC UI. De bestaande geolocatie-items die in dit gedeelte beschikbaar zijn, kunnen rechtstreeks worden gebruikt voor het maken van toegangscontrolebeleid zonder dat afzonderlijke geolocatie-objecten nodig zijn.



strategie voor het creëren van regels

De aanpak voor het creëren van regels varieert op basis van de verkeersgerichtheid en beleidsdoelstellingen.

Voor het blokkeren van inkomend verkeer vanaf specifieke geolocaties

Maak toegangscontroleregels die bronverkeer identificeren dat afkomstig is uit specifieke geografische regio's en blokacties toepassen. Deze regels moeten naar behoren in de regel worden geplaatst om een goede beleidshandhaving te waarborgen.

Voor het regelen van uitgaand verkeer naar specifieke geolocaties

Configureer toegangscontroleregels die bestemmingsverkeer identificeren dat is gericht op specifieke geografische gebieden. Afhankelijk van het beveiligingsbeleid kunnen deze worden geconfigureerd om verkeer naar die bestemmingen toe te staan of te blokkeren.

Eisen voor afzonderlijke regels

Bij de toepassing van bidirectionele geolocatiefiltering zijn afzonderlijke regels voor toegangscontrole nodig omdat:

- Inkomende filtering vereist regels die de kenmerken van de brongeolocatie evalueren.
- Uitgaande filtering vereist regels die bestemmingsgeolocatiekenmerken evalueren.
- Verkeersgerichtheid bepaalt welk geolocatieveld (bron of bestemming) wordt geëvalueerd door de toegangscontrole-engine.

De specifieke regelconfiguratie is afhankelijk van de netwerktopologie, beveiligingsvereisten en de gewenste doelstellingen voor verkeersstroomcontrole voor elke geografische regio.

Oorzaak

De behoefte aan verduidelijking komt voort uit de complexiteit van de implementatie van toegangscontrole op basis van geolocatie, waarbij verschillende regeltypen en configuraties vereist zijn op basis van de verkeersrichting. De beschikbaarheid van reeds bestaande geolocatie-items op het tabblad Netwerken van de toegangscontroleregels voor het beveiligingsbeleid kan verwarring veroorzaken over de vraag of het maken van extra objecten nodig is voor beleidsimplementatie.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.