Configurar o bloqueio de tráfego baseado em geolocalização no FTD para filtragem de tráfego de entrada e saída

Contents

Problema

- Descreva qual é a melhor maneira de bloquear o tráfego com base na geolocalização no Cisco Secure Firewall Threat Defense (FTD), tanto para o tráfego originário de uma região quanto para o tráfego destinado a uma região.
- Surgem dúvidas sobre se regras de controle de acesso separadas são necessárias para filtragem de tráfego de entrada e saída e se objetos adicionais de geolocalização precisam ser criados quando entradas de geolocalização já estão disponíveis na guia Geolocalizações na guia Redes da regra de controle de acesso.

Ambiente

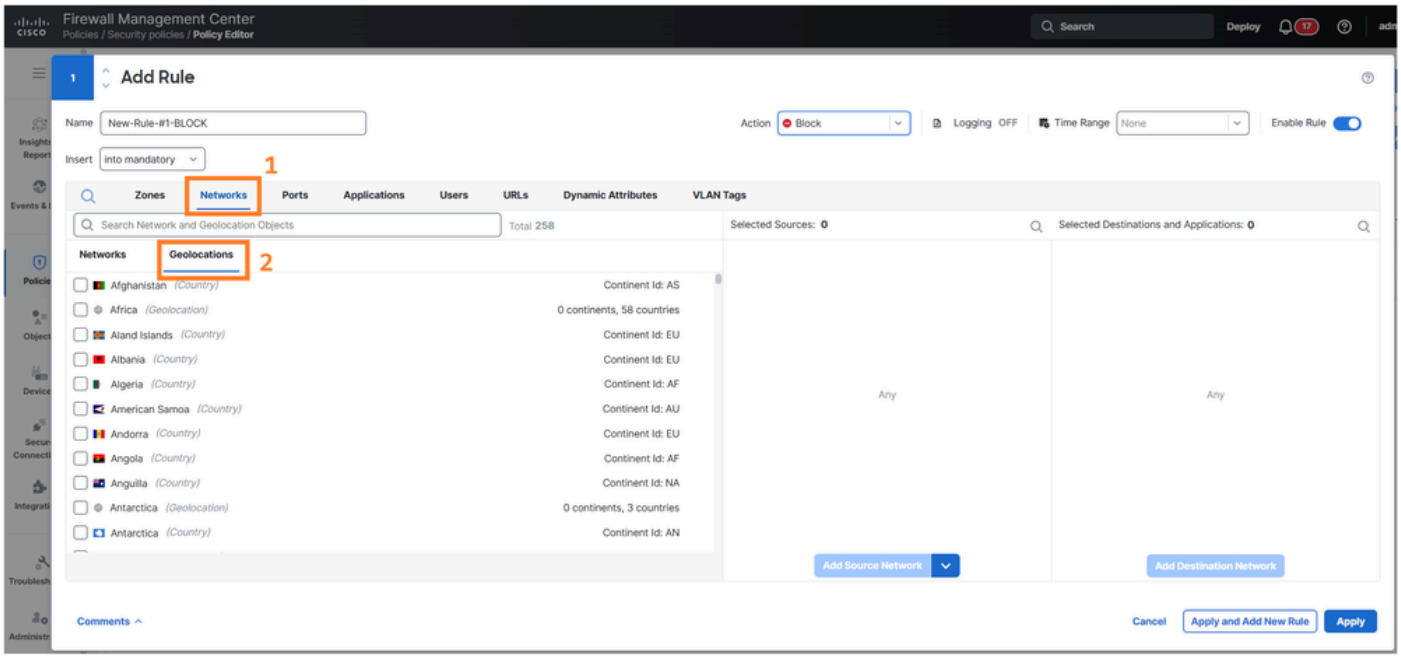
- Software FTD versão 7.1. Outras versões de software também são afetadas.
- Software Cisco Secure Firewall Management Center (FMC) versão 7.1. Outras versões de software também são afetadas.

Resolução

A filtragem de tráfego baseada em geolocalização no Cisco FTD pode ser gerenciada com eficiência usando a funcionalidade de geolocalização existente disponível na guia Redes, seção Regra de política de controle de acesso da interface de usuário (UI) do FMC. A abordagem de configuração depende do sentido específico do tráfego e dos requisitos da política.

Acessando a configuração de geolocalização

Navegue para Policies > Security policies > Policy Editor, edite uma regra e selecione Networks > Geolocations tab na interface do usuário do FMC. As entradas de geolocalização existentes disponíveis nesta seção podem ser utilizadas diretamente para a criação de políticas de controle de acesso sem a necessidade de objetos de geolocalização separados.



Estratégia de criação de regras

A abordagem de criação de regras varia com base na direcionalidade do tráfego e nos objetivos políticos.

Para bloquear o tráfego de entrada de geolocalizações específicas

Crie regras de controle de acesso que identifiquem o tráfego de origem originário de regiões geográficas específicas e aplique ações de bloqueio. Essas regras devem ser posicionadas adequadamente na regra para garantir a aplicação adequada de políticas.

Para controlar o tráfego de saída para geolocalizações específicas

Configure regras de controle de acesso que identifiquem o tráfego de destino direcionado para regiões geográficas específicas. Dependendo da política de segurança, eles podem ser configurados para permitir ou bloquear o tráfego para esses destinos.

Requisitos de regra separada

São necessárias regras de controlo de acesso separadas ao implementar a filtragem de geolocalização bidirecional, porque:

- A filtragem de entrada requer regras que avaliem os atributos de geolocalização de origem.
- A filtragem de saída requer regras que avaliem os atributos de geolocalização de destino.
- A direcionalidade do tráfego determina qual campo de geolocalização (origem ou destino) é avaliado pelo mecanismo de controle de acesso.

A configuração específica da regra depende da topologia da rede, dos requisitos de segurança e dos objetivos de controle de fluxo de tráfego desejados para cada região geográfica.

Causa

A necessidade de esclarecimento surge da complexidade da implementação do controle de acesso baseado em geolocalização, onde diferentes tipos de regras e configurações são necessárias com base no sentido do tráfego. A disponibilidade de entradas de geolocalização pré-existentes na guia Redes das regras de controle de acesso de política de segurança pode criar confusão sobre a necessidade de criação de objetos adicionais para a implementação da política.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.