Desative o Proxy ARP nas interfaces FTD usando o FlexConfig

Problema

Os hosts em uma interface FTD não podem usar endereços IP atribuídos estaticamente e relatar erros de "endereço IP duplicado" antes de retornar aos endereços 169.254.x.x. A análise de captura de pacotes revela que quando o host envia um ARP gratuito (prova ARP) para seu próprio endereço IP, o firewall responde reivindicando a propriedade desse endereço IP, evitando a atribuição bem-sucedida de IP estático.

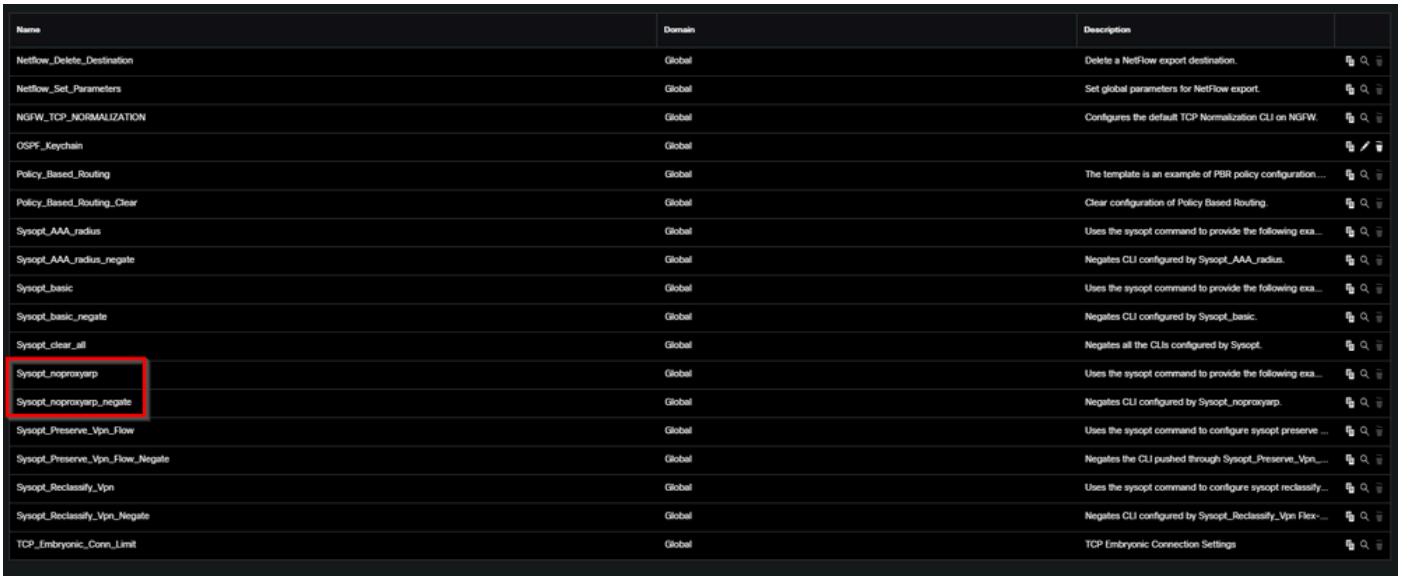
Ambiente

- Cisco Secure Firewall 2120 executando a versão 7.4.4 do software FTD (aplicável a todas as versões e modelos)
- Cisco Secure Firewall Management Center (FMC) para gerenciamento de dispositivos
- Proxy ARP habilitado no FTD por padrão.

Resolução

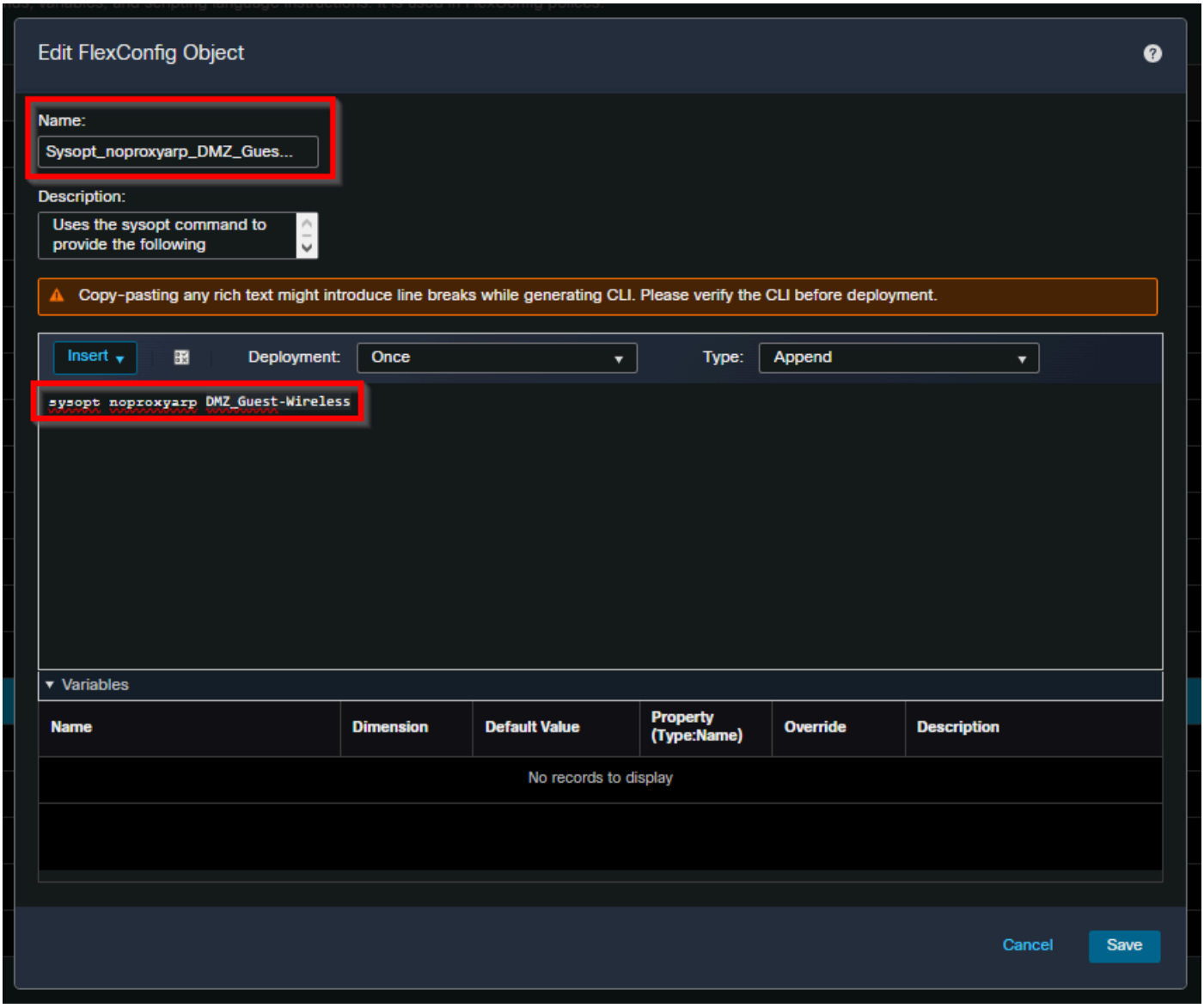
O problema é resolvido desabilitando o Proxy ARP na interface afetada usando uma política FlexConfig implantada através do FMC. Isso impede que o firewall responda às sondas ARP para endereços IP que ele não possui explicitamente.

1: Navegue até a seção FlexConfig no FMC e crie uma nova política FlexConfig para desativar o Proxy ARP na interface específica. Sysopt_noproxyarp e a negação Sysopt_noproxyarp_negate são objetos padrão no FMC e podem ser clonados para uso personalizado.



inline_image_0.png

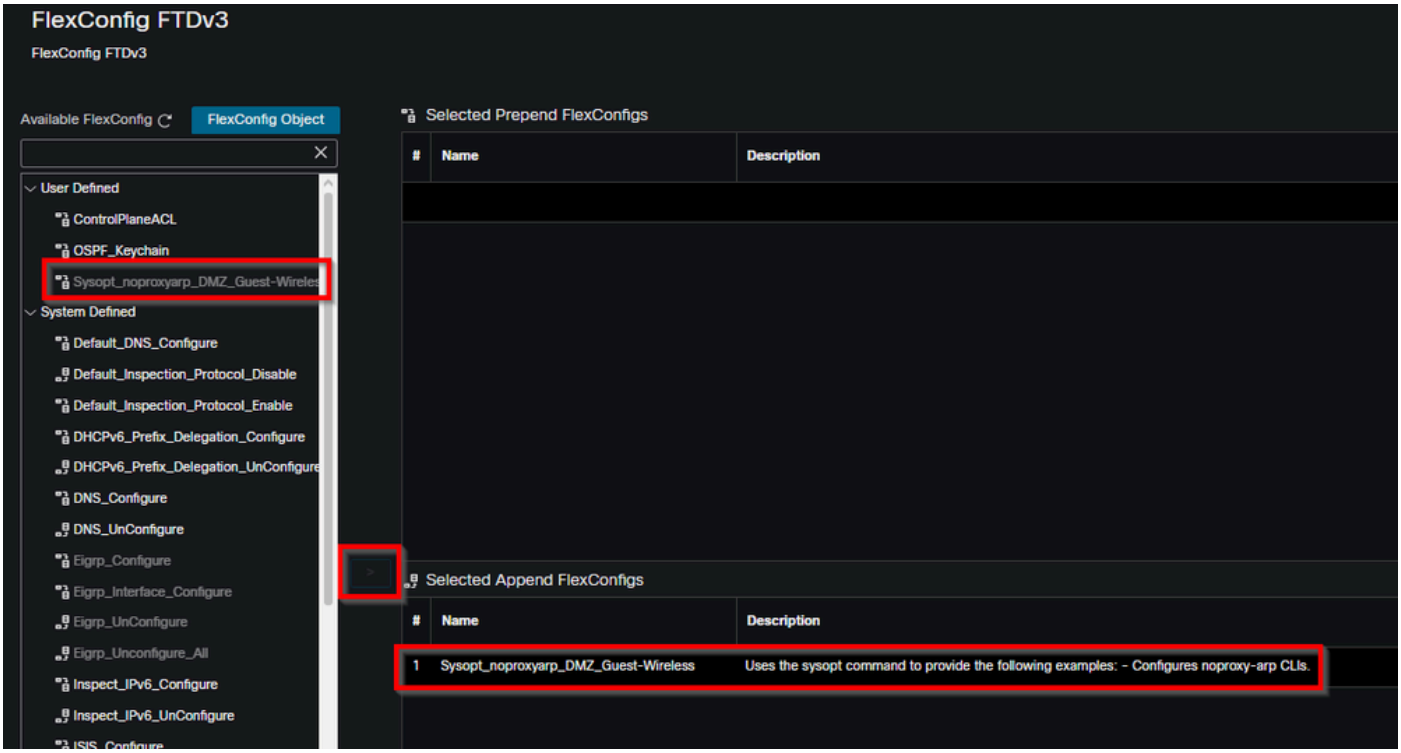
2: Adicione o comando de configuração à política FlexConfig sysopt noproxyarp IFNAME:



inline_image_1.png

Substitua IFNAME pelo nome real da interface afetada.

3: Associe o novo objeto à política FlexConfig do FTD e implante-o por meio do FMC. A configuração é aplicada para desabilitar o comportamento Proxy ARP na interface especificada.



inline_image_2.png

4: Após a implantação, teste a atribuição de IP estático no host afetado. O firewall não deve mais ser capaz de responder às sondas ARP para endereços IP não atribuídos, permitindo que os hosts usem com êxito suas configurações de IP estático sem erros de endereço IP duplicado.

Quando aplicável, considere desabilitar o Proxy ARP no nível de regra NAT em vez de em toda a interface para minimizar o impacto não intencional em outras funções de rede. Isso fornece um controle mais granular sobre o comportamento do Proxy ARP.

Causa

O Proxy ARP (Proxy Address Resolution Protocol) foi habilitado na interface FTD, fazendo com que o firewall respondesse às sondas ARP para endereços IP que não possuía explicitamente. Esse comportamento resultou na detecção de hosts de uma condição de endereço IP duplicado durante a atribuição de endereço estático. A funcionalidade ARP de Proxy do firewall estava respondendo com seu próprio endereço MAC quando os hosts executaram solicitações ARP gratuitas, fazendo com que parecesse que o endereço IP desejado já estava em uso por outro

dispositivo.

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.