Proxy-ARP uitschakelen op FTD-interfaces met FlexConfig

uitgeven

Hosts op een FTD-interface kunnen geen statisch toegewezen IP-adressen gebruiken en "duplicate IP address"-fouten melden voordat ze terugvallen naar 169.254.x.x-adressen. Analyse van pakketregistratie laat zien dat wanneer de host een gratuite ARP (ARP-sonde) voor zijn eigen IP-adres verzendt, de firewall reageert door het eigendom van dat IP-adres te claimen, waardoor een succesvolle statische IP-toewijzing wordt voorkomen.

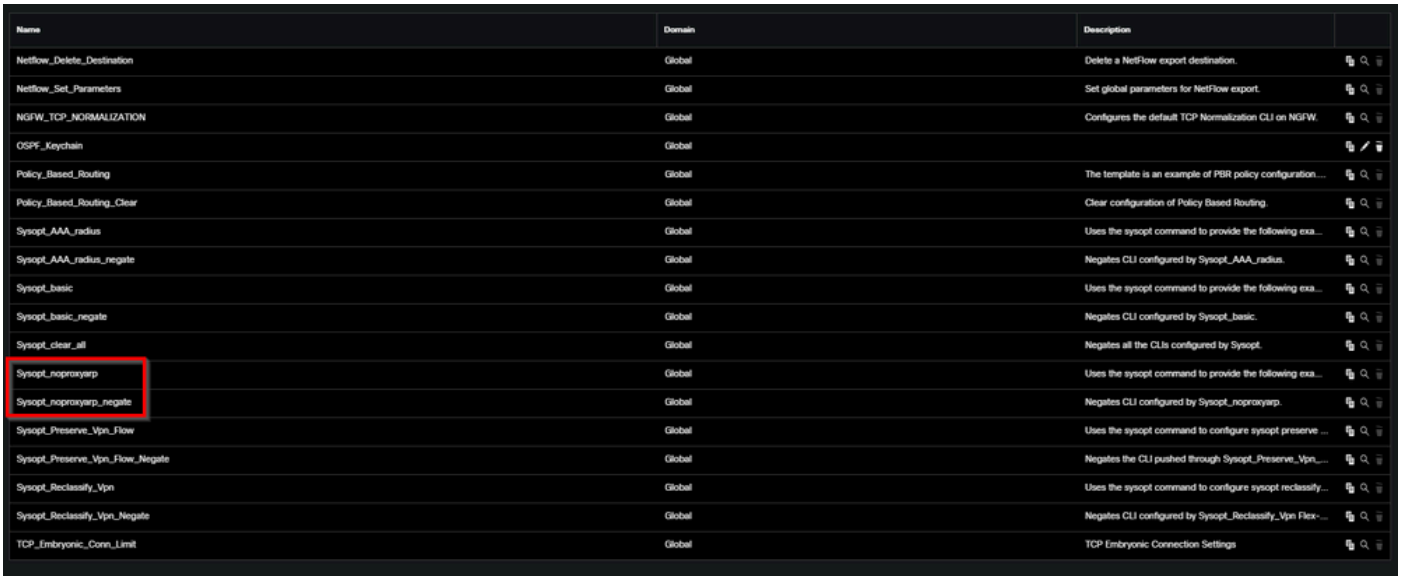
milieu

- Cisco Secure Firewall 2120 met FTD-softwareversie 7.4.4 (van toepassing op alle versies en modellen)
- Cisco Secure Firewall Management Center (FMC) voor apparaatbeheer
- Proxy ARP standaard ingeschakeld op FTD.

resolutie

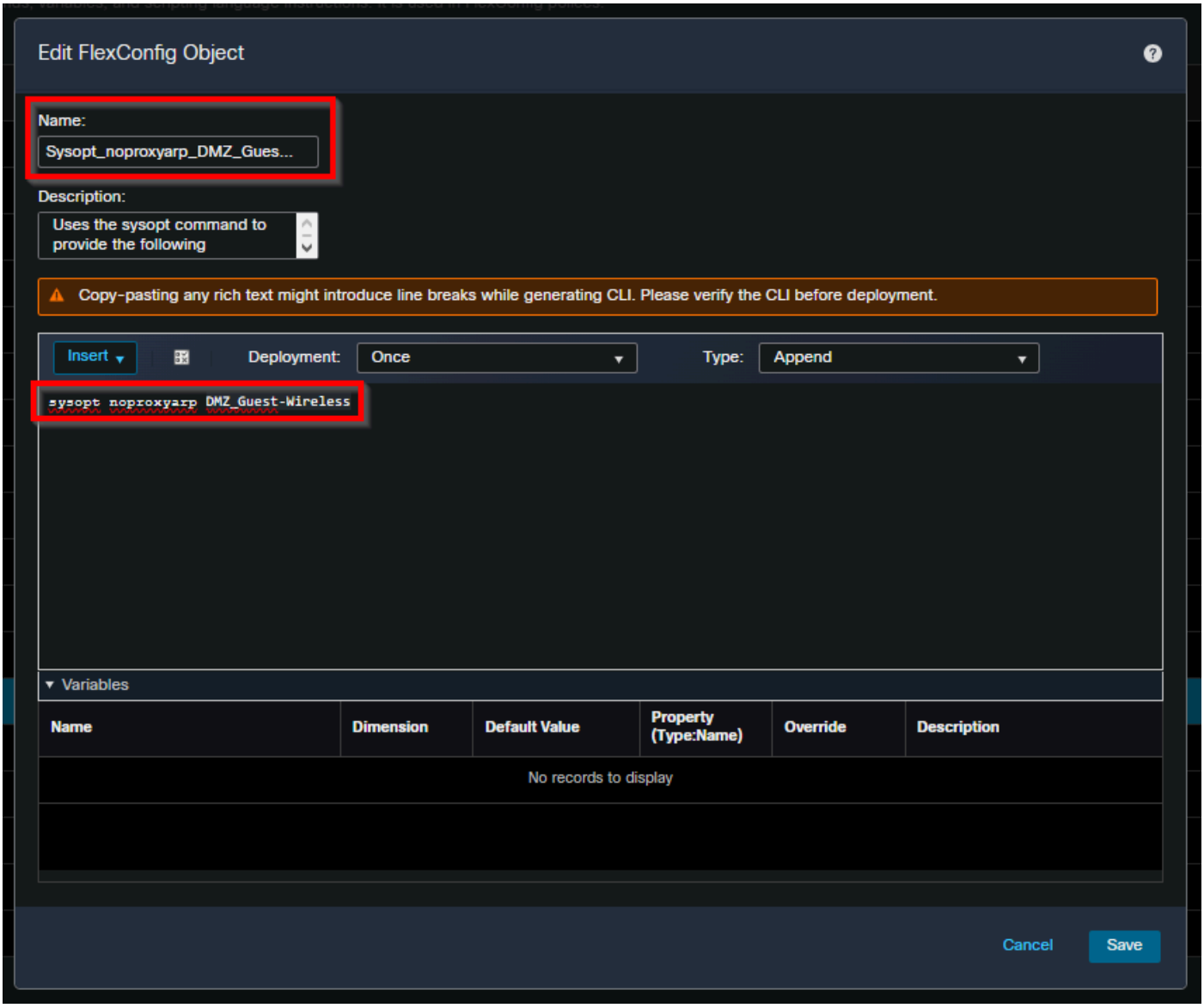
Het probleem wordt opgelost door Proxy ARP op de betreffende interface uit te schakelen met behulp van een FlexConfig-beleid dat via FMC wordt geïmplementeerd. Dit voorkomt dat de firewall reageert op ARP-sondes voor IP-adressen die hij niet expliciet bezit.

1: Navigeer naar de sectie FlexConfig in FMC en maak een nieuw FlexConfig-beleid om Proxy ARP op de specifieke interface uit te schakelen. De Sysopt_noproxyarp en de negating Sysopt_noproxyarp_negate zijn standaardobjecten in de FMC en kunnen worden gekloond voor aangepast gebruik.



inline_image_0.png

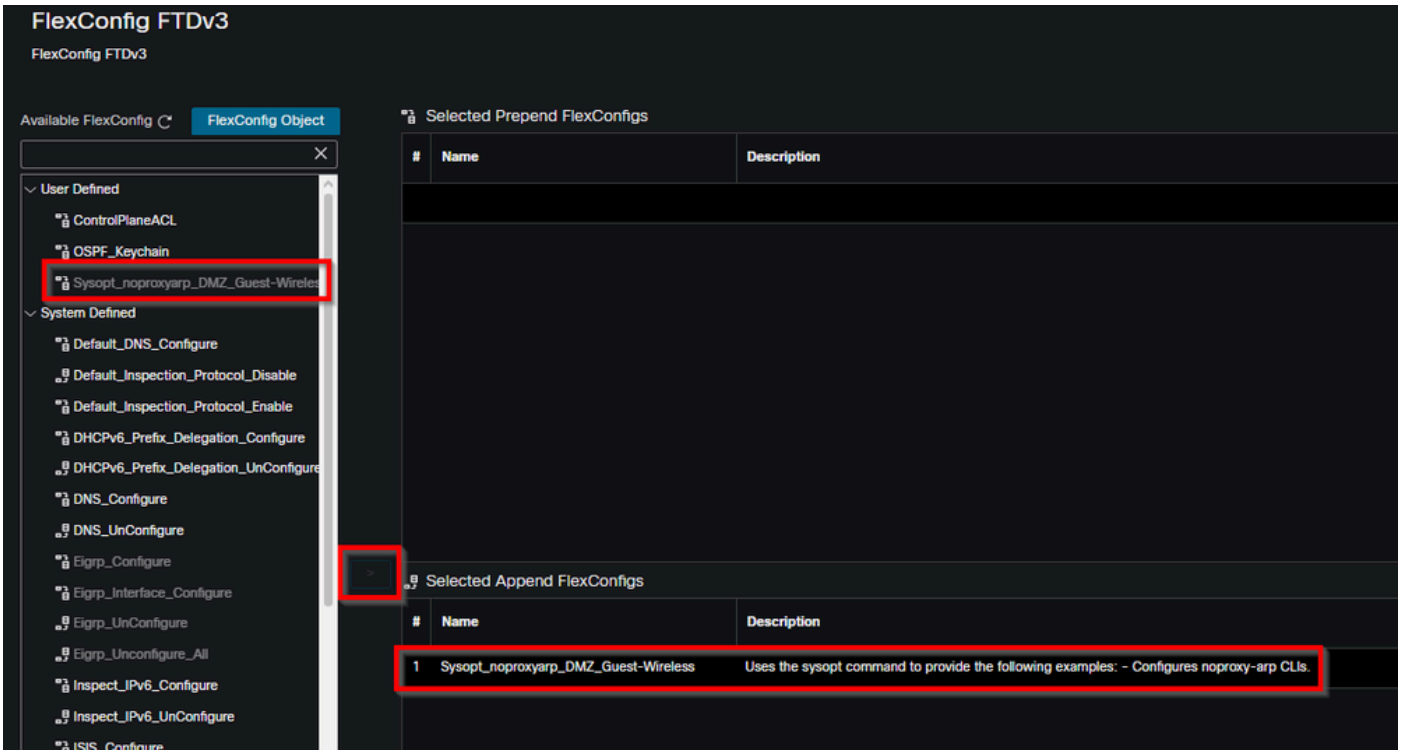
2: Voeg de configuratieopdracht toe aan het FlexConfig-beleidssysopt noproxyarp IFNAME:



inline_image_1.png

Vervang IFNAME door de werkelijke naam van de betreffende interface.

3: Koppel het nieuwe object aan het FlexConfig-beleid van de FTD en implementeer het via FMC. De configuratie wordt toegepast om Proxy ARP-gedrag op de opgegeven interface uit te schakelen.



inline_image_2.png

4: Test na implementatie de statische IP-toewijzing op de betreffende host. De firewall mag niet langer in staat zijn om te reageren op ARP-probes voor niet-toegewezen IP-adressen, waardoor hosts hun statische IP-configuraties met succes kunnen gebruiken zonder dubbele IP-adresfouten.

Overweeg indien van toepassing het uitschakelen van Proxy ARP op het niveau van de NAT-regel in plaats van interfacebreed om onbedoelde gevolgen voor andere netwerkfuncties te minimaliseren. Dit biedt meer gedetailleerde controle over het gedrag van de proxy-ARP.

Oorzaak

Proxy Address Resolution Protocol (Proxy ARP) werd ingeschakeld op de FTD-interface, waardoor de firewall reageerde op ARP-sondes voor IP-adressen die het niet expliciet bezat. Dit gedrag leidde ertoe dat hosts een dubbele IP-adresvoorwaarde detecteerden tijdens de toewijzing van statische adressen. De firewall Proxy ARP-functionaliteit reageerde met een eigen MAC-adres

wanneer hosts gratuite ARP-verzoeken uitvoerden, waardoor het leek alsof het gewenste IP-adres al door een ander apparaat werd gebruikt.

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.