Disable Proxy ARP on FTD Interfaces Using FlexConfig

Issue

Hosts on an FTD interface are unable to use statically assigned IP addresses and report "duplicate IP address" errors

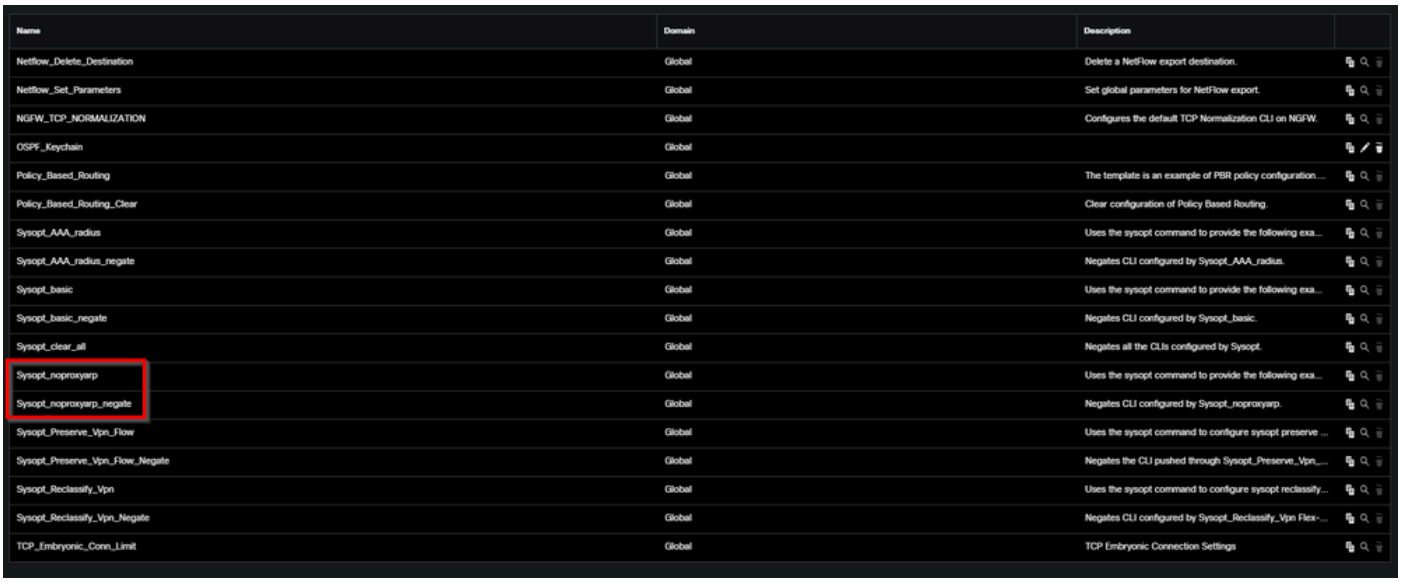
Environment

- Cisco Secure Firewall 2120 running FTD software version 7.4.4 (applicable to all versions and models)
- Cisco Secure Firewall Management Center (FMC) for device management
- Proxy ARP enabled on FTD by default.

Resolution

The issue is resolved by disabling Proxy ARP on the affected interface using a FlexConfig policy deployed through

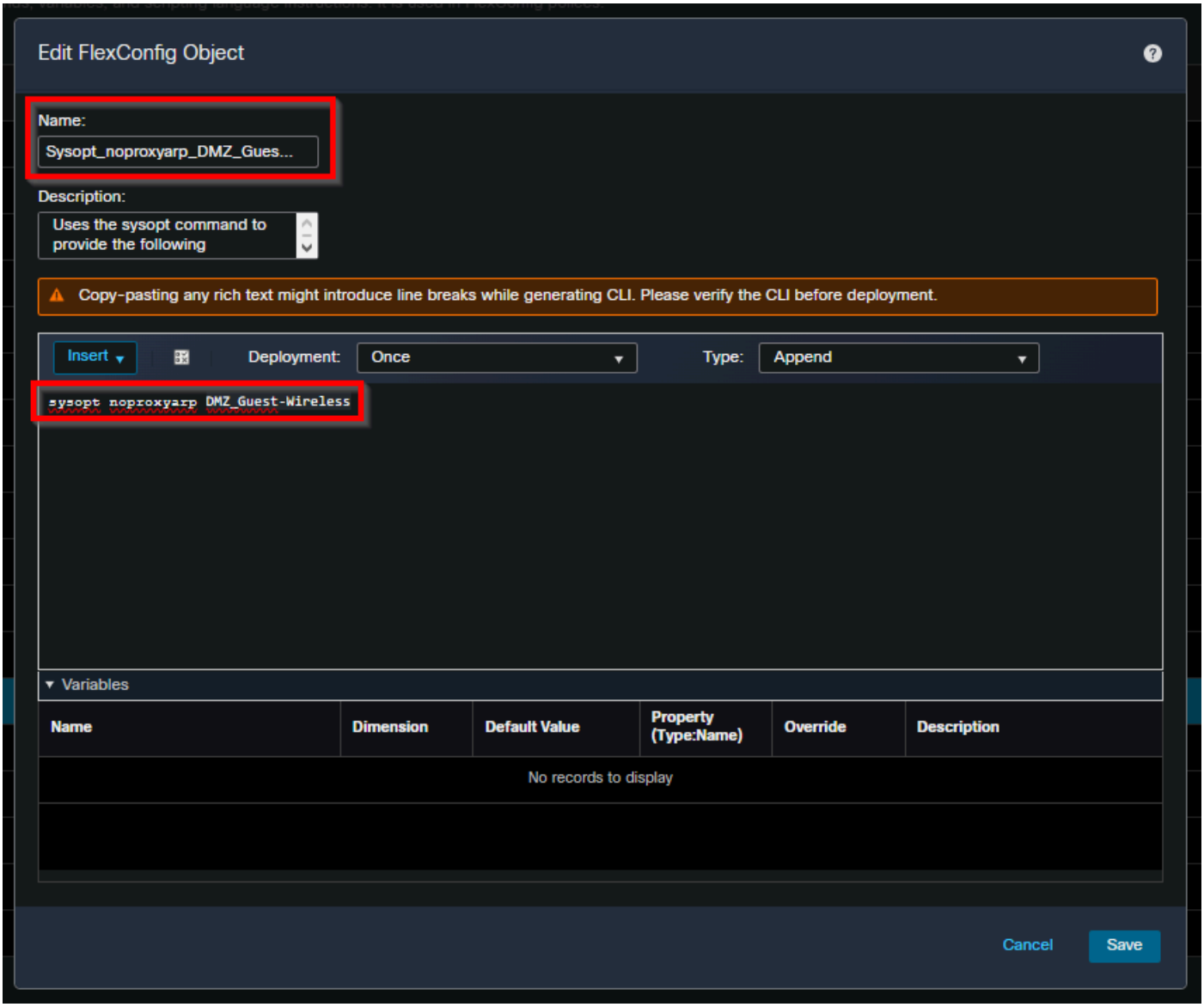
1: Navigate to the FlexConfig section in FMC and create a new FlexConfig policy to disable Proxy ARP on the spec



Name	Domain	Description
Netflow_Delete_Destination	Global	Delete a NetFlow export destination.
Netflow_Set_Parameters	Global	Set global parameters for NetFlow export.
NGFW_TCP_NORMALIZATION	Global	Configures the default TCP Normalization CLI on NGFW.
OSPF_Keychain	Global	
Policy_Based_Routing	Global	The template is an example of PBR policy configuration....
Policy_Based_Routing_Clear	Global	Clear configuration of Policy Based Routing.
Sysopt_AAA_radius	Global	Uses the sysopt command to provide the following exa...
Sysopt_AAA_radius_negate	Global	Negates CLI configured by Sysopt_AAA_radius.
Sysopt_basic	Global	Uses the sysopt command to provide the following exa...
Sysopt_basic_negate	Global	Negates CLI configured by Sysopt_basic.
Sysopt_clear_all	Global	Negates all the CLIs configured by Sysopt.
Sysopt_noproxyarp	Global	Uses the sysopt command to provide the following exa...
Sysopt_noproxyarp_negate	Global	Negates CLI configured by Sysopt_noproxyarp.
Sysopt_Preserve_Vpn_Flow	Global	Uses the sysopt command to configure sysopt preserve ...
Sysopt_Preserve_Vpn_Flow_Negate	Global	Negates the CLI pushed through Sysopt_Preserve_Vpn_...
Sysopt_Reclassify_Vpn	Global	Uses the sysopt command to configure sysopt reclassify...
Sysopt_Reclassify_Vpn_Negate	Global	Negates CLI configured by Sysopt_Reclassify_Vpn Flex-...
TCP_Embryonic_Conn_Limit	Global	TCP Embryonic Connection Settings

inline_image_0.png

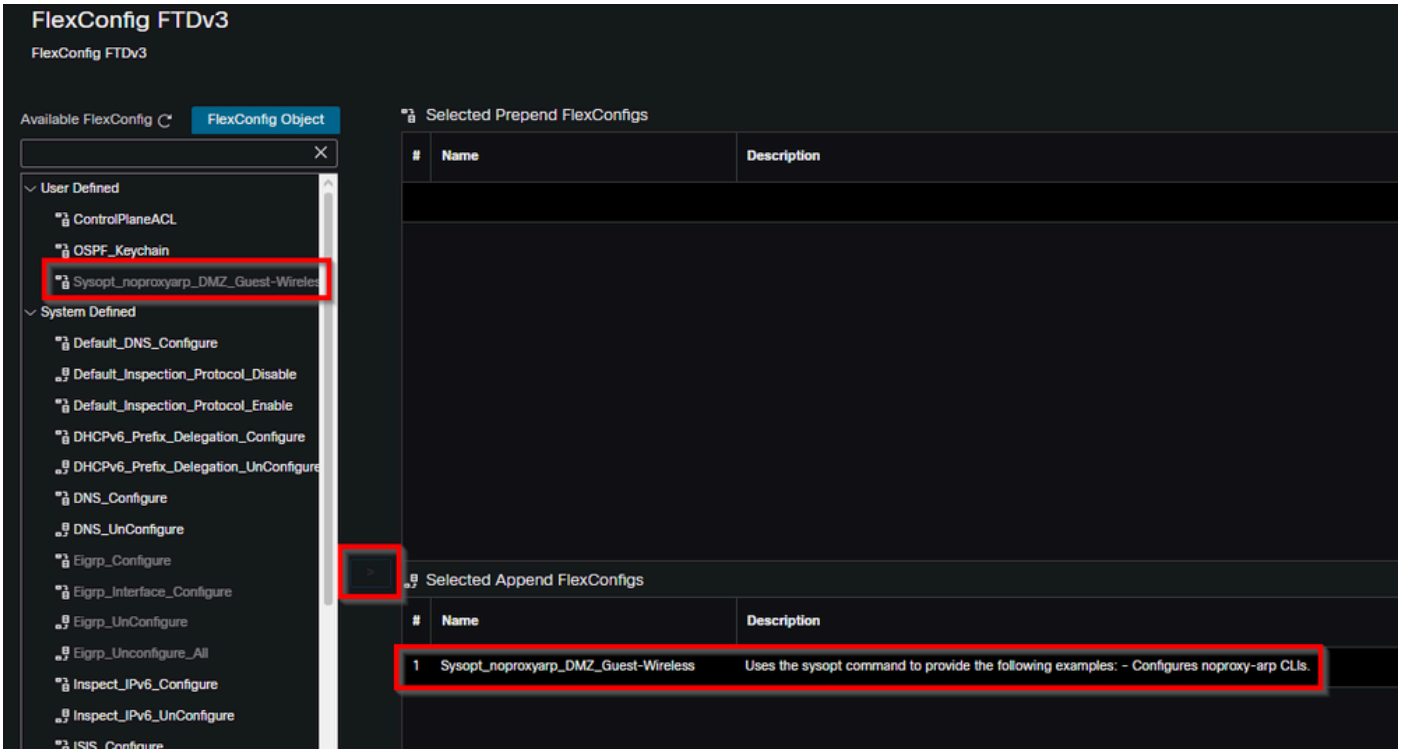
2: Add the configuration command to the FlexConfig policy **sysopt noproxyarp IFNAME**:



inline_image_1.png

Replace **IFNAME** with the actual name of your affected interface.

3: Associate the new object to the FlexConfig policy of the FTD and deploy it through FMC. The configuration is applied to disable Proxy ARP behavior on the specified interface.



inline_image_2.png

4: After deployment, test the static IP assignment on the affected host. The firewall must no longer be able to
respond to ARP probes for unassigned IP addresses, allowing hosts to successfully use their static IP configurations

When applicable, consider disabling Proxy ARP at the NAT rule level rather than interface-
wide to minimize unintended impact on other network functions. This provides more granular control over Proxy AR

Cause

Proxy Address Resolution Protocol (Proxy ARP) was enabled on the FTD interface, causing the firewall to respond
Proxy ARP functionality was responding with its own MAC address when hosts performed gratuitous ARP requests

Related Content

- Cisco Technical Support & Downloads