使用FlexConfig在FTD介面上停用代理ARP

問題

FTD介面上的主機無法使用靜態分配的IP位址，並在回落到169.254.x.x位址之前報告「重複的IP位址」錯誤。封包擷取分析顯示，當主機為自己的IP位址傳送無償ARP（ARP探測）時，防火牆會回應宣告對該IP位址的所有權，因此防止靜態IP分配成功。

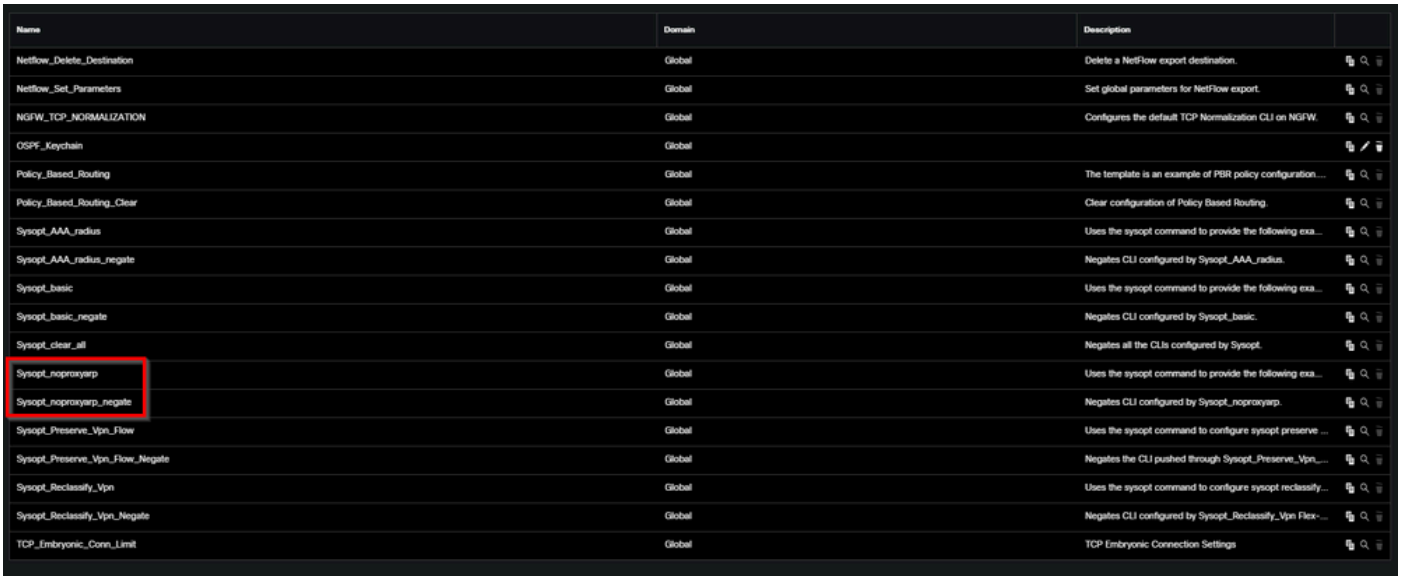
環境

- 執行FTD軟體版本7.4.4的Cisco安全防火牆2120（適用於所有版本和型號）
- 適用於裝置管理的思科安全防火牆管理中心(FMC)
- 預設情況下，FTD上啟用代理ARP。

解析

通過使用通過FMC部署的FlexConfig策略，在受影響的介面上禁用代理ARP可以解決此問題。這可防止防火牆響應其未明確擁有的IP地址的ARP探測。

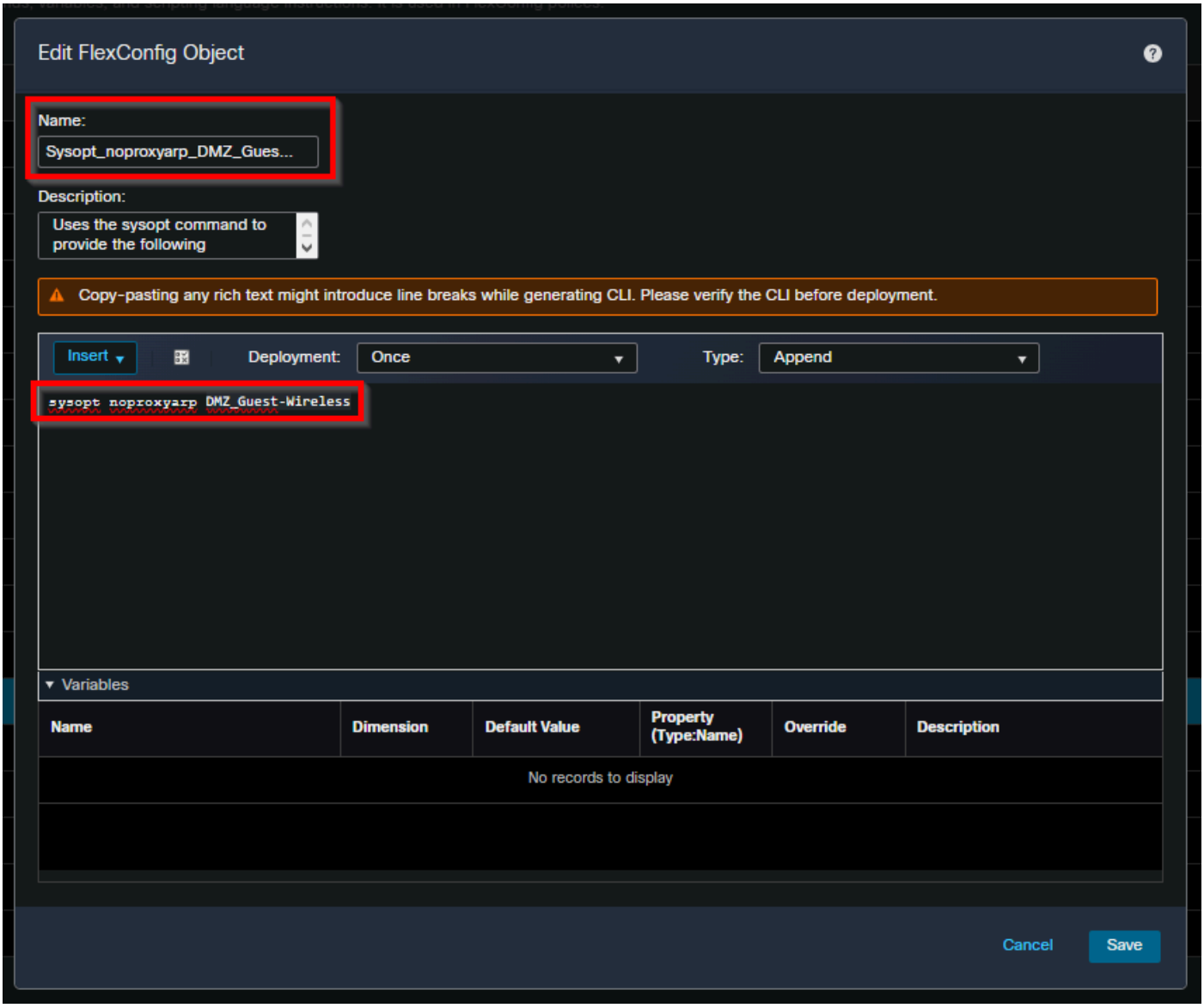
1：導航到FMC中的FlexConfig部分，建立新的FlexConfig策略以禁用特定介面上的代理ARP。Sysopt_noproxyarp和否定的Sysopt_noproxyarp_negate是FMC中的預設對象，可以克隆供自定義使用。



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

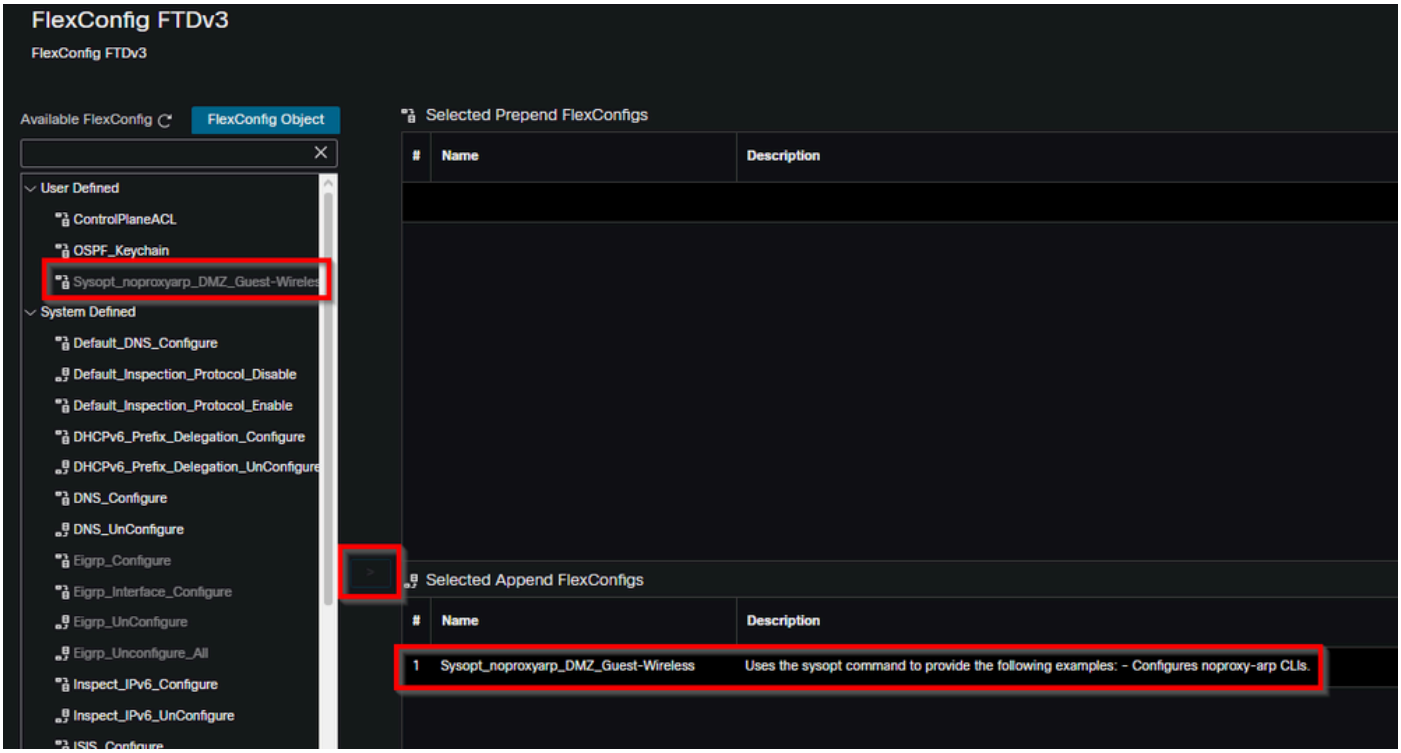
2：將配置命令新增到FlexConfig policy sysopt noproxyarp IFNAME:



inline_image_1.png

用受影響介面的實際名稱替換IFNAME。

3：將新對象關聯到FTD的FlexConfig策略，並通過FMC進行部署。應用該配置可禁用指定介面上的代理ARP行為。



inline_image_2.png

4：部署後，測試受影響主機上的靜態IP分配。防火牆必須無法再響應未分配IP地址的ARP探測，從而允許主機成功使用其靜態IP配置，而不會出現重複的IP地址錯誤。

如果適用，請考慮在NAT規則級別而不是在介面範圍禁用代理ARP，以最小化對其他網路功能的意外影響。這樣可以更精細地控制代理ARP行為。

原因

在FTD介面上啟用代理位址解析通訊協定（代理ARP），導致防火牆回應針對其未明確擁有的IP位址的ARP探測。此行為導致主機在靜態位址分配期間偵測到重複的IP位址情況。當主機執行無償ARP要求時，防火牆代理ARP功能會以自己的MAC位址回應，因此看起來好像所需IP位址已被其他裝置使用。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。