

# 使用FlexConfig在FTD接口上禁用代理ARP

## 问题

FTD接口上的主机无法使用静态分配的IP地址并报告“重复的IP地址”错误，然后回退到169.254.x.x地址。数据包捕获分析显示，当主机为自己的IP地址发送无偿ARP（ARP探测）时，防火墙会响应声明该IP地址的所有权，从而阻止静态IP分配成功。

## 环境

- 运行FTD软件版本7.4.4的Cisco Secure Firewall 2120（适用于所有版本和型号）
- 用于设备管理的思科安全防火墙管理中心(FMC)
- 默认情况下，代理ARP在FTD上启用。

## 分辨率

通过使用通过FMC部署的FlexConfig策略，在受影响的接口上禁用代理ARP即可解决此问题。这可防止防火墙响应其未明确拥有的IP地址的ARP探测。

1：导航到FMC中的FlexConfig部分，创建新的FlexConfig策略以禁用特定接口上的代理ARP。Sysopt\_noproxyarp和否定的Sysopt\_noproxyarp\_negate是FMC中的默认对象，可以克隆以供自定义使用。

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 reclassif...
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 : 将配置命令添加到FlexConfig策略sysopt noproxyarp IFNAME:

### Edit FlexConfig Object

**Name:**  
Sysopt\_noproxyarp\_DMZ\_Gues...

**Description:**  
Uses the sysopt command to provide the following

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

**Insert** **Deployment:** Once **Type:** Append

```
sysopt noproxyarp DMZ_Guest-Wireless
```

▼ Variables

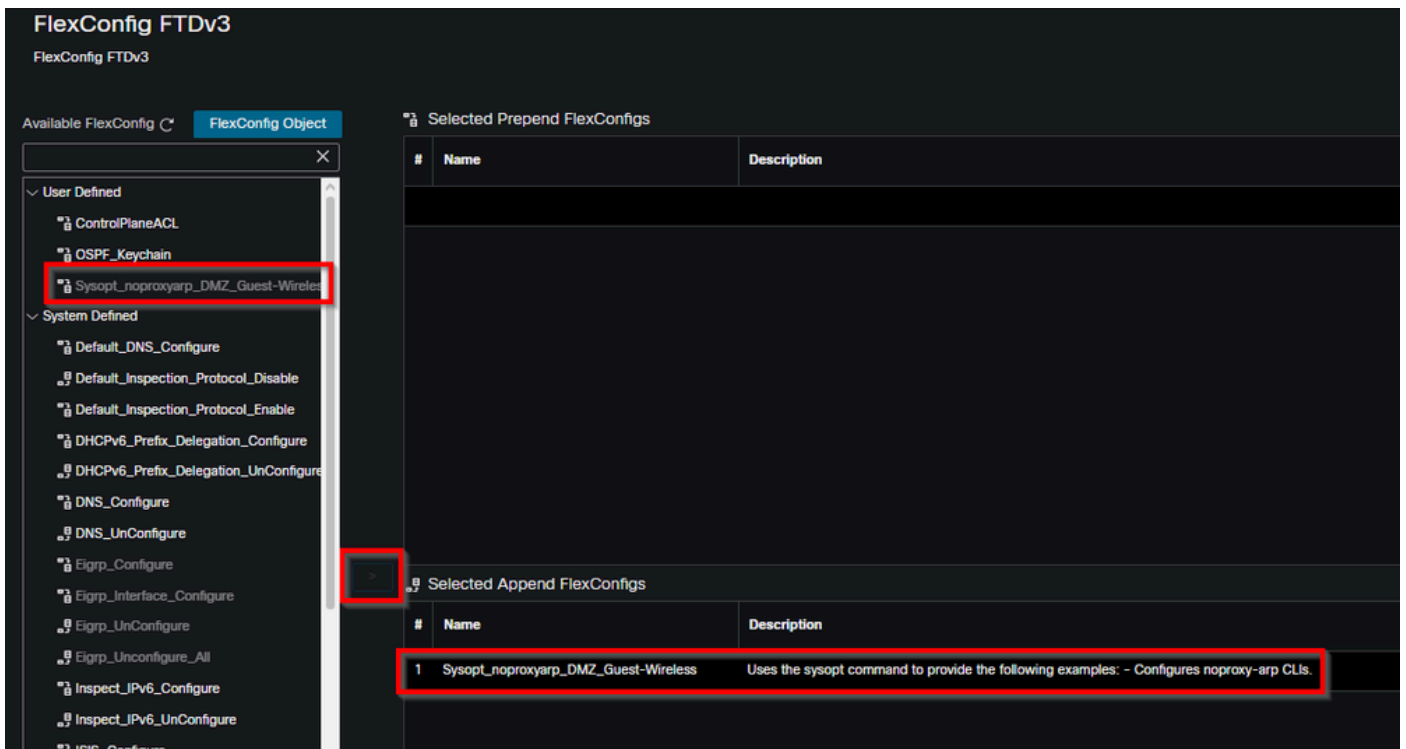
Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

Cancel Save

inline\_image\_1.png

用受影响接口的实际名称替换IFNAME。

3：将新对象关联到FTD的FlexConfig策略并通过FMC进行部署。应用此配置可禁用指定接口上的代理ARP行为。



inline\_image\_2.png

4：部署后，测试受影响主机上的静态IP分配。防火墙必须无法再响应未分配IP地址的ARP探测，从而允许主机成功使用其静态IP配置，而不会出现重复IP地址错误。

如果适用，请考虑在NAT规则级别而不是在接口范围内禁用代理ARP，以最大程度地减少对其他网络功能的意外影响。这样可以对代理ARP行为进行更精细的控制。

## 原因

在FTD接口上启用了代理地址解析协议（代理ARP），导致防火墙响应针对其未明确拥有的IP地址的ARP探测。此行为导致主机在静态地址分配期间检测到重复的IP地址条件。当主机执行无偿ARP请求时，防火墙代理ARP功能将使用自己的MAC地址进行响应，使其看起来好像所需IP地址已被其他设备使用。

## 相关内容

- [思技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。