FlexConfigを使用したFTDインターフェイスでのプロキシARPの無効化

お問い合わせ内容

FTDインターフェイス上のホストは、169.254.x.xアドレスにフォールバックする前に、静的に割り当てられたIPアドレスを使用できず、「重複IPアドレス」エラーを報告します。 パケットキャプチャの分析により、ホストが自分のIPアドレスのgratuitous ARP（ARPプローブ）を送信すると、ファイアウォールがそのIPアドレスの所有権を主張して応答するため、スタティックIP割り当てが正常に行われないことがわかります。

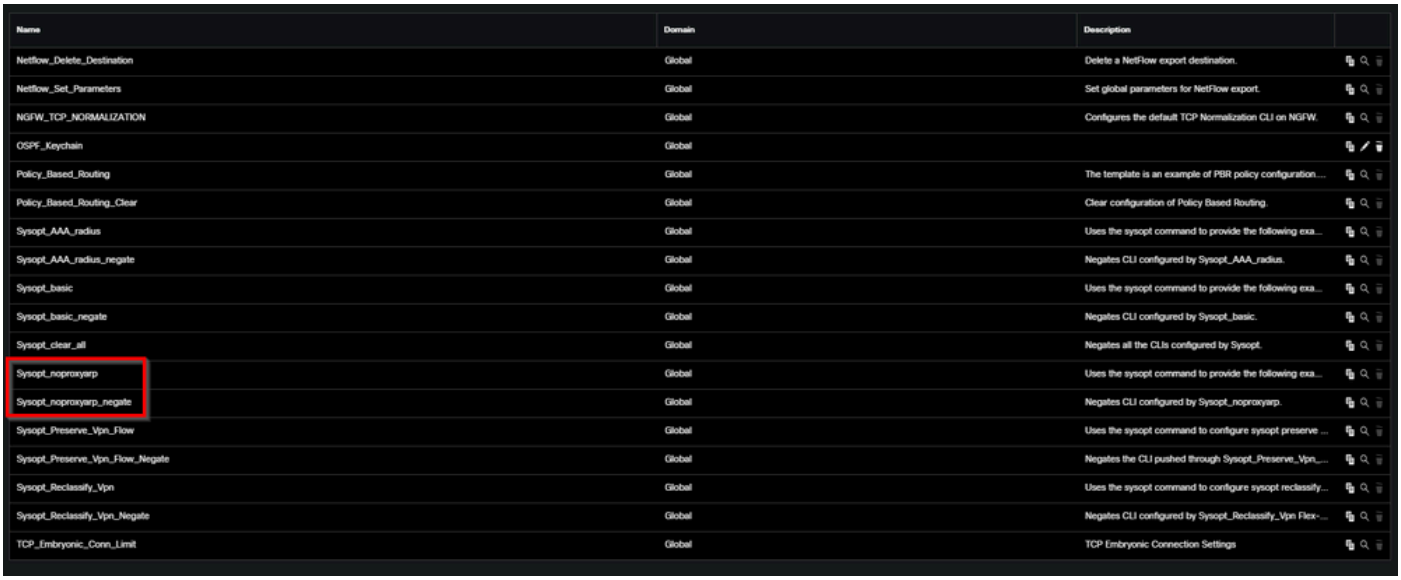
環境

- FTDソフトウェアバージョン7.4.4を実行しているCisco Secure Firewall 2120（すべてのバージョンとモデルに適用可能）
- デバイス管理用Cisco Secure Firewall Management Center(FMC)
- FTDではデフォルトでプロキシARPが有効になっています。

解決策

この問題は、FMCを介して導入されたFlexConfigポリシーを使用して、該当するインターフェイスのプロキシARPを無効にすることで解決されます。 これにより、明示的に所有していないIPアドレスのARPプローブにファイアウォールが応答しなくなります。

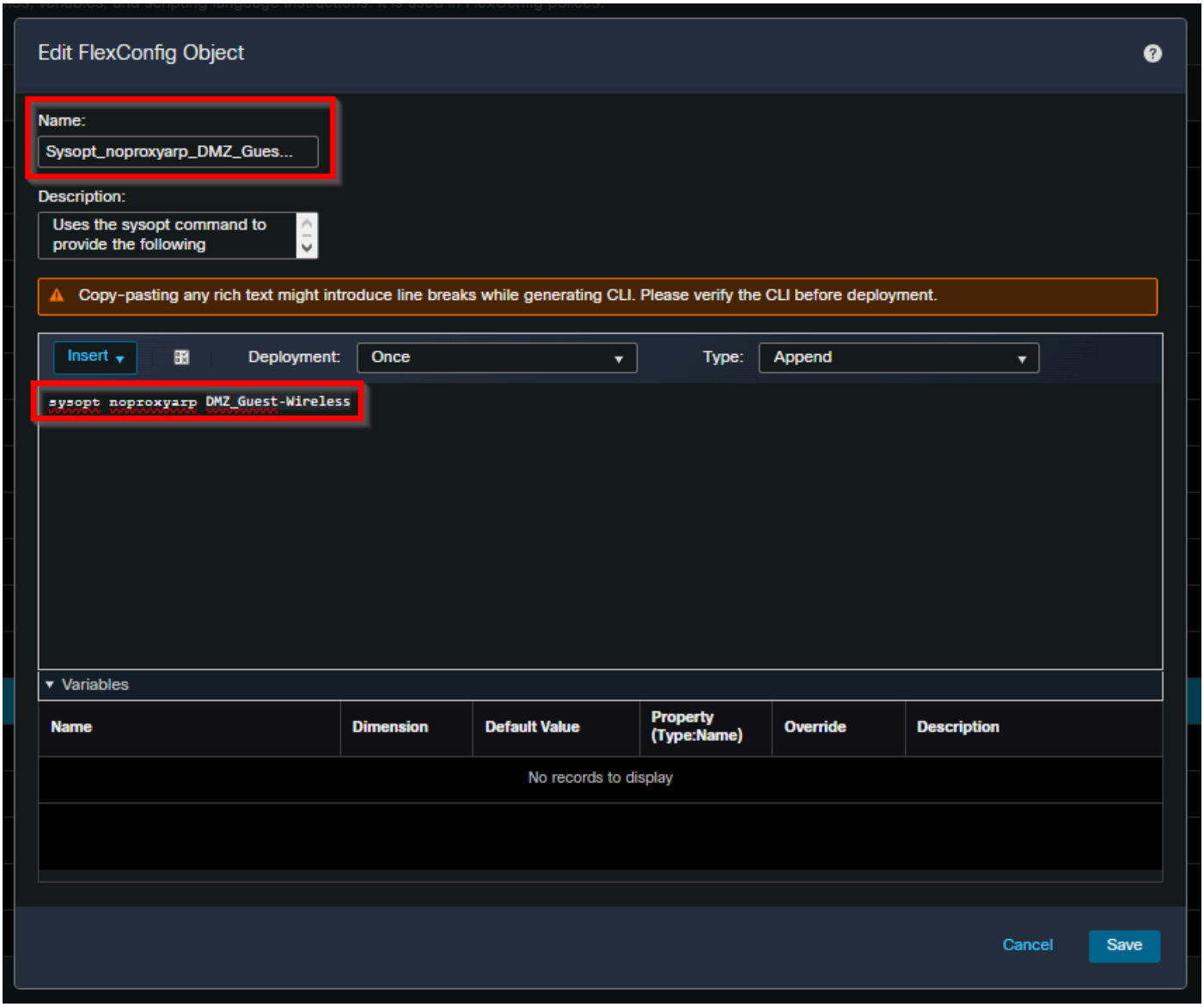
1:FMCのFlexConfigセクションに移動し、新しいFlexConfigポリシーを作成して特定のインターフェイスでプロキシARPを無効にします。 Sysopt_noproxyarpと否定Sysopt_noproxyarp_negateはFMCのデフォルトオブジェクトであり、カスタム使用のためにクローンを作成できます。



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 (インラインイメージ_0.png)

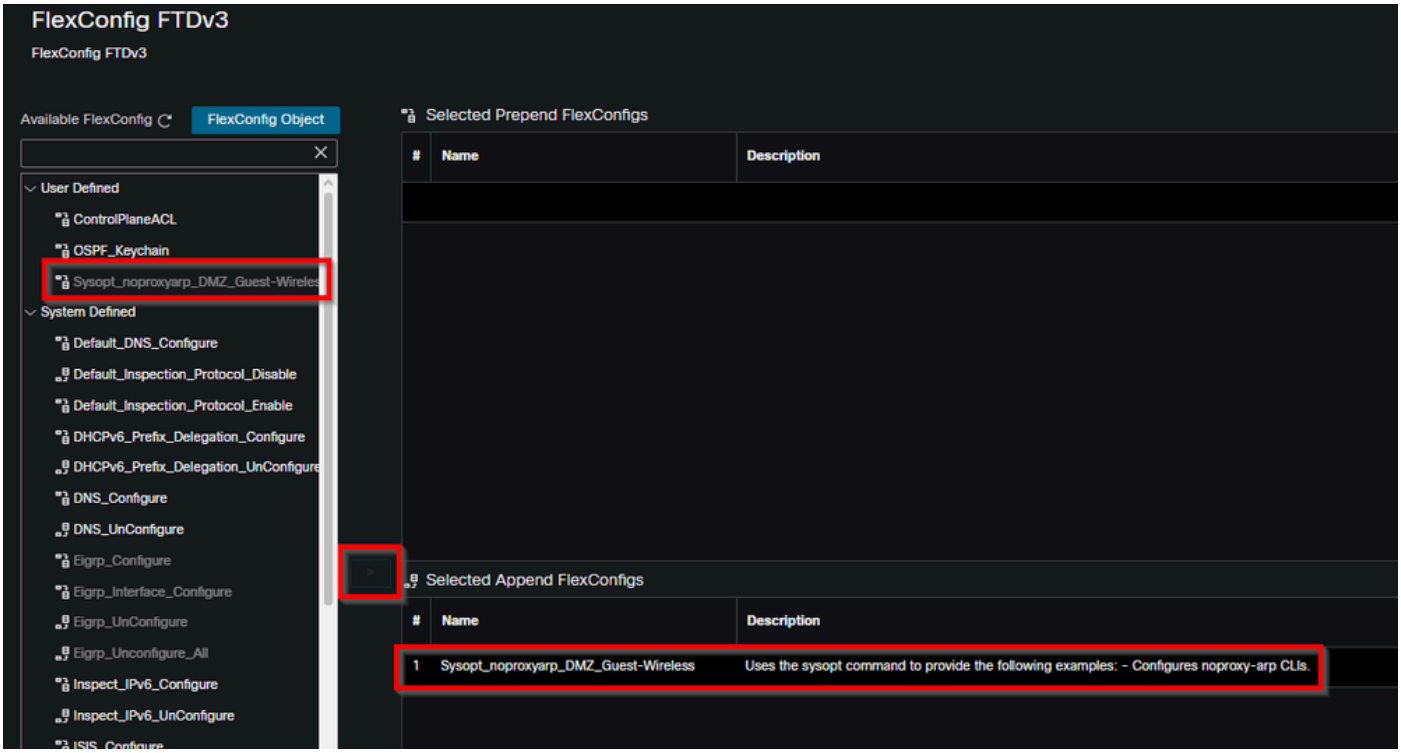
2: FlexConfigポリシーsysopt noproxyarp IFNAMEに設定コマンドを追加します。



inline_image_1.pngファイル

IFNAMEは該当するインターフェイスの実際の名前で置き換えます。

3：新しいオブジェクトをFTDのFlexConfigポリシーに関連付け、FMCを介して展開します。 この設定は、指定したインターフェイスでプロキシARPの動作を無効にするために適用されます。



inline_image_2.pngファイル

4：導入後、影響を受けるホストでスタティックIP割り当てをテストします。 ファイアウォールは、割り当てられていないIPアドレスのARPプローブに応答できなくなり、ホストがスタティックIP設定を使用しても、IPアドレスの重複エラーは発生しません。

必要に応じて、他のネットワーク機能への意図しない影響を最小限にするために、プロキシARPをインターフェイス全体ではなくNATルールレベルで無効にすることを検討してください。 これにより、プロキシARPの動作をより詳細に制御できます。

原因

プロキシARP（Proxy Address Resolution Protocol；アドレス解決プロトコル）がFTDインターフェイスで有効にされていたため、ファイアウォールが明示的に所有していないIPアドレスのARPプローブに応答する原因となっていました。 この動作により、ホストはスタティックアドレスの割り当て中に重複IPアドレスの状態を検出しました。 ホストがgratuitous ARP要求を実行すると、ファイアウォールプロキシARP機能は自身のMACアドレスで応答し、目的のIPアドレスが別のデバイスですでに使用されているように見せかけました。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。