Deaktivieren von Proxy-ARP an FTD-Schnittstellen mithilfe von FlexConfig

Problem

Hosts auf einer FTD-Schnittstelle können statisch zugewiesene IP-Adressen nicht verwenden und Fehler bei "doppelten IP-Adressen" melden, bevor sie auf 169.254.x.x-Adressen zurückgreifen. Die Paketerfassungsanalyse zeigt, dass die Firewall, wenn der Host einen überflüssigen ARP (ARP-Test) für seine eigene IP-Adresse sendet, reagiert und den Besitz dieser IP-Adresse beansprucht, wodurch eine erfolgreiche statische IP-Zuweisung verhindert wird.

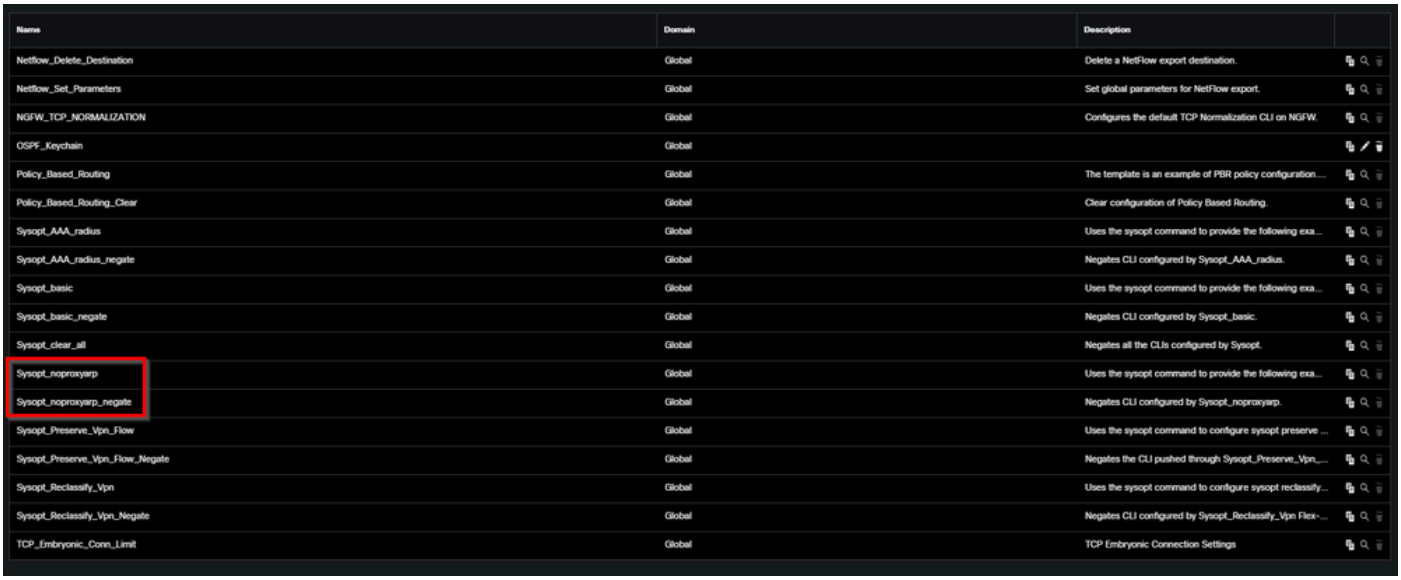
Umwelt

- Cisco Secure Firewall 2120 mit FTD-Software, Version 7.4.4 (für alle Versionen und Modelle)
- Cisco Secure Firewall Management Center (FMC) für das Gerätemanagement
- Proxy-ARP ist auf FTD standardmäßig aktiviert.

Auflösung

Das Problem wird behoben, indem der Proxy-ARP auf der betroffenen Schnittstelle mithilfe einer FlexConfig-Richtlinie deaktiviert wird, die über FMC bereitgestellt wird. Dadurch wird verhindert, dass die Firewall auf ARP-Tests für IP-Adressen reagiert, die ihr nicht explizit gehören.

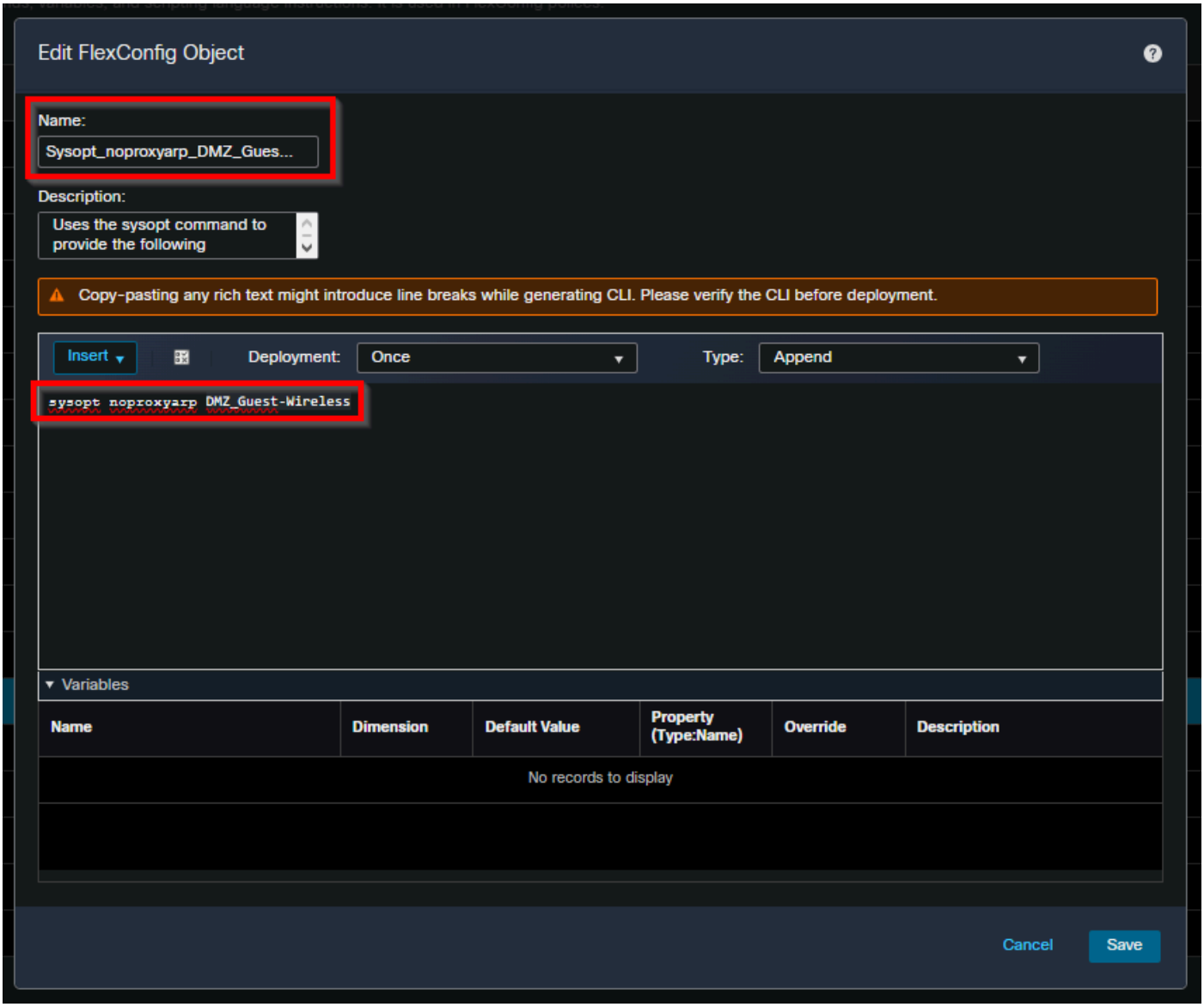
1: Navigieren Sie zum Abschnitt "FlexConfig" in FMC, und erstellen Sie eine neue FlexConfig-Richtlinie, um das Proxy-ARP auf der spezifischen Schnittstelle zu deaktivieren. Sysopt_noproxyarp und das negierende Sysopt_noproxyarp_negate sind Standardobjekte im FMC und können für die benutzerdefinierte Verwendung geklont werden.



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

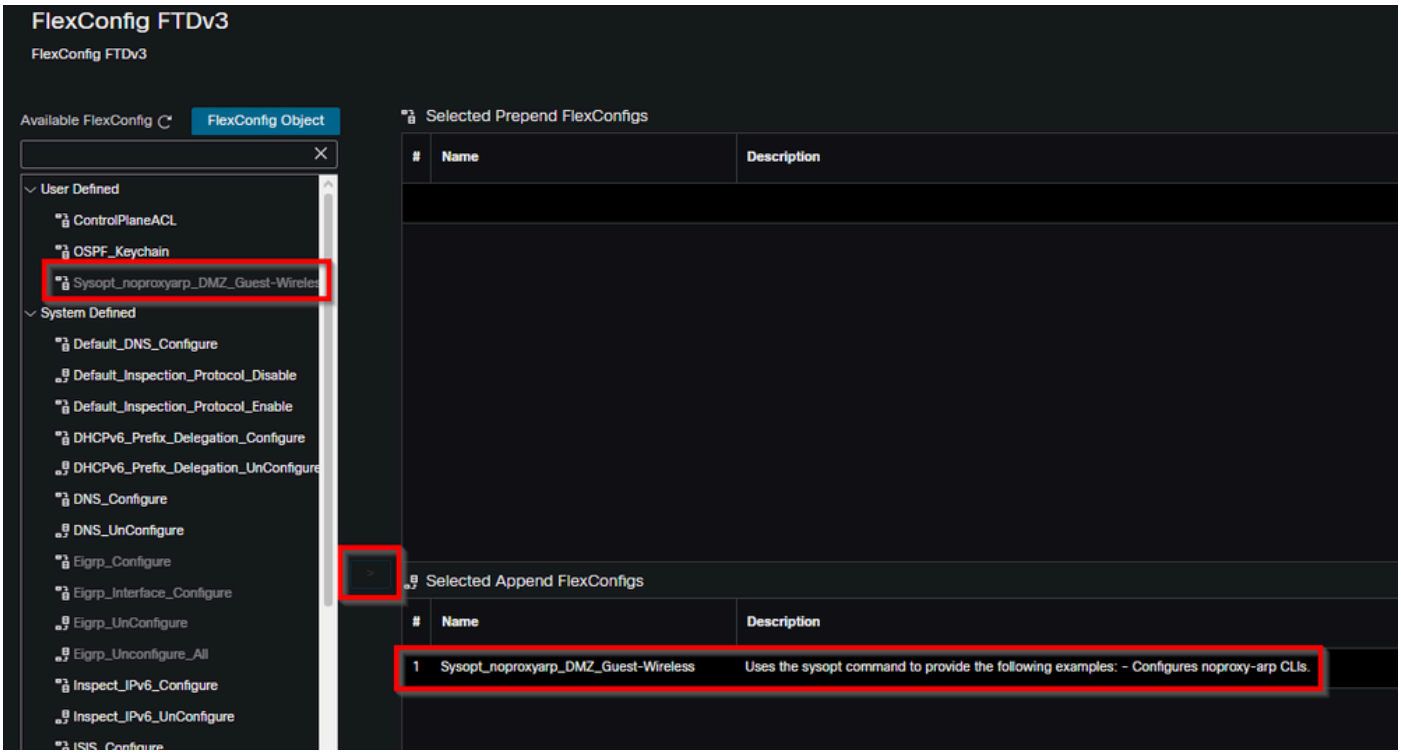
2: Fügen Sie den Konfigurationsbefehl der FlexConfig-Richtlinie sysopt noproxyarp IFNAME hinzu:



inline_image_1.png

Ersetzen Sie IFNAME durch den tatsächlichen Namen der betroffenen Schnittstelle.

3: Ordnen Sie das neue Objekt der FlexConfig-Richtlinie des FTD zu, und stellen Sie es über FMC bereit. Die Konfiguration wird angewendet, um das Proxy-ARP-Verhalten auf der angegebenen Schnittstelle zu deaktivieren.



inline_image_2.png

4: Testen Sie nach der Bereitstellung die statische IP-Zuweisung auf dem betroffenen Host. Die Firewall darf nicht mehr auf ARP-Tests für nicht zugewiesene IP-Adressen reagieren, sodass Hosts ihre statischen IP-Konfigurationen ohne Fehler bei doppelten IP-Adressen erfolgreich verwenden können.

Wenn zutreffend, sollten Sie das Proxy-ARP auf NAT-Regelebene und nicht auf der gesamten Schnittstelle deaktivieren, um unbeabsichtigte Auswirkungen auf andere Netzwerkfunktionen zu minimieren. Dies ermöglicht eine detailliertere Kontrolle des Proxy-ARP-Verhaltens.

Ursache

Das Proxy Address Resolution Protocol (Proxy ARP) wurde auf der FTD-Schnittstelle aktiviert, wodurch die Firewall auf ARP-Tests für IP-Adressen reagierte, die ihr nicht explizit gehörten.

Dieses Verhalten führte dazu, dass Hosts während der Zuweisung statischer Adressen eine doppelte IP-Adressbedingung erkannten. Die Firewall-Proxy-ARP-Funktion reagierte mit ihrer eigenen MAC-Adresse, wenn Hosts überflüssige ARP-Anfragen durchführten, sodass es so aussah, als ob die gewünschte IP-Adresse bereits von einem anderen Gerät verwendet wurde.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.