Disabilita ARP proxy sulle interfacce FTD tramite FlexConfig

Problema

Gli host su un'interfaccia FTD non sono in grado di utilizzare indirizzi IP assegnati in modo statico e di segnalare errori di "indirizzo IP duplicato" prima di eseguire il fallback a indirizzi 169.254.x.x. L'analisi dell'acquisizione dei pacchetti rivela che quando l'host invia un ARP gratuito (sonda ARP) per il proprio indirizzo IP, il firewall risponde rivendicando la proprietà di tale indirizzo IP, impedendo la riuscita dell'assegnazione statica dell'IP.

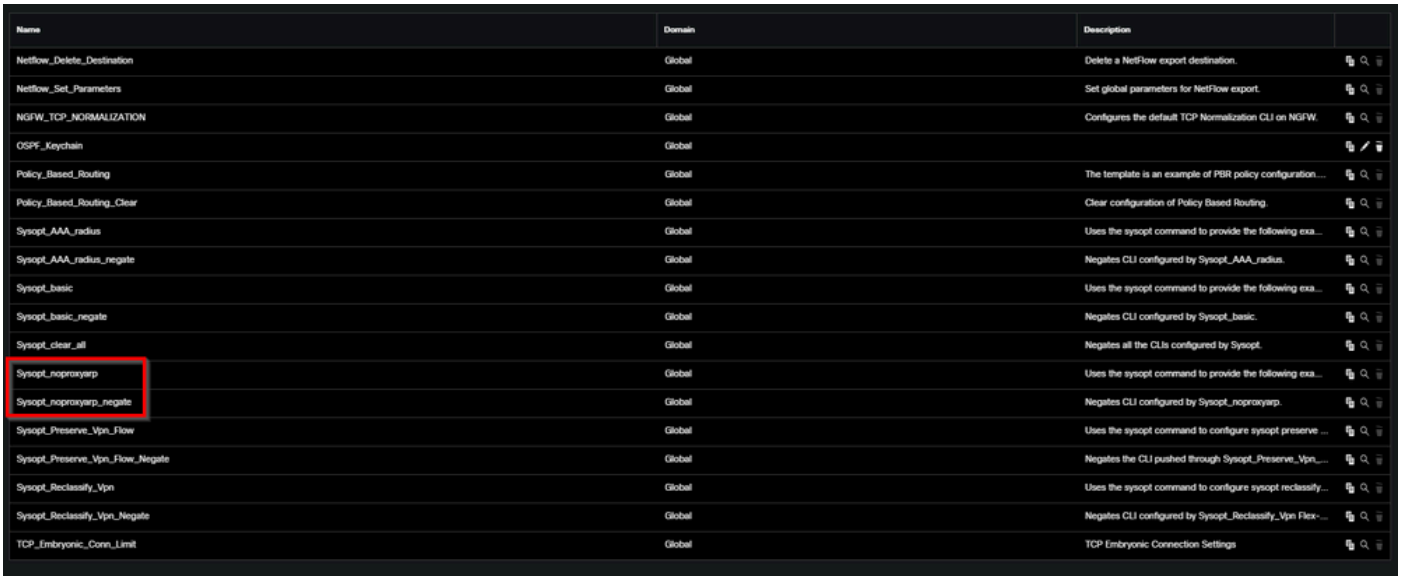
Ambiente

- Cisco Secure Firewall 2120 con software FTD versione 7.4.4 (applicabile a tutte le versioni e i modelli)
- Cisco Secure Firewall Management Center (FMC) per la gestione dei dispositivi
- ARP proxy abilitato su FTD per impostazione predefinita.

Risoluzione

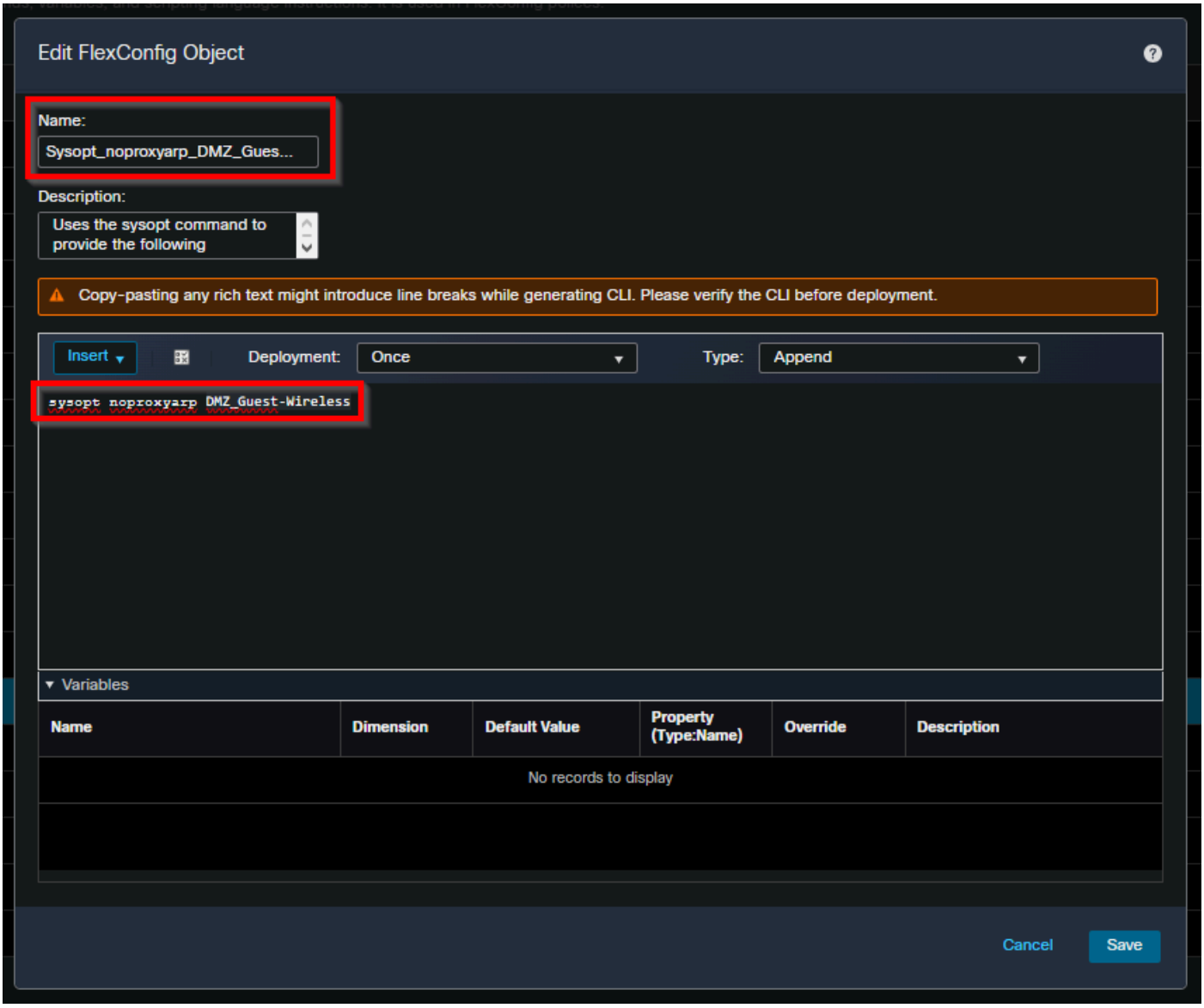
Il problema viene risolto disabilitando ARP proxy sull'interfaccia interessata utilizzando un criterio FlexConfig distribuito tramite FMC. In questo modo il firewall non risponde alle richieste ARP per gli indirizzi IP di cui non è esplicitamente proprietario.

1: Passare alla sezione FlexConfig in FMC e creare un nuovo criterio FlexConfig per disabilitare l'ARP proxy nell'interfaccia specifica. Sysopt_noproxyarp e Sysopt_noproxyarp_negate in negazione sono oggetti predefiniti in FMC e possono essere clonati per un utilizzo personalizzato.



inline_image_0.png

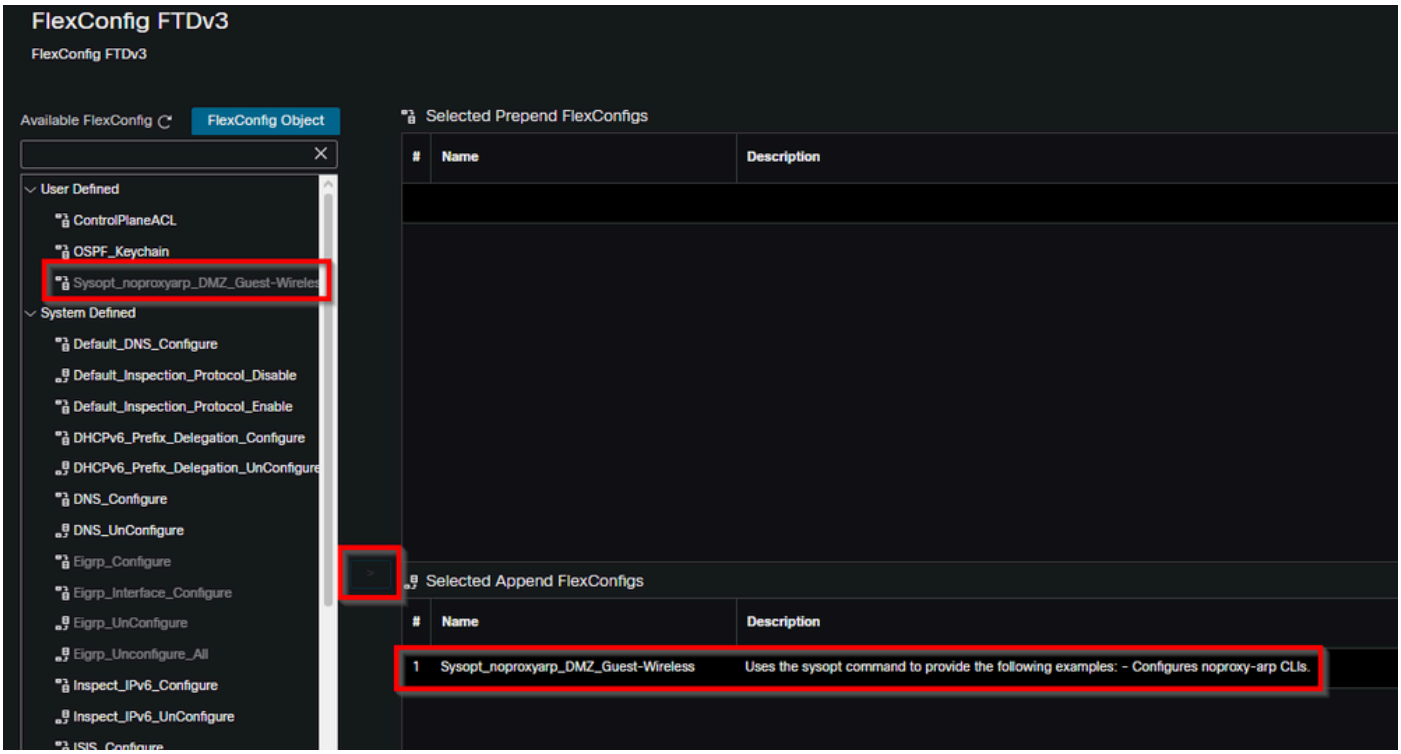
2: Aggiungere il comando di configurazione al criterio FlexConfig sysopt noproxyarp NOMEIF:



inline_image_1.png

Sostituire IFNAME con il nome effettivo dell'interfaccia interessata.

3: Associare il nuovo oggetto al criterio FlexConfig di FTD e distribuirlo tramite FMC. La configurazione viene applicata per disabilitare il comportamento ARP proxy sull'interfaccia specificata.



inline_image_2.png

4: Dopo la distribuzione, verificare l'assegnazione IP statico sull'host interessato. Il firewall non deve più essere in grado di rispondere alle richieste ARP per gli indirizzi IP non assegnati, consentendo agli host di utilizzare correttamente le proprie configurazioni IP statiche senza errori di indirizzi IP duplicati.

Se applicabile, valutare la possibilità di disabilitare ARP proxy a livello di regola NAT anziché a livello di interfaccia per ridurre al minimo l'impatto indesiderato su altre funzioni di rete. In questo modo si ottiene un controllo più granulare del comportamento di ARP proxy.

Causa

Il protocollo ARP (Proxy Address Resolution Protocol) è stato abilitato sull'interfaccia FTD. Di conseguenza, il firewall risponde alle richieste ARP per gli indirizzi IP di cui non è proprietario in modo esplicito. A causa di questo comportamento, gli host rilevano una condizione di indirizzo IP duplicata durante l'assegnazione degli indirizzi statici. La funzionalità ARP del proxy del firewall

rispondeva con il proprio indirizzo MAC quando gli host eseguivano richieste ARP gratuite, facendo sembrare che l'indirizzo IP desiderato fosse già in uso da un altro dispositivo.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).