# FlexConfig를 사용하여 FTD 인터페이스에서 프록시 ARP 비활성화

## 문제

FTD 인터페이스의 호스트는 정적으로 할당된 IP 주소를 사용할 수 없으며 169.254.x.x 주소로 돌아가기 전에 "중복 IP 주소" 오류를 보고할 수 없습니다. 패킷 캡처 분석을 통해 호스트가 자체 IP 주소에 대해 불필요한 ARP(ARP 프로브)를 보내면 방화벽이 해당 IP 주소의 소유권을 주장하는 응답을 하게 되므로, 고정 IP 할당이 제대로 수행되지 않습니다.

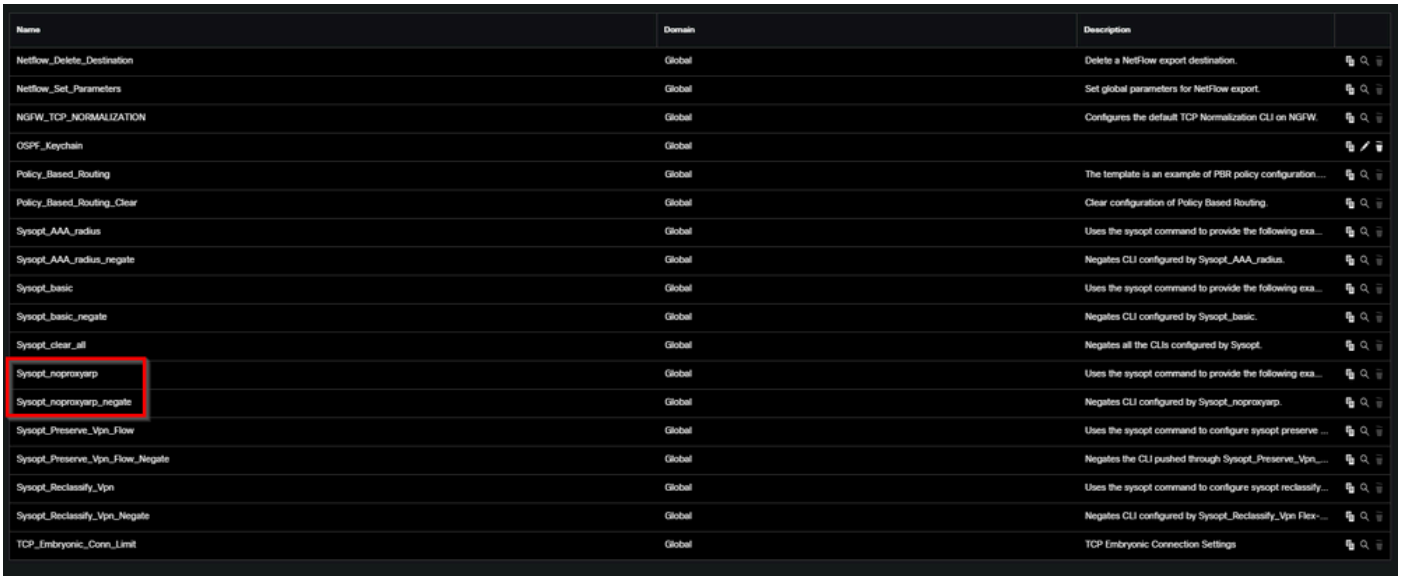
## 환경

- FTD 소프트웨어 버전 7.4.4를 실행하는 Cisco Secure Firewall 2120(모든 버전 및 모델에 적용 가능)
- 장치 관리를 위한 Cisco FMC(Secure Firewall Management Center)
- 프록시 ARP는 기본적으로 FTD에서 활성화되어 있습니다.

## 해결

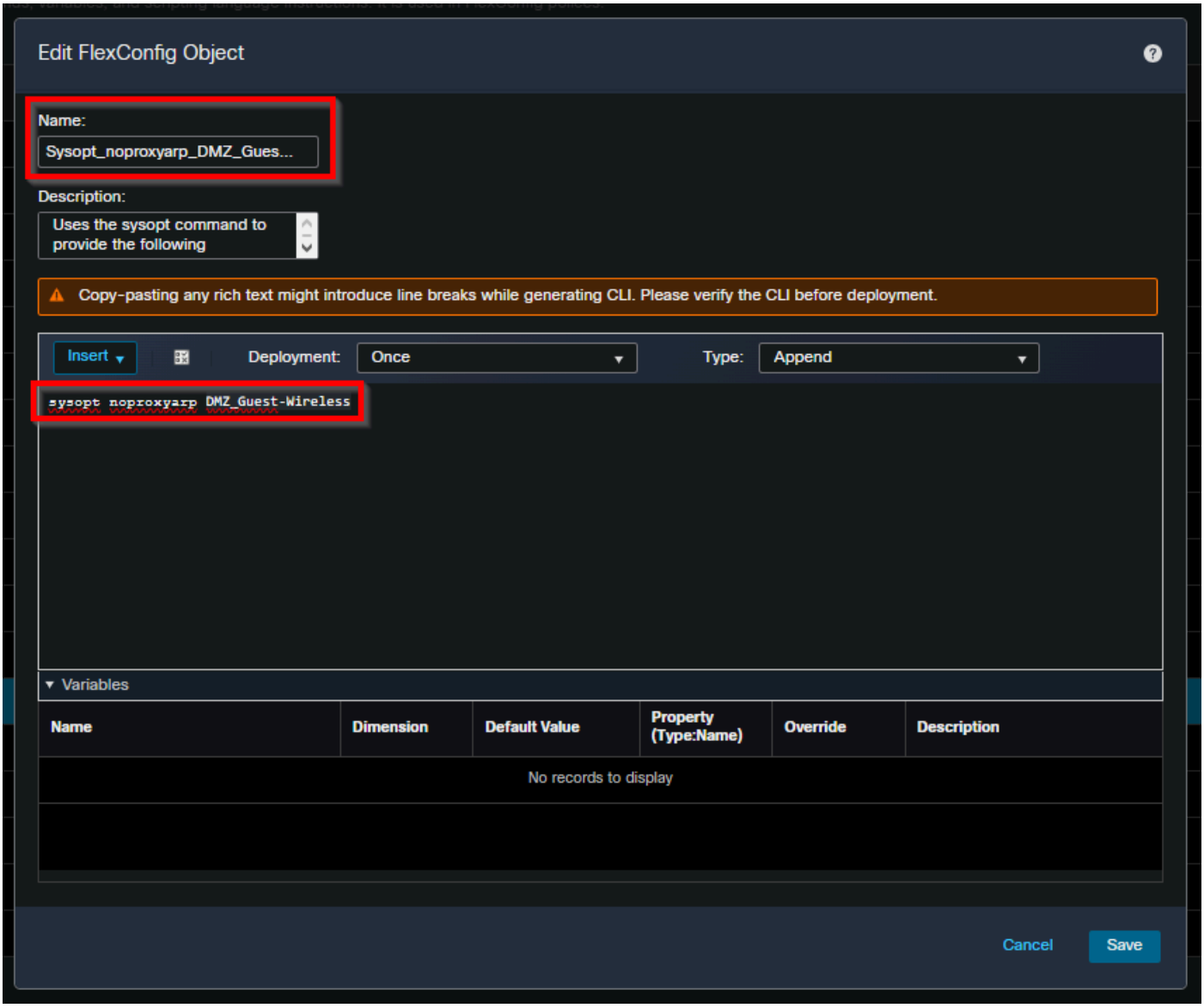
이 문제는 FMC를 통해 배포된 FlexConfig 정책을 사용하여 영향을 받는 인터페이스에서 프록시 ARP를 비활성화함으로써 해결됩니다. 따라서 방화벽이 명시적으로 소유하지 않는 IP 주소에 대한 ARP 프로브에 응답하지 않습니다.

1: FMC의 FlexConfig 섹션으로 이동하여 새 FlexConfig 정책을 생성하여 특정 인터페이스에서 프록시 ARP를 비활성화합니다. Sysopt_noproxyarp 및 부정 Sysopt_noproxyarp_negate는 FMC의 기본 개체이며 사용자 정의 사용을 위해 복제할 수 있습니다.




inline_image_0.png

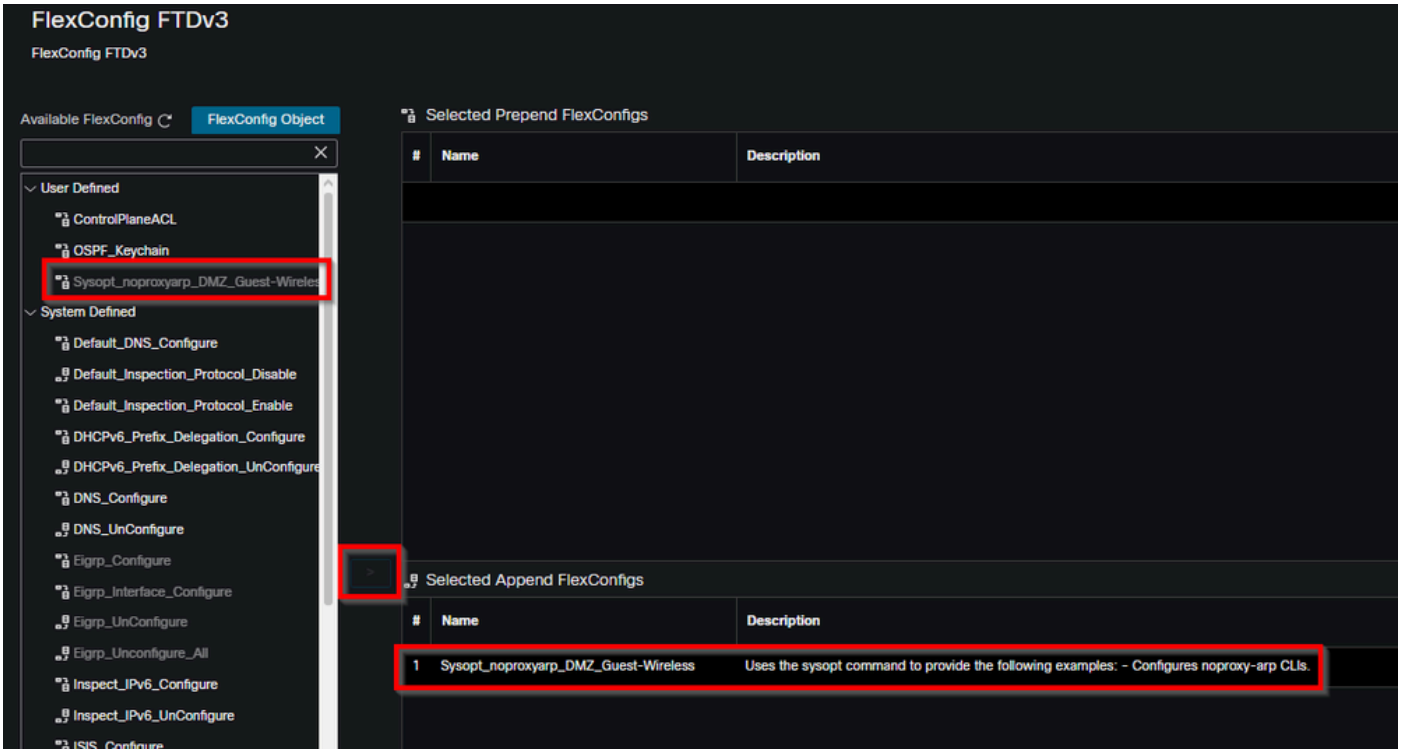
2: FlexConfig 정책 sysopt noproxyarp IFNAME에 configuration 명령을 추가합니다.




인라인 이미지_1.png

IFNAME을 영향을 받는 인터페이스의 실제 이름으로 대체합니다.

3: 새 개체를 FTD의 FlexConfig 정책에 연결하고 FMC를 통해 배포합니다. 지정된 인터페이스에서 프록시 ARP 동작을 비활성화하도록 구성이 적용됩니다.




inline_image_2.png

4: 배포 후 영향을 받는 호스트에서 고정 IP 할당을 테스트합니다. 방화벽은 더 이상 할당되지 않은 IP 주소에 대한 ARP 프로브에 응답할 수 없어야 하며, 따라서 호스트에서 중복 IP 주소 오류 없이 고정 IP 구성을 성공적으로 사용할 수 있습니다.

해당되는 경우 다른 네트워크 기능에 대한 의도하지 않은 영향을 최소화하기 위해 인터페이스 전반이 아닌 NAT 규칙 레벨에서 프록시 ARP를 비활성화하는 것이 좋습니다. 그러면 프록시 ARP 동작을 보다 세밀하게 제어할 수 있습니다.

## 원인

프록시 ARP(Address Resolution Protocol)가 FTD 인터페이스에서 활성화되었으므로 방화벽이 명시적으로 소유하지 않은 IP 주소에 대한 ARP 프로브에 응답했습니다. 이로 인해 고정 주소 할당 중에 호스트에서 중복된 IP 주소 조건을 감지했습니다. 호스트가 불필요한 ARP 요청을 수행할 때 방화벽 프록시 ARP 기능은 고유한 MAC 주소로 응답하므로, 원하는 IP 주소가 다른 디바이스에서 이미 사용되고 있는 것처럼 보입니다.

## 관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.