# DNS 검사가 활성화된 상태에서 FTD를 통과하지 못한 대규모 UDP DNS 응답 확인

## 목차

## 문제

트래픽이 Cisco FTD(Firepower Threat Defense) 방화벽을 통해 서로 다른 VLAN의 VM 간에 이동할 경우 패킷 크기가 큰(약 1800-4000바이트) DNS 패킷이 실패합니다. 방화벽을 통과하지 않고 동일한 VLAN의 VM 간에 통신이 발생할 경우 동일한 DNS 트래픽이 성공합니다. 트러블슈팅 중에 프래그먼트된 DNS 응답 패킷이 FTD 방화벽에 의해 완전히 리어셈블되고 있으며, 이그레스 아웃될 때 클라이언트의 MTU 기능을 초과하는 하나의 큰 패킷으로 전송되어 클라이언트가 패킷을 삭제하는 것이 발견되었습니다.

## 환경

- 제품군: Cisco Secure Firewall 4200 Series에서 처음으로 확인되는 것처럼, 다른 플랫폼도 영향을 받을 수 있습니다.
- 소프트웨어 버전: FTD 소프트웨어 버전 7.6.2.1에서 처음으로 볼 수 있는 다른 소프트웨어 버전도 영향을 받을 수 있습니다.
- 방화벽 인터페이스 MTU는 9000바이트입니다.
- DNS 검사가 활성화되었습니다.
- 표준 1500바이트 MTU로 구성된 영향을 받는 클라이언트 시스템.
- 대규모 SRV 레코드 쿼리에 대한 조각화된 응답을 생성하는 DNS 서버입니다.

## 해결

방화벽 인터페이스 MTU 컨피그레이션을 조정하여 문제를 해결했습니다. 이러한 접근 방식을 사용

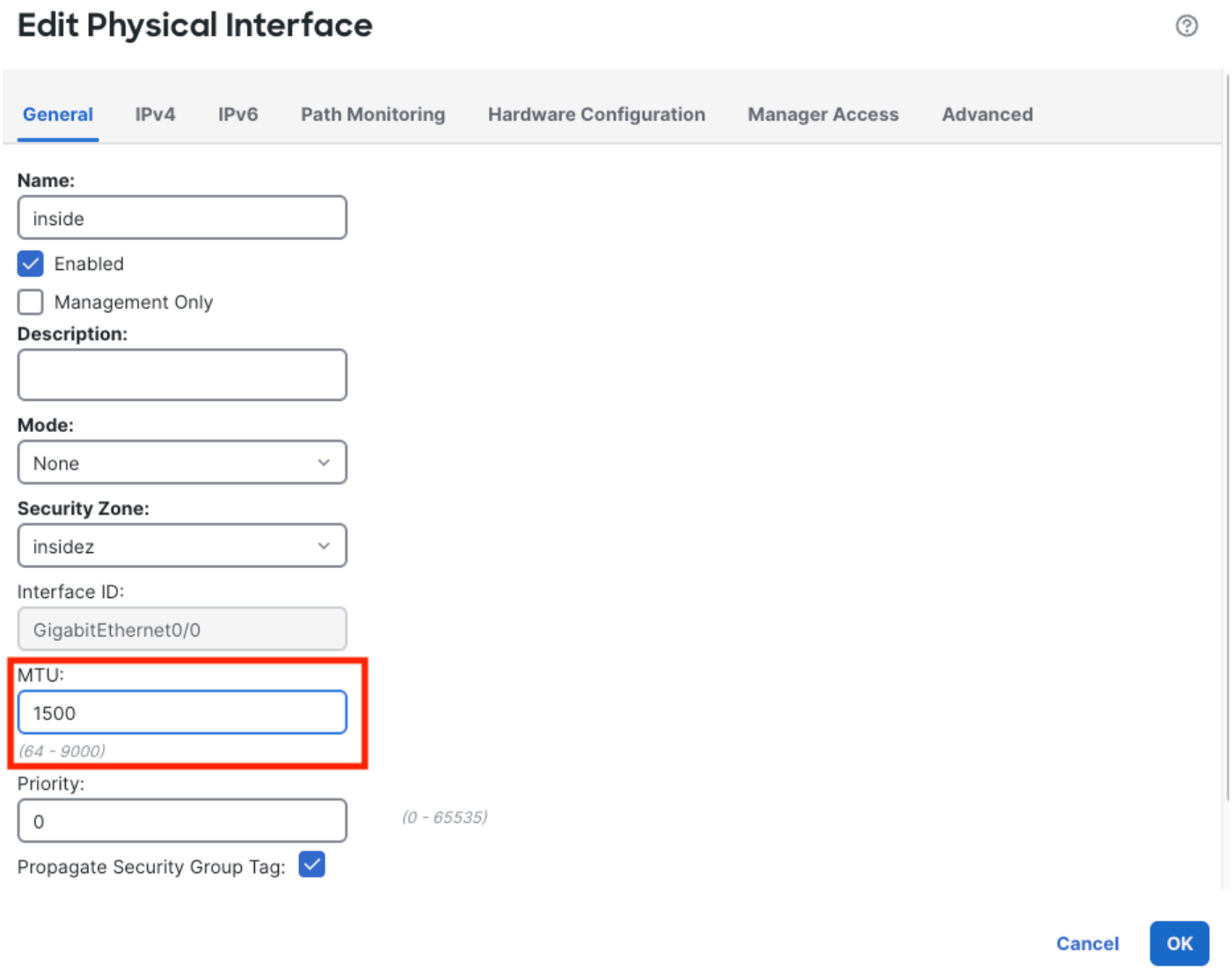
하여 이 문제를 해결할 수 있습니다.

## 옵션 1: 다른 네트워크 디바이스에서 허용하는 경우 인터페이스 MTU를 1500으로 조정(권장)

리어셈블된 패킷의 적절한 리프래그먼트화를 보장하려면 방화벽 이그레스 인터페이스 MTU를 9000바이트에서 1500바이트로 변경합니다.

```
ASA:
device# configure terminal
device(config)# interface gigabitethernet0/0
device(config-if)# mtu 1500
device(config-if)# exit

FTD:
Change MTU from FMC GUI
```




MTU 컨피그레이션을 확인합니다.

```
device# show interface gigabitethernet0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is i82580 rev03, BW 1000000 Kbit, DLY 10 usec
  Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
  Available but not configured via nameif
  MAC address 0050.56bb.09c8, MTU 1500
```

## 옵션 2: DNS 검사 비활성화(대체 해결 방법, 권장하지 않음)

---

참고: 보안 요구 사항에 따라 DNS 검사를 비활성화할 수 있으며 방화벽이 경계 방화벽이 아닌 경우 정책 맵에서 DNS 검사를 비활성화하는 것을 고려해 볼 수 있습니다. (DNS 트래픽이

---

많은 경우 총 연결 수도 증가할 수 있습니다.)

```
ASA:
device# configure terminal
device(config)# policy-map global_policy
device(config-pmap)# class inspection_default
device(config-pmap-c)# no inspect dns
device(config-pmap-c)# exit

FTD:
> configure inspection dns disable
```

### 확인 단계

확인을 구현한 후 DNS 기능을 확인합니다.

큰 응답으로 DNS 확인 테스트:

```
dig @dns_server_ip _ldap._tcp.domain.com SRV
```

방화벽 패킷 처리 모니터링:

```
Collect packet packets on ingress and egress interface to analyse in WireShark
```

## 원인

FTD에서 DNS 검사가 활성화되면 방화벽 라이나는 프래그먼트된 DNS 패킷의 전체 리어셈블리를 수행하여 검사 엔진(Snort)이 전체 DNS 페이로드를 검사할 수 있도록 합니다. 검사 후 이그레스 인터페이스 MTU가 리어셈블된 패킷 크기보다 큰 경우 방화벽은 패킷을 다시 프래그먼트하지 않고 하나의 큰 프레임으로 전달합니다.

9000바이트의 MTU로 구성된 방화벽 인터페이스에서는 리어셈블된 DNS 응답(약 1884바이트)을 단일 패킷으로 전송할 수 있습니다. 그러나 클라이언트 시스템은 표준 MTU 1500바이트로 구성되었으며 이러한 큰 패킷을 수락할 수 없으므로 트래픽이 손실됩니다.

리어셈블된 패킷 크기보다 큰 인터페이스 MTU 설정으로 lina에서 DNS 검사가 활성화된 경우 이 동작이 예상됩니다.

- 리나 DNS 검사: 심층 패킷 검사를 위해 전체 리어셈블리를 수행합니다. 자세한 내용은 이 DOC 결함 CSCwv66007을 참조하십시오.
- Snort 3: 물리적 리어셈블리 없이 검사를 위해 논리적(가상) 리어셈블리를 수행합니다.

## 관련 콘텐츠

- Cisco 기술 지원 및 다운로드
- CSCwv66007(DOC:Clarify ASA/FTD fragmentation reassembly behavior with enabled policy-map feature that reassemble full reassembly)

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.