在啟用DNS檢查的情況下，解析無法通過FTD的大型UDP DNS響應

目錄

問題

當流量透過思科Firepower威脅防禦(FTD)防火牆在不同VLAN中的虛擬機器之間傳輸時，具有大封包大小（約1800-4000位元組）的DNS封包會失敗。相同VLAN中的VM之間發生通訊時，相同DNS流量會成功，但不通過防火牆。在疑難排解期間，發現分段的DNS回覆封包在退出時由FTD防火牆完全重組，且以超過使用者端MTU能力的單一大型封包形式傳送，導致使用者端捨棄封包。

環境

- 產品系列：第一次在思科安全防火牆4200系列上看到時，其他平台也可能會受到影響。
- 軟體版本:在FTD軟體版本7.6.2.1上首次顯示，其他軟體版本也可能受到影響。
- 防火牆介面MTU is 9000 bytes
- 已啟用DNS檢測。
- 配置了標準1500位元組MTU的受影響客戶端電腦。
- DNS伺服器為大型SRV記錄查詢生成分段響應。

解析

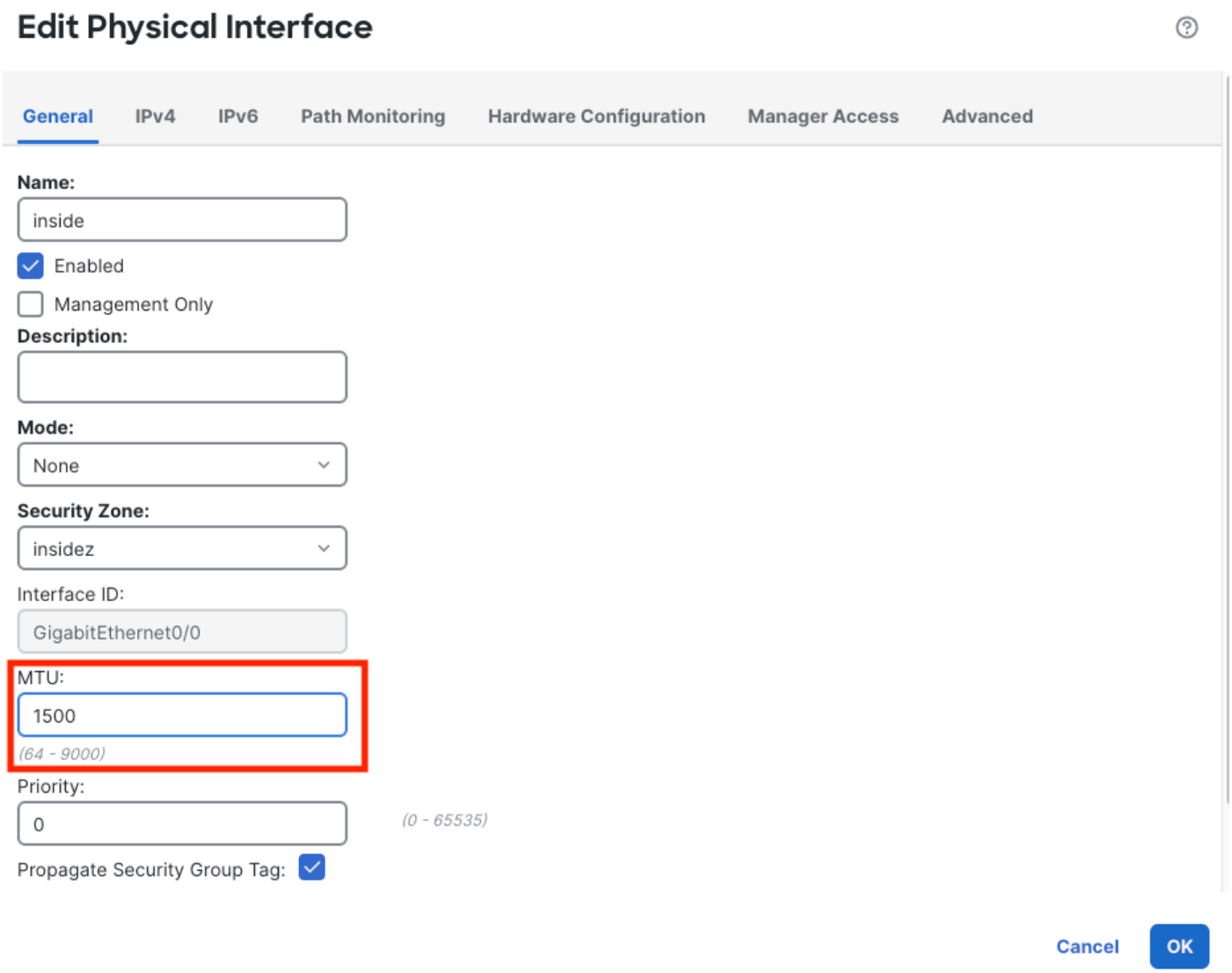
通過調整防火牆介面MTU配置解決了此問題。可以使用以下方法解決此問題：

選項 1:如果其他網路裝置允許，將介面MTU調整為1500（推薦）

將防火牆輸出介面MTU從9000變更為1500位元組，以確保重組封包正確重新分段：

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

FTD:
Change MTU from FMC GUI
```



驗證MTU設定：

```
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
```

選項 2:禁用DNS檢查（替代的解決方法，但不推薦）



附註：如果根據安全要求，可以接受禁用DNS檢查，並且防火牆不是邊界防火牆，則可以考慮從策略對映中禁用DNS檢查。（如果DNS流量高，這也可能增加總連線數）：

```
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
```

驗證步驟

實施解析後，驗證DNS功能：

測試具有大響應的DNS解析：

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

監控防火牆封包處理：

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

原因

在FTD上啟用DNS檢查時，防火牆lina會執行分段DNS封包的完整重組，允許檢查引擎(Snort)檢查完整的DNS負載。檢查後，如果輸出介面MTU大於重組後的資料包大小，防火牆會將資料包作為單個大型幀轉發，而不對其進行重新分段。

防火牆介面設定了9000位元組的MTU，允許重組的DNS回應（約1884位元組）作為單一封包傳輸。但是，使用標準MTU 1500位元組的使用者端機器無法接受這些較大的封包，因此導致流量捨棄。

當在介面MTU設定大於重組封包大小的lina上啟用DNS檢查時，預期會發生此行為。

- LINA DNS檢查：執行完全重組以進行深度資料包檢測。(有關詳細資訊，請參閱此DOC缺陷CSCwv66007。)
- Snort 3:執行邏輯（虛擬）重組以進行檢查，而無需物理重組。

相關內容

- 思科技術支援與下載
- CSCwv66007(DOC：使用已啟用且需要完全重組的策略對映功能闡明ASA/FTD分段重組行為)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。