DNSインスペクションが有効な場合にFTDで失敗する大きなUDP DNS応答を解決する

内容

問題

トラフィックがCisco Firepower Threat Defense(FTD)ファイアウォールを経由して異なるVLANのVM間を通過する場合、大きなパケットサイズ（約1800 ~ 4000バイト）のDNSパケットで障害が発生します。同じDNSトラフィックは、同じVLAN内のVM間でファイアウォールを通過せずに通信が行われると成功します。トラブルシューティング中、フラグメント化されたDNS応答パケットが出力される際にFTDファイアウォールによって完全に再構成され、クライアントのMTU機能を超える単一の大きなパケットとして送信されることが判明し、その結果、クライアントでパケットの廃棄が発生します。

環境

- 製品ファミリ：Cisco Secure Firewall 4200シリーズで初めて使用された他のプラットフォームも影響を受ける可能性があります。
- ソフトウェアバージョン：最初にFTDソフトウェアバージョン7.6.2.1で確認されたが、他のソフトウェアバージョンも影響を受ける可能性がある。
- ファイアウォールインターフェイスMTUが9,000バイト
- DNSインスペクションが有効になっています。
- 該当するクライアントマシンでは、標準の1500バイトのMTUが設定されています。
- 大規模なSRVレコードクエリに対する断片化された応答を生成するDNSサーバー。

解決方法

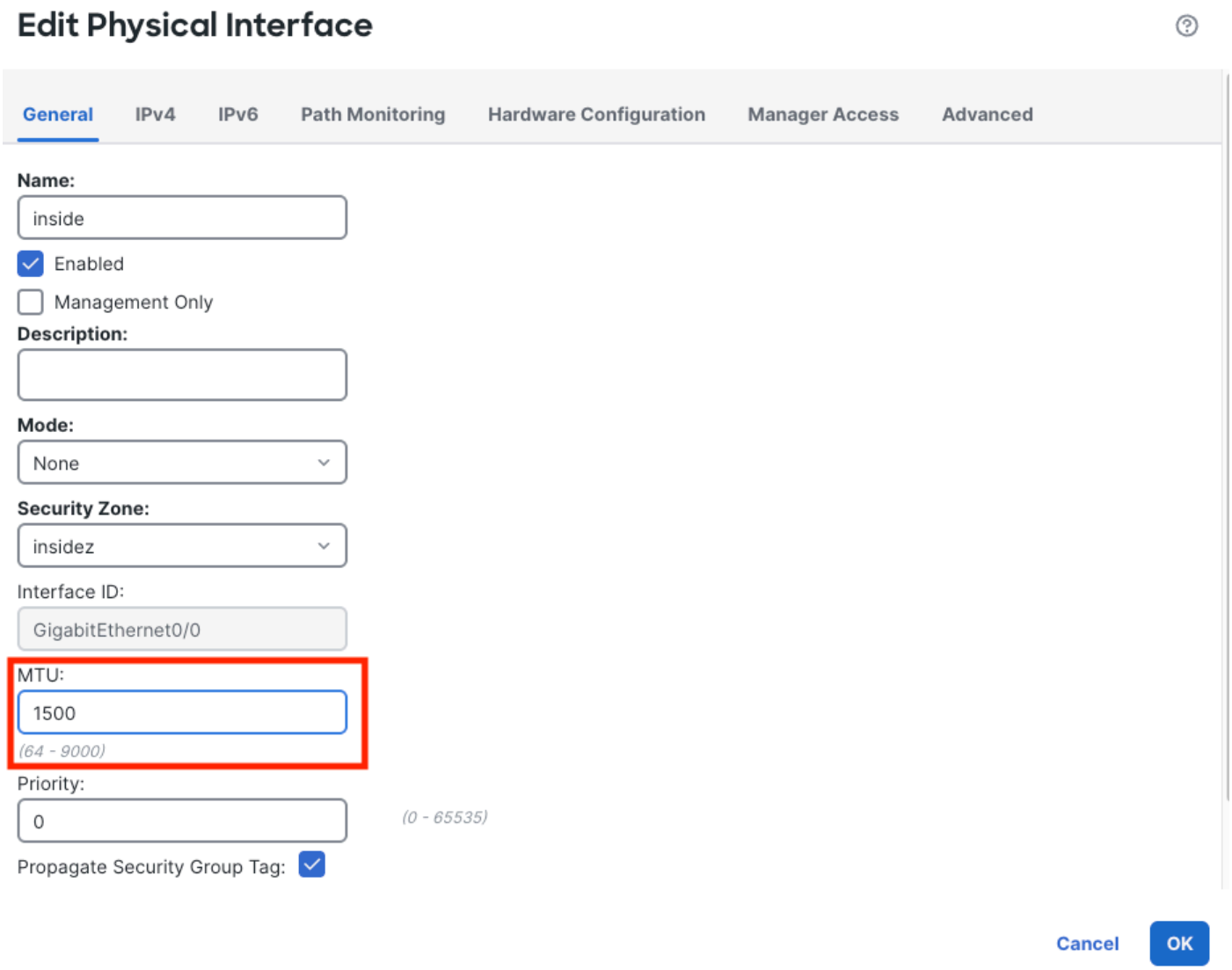
この問題は、ファイアウォールインターフェイスのMTU設定を調整することで解決されました。この問題に対処するには、次の方法を使用できます。

オプション1：他のネットワークデバイスで許可されている場合は、インターフェイスMTUを1500に調整する（推奨）

再アセンブルされたパケットが適切に再フラグメンテーションされるように、ファイアウォール出力インターフェイスMTUを9000バイトから1500バイトに変更します。

```
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設定を確認します。

```
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
```

オプション2:DNSインスペクションを無効にする（別の回避策があるが推奨されない）

注：セキュリティ要件に従ってDNSインスペクションを無効にしても構わない場合、およびファイアウォールが境界ファイアウォールではない場合は、ポリシーマップからDNSインスペクションを無効にすることを検討できます。（DNSトラフィックが多い場合は、これによって接続の総数が増えることもあります）。

```
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
```

確認手順

解決を実装したら、DNSの機能を確認します。

大きな応答でDNS解決をテストします。

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

ファイアウォールパケット処理の監視：

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

原因

FTDでDNSインスペクションが有効になっている場合、ファイアウォール回線はフラグメント化DNSパケットの完全なリアセンブルを実行し、インスペクションエンジン(Snort)が完全なDNSペイロードを検査できるようにします。インスペクション後に、出力インターフェイスのMTUが再構成されたパケットサイズよりも大きい場合、ファイアウォールはパケットを再フラグメント化

することなく1つの大きなフレームとして転送します。

9000バイトのMTUで設定されたファイアウォールインターフェイスにより、再構成されたDNS応答（約1884バイト）を単一パケットとして送信できます。ただし、クライアントマシンが標準MTUとして1500バイトに設定されているため、これらの大きなパケットを受け入れることができず、トラフィックが廃棄されます。

再構成されたパケットサイズよりも大きいインターフェイスMTU設定を持つ回線でDNSインスペクションが有効になっている場合は、この動作が予想されます。

- LINA DNSインスペクション：ディープパケットインスペクションの完全なリアセンブルを実行します。（詳細については、このDOCCSCwv66007を参照してください）。
- Snort 3：物理リアセンブリを行わずに、検査のための論理（仮想）リアセンブリを行う。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード
- CSCwv66007（DOC：完全な再構成を必要とするポリシーマップ機能を有効にした場合の、ASA/FTDフラグメンテーションの再構成の動作を明確化）

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。