在启用DNS检测的情况下，通过FTD解析失败的大型UDP DNS响应

目录

问题

当流量通过思科Firepower威胁防御(FTD)防火墙在不同的VLAN中的VM之间传输时，具有大数据包大小的DNS数据包（大约1800-4000字节）会失败。当同一VLAN中的VM之间发生通信而不通过防火墙时，同一DNS流量成功。在故障排除过程中，发现分片的DNS应答数据包在流出时由FTD防火墙完全重组，并以超过客户端MTU能力的单个大数据包的形式发送，从而导致客户端丢弃数据包。

环境

- 产品系列：首先在Cisco Secure Firewall 4200系列上看到，其他平台也会受到影响。
- 软件版本:在FTD软件版本7.6.2.1上首次发现，其他软件版本也可能受到影响。
- 防火墙接口MTU为9000字节
- 已启用DNS检测。
- 使用标准1500字节MTU配置的受影响客户端计算机。
- DNS服务器为大型SRV记录查询生成分段响应。

分辨率

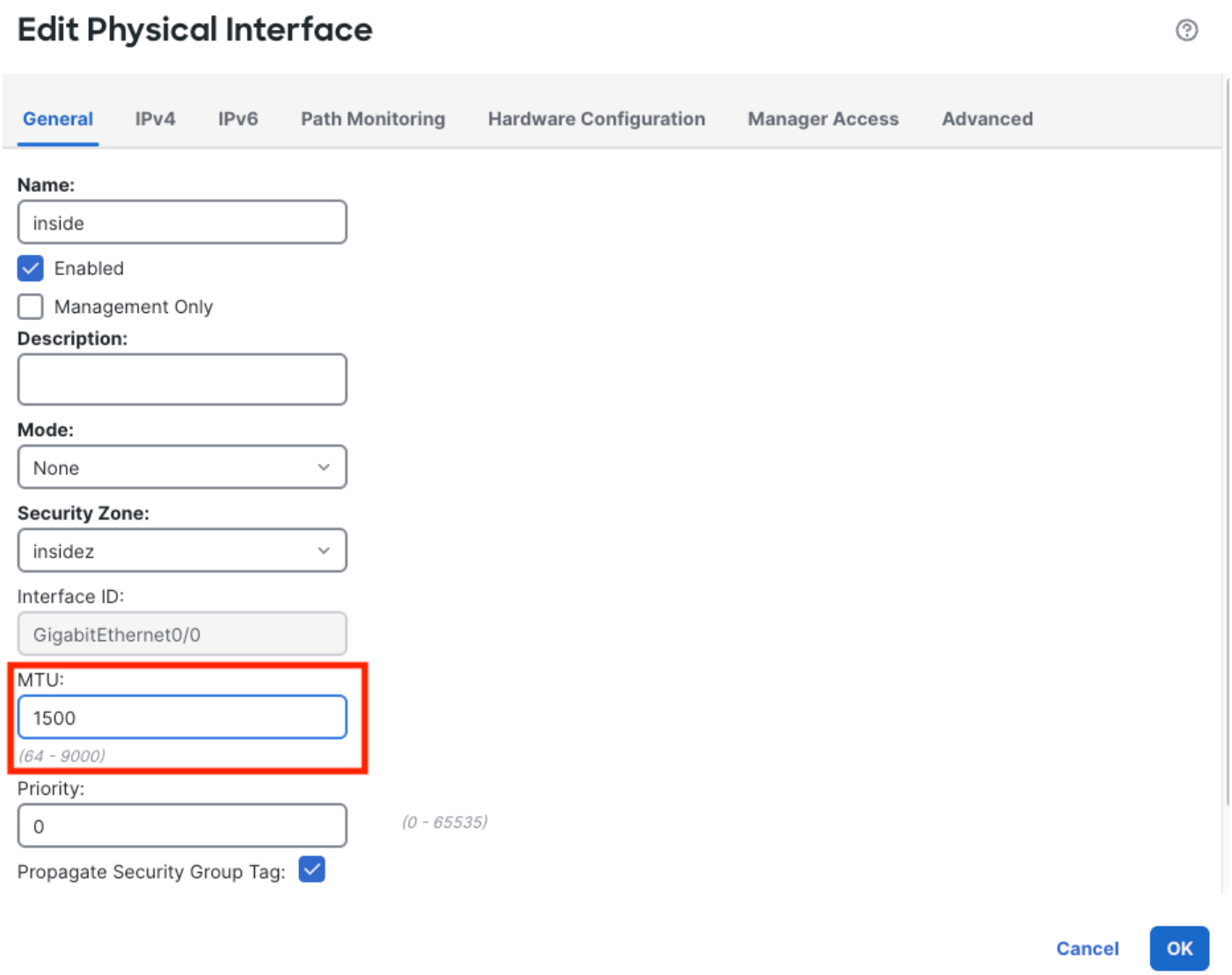
通过调整防火墙接口MTU配置解决了此问题。可以使用以下方法解决此问题：

选项 1：如果其他网络设备允许，将接口MTU调整为1500（推荐）

将防火墙出口接口MTU从9000字节更改为1500字节，以确保重新组合的数据包正确重新分段：

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

FTD:
Change MTU from FMC GUI
```



验证MTU配置：

```
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
```

选项 2：禁用DNS检测（不建议使用替代解决方法）



注意：如果根据安全要求可以禁用DNS检测，并且防火墙不是边界防火墙，则可以考虑从策略映射中禁用DNS检测。（如果DNS流量很高，这也可能增加总连接数）：

```
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
```

验证步骤

实施解析后，验证DNS功能：

测试具有大响应的DNS解析：

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

监控防火墙数据包处理：

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

原因

在FTD上启用DNS检查时，防火墙lina会对分段的DNS数据包执行完全重组，以允许检查引擎(Snort)检查完整的DNS负载。检查后，如果出口接口MTU大于重组的数据包大小，防火墙会将该数据包作为单个大型帧转发，而不对其进行重新分段。

防火墙接口配置了9000字节的MTU，允许重组的DNS响应（约1884字节）作为单个数据包进行传输。但是，配置了标准MTU 1500字节的客户端计算机无法接受这些较大的数据包，导致流量丢弃。

当在接口MTU设置大于重组数据包大小的lina上启用DNS检测时，预期出现此行为。

- LINA DNS检测：执行完全重组以进行深度数据包检测。（有关详细信息，请参阅此DOC缺陷CSCwv66007。）
- Snort 3:执行逻辑（虚拟）重组以进行检查，而无需物理重组。

相关内容

- 思科技术支持和下载
- CSCwv66007（DOC：使用需要完全重组的已启用策略映射功能明确ASA/FTD分段重组行为）

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。