Auflösung großer UDP-DNS-Antworten bei FTD mit aktivierter DNS-Inspektion

Inhalt

Problem

DNS-Pakete mit großen Paketen (etwa 1800-4000 Byte) schlagen fehl, wenn der Datenverkehr zwischen VMs in verschiedenen VLANs über eine Cisco FirePOWER Threat Defense (FTD)-Firewall verläuft. Derselbe DNS-Datenverkehr wird erfolgreich verarbeitet, wenn die Kommunikation zwischen VMs im selben VLAN stattfindet, ohne die Firewall zu passieren. Bei der Fehlerbehebung wurde festgestellt, dass fragmentierte DNS-Antwortpakete von der FTD-Firewall beim Auslagern vollständig wieder zusammengesetzt und als einzelne große Pakete versendet wurden, die die MTU-Kapazität des Clients überstiegen, sodass der Client die Pakete verwarf.

Umwelt

- Produktfamilie: Wie die Cisco Secure Firewall der Serie 4200 zeigt, können auch andere Plattformen betroffen sein.
- Software-Version: Zuerst auf FTD-Software-Version 7.6.2.1 gesehen, können auch andere Softwareversionen betroffen sein.
- Firewall-Schnittstellen-MTU beträgt 9.000 Byte
- DNS-Inspektion aktiviert.
- Betroffene Client-Computer, die mit einer MTU von 1.500 Byte konfiguriert sind.
- DNS-Server, die fragmentierte Antworten für große Abfragen von SRV-Datensätzen generieren.

Auflösung

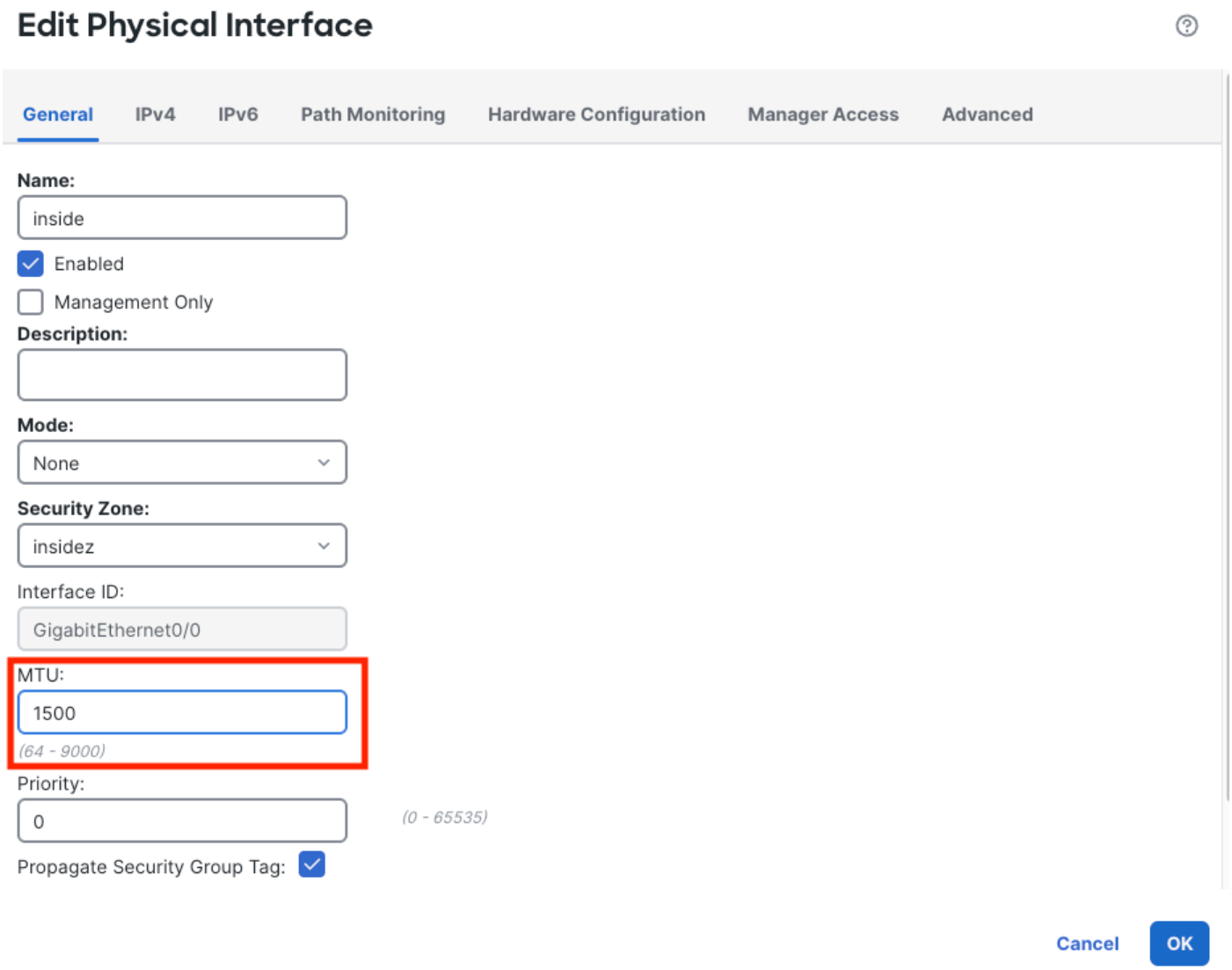
Das Problem wurde durch die Anpassung der MTU-Konfiguration der Firewall-Schnittstelle behoben. Diese Ansätze können zur Lösung dieses Problems eingesetzt werden:

Option 1: Stellen Sie die Schnittstellen-MTU auf 1500 ein, wenn andere Netzwerkgeräte dies zulassen (empfohlen).

Ändern Sie die MTU der Firewall-Ausgangsschnittstelle von 9.000 auf 1.500 Byte, um eine ordnungsgemäße erneute Fragmentierung der wieder zusammengesetzten Pakete sicherzustellen:

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

FTD:
Change MTU from FMC GUI
```



Überprüfen Sie die MTU-Konfiguration:

```
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
```

Option 2: Deaktivieren der DNS-Überprüfung (alternative Problemumgehung, aber nicht empfohlen)

Anmerkung: Wenn die Deaktivierung der DNS-Inspektion gemäß den Sicherheitsanforderungen zulässig ist und die Firewall keine Perimeter-Firewall ist, können Sie die DNS-Inspektion aus der Richtlinienzuordnung deaktivieren. (Bei hohem DNS-Datenverkehr kann dies auch zu einer Erhöhung der Gesamtanzahl der Verbindungen führen.)

```
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
```

Verifizierungsschritte

Überprüfen Sie nach der Implementierung der Auflösung die DNS-Funktionalität:

DNS-Auflösung mit großen Antworten testen:

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

Überwachung der Firewall-Paketverarbeitung:

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

Ursache

Wenn die DNS-Überprüfung auf FTD aktiviert ist, führt die Firewall-Lina eine vollständige Reassemblierung fragmentierter DNS-Pakete durch, damit die Prüfungs-Engine (Snort) die vollständige DNS-Payload untersuchen kann. Wenn die MTU der Ausgangsschnittstelle nach der

Überprüfung größer als die neu zusammengesetzte Paketgröße ist, leitet die Firewall das Paket als einen einzigen großen Frame weiter, ohne es erneut zu fragmentieren.

Die Firewall-Schnittstelle wurde mit einer MTU von 9.000 Byte konfiguriert, sodass wieder zusammengesetzte DNS-Antworten (ca. 1.884 Byte) als einzelne Pakete übertragen werden können. Die Client-Computer konfigurierten jedoch eine Standard-MTU von 1.500 Byte und konnten diese größeren Pakete nicht akzeptieren, was zu einem Verlust des Datenverkehrs führte.

Das Verhalten wird erwartet, wenn die DNS-Inspektion auf einer Leitung aktiviert wird, deren MTU-Einstellungen für die Schnittstelle größer sind als die neu zusammengesetzte Paketgröße.

- LINA DNS Inspection: Vollständige Reassemblierung für eingehende Paketprüfung (Weitere Informationen finden Sie in diesem DOC-Defekt unter CSCwv66007.)
- Snort 3: Führt eine logische (virtuelle) Reassemblierung für die Überprüfung ohne physische Reassemblierung durch.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco
- CSCwv66007 (DOC: Klärung des ASA/FTD-Fragmentierungs-Reassemblierungsverhaltens mit aktivierter Policy-Map-Funktion, die eine vollständige Reassemblierung erfordert)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.