Grote UDP-DNS-reacties oplossen Falen via FTD met DNS-inspectie ingeschakeld

Inhoud

uitgifte

DNS-pakketten met grote pakketgroottes (ongeveer 1800-4000 bytes) mislukken wanneer verkeer tussen VM's in verschillende VLAN's wordt doorlopen via een Cisco Firepower Threat Defense (FTD)-firewall. Hetzelfde DNS-verkeer slaagt wanneer er communicatie plaatsvindt tussen VM's in hetzelfde VLAN zonder door de firewall te gaan. Tijdens het oplossen van problemen werd ontdekt dat gefragmenteerde DNS-antwoordpakketten volledig opnieuw werden geassembleerd door de FTD-firewall bij het uitschakelen en verzonden als afzonderlijke grote pakketten die de MTU-capaciteit van de client overschrijden, waardoor de client de pakketten liet vallen.

milieu

- Productfamilie: Voor het eerst gezien op Cisco Secure Firewall 4200-serie, kunnen ook andere platforms worden beïnvloed.
- Softwareversie: Voor het eerst gezien op FTD-softwareversie 7.6.2.1, kunnen ook andere softwareversies worden beïnvloed.
- Firewall-interface MTU is 9000 bytes
- DNS-inspectie ingeschakeld.
- Betrokken clientmachines geconfigureerd met standaard 1500 byte MTU.
- DNS-servers die gefragmenteerde reacties genereren voor grote SRV-recordquery's.

resolutie

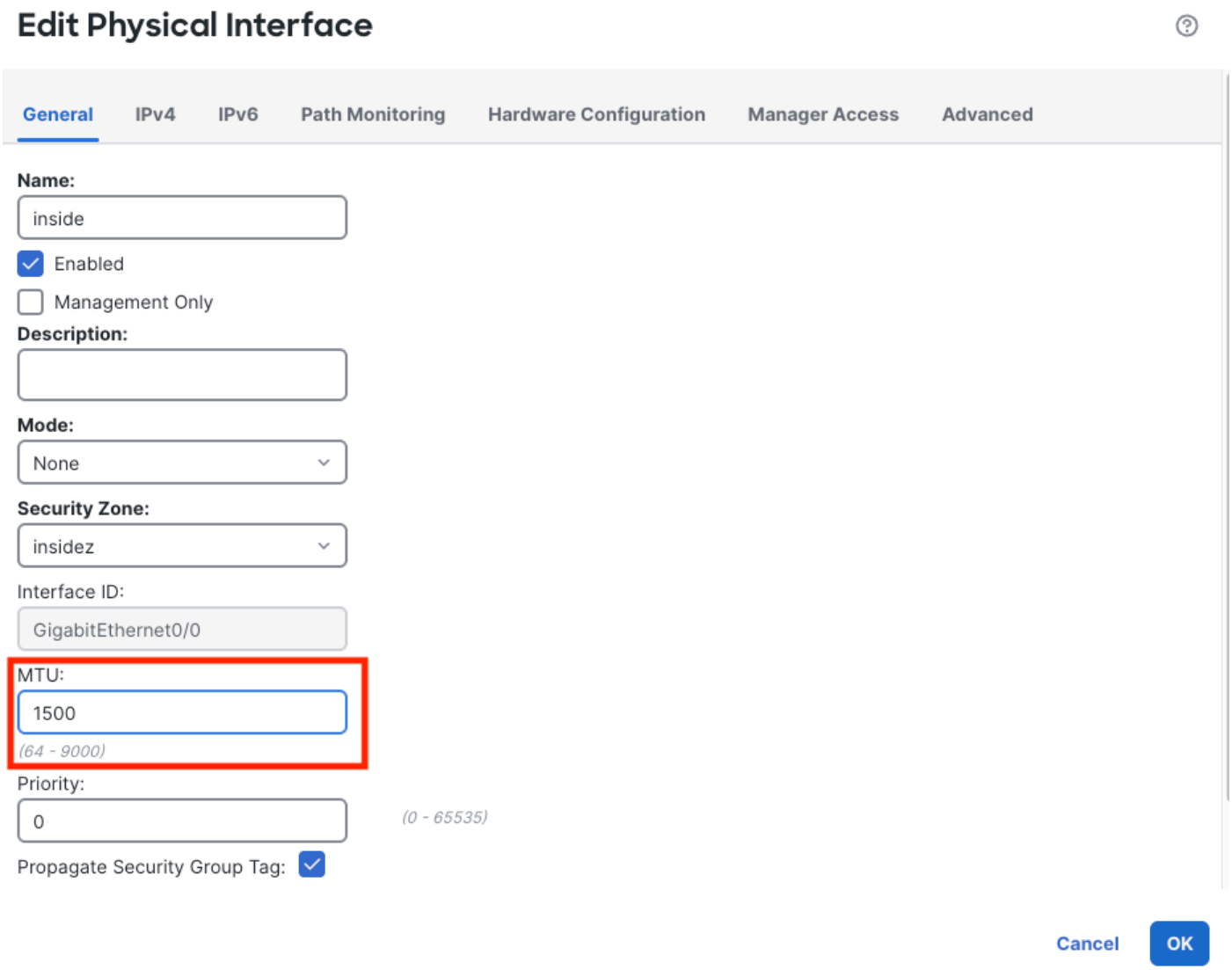
Het probleem is opgelost door de configuratie van de firewall-interface MTU aan te passen. Deze methoden kunnen worden gebruikt om dit probleem aan te pakken:

Optie 1: pas de interface MTU aan tot 1500 als andere netwerkapparaten dit toestaan (aanbevolen)

Verander de firewall egress interface MTU van 9000 naar 1500 bytes om te zorgen voor een goede herfragmentatie van opnieuw geassembleerde pakketten:

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

FTD:
Change MTU from FMC GUI
```



Controleer de MTU-configuratie:

```
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
```

Optie 2: DNS-inspectie uitschakelen (alternatieve oplossing, maar niet aanbevolen)

Opmerking: als het uitschakelen van DNS-inspectie acceptabel is volgens de beveiligingsvereisten en als de firewall geen firewall voor de perimeter is, kunt u overwegen

---

om DNS-inspectie uit te schakelen op de beleidskaart. (Dit kan ook het aantal totale verbindingen verhogen als het DNS-verkeer hoog is):

```
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
```

Verificatiestappen

Controleer na het implementeren van de resolutie de DNS-functionaliteit:

DNS-resolutie testen met grote responsen:

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

Firewallpakketverwerking controleren:

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

Oorzaak

Wanneer DNS-inspectie is ingeschakeld op FTD, voert de firewall lina de volledige herassemblage van gefragmenteerde DNS-pakketten uit om de inspectiemotor (Snort) in staat te stellen de volledige DNS-payload te onderzoeken. Na inspectie, als de uitgang interface MTU groter is dan de opnieuw geassembleerde pakketgrootte, stuurt de firewall het pakket door als een enkel groot frame zonder het opnieuw te fragmenteren.

De firewall-interface is geconfigureerd met een MTU van 9000 bytes, waardoor opnieuw

geassembleerde DNS-responsen (ongeveer 1884 bytes) als afzonderlijke pakketten kunnen worden verzonden. De clientmachines waren echter geconfigureerd met een standaard MTU van 1500 bytes en konden deze grotere pakketten niet accepteren, waardoor het verkeer daalde.

Het gedrag wordt verwacht wanneer DNS-inspectie is ingeschakeld op lina-interface met MTU-instellingen die groter zijn dan de opnieuw geassembleerde pakketgrootte.

- LINA DNS-inspectie: voert volledige reassembly uit voor diepe pakketinspectie. (Raadpleeg dit DOC-defect CSCwv66007 voor meer informatie.)
- Snort 3: Voert logische (virtuele) reassembly uit voor inspectie zonder fysieke reassembly.

Gerelateerde inhoud

- Cisco Technical Support en downloads
- CSCwv66007 (DOC: Verduidelijk het fragmentatiehermontagegedrag van ASA/FTD met een ingeschakelde beleidskaartfunctie die volledige hermontage vereist)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.