Risolvi risposte DNS UDP di grandi dimensioni non riuscite tramite FTD con ispezione DNS abilitata

Sommario

Problema

I pacchetti DNS con dimensioni di pacchetto grandi (circa 1800-4000 byte) hanno esito negativo quando il traffico attraversa le VM in VLAN diverse attraverso un firewall Cisco Firepower Threat Defense (FTD). Lo stesso traffico DNS ha esito positivo quando la comunicazione avviene tra VM nella stessa VLAN senza passare attraverso il firewall. Durante la risoluzione dei problemi, è stato rilevato che i pacchetti di risposta DNS frammentati venivano completamente ricomposti dal firewall FTD in uscita e inviati come pacchetti di grandi dimensioni che superavano la capacità MTU del client, causando il rifiuto dei pacchetti da parte del client.

Ambiente

- Famiglia di prodotti: Il problema può essere rilevato per la prima volta su Cisco Secure Firewall serie 4200 e su altre piattaforme.
- Versione del software: La prima volta che viene visto sul software FTD versione 7.6.2.1, possono essere interessate anche altre versioni software.
- L'MTU dell'interfaccia del firewall è di 9000 byte
- Ispezione DNS abilitata.
- Computer client interessati configurati con MTU standard da 1500 byte.
- Server DNS che generano risposte frammentate per query su record SRV di grandi dimensioni.

Risoluzione

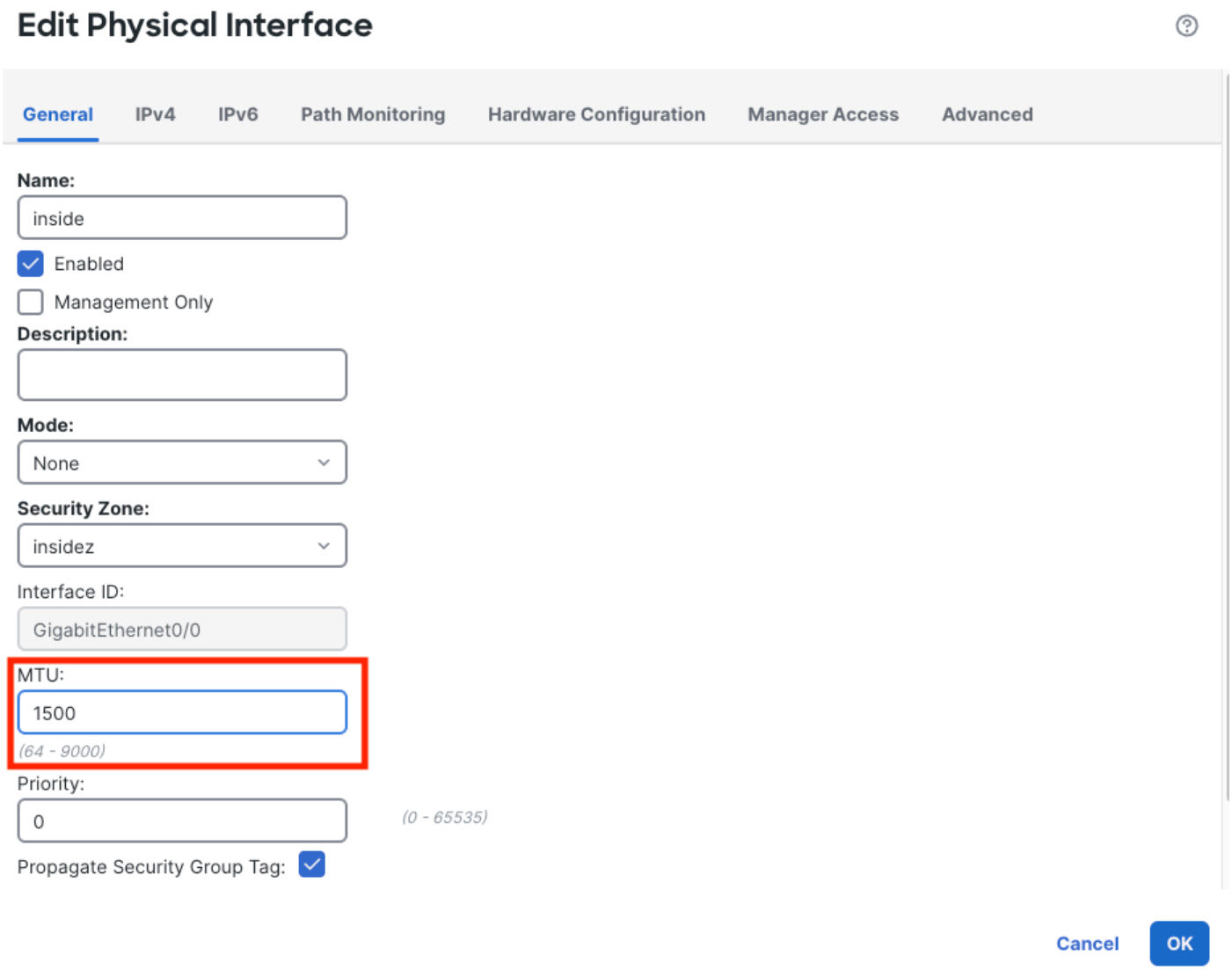
Il problema è stato risolto regolando la configurazione MTU dell'interfaccia del firewall. Per risolvere questo problema, è possibile utilizzare i seguenti approcci:

Opzione 1: Regola l'MTU dell'interfaccia a 1500 se altri dispositivi di rete lo consentono (scelta consigliata)

Modificare l'MTU dell'interfaccia in uscita del firewall da 9000 a 1500 byte per assicurare la corretta riframmentazione dei pacchetti ricomposti:

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

FTD:
Change MTU from FMC GUI
```



Verificare la configurazione MTU:

```
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
```

Opzione 2: Disabilita ispezione DNS (soluzione alternativa ma non consigliata)

Nota: Se la disattivazione dell'ispezione DNS è accettabile in base ai requisiti di sicurezza e se il firewall non è un firewall perimetrale, è possibile disattivare l'ispezione DNS dalla

---

mappa dei criteri. In questo modo è possibile aumentare anche il numero totale di connessioni se il traffico DNS è elevato:

```
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
```

Fasi di verifica

Dopo aver implementato la risoluzione, verificare la funzionalità DNS:

Verifica risoluzione DNS con risposte grandi:

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

Monitoraggio elaborazione pacchetti firewall:

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

Causa

Quando l'ispezione DNS è abilitata su FTD, la linea del firewall esegue il riassemblaggio completo dei pacchetti DNS frammentati per consentire al motore di ispezione (Snort) di esaminare il payload DNS completo. Dopo l'ispezione, se l'MTU dell'interfaccia in uscita è più grande delle dimensioni del pacchetto ricomposto, il firewall inoltra il pacchetto come un unico frame di grandi dimensioni senza frammentarlo nuovamente.

L'interfaccia del firewall è configurata con una MTU di 9000 byte, consentendo la trasmissione di

risposte DNS ricomposte (circa 1884 byte) come pacchetti singoli. Tuttavia, i client configurati con MTU standard di 1500 byte non sono in grado di accettare pacchetti di dimensioni maggiori, con conseguente perdita del traffico.

Questo comportamento è previsto quando l'ispezione DNS è abilitata su una linea con impostazioni MTU dell'interfaccia superiori alle dimensioni del pacchetto riassemblato.

- Ispezione DNS LINA: Esegue il riassemblaggio completo per l'ispezione approfondita dei pacchetti. (per ulteriori informazioni, fare riferimento a questo difetto DOC CSCwv6007).
- Snort 3 Esegue il riassemblaggio logico (virtuale) per l'ispezione senza riassemblaggio fisico.

Contenuto correlato

- Supporto tecnico Cisco e download
- CSCwv6007 (DOC:Clarify ASA/FTD frammentazione comportamento di riassemblaggio con una funzione di mappatura dei criteri abilitata che richiede il riassemblaggio completo)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).