Resuelva los errores de las respuestas grandes de DNS UDP mediante FTD con la inspección de DNS habilitada

Contenido

Problema

Los paquetes DNS con tamaños de paquete grandes (aproximadamente 1800-4000 bytes) fallan cuando el tráfico atraviesa entre VM en diferentes VLAN a través de un firewall Cisco Firepower Threat Defence (FTD). El mismo tráfico DNS tiene éxito cuando se produce la comunicación entre las VM de la misma VLAN sin pasar a través del firewall. Durante la resolución de problemas, se descubrió que los paquetes de respuesta DNS fragmentados estaban siendo completamente reensamblados por el firewall FTD al egresar y enviados como paquetes grandes únicos que excedían la capacidad de MTU del cliente, lo que hacía que el cliente descartara los paquetes.

Entorno

- Familia de productos: Si se observa por primera vez en Cisco Secure Firewall serie 4200, también pueden verse afectadas otras plataformas.
- Versión del software: Si se observa por primera vez en la versión de software FTD 7.6.2.1, también pueden verse afectadas otras versiones de software.
- La MTU de la interfaz de firewall es de 9000 bytes
- Inspección de DNS habilitada.
- Equipos cliente afectados configurados con MTU estándar de 1500 bytes.
- Servidores DNS que generan respuestas fragmentadas para consultas de registro SRV grandes.

Resolución

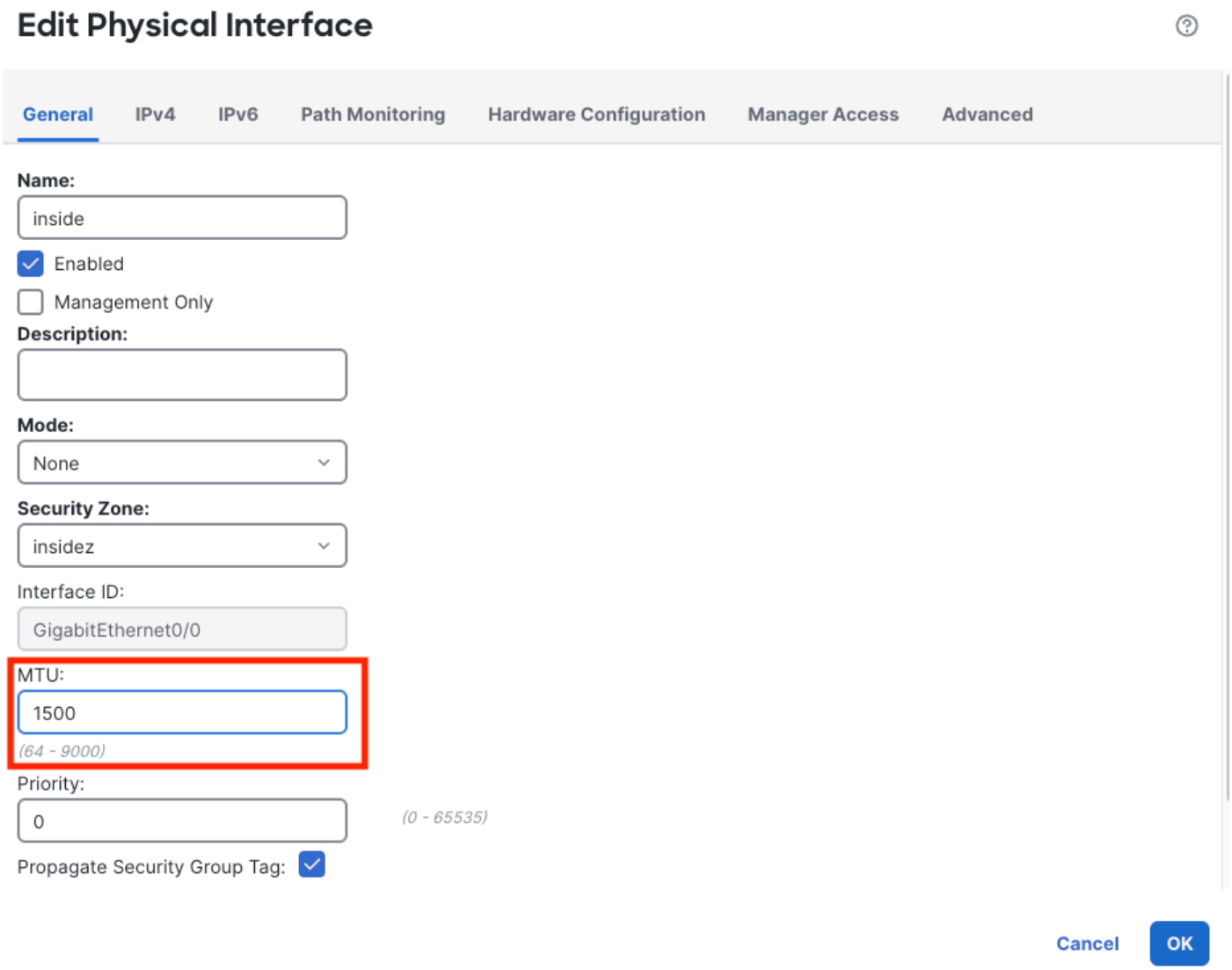
El problema se resolvió ajustando la configuración de MTU de la interfaz de firewall. Estos enfoques se pueden utilizar para abordar este problema:

Opción 1: Ajustar la MTU de la interfaz a 1500 si otros dispositivos de red lo permiten (recomendado)

Cambie la MTU de la interfaz de salida del firewall de 9000 a 1500 bytes para garantizar una refragmentación adecuada de los paquetes reensamblados:

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

FTD:
Change MTU from FMC GUI
```



Verifique la configuración de 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
```

Opción 2: Desactivar inspección de DNS (solución alternativa, pero no recomendada)

Nota: Si desactivar la inspección de DNS es aceptable según los requisitos de seguridad y si el firewall no es un firewall perimetral, puede considerar desactivar la inspección de DNS desde el mapa de políticas. (Esto también puede aumentar el número total de conexiones si el tráfico DNS es alto):

```
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
```

Pasos de verificación

Después de implementar la resolución, verifique la funcionalidad de DNS:

Probar resolución DNS con respuestas grandes:

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

Supervisar el procesamiento de paquetes de firewall:

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

Causa

Cuando la inspección de DNS está activada en FTD, la línea de firewall realiza un reensamblado completo de paquetes DNS fragmentados para permitir que el motor de inspección (Snort) examine la carga útil de DNS completa. Después de la inspección, si la MTU de la interfaz de salida es mayor que el tamaño del paquete reensamblado, el firewall reenvía el paquete como

una sola trama grande sin volver a fragmentarlo.

La interfaz de firewall configurada con una MTU de 9000 bytes, permite que las respuestas DNS reensambladas (aproximadamente 1884 bytes) se transmitan como paquetes únicos. Sin embargo, las máquinas cliente configuradas con MTU estándar de 1500 bytes y no pudieron aceptar estos paquetes más grandes, lo que provocó la pérdida de tráfico.

El comportamiento se espera cuando la inspección de DNS está habilitada en línea con configuraciones de MTU de interfaz mayores que el tamaño del paquete reensamblado.

- Inspección de DNS LINA: Realiza un reensamblado completo para una inspección profunda de paquetes. (Consulte este defecto de DOC CSCwv66007 para obtener más detalles.)
- Snort 3: Realiza un reensamblado lógico (virtual) para inspección sin reensamblado físico.

Contenido relacionado

- Soporte técnico y descargas de Cisco
- CSCwv66007 (DOC:Clarifique el comportamiento de reensamblado de fragmentación de ASA/FTD con una función de policy-map habilitada que requiere un reensamblado completo)

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).