Resolve Large UDP DNS Responses Failing through FTD with DNS Inspection Enabled

Contents

Issue

DNS packets with large packet sizes (approximately 1800-4000 bytes) fail when traffic traverses between VMs in different VLANs through a Cisco Firepower Threat Defense (FTD) firewall. The same DNS traffic succeeds when communication occurs between VMs in the same VLAN without passing through the firewall. During troubleshooting, it was discovered that fragmented DNS reply packets were being fully reassembled by the FTD firewall when egressing out and sent as single large packets exceeding the client's MTU capability, causing the client to drop the packets.

Environment

- Product family: First seen on Cisco Secure Firewall 4200 Series, other platforms can also be affected.
- Software version: First seen on FTD software version 7.6.2.1, other software versions can also be affected.
- Firewall interface MTU is 9000 bytes
- DNS inspection enabled.
- Affected client machines configured with standard 1500 byte MTU.
- DNS servers generating fragmented responses for large SRV record queries.

Resolution

The issue was resolved by adjusting the firewall interface MTU configuration. These approaches can be used to address this problem:

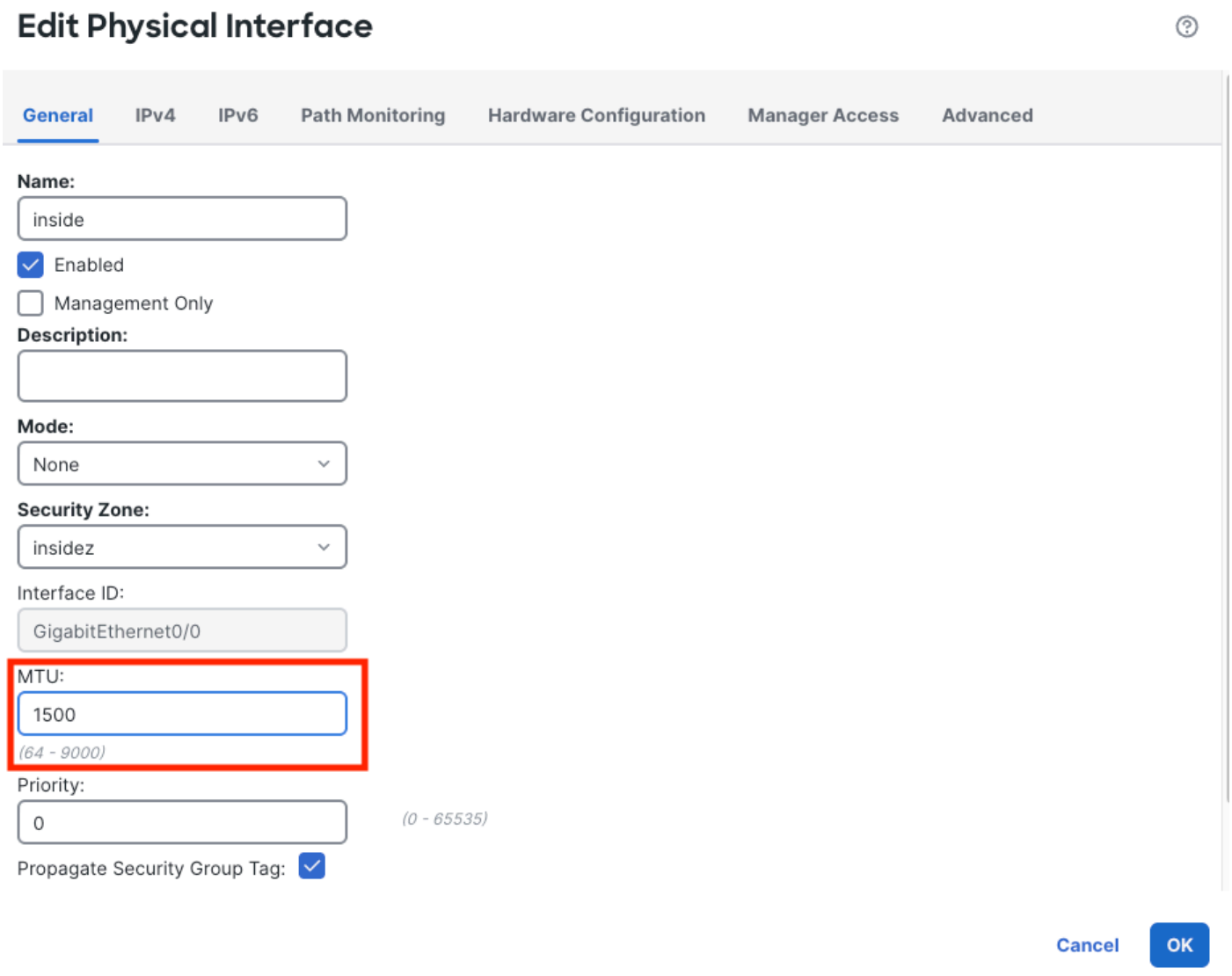
Option 1: Adjust Interface MTU to 1500 if Other Network Devices Allow It

(Recommended)

Change the firewall egress interface MTU from 9000 to 1500 bytes to ensure proper re-fragmentation of reassembled packets:

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

FTD:
Change MTU from FMC GUI
```



Verify the MTU configuration:

```
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: Disable DNS Inspection (Alternative Workaround but Not Recommended)



Note: If disabling DNS inspection is acceptable as per security requirements and if firewall is not perimeter firewall, you can consider disabling DNS inspection from the policy map. (This can also increase number of total connections if DNS traffic is high):

```
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
```

Verification Steps

After implementing the resolution, verify DNS functionality:

Test DNS resolution with large responses:

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

Monitor firewall packet processing:

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

Cause

When DNS inspection is enabled on FTD, the firewall lina performs full reassembly of fragmented DNS packets to allow the inspection engine (Snort) to examine the complete DNS payload. After inspection, if the egress interface MTU is larger than the reassembled packet size, the firewall forwards the packet as a single large frame without re-fragmenting it.

The firewall interface configured with an MTU of 9000 bytes, allowing reassembled DNS responses (approximately 1884 bytes) to be transmitted as single packets. However, the client machines configured with standard MTU of 1500 bytes and could not accept these larger packets, resulting in dropped traffic.

The behavior is expected when DNS inspection is enabled on lina with interface MTU settings larger than the reassembled packet size.

- LINA DNS inspection: Performs full reassembly for deep packet inspection. (Refer this DOC defect CSCwv66007 for more details.)
- Snort 3: Performs logical (virtual) reassembly for inspection without physical reassembly.

Related Content

- Cisco Technical Support & Downloads
- CSCwv66007 (DOC:Clarify ASA/FTD fragmentation reassembly behaviour with a enabled policy-map feature which requires full reassembly)