Resolver Falha de Respostas UDP DNS Grandes por FTD com Inspeção de DNS Habilitada

Contents

Problema

Os pacotes DNS com pacotes grandes (aproximadamente 1800-4000 bytes) falham quando o tráfego atravessa entre VMs em VLANs diferentes através de um firewall Cisco Firepower Threat Defense (FTD). O mesmo tráfego DNS é bem-sucedido quando a comunicação ocorre entre VMs na mesma VLAN sem passar pelo firewall. Durante a solução de problemas, descobriu-se que os pacotes fragmentados de resposta DNS estavam sendo totalmente remontados pelo firewall FTD ao sair e serem enviados como pacotes grandes únicos excedendo a capacidade de MTU do cliente, fazendo com que o cliente descartasse os pacotes.

Ambiente

- Linha de produtos: Vistas pela primeira vez no Cisco Secure Firewall 4200 Series, outras plataformas também podem ser afetadas.
- Versão de software: Vistas pela primeira vez no software FTD versão 7.6.2.1, outras versões de software também podem ser afetadas.
- O MTU da interface do firewall tem 9000 bytes
- Inspeção de DNS habilitada.
- Máquinas cliente afetadas configuradas com MTU padrão de 1500 bytes.
- Servidores DNS gerando respostas fragmentadas para consultas de registros SRV grandes.

Resolução

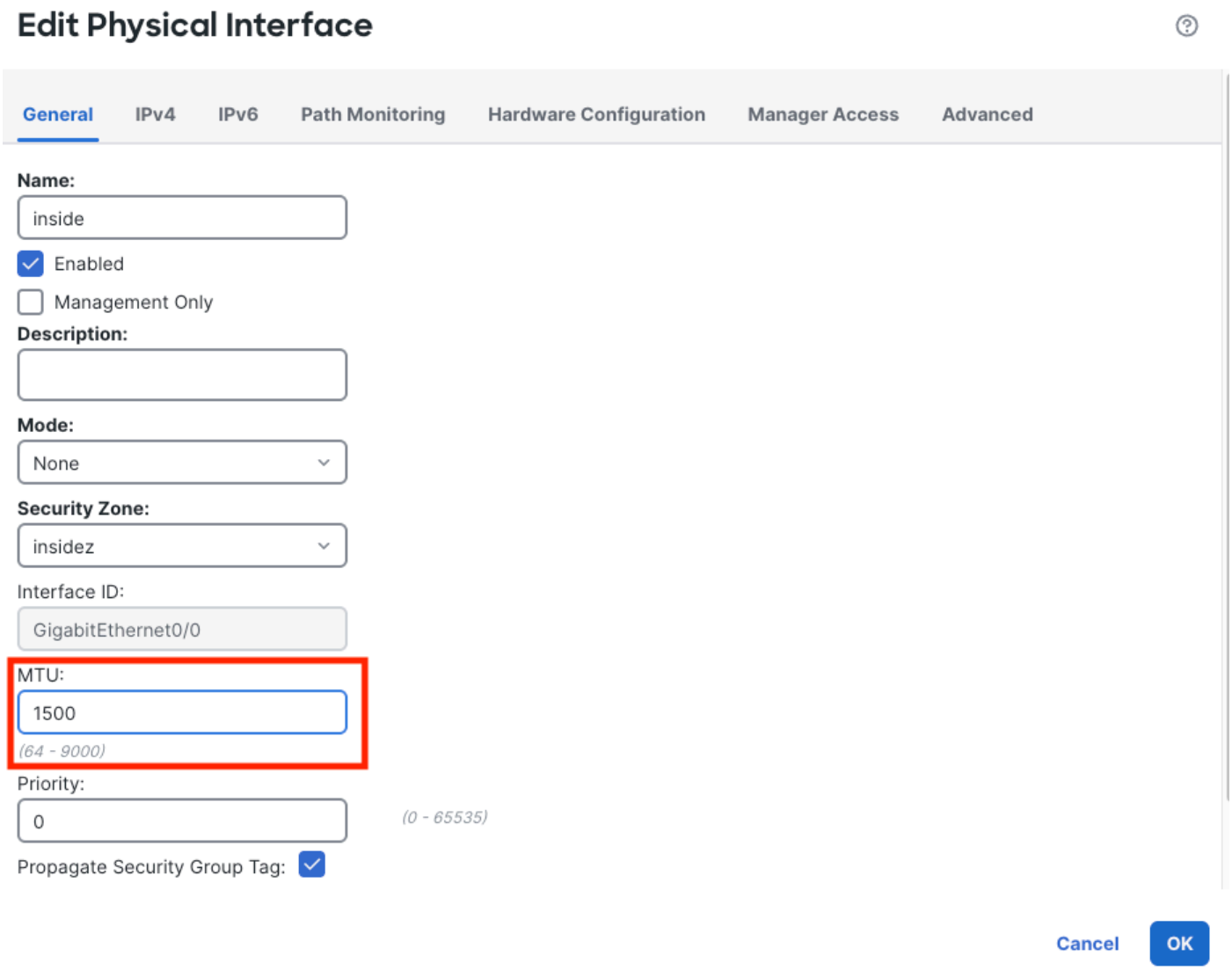
O problema foi resolvido ajustando-se a configuração MTU da interface do firewall. Essas abordagens podem ser usadas para resolver esse problema:

Opção 1: Ajustar a MTU da interface para 1500 se outros dispositivos de rede permitirem (recomendado)

Altere o MTU da interface de saída do firewall de 9000 para 1500 bytes para garantir a refragmentação adequada dos pacotes reagrupados:

```
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 a configuração 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
```

Opção 2: Desabilitar Inspeção de DNS (Solução Alternativa, mas Não Recomendada)

Note: Se a desabilitação da inspeção de DNS for aceitável de acordo com os requisitos de segurança e se o firewall não for do perímetro, você poderá considerar a desabilitação da inspeção de DNS no mapa de políticas. (Isso também pode aumentar o número total de conexões se o tráfego DNS for 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
```

Etapas de verificação

Após implementar a resolução, verifique a funcionalidade DNS:

Testar a resolução DNS com respostas grandes:

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

Monitorar o processamento de pacotes de firewall:

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

Causa

Quando a inspeção de DNS é habilitada no FTD, a linha de firewall executa a remontagem completa de pacotes DNS fragmentados para permitir que o mecanismo de inspeção (Snort) examine o payload de DNS completo. Após a inspeção, se o MTU da interface de saída for maior que o tamanho do pacote remontado, o firewall encaminhará o pacote como um único quadro

grande sem fragmentá-lo novamente.

A interface de firewall configurada com um MTU de 9000 bytes, permitindo que respostas DNS reagrupadas (aproximadamente 1884 bytes) sejam transmitidas como pacotes únicos. No entanto, as máquinas cliente configuradas com MTU padrão de 1500 bytes e não puderam aceitar esses pacotes maiores, resultando em tráfego descartado.

O comportamento é esperado quando a inspeção de DNS é habilitada na linha com configurações de MTU da interface maiores que o tamanho do pacote remontado.

- Inspeção de DNS LINA: Executa a remontagem completa para inspeção profunda de pacotes. (Consulte esse defeito do DOC CSCwv66007 para obter mais detalhes.)
- Snort 3 Executa remontagem lógica (virtual) para inspeção sem remontagem física.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco
- CSCwv66007 (DOC:Esclareça o comportamento de remontagem de fragmentação de ASA/FTD com um recurso de mapa de políticas habilitado que requer remontagem completa)

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.