Entender mensagens de pacote ICMP "inalcançável - admin proibido filter"

Contents

Problema

Entender as informações de pacote anexadas aos pacotes do Internet Control Message Protocol (ICMP) como "inalcançável - filtro proibido pelo administrador".

Exemplo de captura do Cisco Secure Firewall Threat Defense (FTD):

<#root>

```
device#

show capture CAPO



106 packets captured

   1: 08:12:45.864243       198.51.100.205.7351 > 192.0.2.2.47668:  udp 111
   2: 08:12:46.400812       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   3: 08:12:46.406320       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

unreachable - admin prohibited filter



   4: 08:12:47.936856       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   5: 08:12:47.943936       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   6: 08:12:49.216739       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   7: 08:12:49.222278       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2

 unreachable - admin prohibited filter



   8: 08:12:50.096079       198.51.100.205.7351 > 192.0.2.2.47668:  udp 124
   9: 08:12:50.106363       192.0.2.2 > 198.51.100.205 icmp: host 192.0.2.2
```

```
unreachable - admin prohibited filter
```

Ambiente

Ele pode ser visto em qualquer um destes produtos:

- FTD
- Adaptive Security Appliance (ASA)

Resolução

Entendendo mensagens ICMP tipo 3, código 13

As mensagens "inalcançável - filtro proibido pelo administrador" do ICMP correspondem ao tipo 3 do ICMP, código 13 (destino inalcançável - comunicação proibida administrativamente). Essas mensagens indicam que o tráfego foi explicitamente negado por uma política de segurança ou por uma lista de controle de acesso (ACL), em vez de ficar inacessível devido a problemas de conectividade de rede.

Analisando informações de captura de pacote

Etapa 1. Identificar a origem das mensagens de negação do ICMP

Revise a captura do pacote para identificar quais dispositivos estão gerando as respostas ICMP

Tipo 3, Código 13. Nesse caso, as mensagens de negação originaram-se de endereços IP específicos (192.0.2.2).

Etapa 2. Examinar os cabeçalhos dos pacotes originais

As mensagens de negação do ICMP contêm informações sobre os pacotes originais que foram bloqueados. Isso inclui os endereços IP origem e destino, as informações de protocolo e os números de porta que dispararam a proibição administrativa.

Etapa 3. Correlacionar mensagens de negação com padrões de tráfego

Faça a correspondência entre as respostas ICMP e os fluxos de tráfego específicos que estão sendo negados. Por exemplo, o tráfego UDP para a porta 7351 estava sendo rejeitado pelo dispositivo com o endereço IP 192.0.2.2 na captura CAPO.

Limitações da análise de captura de pacotes

Ao trabalhar com capturas de pacotes exportados por texto, a análise detalhada de pacote por pacote pode ser limitada em comparação com os arquivos pcap binários. Para uma análise abrangente, os arquivos binários de captura de pacotes (formato pcap) fornecem informações mais completas, incluindo:

- Cabeçalhos de pacotes completos e informações de payload
- Informações precisas de temporização
- Recursos completos de decodificação de protocolo
- Opções aprimoradas de filtragem e análise

Causa

A causa raiz geralmente é uma destas:

- ACLs configuradas para negar fluxos de tráfego específicos
- Regras de firewall que bloqueiam determinados protocolos, portas ou endereços IP

Neste exemplo, a mensagem foi causada por uma ACL downstream.

Conteúdo relacionado

- https://datatracker.ietf.org/doc/html/rfc792
- https://datatracker.ietf.org/doc/html/rfc1812
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

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.