Comprender los mensajes de paquetes ICMP "inalcanzable - filtro prohibido por el administrador"

Contenido

Problema

Comprenda la información de paquetes adjunta a los paquetes del protocolo de mensajes de control de Internet (ICMP) "inalcanzable - filtro prohibido por el administrador".

Ejemplo de captura de Cisco Secure Firewall Threat Defence (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

Entorno

Se puede ver en cualquiera de estos productos:

- FTD
- Adaptive Security Appliance (ASA)

Resolución

Descripción de los mensajes ICMP tipo 3, código 13

Los mensajes ICMP "inalcanzable - filtro prohibido por el administrador" corresponden al ICMP tipo 3, código 13 (destino inalcanzable - comunicación prohibida administrativamente). Estos mensajes indican que una política de seguridad o una lista de control de acceso (ACL) ha denegado explícitamente el tráfico en lugar de que sea inaccesible debido a problemas de conectividad de red.

Análisis de Información de Captura de Paquetes

Paso 1. Identifique el origen de los mensajes de negación ICMP

Revise la captura de paquetes para identificar qué dispositivos están generando las respuestas ICMP tipo 3, código 13. En este caso, los mensajes de denegación se originaron a partir de direcciones IP específicas (192.0.2.2).

Paso 2. Examine los encabezados de paquetes originales

Los mensajes de denegación ICMP contienen información sobre los paquetes originales que se bloquearon. Esto incluye las direcciones IP de origen y destino originales, la información de protocolo y los números de puerto que activaron la prohibición administrativa.

Paso 3. Correlación de los mensajes de denegación con los patrones de tráfico

Haga coincidir las respuestas ICMP con los flujos de tráfico específicos que se están denegando. Por ejemplo, el tráfico UDP al puerto 7351 estaba siendo rechazado por el dispositivo con la dirección IP 192.0.2.2 en la captura de CAPO.

Limitaciones del análisis de captura de paquetes

Cuando se trabaja con capturas de paquetes exportados por texto, el análisis detallado paquete por paquete se puede limitar en comparación con los archivos pcap binarios. Para realizar un análisis completo, los archivos de captura de paquetes binarios (formato pcap) proporcionan información más completa, que incluye:

- Encabezados de paquetes completos e información de carga útil
- Información de sincronización precisa
- Funciones completas de decodificación de protocolos
- Opciones mejoradas de filtrado y análisis

Causa

La causa raíz suele ser una de estas:

- ACL configuradas para denegar flujos de tráfico específicos
- Reglas de firewall que bloquean determinados protocolos, puertos o direcciones IP

En este ejemplo, el mensaje fue causado por una ACL descendente.

Contenido 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

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).