Begrijp ICMP Packet Messages " onbereikbaar - admin verboden filter"

Inhoud

uitgeven

Begrijp de pakketinformatie die is gekoppeld aan de ICMP-pakketten (Internet Control Message Protocol) "onbereikbaar - admin verboden filter".

Cisco Secure Firewall Threat Defense (FTD) vastleggen voorbeeld:

<#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
```

milieu

Het is te zien in elk van deze producten:

- FTD
- Adaptieve security applicatie (ASA)

resolutie

ICMP Type 3, Code 13 Berichten begrijpen

ICMP "onbereikbaar - admin verboden filter" berichten komen overeen met ICMP Type 3, Code 13 (Bestemming onbereikbaar - Communicatie administratief verboden). Deze berichten geven aan dat verkeer expliciet is geweigerd door een beveiligingsbeleid of toegangscontrolelijst (ACL) in plaats van onbereikbaar te zijn vanwege problemen met de netwerkconnectiviteit.

Informatie over pakketvastlegging analyseren

Stap 1. Identificeer de bron van ICMP-weigeringsberichten

Controleer de pakketopname om te identificeren welke apparaten de ICMP Type 3, Code 13-antwoorden genereren. In dit geval zijn de weigeringsberichten afkomstig van specifieke IP-

adressen (192.0.2.2).

Stap 2. Bekijk de originele pakketkoppen

De ICMP-weigeringsberichten bevatten informatie over de oorspronkelijke pakketten die zijn geblokkeerd. Dit omvat de oorspronkelijke bron- en bestemmings-IP-adressen, protocolinformatie en poortnummers die het administratieve verbod hebben geactiveerd.

Stap 3. Berichten weigeren met verkeerspatronen correleren

De ICMP-antwoorden afstemmen op de specifieke verkeersstromen die worden geweigerd. Bijvoorbeeld, UDP-verkeer naar poort 7351 werd afgewezen door het apparaat met IP-adres 192.0.2.2 in de CAPO-opname.

Beperkingen voor analyse van pakketafvang

Bij het werken met tekst-geëxporteerde pakketopnames kan gedetailleerde pakketanalyse beperkt zijn in vergelijking met binaire pcap-bestanden. Voor een uitgebreide analyse bieden binaire pakketregistratiebestanden (pcap-indeling) meer volledige informatie, waaronder:

- Volledige pakketkoppen en payload-informatie
- Nauwkeurige timing informatie
- Volledige mogelijkheden voor protocoldecodering
- Verbeterde opties voor filtering en analyse

Oorzaak

De onderliggende oorzaak is meestal een van deze:

- ACL's geconfigureerd om specifieke verkeersstromen te weigeren
- Firewallregels die bepaalde protocollen, poorten of IP-adressen blokkeren

In dit voorbeeld werd het bericht veroorzaakt door een downstream ACL.

Verwante inhoud

- 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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.