FTD-implementatiefout voor veilige firewall

uitgeven

Netwerkonderbrekingen en -uitval zijn waargenomen op Cisco Firewall Threat Defense (FTD). Herhaalde incidenten hebben geleid tot geweigerd verkeer, waaronder SNMP-communicatie, en hebben het opnieuw opstarten van apparaten en voortdurende monitoring vereist om de hoofdoorzaak te identificeren en verdere impact te beperken.

milieu

- Cisco Secure Firewall Firepower 1140-apparaten (heeft invloed op elk FTD-model)
- FTD-softwareversies: 7.4.2.4 (andere versies ook beïnvloed)
- Dynamisch objectgebaseerd toegangscontrolebeleid (ACS)
- Frequente beleidsimplementaties

resolutie

Om de terugkerende failover- en beleidsimplementatieproblemen op FTD-apparaten van Cisco Secure Firewall aan te pakken, moet een uitgebreide reeks stappen voor probleemoplossing en probleemoplossing worden gevolgd. De vermelde workflow is gestructureerd om een duidelijke scheiding en uitleg van elke stap te bieden, inclusief bewaking, gegevensverzameling, diagnostiek en upgradebegeleiding.

1: Gebruik packet-tracers om routering en toegang voor het beoogde verkeer te controleren.

```
firepower# packet-tracer input INPUTNAMEIF tcp SRCIP 54321 DSTIP 443
firepower# packet-tracer input INPUTNAMEIF icmp SRCIP 8 0 DSTIP
```

2: Gebruik opnames op de FTD om te bepalen of pakketten worden gedropt bij binnenkomst 'door geconfigureerde regel', hoewel er een geldige regel en route bestaat voor het verkeer.

```
firepower# capture 1 interface INPUTIFNAME trace detail trace-count 1000 match ip host SRCIP host DSTIP
firepower# capture x type asp-drop all match ip host SRCIP host DSTIP
firepower# show capture
capture 1 type raw-data trace detail trace-count 1000 interface inside [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
capture x type asp-drop all [Capturing - 31565 bytes]
  match ip 10.1.1.0 255.255.255.0 any
```

3: Controleer de FTD-berichtenlogboeken voor bewijs van een defect CSCwo78475.

```
> expert
admin@FTD-1:~$ sudo su
Password:
root@FTD-1:/Volume/home/admin# cat /ngfw/var/log/messages | grep -E "New inspector|did not finish|swapp
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector is not initializing Identity API because it's a
Feb 10 18:35:03 FTD-device SF-IMS[28366]: New inspector has different policy groups or ABP name to ID m
Feb 10 18:35:10 FTD-device SF-IMS[28366]: Reading the muster data snapshot did not finish in time: 4 se
Feb 10 18:36:22 FTD-device SF-IMS[28366]: Identity API state swapped
```

4: Koppel de tijdstempels voor deze logs aan die voor implementatielogs in de FTD.

```
Feb 10 18:34:45 FTD-device policy_apply.pl[18923]: INFO  Deployment type is NORMAL_DEPLOYMENT and devic
Feb 10 18:37:03 FTD-device policy_apply.pl[30894]: INFO  finalizeDeviceDeployment - sandbox = /var/cisc
```

5: Als de FTD's zich in HA bevinden, failover naar de stand-by FTD en hetzelfde nadien controleren om het verkeer te herstellen.

6: Als in de FTD overeenkomende logs en voorwaarden worden gevonden, wordt het apparaat beïnvloed door het defect en kan het worden bijgewerkt naar 7.4.3. In de tussentijd kunnen implementaties worden beperkt tot na kantooruren om de impact op het verkeer te verminderen.

Oorzaak

De onderliggende oorzaak van de waargenomen verkeerseffecten en problemen met beleidsimplementatie wordt toegeschreven aan bekende gebreken in FTD-software, met name:

- Cisco Bug ID CSCwo78475: verkeer raakt onjuiste regels voor toegangscontrolebeleid (ACP) tijdens beleidsimplementatie op FTD-apparaten met dynamische objecten. Dit kan ertoe leiden dat legitiem verkeer wordt geweigerd, zelfs als er goede regels bestaan in de actieve configuratie. Opgelost in versie 7.4.3.

Verwante inhoud

- Cisco Bug ID CSCwo78475: Verkeer raakt onjuiste ACS-regels tijdens beleidsimplementatie op FTD met dynamische objecten
- Technische ondersteuning en downloads van Cisco: Technische ondersteuning en downloads van Cisco

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.