FTD-Bereitstellungsfehler bei sicherer Firewall

Problem

Netzwerkstörungen und -ausfälle wurden bei der Cisco Firewall Firepower Threat Defense (FTD) beobachtet. Wiederholte Vorfälle haben zu einer Ablehnung des Datenverkehrs geführt, einschließlich SNMP-Kommunikation, und erforderten einen Neustart der Geräte und eine laufende Überwachung, um die Ursache zu identifizieren und weitere Auswirkungen zu minimieren.

Umwelt

- Cisco Secure Firewall FirePOWER 1140-Appliances (Auswirkungen auf jedes FTD-Modell)
- FTD-Softwareversionen: 7.4.2.4 (andere Versionen ebenfalls betroffen)
- Dynamische objektbasierte Zugriffskontrollrichtlinien (ACPs)
- Häufige Richtlinienbereitstellungen

Auflösung

Um die wiederkehrenden Failover- und Richtlinienbereitstellungsprobleme bei Cisco Secure Firewall FTD-Geräten zu beheben, müssen umfassende Schritte zur Fehlerbehebung und Problembehebung durchgeführt werden. Der aufgelistete Workflow ist so strukturiert, dass jede Phase klar getrennt und erläutert wird, einschließlich Überwachung, Datenerfassung, Diagnose und Upgrade-Anleitungen.

1: Verwenden Sie Paket-Tracer, um die Weiterleitung und den Zugriff für den beabsichtigten Datenverkehr zu überprüfen.

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

2: Verwenden Sie Erfassungen im FTD, um zu ermitteln, ob Pakete bei der Eingabe "nach konfigurierter Regel" verworfen werden, obwohl eine gültige Regel und Route für den Datenverkehr vorhanden sind.

```
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: Überprüfen Sie die FTD-Nachrichtenprotokolle auf Fehlernachweise 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: Ordnen Sie die Zeitstempel für diese Protokolle den Zeitstempeln für Bereitstellungsprotokolle im FTD zu.

```
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: Wenn sich die FTDs in Hochverfügbarkeit befinden, Failover auf den Standby-FTD und anschließend Überprüfung desselben, um eine Wiederherstellung des Datenverkehrs sicherzustellen.

6: Wenn im FTD übereinstimmende Protokolle und Bedingungen gefunden werden, ist das Gerät vom Fehler betroffen und kann auf Version 7.4.3 aktualisiert werden. In der Zwischenzeit können Bereitstellungen auf Stunden nach dem Ausfall beschränkt werden, um die Auswirkungen auf den Datenverkehr zu reduzieren.

Ursache

Die Ursache für die festgestellten Auswirkungen auf den Datenverkehr und Probleme bei der Richtlinienbereitstellung wird auf bekannte Fehler zurückgeführt, die FTD-Software beeinträchtigen, insbesondere:

- Cisco Bug-ID CSCwo78475: Der Datenverkehr trifft während der Richtlinienbereitstellung auf FTD-Geräten mit dynamischen Objekten auf falsche Zugriffskontrollrichtlinien (ACP, Access Control Policy)-Regeln. Dies kann dazu führen, dass legitimer Datenverkehr abgelehnt wird, selbst wenn in der aktuellen Konfiguration entsprechende Regeln vorhanden sind. Behoben in Version 7.4.3.

Verwandte Inhalte

- Cisco Bug-ID CSCwo78475: Datenverkehr trifft falsche ACP-Regeln während der Richtlinienbereitstellung auf FTD mit dynamischen Objekten
- Technischer Support und Downloads von Cisco: Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.