Secure Firewall FTD Deployment Failure

Issue

Network disruptions and outages have been observed on Cisco Firewall Firepower Threat Defense (FTD). Repeated incidents have led to denied traffic, including SNMP communications, and have required device reboots and ongoing monitoring to identify the root cause and mitigate further impact.

Environment

- Cisco Secure Firewall Firepower 1140 appliances (impacts any FTD model)
- FTD software versions: 7.4.2.4 (other versions also impacted)
- Dynamic object-based Access Control Policies (ACPs)
- Frequent policy deployments

Resolution

To address the recurring failover and policy deployment issues on Cisco Secure Firewall
FTD devices, adher to
a comprehensive set of troubleshooting and remediation steps. The workflow listed is structured to provide clear sep

1: Use packet-tracers to check routing and access for the intended traffic.

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

2: Use captures at the FTD to determine if packets are being dropped upon entry 'by configured rule' even though a v

```
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: Check the FTD messages logs for evidence of defect Cisco bug ID 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: Match the timestamps for these logs with those for deployment logs in the 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: If the FTDs are in HA, failover to the standby FTD and check the same afterward to ensure traffic recovery.

6: If matching logs and conditions are found in the FTD, the device is impacted by the defect and can be upgraded to
hours to reduce traffic impact.

Cause

The underlying cause of the observed traffic impacts
and policy deployment issues is attributed to known defect affecting FTD software, notably:

- **Cisco bug ID CSCwo78475:** Traffic hits incorrect Access Control Policy (ACP) rules during policy deploym

Related Content

- Cisco bug ID CSCwo78475: Traffic hits incorrect ACP rules during policy deployment on FTD with dynamic objects

- Cisco Technical Support & Downloads: Cisco Technical Support & Downloads