Error de implementación de FTD de firewall seguro

Problema

Se han observado interrupciones y cortes de la red en Cisco Firewall Firepower Threat Defense (FTD). Los repetidos incidentes han dado lugar a tráfico denegado, incluidas las comunicaciones SNMP, y han requerido reinicios de dispositivos y supervisión continua para identificar la causa principal y mitigar el impacto adicional.

Entorno

- Dispositivos Cisco Secure Firewall Firepower 1140 (afecta a cualquier modelo FTD)
- Versiones de software FTD: 7.4.2.4 (otras versiones también afectadas)
- Políticas de control de acceso (ACP) dinámicas basadas en objetos
- Implementaciones de políticas frecuentes

Resolución

Para solucionar los problemas recurrentes de conmutación por fallo e implementación de políticas en los dispositivos Cisco Secure Firewall FTD, se debe seguir un completo conjunto de pasos de solución de problemas y corrección. El flujo de trabajo mostrado está estructurado para proporcionar una separación y explicación claras de cada paso, incluida la supervisión, la recopilación de datos, el diagnóstico y la guía de actualización.

1: Utilice rastreadores de paquetes para verificar el ruteo y el acceso para el tráfico deseado.

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

2: Utilice capturas en el FTD para determinar si los paquetes se descartan al ingresar 'por regla configurada' aunque exista una regla y una ruta válidas para el tráfico.

```
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: Verifique los registros de mensajes FTD para detectar evidencia de defecto 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: Haga coincidir las marcas de tiempo de estos registros con las de los registros de implementación del 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: Si los FTD se encuentran en HA, realice una conmutación por error al FTD en espera y verifíquelo después para garantizar la recuperación del tráfico.

6: Si se encuentran registros y condiciones coincidentes en el FTD, el dispositivo se ve afectado por el defecto y se puede actualizar a 7.4.3. Mientras tanto, las implementaciones se pueden limitar a horas posteriores para reducir el impacto del tráfico.

Causa

La causa subyacente de los impactos de tráfico observados y los problemas de implementación de políticas se atribuye a defectos conocidos que afectan al software FTD, en particular:

- Id. de error de Cisco CSCwo78475: El tráfico alcanza reglas de política de control de acceso (ACP) incorrectas durante la implementación de políticas en dispositivos FTD con objetos dinámicos. Esto puede dar lugar a que se rechace el tráfico legítimo, incluso cuando existan reglas adecuadas en la configuración en ejecución. Corregido en la versión 7.4.3.

Contenido relacionado

- ID de bug de Cisco CSCwo78475: El tráfico alcanza reglas ACP incorrectas durante la implementación de políticas en FTD con objetos dinámicos
- Soporte técnico y descargas de Cisco: Soporte técnico y descargas de Cisco

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).