Falha na implantação do FTD com firewall seguro

Problema

Interrupções e interrupções de rede foram observadas no Cisco Firewall Firepower Threat Defense (FTD). Os incidentes repetidos levaram à negação de tráfego, incluindo comunicações SNMP, e exigiram reinicializações de dispositivo e monitoramento contínuo para identificar a causa raiz e mitigar o impacto adicional.

Ambiente

- Dispositivos Cisco Secure Firewall Firepower 1140 (afeta qualquer modelo de FTD)
- Versões do software FTD: 7.4.2.4 (outras versões também são afetadas)
- Políticas de Controle de Acesso (ACPs) dinâmicas baseadas em objetos
- Implantações frequentes de políticas

Resolução

Para resolver os problemas recorrentes de failover e implantação de política em dispositivos FTD do Cisco Secure Firewall, um conjunto abrangente de etapas de solução de problemas e correção deve ser seguido. O fluxo de trabalho listado é estruturado para fornecer separação e explicação claras de cada etapa, incluindo monitoramento, coleta de dados, diagnóstico e orientação de atualização.

1: Use rastreadores de pacotes para verificar o roteamento e o acesso ao tráfego pretendido.

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

2: Use capturas no FTD para determinar se os pacotes estão sendo descartados na entrada 'por regra configurada', mesmo que uma regra e uma rota válidas existam para o tráfego.

```
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 os logs de mensagens do FTD para obter evidências de defeito 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: Associe os timestamps desses logs com aqueles dos logs de implantação no 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: Se os FTDs estiverem em HA, faça failover para o FTD de standby e verifique o mesmo depois para garantir a recuperação do tráfego.

6: Se registros e condições correspondentes forem encontrados no FTD, o dispositivo será afetado pelo defeito e poderá ser atualizado para a versão 7.4.3. Enquanto isso, as implantações poderão ser limitadas ao horário extra para reduzir o impacto no tráfego.

Causa

A causa subjacente dos impactos de tráfego observados e dos problemas de implantação de

políticas é atribuída a um defeito conhecido que afeta o software do FTD, nomeadamente:

- ID de bug Cisco CSCwo78475: o tráfego atinge regras incorretas de ACP (Access Control Policy, Política de controle de acesso) durante a implantação de política em dispositivos FTD com objetos dinâmicos. Isso pode resultar na negação de tráfego legítimo, mesmo quando existem regras apropriadas na configuração em execução. Corrigido na versão 7.4.3.

Conteúdo relacionado

- ID de bug Cisco CSCwo78475: O tráfego atinge regras incorretas de ACP durante a implantação da política no FTD com objetos dinâmicos
- Suporte técnico e downloads da Cisco: Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.