Errore di distribuzione FTD firewall protetto

Problema

Su Cisco Firewall Firepower Threat Defense (FTD) sono state osservate interruzioni e interruzioni della rete. La ripetizione degli incidenti ha causato la negazione del traffico, incluse le comunicazioni SNMP, e ha richiesto il riavvio dei dispositivi e il monitoraggio continuo per identificare la root cause e ridurre l'ulteriore impatto.

Ambiente

- Appliance Cisco Secure Firewall Firepower 1140 (impatto su qualsiasi modello FTD)
- Versioni software FTD: 7.4.2.4 (anche altre versioni interessate)
- Criteri di controllo di accesso dinamici basati su oggetti
- Distribuzioni frequenti di criteri

Risoluzione

Per risolvere i problemi ricorrenti di failover e distribuzione dei criteri nei dispositivi FTD Cisco Secure Firewall, è necessario seguire una serie completa di passaggi per la risoluzione dei problemi e la risoluzione dei problemi. Il flusso di lavoro elencato è strutturato in modo da fornire una separazione e una spiegazione chiare di ogni passaggio, incluse le istruzioni di monitoraggio, raccolta dei dati, diagnostica e aggiornamento.

1: utilizzare i tracciatori di pacchetti per controllare il routing e l'accesso al traffico previsto.

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

2: Utilizzare le acquisizioni effettuate nell'FTD per determinare se i pacchetti vengono scartati all'immissione 'tramite regola configurata', anche se per il traffico esistono una regola e una route valide.

```
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: Controllare i registri dei messaggi FTD per individuare eventuali difetti di 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: abbinare i timestamp per questi log a quelli per i log di distribuzione nell'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 i FTD sono in HA, eseguire il failover sull'FTD standby e controllare lo stesso in seguito per assicurare il ripristino del traffico.

6: Se vengono trovati log e condizioni corrispondenti nell'FTD, il dispositivo è interessato dal difetto e può essere aggiornato alla versione 7.4.3. Nel frattempo, le installazioni possono essere limitate al fuori orario per ridurre l'impatto sul traffico.

Causa

La causa alla base degli impatti sul traffico e dei problemi di implementazione delle politiche è

attribuita a un difetto noto che influisce sul software FTD, in particolare:

- Cisco Bug ID CSCwo78475: il traffico supera le regole errate dei criteri di controllo di accesso (ACP) durante la distribuzione dei criteri sui dispositivi FTD con oggetti dinamici. Ciò può causare il rifiuto del traffico legittimo, anche se esistono regole corrette nella configurazione in esecuzione. Risolto nella versione 7.4.3.

Contenuto correlato

- Cisco ID bug CSCwo78475: Il traffico supera le regole ACP non corrette durante la distribuzione dei criteri in FTD con oggetti dinamici
- Supporto tecnico Cisco e download: Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).