Problemen oplossen FMC-verkeer laat oude ACK-pakketten vallen na beëindiging TCP

Inhoud

uitgifte

In dit document wordt beschreven waarom FTD zich aanmeldt bij acl-drop-gebeurtenissen voor retourverkeer van FMC naar clientsystemen, met name ACK-pakketten die aankomen nadat TCP-verbindingen al zijn beëindigd door RST-pakketten van de client. De druppels zijn een product van een race-conditie op microsecondenniveau tussen Windows TCP-stapelgedrag en FMC's RFC 793-compatibele ACK-generatie. Er is geen service-impact en er is geen oplossing nodig.


Let op: dit is verwacht gedrag. De acl-drop gebeurtenissen zijn veilig om uit te filteren in monitoringsystemen zodra dit patroon is bevestigd.

Symptomen:

- FTD-firewalllogs tonen acl-drop-gebeurtenissen voor retourverkeer van FMC naar clientsystemen (JumpHost in dit voorbeeld)
- Drops vinden plaats op TCP-poort 443 (HTTPS)-verbindingen tussen FMC- en clientsystemen
- Gebeurtenissen verschijnen in FMC unified events als geblokkeerde pakketten
- Redencodes voor vallen die worden gezien bij opnames: tcp-rstfin-ooo, tcp-not-syn, acl-drop
- Er wordt geen werkelijke impact op de service waargenomen, ondanks de geregistreerde dalingen

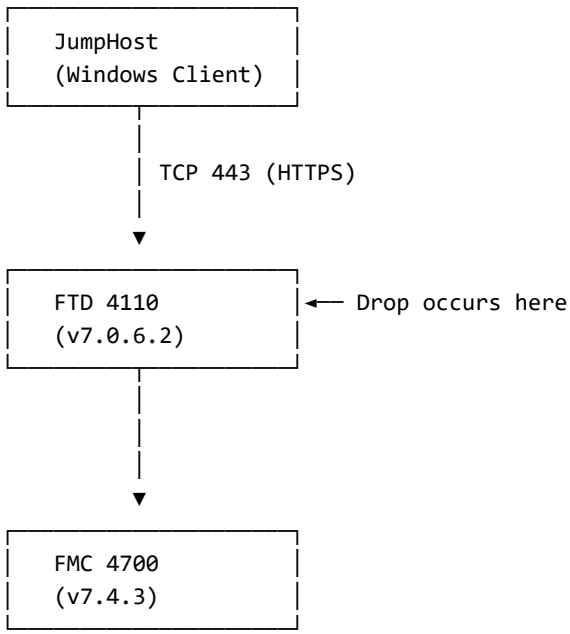
milieu

· Firewall: Cisco Secure Firewall Threat Defense (FTD) met versie 7.0.x, 7.2.x, 7.4.x of hoger (FPR-1000/2100/3100/4100/4200/9300 of FTDv)

· Management Center: Cisco Secure Firewall Management Center (FMC) 4600 / 4700 / FMCv met versie 7.2.x, 7.4.x of hoger

· Clientsysteem: Windows OS (JumpHost, Workstation of Server) via browser/API via HTTPS (TCP 443)

Eenvoudige topologie



resolutie

pakketvolgorde

Deze reeks gaat consequent vooraf aan de gelogde druppels:

```
Packet Flow & Timing Collision:
```

Step	Packet Direction	TCP Flags	Delta Timing	Description / State
1.	FMC ——► Client	[FIN, ACK]	T=0	FMC initiates graceful session close.
2.	Client → FMC	[ACK]	+0.2 ms	Client acknowledges FMC FIN.
3.	Client → FMC	[FIN, ACK]	+3ms - 13s	Application closes its half of socket.
4.	Client → FMC	[RST, ACK]	+15 - 31 µs	Windows immediately destroys socket.
5.	[FTD Firewall Action]	---	Immediate	FTD receives RST, purges connection from st
6.	FMC ——► Client	[ACK]	+0.06 - 2.2 ms	RFC 793 mandatory ACK for Step 3 FIN arrives.
7.	[FTD Firewall Action]	[acl-drop]	Immediate	No state table entry found -> Dropped as ac

---

Opmerking: de stappen 5 en 7 zijn het botsingspunt. De RST zorgt voor onmiddellijke statusverwijdering (stap 6) en de verplichte ACK van de FMC's (stap 7) komt aan in het venster tussen statusverwijdering en de volgende pakketbeoordelingscyclus.

TAC-onderzoeksmethodologie

Gebruik de volgende drie-tier correlatie proces bij het onderzoeken van vermoedelijke verouderde ACK druppels:

Stap 1 — Verzamel gegevens

- FTD-pakketopnamen op ingress, egress-interfaces en asp-drops
- TCP-dump van FMC gefilterd op poort 443

```
> system support diagnostic-cli
ciscoasa# capture ASP_DROP type asp-drop acl-drop
ciscoasa# show capture ASP_DROP | include 443
1: 10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104, win 501, length 0 (acl-
```

Stap 2 — Extraheren en correleren

· Extract 5-tuple van de asp drop capture geeft de druppels en redenen (tcp-rstfin-ooo, tcp-not-syn, acl-drop)

· Reconstrueer de tabel met de verbindingsstatus met behulp van ingress- en egress-opnames: identificeer SYN, FIN/RST en de exacte tijdstempels

· Correleer de druppel, de tijdstempel op de ingang / uitgang vangt tegen de sessie einde-van-leven tijdstempel

```
ciscoasa# show capture CAP_IN | include 10.10.10.50.55137
10:14:22.102110 10.10.10.50.55137 > 10.10.32.15.443: Flags [F.], seq 3829103, ack 1024
10:14:22.102128 10.10.10.50.55137 > 10.10.32.15.443: Flags [R.], seq 3829104, ack 1024
10:14:22.102345 10.10.32.15.443 > 10.10.10.50.55137: Flags [.], ack 3829104 (DROPPED)
```

Opmerking: de FMC ACK-reeks bevestigt het FIN-volgnummer $+ 1$, waarmee wordt bevestigd dat het een RFC-reactie is op een reeds beëindigde verbinding.

Stap 3 — Patroon bevestigen

- Drops bevestigen vindt alleen plaats nadat RST is verwerkt en niet tijdens actieve sessies
- Controleer of het gedropte pakket een ACK is met volgnummer = FIN_Seq + 1 (verplichte RFC 793-respons)
- Controleer of de uitval van de toepassing niet overeenkomt met de uitvalgebeurtenissen

---

Tip: In het referentiegeval (SR 700468261) werd RST in 54 van de 55 sessies als eindpakket vermeld. Eén sessie (poort 55137) toonde FMC's ACK die 0,024 ms na de RST aankwam, wat direct de timing van de race-conditie aantoonde.

---

resolutie

Er is geen sanering nodig. Dit gedrag is volledig in overeenstemming met de TCP RFC-normen en het stateful firewall-ontwerp. Er is geen defect, verslechtering van de prestaties of gegevensverlies.

Wanneer te escaleren

Waarschuwing: escaleer NIET alleen op basis van dit valpatroon. Escaleer alleen als aan de voorwaarden in de volgende sectie is voldaan.

- Drops treden op tijdens actieve sessies - niet na RST of FIN / ACK-uitwisseling
- Toepassingsfouten, time-outs voor sessies of ontoegankelijkheid van de FMC-gebruikersinterface worden waargenomen
- Het valvolume neemt in de loop van de tijd toe zonder een overeenkomstige toename van het verbindingsvolume
- Het valpatroon wijkt af van de in dit artikel beschreven volgorde

Oorzaak

De dalingen zijn het gevolg van een race-conditie op microsecondetijdschaal tussen drie onafhankelijk correcte gedragingen:

1. Windows TCP Stack Optimization: Wanneer een Windows-toepassing een socket sluit waar het externe uiteinde al FIN heeft verzonden, verzendt Windows onmiddellijk een FIN-ACK. Dit is na de RST-ACK binnen 15 - 31 seconden om onmiddellijk geheugen en TCP-besturingsblokken vrij te maken.
2. FTD Stateful Connection Removal: Na ontvangst van het RST-pakket wordt de verbinding door FTD onmiddellijk afgebroken en verwijderd uit de statustabel (aansluittabel) om de statusbeveiliging te behouden.
3. Naleving van FMC RFC 793: Volgens de specificaties van RFC 793 genereert de FMC TCP-stack een ACK waarin de FIN van de client wordt bevestigd (reeks $+ 1$). Vanwege systeemplanning en propagatievertraging bereikt dit ACK de FTD.
   0,06 -- 2,2 ms nadat de RST de verbinding al heeft doorgespoeld.
4. FTD Drop Evaluation: Aangezien er geen overeenkomende verbinding bestaat in de statustabel en het pakket alleen de ACK-vlag heeft (geen SYN), evalueert FTD deze ten opzichte van de Access Control List (ACL). Zonder een expliciete vergunning voor out-of-state ACK's, laat FTD het pakket vallen als acl-drop / tcp-not-syn.

Gerelateerde inhoud

- RFC 793 — Transmission Control Protocol
- Reden voor ASP-daling
- SR Referentie: 700468261 (Intern)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.