Nexus 7000 Protocol voor probleemoplossing (ARP) - firewall zonder inband Capture

Inhoud

Inleiding

Dit document beschrijft hoe u de ARP storm zonder inband ARP-verkeer kunt oplossen.

Achtergrond

ARP storm is een gewone denial-of-service (DoS) aanval die u in de datacenteromgeving ziet.

De gemeenschappelijke schakelaar logica om ARP pakje aan te gaan is dat:

- ARP-pakket met Application Media Access Control (MAC)
- ARP-pakket met MAC van de eenrichtingsbestemming, dat tot de switch behoort

zal door ARP in de software worden verwerkt als de Switch Virtual Interface (SVI) in het ontvangende VLAN is geïnstalleerd.

Door deze logica, als er één of meer maliceuze hosts zijn blijven het verzenden van ARP-verzoek in een VLAN, waar een switch de gateway van dat VLAN is. Het ARP-verzoek wordt in software verwerkt en zorgt ervoor dat de switch overweldigd is. In één of andere oudere het switchmodel en de versie van Cisco, zult u zien dat het ARP-proces het CPU-gebruik tot op hoog niveau brengt en het systeem te druk is om ander besturingsplanverkeer aan te kunnen. De gebruikelijke manier om een dergelijke aanval te traceren is inband opname te laten uitvoeren om de bron MAC van de ARP-storm te identificeren.

In het datacentrum waar Nexus 7000 optreedt als aggregatiegateway, wordt een dergelijke impact door CoPP op Nexus 7000 Series-switches verminderd. U kunt nog steeds Ethanalyzer voor inband-opname op de Nexus 7000-gids voor probleemoplossing gebruiken om de bron MAC van de ARP-storm te identificeren, aangezien Controle van Plane Policing (CoPP) slechts een vertraging van de afwikkeling is, maar de ARP-storm die naar de CPU overspoelt niet verliest.

Wat denk je van dit scenario waarin:

- SVI is omlaag
- Geen excessief ARP-pakket dat wordt opgevoerd naar CPU
- Geen hoge CPU's door ARP-proces

De switch ziet echter nog steeds een ARP-gerelateerd probleem, bijvoorbeeld een direct aangesloten host heeft onvolledige ARP. Is het mogelijk veroorzaakt door ARP storm?

Het antwoord is ja op Nexus 7000.

Root-oorzaak

In het linecard-ontwerp van de nexus 7000, om ARP-pakketproces in CoPP te ondersteunen, zal een ARP-verzoek een speciale logische interface (LIF) besturen en vervolgens wordt de snelheid beperkt door CoPP in expediteur (FE). Dit gebeurt ongeacht of je een SVI-account hebt voor de VLAN of niet.

Terwijl de definitieve beslissing van FE om het ARP-verzoek niet naar inband CPU te sturen (in het geval geen SVI up voor het VLAN), wordt de CoP-teller nog steeds bijgewerkt. Het leidt tot CoPP verzadigd met excessief ARP verzoek en het laten vallen van legitiem ARP verzoek/antwoord. In dit scenario, zult u geen excessieve inband ARP pakketten zien maar nog steeds door ARP storm worden beïnvloed.

We hebben een aangescherpt bug CSCub47533 ingediend voor dit CoPP dag één gedrag.

Oplossing

Er zouden een paar opties kunnen zijn om de bron van ARP storm in dit scenario te identificeren. Eén effectieve optie is:

- Identificeer eerst welke module de ARP storm komt

```
N7K# sh policy-map interface control-plane class copp-system-p-class-normal
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match exception ip multicast directly-connected-sources
match exception ipv6 multicast directly-connected-sources
match protocol arp
set cos 1
police cir 680 kbps bc 250 ms
conform action: transmit
violate action: drop
 module 3:
conformed 4820928 bytes,
5-min offered rate 0 bytes/sec
peak rate 104 bytes/sec at Thu Aug 25 08:12:12 2016
 violated 9730978848 bytes,
       5-min violate rate 6983650 bytes/sec
       peak rate 7632238 bytes/sec at Thu Aug 25 00:43:33 2016
module 4:
conformed 4379136 bytes,
5-min offered rate 0 bytes/sec
peak rate 38 bytes/sec at Wed Aug 24 07:12:09 2016
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
...
```

- 2gebruik ELAM Procedure om alle ARP pakket op te nemen dat de module aanslaat. Misschien moet je het meerdere keren doen. Maar als er een storm aan de gang is, is de kans

dat u het violette ARP-pakket opneemt veel beter dan het legitieme ARP-pakket. Identificeer de bron MAC en VLAN van de ELAM vangst.