Nexus 7000 Troubleshoot Address Resolution Protocol (ARP) Storm Without In-Band Capture

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der ARP-Sturm ohne inband-ARP-Datenverkehr behoben wird.

Hintergrund

Ein ARP-Sturm ist ein häufiger Denial-of-Service (DoS)-Angriff, den Sie in der Rechenzentrumsumgebung sehen würden.

Die gängige Switch-Logik zur Verarbeitung von ARP-Paketen lautet wie folgt:

- ARP-Paket mit Broadcast Destination Media Access Control (MAC)
- ARP-Paket mit Unicast-Ziel-MAC, das zum Switch gehört

wird über den ARP-Prozess in der Software verarbeitet, wenn die Switch Virtual Interface (SVI) im empfangenden VLAN aktiviert ist.

Wenn ein oder mehrere bösartige Hosts weiterhin ARP-Anfragen in einem VLAN senden, wobei ein Switch das Gateway dieses VLAN ist, Die ARP-Anfrage wird softwarebasiert verarbeitet, wodurch der Switch überlastet wird. Bei älteren Cisco Switch-Modellen und -Versionen wird der ARP-Prozess die CPU-Auslastung auf ein hohes Niveau anheben und das System ist zu beschäftigt, um anderen Steuerungsebenen-Datenverkehr zu verarbeiten.Die gängige Methode zur Nachverfolgung eines solchen Angriffs ist die In-Band-Erfassung, um die Quell-MAC des ARP-Sturms zu identifizieren.

In Rechenzentren, in denen der Nexus 7000 als Aggregation Gateway fungiert, werden diese Auswirkungen durch CoPP auf Nexus Switches der Serie 7000 reduziert. Sie können auf dem Nexus 7000 weiterhin Inband-Ethanalyzer zur Fehlerbehebung ausführen, um die Quell-MAC des ARP-Sturms zu identifizieren, da Control Plane Policing (CoPP) nur ein Banditen ist, der langsamer ist, aber nicht den ARP-Sturm auf die CPU auslöst.

Wie sieht es mit diesem Szenario aus:

- SVI ist ausgefallen.
- Kein übermäßiges ARP-Paket auf CPU beschränkt
- Keine hohe CPU aufgrund des ARP-Prozesses

Der Switch sieht jedoch weiterhin ARP-bezogene Probleme, z. B. wenn der direkt verbundene

Host unvollständige ARP-Protokolle hat. Ist es möglich durch den Sturm von ARP verursacht?

Die Antwort lautet "Ja" für Nexus 7000.

Ursache

Im Design der Nexus 7000-Linecard wird zur Unterstützung des ARP-Paketprozesses in CoPP für die ARP-Anforderung eine spezielle logische Schnittstelle (LIF) bereitgestellt. Anschließend wird die Rate durch CoPP in der Forwarding Engine (FE) begrenzt. Dies geschieht unabhängig davon, ob eine SVI für das VLAN vorhanden ist oder nicht.

Während die endgültige Weiterleitungsentscheidung der FE darin besteht, die ARP-Anforderung nicht an die In-Band-CPU zu senden (falls keine SVI für das VLAN vorhanden ist), wird der CoPP-Zähler trotzdem aktualisiert. Dies führt dazu, dass CoPP mit übermäßigen ARP-Anfragen gesättigt ist und legitime ARP-Anfragen/Antworten verworfen werden. In diesem Szenario werden keine übermäßigen In-Band-ARP-Pakete angezeigt, aber noch von einem ARP-Sturm betroffen.

Wir haben einen verbesserten Bug CSCub47533 für dieses Verhalten von Tag 1 eingereicht.

Lösung

In diesem Szenario gibt es möglicherweise einige Optionen, um die Quelle des ARP-Sturms zu identifizieren. Eine effektive Option ist:

- Ermitteln Sie zuerst, von welchem Modul der ARP-Sturm kommt.

```
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
...
```

- Zweite Verwendung des ELAM-Verfahrens zur Erfassung aller ARP-Pakete, die das Modul

erreichen Vielleicht müssen Sie es mehrere Male tun. Wenn jedoch ein Sturm stattfindet, ist die Wahrscheinlichkeit, dass Sie das verletzte ARP-Paket erfassen, viel besser als das legitime ARP-Paket. Identifizieren Sie die Quell-MAC und das VLAN aus der ELAM-Erfassung.