Palo Alto

- Flytt av nät eller routing
- AUX-Portar för HA-kommunikation på 5000-serien
- Packet Capture
- BGP
- Epost från Panorama vid misslyckad commit
- Session-konfiguration
- SNMP
- Multicast
- System-loggar i CLI
- tcpdump management-interface

Flytt av nät eller routing

När man behöver flytta ett nät eller en rutt har jag stött på patrull, trots att man har gjort rätt enligt konstens alla regler (dvs regelverk och routing stämmer).

I mitt fall så såg jag inte all trafik jag förväntade mig i ett brandväggspar, i det andra såg jag bara trafik från en riktning och de sessionerna blev incomplete. När jag gjorde en packet capture direkt på klustret så syndes dock trafiken. I det här scenariot var det GRE-trafik det handlade om, men jag har stött på det med TCP tidigare.

Det berodde på att en gammal session låg kvar i brandväggsklustret som var knutet mot det gamla interfacet. Jag var tvungen att hitta sessions ID:t i CLI och döda sessionen.

AUX-Portar för HA-kommunikation på 5000-serien

Följer man det här dokumentet korrekt så kommer man inte ha några problem.

Men glömmer man att aktivera ICMP på interfacen så kan det fungera tills det inte gör det. Jag var med om en uppsättning 5250-brandväggar som det inte var aktiverat på. Enda fram till uppgradering till 10.2.13-h3, vid första försöket, och 11.1.6-h10 vid andra försöket. 10.2.10-h9 var sista det fungerade på.

När den patchade brandväggen blev online gick de fysiska interfacen upp men brandväggarna såg inte varandra, vilket ledde till ett Active/Active / split-brain-scenario.

Efter ICMP aktiverades på interfacen fungerade det igen. Så trots att det alltid har varit ett krav har det lirat 9.x, 10.0.x, 10.1.x och delar av 10.2.x... tills det inte längre lirade.

Packet Capture

Multicast

Gör man en klassisk packet capture via Monitor -> Packet Capture så kan man inte kolla efter source IP, för då matchar man inte IGMP join paketen. Istället bör man kolla efter destination, ex. 224.0.0.22.

BGP

Kommandona nedan kan behöva bytas till advanced-routing och logical-router, om man kör det läget.

To restart/refresh BGP sessions, run the following commands:

- For self initiation:
  `> test routing bgp virtual-router default restart self` (for restarting BGP connections)
  `> test routing bgp virtual-router default refresh self` (for refreshing BGP connections)
- From Peer side:
  `> test routing bgp virtual-router default restart peer <BGP peer>` (for restarting BGP connections)
  `> test routing bgp virtual-router default refresh peer <BGP peer>` (for refreshing BGP connections)

Epost från Panorama vid misslyckad commit

Väldigt bra att bli notifierad om en commit misslyckas.

Jag konfigurerade enligt den här reddit-tråden för att få epost när commit misslyckas till en brandvägg som hanteras via Panorama.

> In the Collector Group > Collector Log Forwarding > System Tab.
> Created a filter to email to my team. Filter : (description contains 'CommitAll job failed')

För att hantera commits som misslyckas direkt i Panorama gäller nog nedan:

> go to panorama tab > log settings > system > Add
>
> Set the relevant filter which catches failed commits - you'll have to double check but it may be something like (description contains 'CommitAll job failed'). Try by yourself in monitor > system tab until you find the right filter.
>
> Finally, set the email profile to use (you may have to create one, specifying your SMTP relay and other details).

Session-konfiguration

Device > Setup > Session

Rematch session vill man ha aktiverat. Annars så slår inte regelverksförändringar på etablerade sessioner. Det är inte produktionsstörande att aktivera.

SNMP

Man kan antingen köra SNMPv2 eller SNMPv3, inte båda samtidigt.

Multicast

Den här artikeln är skriven enligt att advanced routing är aktiverat.

Skillnader legacy routing / advanced routing

I ett långt supportärende om SSM fick vi till slut följande information av PA TAC:

> *After Analyzing the Pcaps we can see the packets are coming with any source.*
> *Since we are using Dynamic IGMP, source IP must be included in the Packet for Firewall to Process further so that it's FIB can be populated*
>
> *For Static IGMP, we are specifying Source in Firewall configuration itself so that if IGMP packets come from that particular source will be allowed*
> *While Dynamic IGMP has an option to add Filters, those are basically like access list which either allows or denies the traffic but it will not be enforced as Source*
>
> *Why it is working on Legacy Routing but not Adv. Routing?*
> *==> Legacy routing is relaxed compared to Adv. Routing which is much more strict and in compliance with RFC.*

M.a.o., IGMPv3 Membership Reports behöver en source IP och kan inte använda sig av ASM. Advanced routing generellt följer tydligen RFCerna bättre.

IGMP

IGMP Static Join

Konfigurerar man ett static join värde under Logical Router -> LR-namn -> Multicast -> IGMP -> Static så skickas automatiskt ett PIM Join-meddelande uppströms. I konfigurationen behövs ett namn, ett interface med en lyssnare (mot receiver), en grupp-adress och en source-adress. Source-adressen måste vara en /32.

System-loggar i CLI

Det kan vara segt att ta fram system-loggar. Med kommandot nedan kan man hitta relevanta loggar i CLI istället:

`show log system object equal ethernet1/23`

ethernet1/23 byts ut till det man letar efter.

Vill man se dagens loggar måste man ange start-time, annars får man se ALLA loggar: `show log system start-time equal 2025/12/19@06:00:00`

tcpdump management-interface

Det går att göra tcpdump för management-interfacet. Se artikel här: https://docs.paloaltonetworks.com/ngfw/administration/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface

Vid felsökning neighbor solicitation/advertisement på Panorama har följande använts:

- tcpdump filter "ip6 and icmp6" = Starta insamling med listat filter
- view-pcap mgmt-pcap mgmt.pcap = Se filen. Filen skrivs över varje gång man startar en insamling med ovan kommando