Wednesday, May 09th 2018

LD4 Connection issue – Incident Report

Contents

1. Incident description:

The service was partially and intermittently not accessible to smartTrade clients in LD4.

2. Event timeline

Please find below a description of all the events in chronological order.

Date time (UTC)	Description
2018/05/09 17:34	smartTrade monitoring tool raised an alert for on LD4 site for some incoming and outgoing connections leading to not being able to connect to some venues or for clients to have troubles to access some smartTrade services.
2018/05/09 17:35	smartTrade started to contact its clients to notify about a network issue in LD4 site.
2018/05/09 18:08	smartTrade updated the clients that its team still working to get the issue resolved
2018/05/09 18:49	smartTrade started to contact its clients to notify that the network issue in LD4 is fixed.
2018/05/09 20:02	The network issue is faced.
2018/05/09 20:04	smartTrade started to contact its clients to notify that the network issue occurred again.
2018/05/10 02:07	The network issue to LD4 is totally fixed and stabilized and smartTrade started to check the sanity of environments and to notify about the resolution.

3. Root cause:

The smartTrade LD4 infrastructure is protected by a cluster of redundant firewalls (primary and secondary) to handle failover.
The ARP table of both firewalls of the cluster have been flooded by a broad range of IP addresses. This caused instability of the cluster and issues to initiate and receive connections, as well as keeping them alive.

4. Investigation steps and corrective actions:

- The Ops team has been notified immediately by the Client Services team that sessions with clients were disconnecting (picked up in Centreon)
- We immediately logged into our primary firewall and observed that the cluster had failed over to the secondary (which caused the expected drop in connections)
- We began to investigate what was causing the overload and saw that our arp table was getting overloaded to the point that we could not pass traffic correctly between the two firewalls (which caused them to instantly fail-over)
- Sessions were not re-establishing right away (as they should have with the failover). We decided to fail back over to fw1 to see if sessions would re-establish there
- Sessions began to re-establish on fw1 and platform had stabilized for a short amount of time
- Again, we noticed a fail-over from fw1/fw2. We decided at this point that the best course of action would be to reboot fw1. Fw2 was still overloaded at this point and could not handle the network traffic
- After fw1 had rebooted, we were still experiencing issues with fw2 and decided to fail-over again to fw1. Fw1 was at this point active but not accepting any connections from clients
- From the datacenter, we manually powered off the fw2 to completely isolate fw1
- We decided to increase the size of the arp tables - this temporarily fixed the issue and indicated we were on the right track
- By analyzing the content of the arp table, we found that the address flooding us were coming from the same prefix and reached out to Cogent (Internet provider) to block the prefix from reaching us
- We continued to increase the ARP cache until we the network was stable
- Once fw1 was stable, we did bring back up fw2

5. Measures for the future avoidance of similar occurrences:

smartTrade is working with his Internet providers to put in place a mitigation plan.