Sharedband
Faster Broadband Today

Incident Report

Sharedband Service outage London 09th June 2018

Executive Summary

On the 9th June at 20:45, Sharedband suffered a sustained Denial of Service attack towards an aggregation server. The volume of traffic caused timeouts and service disruption for customers.

At 20:51 the volume of traffic caused one of the boarder routers to reboot. All the traffic shifted to the redundant boarder router and at 20:55 it too rebooted.

Both routers had stabilised by 21:02 and routing protocols established adjacencies. Customer routers started to connect to their respective Aggregation Services and by 21:10 traffic levels on the network had restored to normal.

Table of Contents

Incident Details

On the 9th June at 20:45, Sharedband suffered a sustained Denial of Service attack against a Production Aggregation server. The volume of traffic caused time outs for customers and at 20:47 the first system alerts were received.

Engineers proceeded to connect to the environment to establish the cause of the system alerts. At 20:51, the primary boarder router failed due to load and rebooted. This caused routing protocols to converge and traffic shifted to the redundant boarder router.

At 20:55 the redundant router also rebooted due to load. By this time the primary router was up but routing adjacencies had not yet established. By 21:02 routing protocols had established adjacencies to upstream routers again and traffic started to flow across the network again. This allowed customer routers to connect to the service again.

At 21:10, traffic levels had returned to normal and the incident had cleared.

Root Cause Analysis

Due to primary connectivity being disrupted to the routers, engineers had to connect to the routers via the emergency Out-Of-Band management network. By this time, the routers had rebooted, and the Denial of Service attack had stopped. Engineers were unable to establish the attach method or vector used against the Aggregation Service. Due volume of traffic it is suspected that this was some type of amplification attack.

Mitigation

At this point it is expected that this was an isolated event and amplification attacks are extremely difficult to prevent at the network perimeter. We are monitoring the network carefully for signs of any further attempts at a Denial of Service.