Network Playbook against DDoS in DNS and CDNs (abstract)

A S M Rizvi
USC/ISI

Leandro Bertholdo
University of Twente

Joao Ceron
SIDN Labs

John Heidemann
USC/ISI

IP anycast is used by DNS and CDN services to provide service from multiple geographic locations with the same IP address. Anycast increases the aggregate capacity of a service, and each site operates independently, so a Distributed Denial-of-Service (DDoS) event affecting one site may leave the others without overload. Anycast uses BGP to associate users in different networks with different sites, dividing the world into *catchments*.

DDoS attacks make a service unavailable to the legitimate clients by exhausting the service resources [3]. DDoS attacks are getting bigger, and recent reports show attacks with 2.4 Tb/s intensity that surpass previous largest intensity [6, 9]. The vulnerabilities in millions of IoT devices, and the availability of automated tools make it easier to run these attacks.

Though anycast can provide capacity and can isolate the attackers into certain catchments, DDoS remains common and can harm services using anycast. During an attack, if some sites have excess capacity, operators would like to shift traffic to serve more customers successfully. Prior studies indicate that operators use traffic engineering to shift traffic [5], but using these techniques effectively is still not documented.

Contribution: In this abstract, we propose to build "network playbooks'. A playbook can help decision about how to use TE to make an informed decision, rather than guessing or making routing changes based only on prior experience. A playbook will give the operators confidence in their decisions, guide them about the implications of TE changes, and help the operators make decisions promptly. Operators build playbooks ahead of time (proactively, before an attack) by evaluating all possible routing configurations and their impacts over traffic distribution. During an attack, operators can use the playbook to choose a routing configuration. If any routing option from the playbook is likely to keep the traffic load within the limit of each site, an operator can announce that routing configuration. After the announcement, operators should observe the results of the TE, then deploy additional changes if necessary. We focus only on the "network playbook" part here, the detailed defenese approach is in our full paper [8].

Building the playbook: We build the playbook prior to an attack event with all the possible routing options and their impacts over traffic distribution. Since we do not want any service interruption, we build the playbook using a test prefix. We suggest to build the playbook once every week or month because of the changes in the BGP routing [8].

BGP is the tool to make routing changes and control the traffic distribution among anycast sites. We use three BGP mechanisms to build the playbook: path prepending, BGP communities, and path poisoning [1, 4]. We observe the new traffic distribution after a routing change using Verfploeter [2]. Verfploeter can predict the load at each site by mapping /24 networks to anycast sites.

Routing Policy	Traffic to Site (%) AMS	BOS	CNF
(a) Route-server	15	35	55
(b) All-IXP-Peers/Poison transits	15	35	45
(c) 2xPrepend AMS	25	35	45
(d) 1xPrepend AMS	35	25	35
(e) -1xPrepend BOS	45	45	15
(f) -1xPrepend CNF	45	5	45
(g) Transit-1	45	25	35
(h) Transit-2	55	15	25
(i) Poison Tier-1/Transit-2	35	25	35
(j) Poison Transit-1	55	25	25
(k) Baseline	65	15	15
(l) 1,2xPrepend BOS	65	5	25
(m) 1,2,3xPrepend CNF	75	15	5
(n) -1,-2,-3xPrepend AMS	85	5	5

Table 1: A sample network playbook with three anycast sites (colors showing the traffic compared to the baseline distribution).

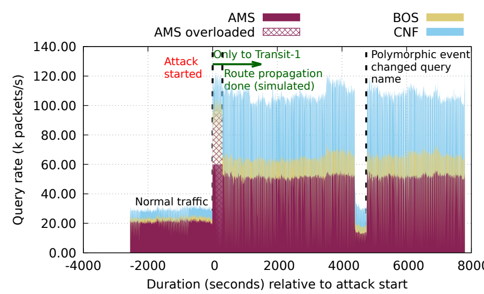

Figure 1: B root attack and response.

Playbook: We can see a sample playbook with three sites from Peering testbed in Table 1. The playbook shows traffic distribution at different routing configurations. During an attack, operators can select from these options and can predict the impact over other anycast sites.

Real-world attack and response: We show an attack event from 2017-03-06 captured at B root in Figure 1 [7]. We assume the capacity at each site is 60 k packets/s. The attack starts at time 0 which overloads AMS site (striped area). We look over the playbook to find a routing option that will redistribute the total load. We announce only to Transit-1 using a community string. After the propagation of new routing announcement (after 300 s), there is no striped area which indicates the mitigation of the attack event. Using this real-world event, we show the applicability of a network playbook. Our defense takes decisions based on the traffic volume; getting attack prefixes and using per prefix mapping can make even accurate predictions.

REFERENCES

[1] Matthew Caesar and Jennifer Rexford. BGP routing policies in ISP networks. 19(6):5–11, November 2005.

[2] Wouter B. de Vries, Ricardo de O. Schmidt, Wes Hardaker, John Heidemann, Pieter-Tjerk de Boer, and Aiko Pras. Verfploeter: Broad and load-aware anycast mapping. In *Proceedings of the ACM Internet Measurement Conference*, London, UK, 2017.

[3] Tom Emmons. 2021: Volumetric ddos attacks rising fast. https://www.akamai.com/blog/security/2021-volumetric-ddos-attacks-rising-fast/, 2021. [Online; accessed 23-October-2021].

[4] Ethan Katz-Bassett, David R Choffnes, Ítalo Cunha, Colin Scott, Thomas Anderson, and Arvind Krishnamurthy. Machiavellian routing: improving internet availability with bgp poisoning. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, pages 1–6, 2011.

[5] Giovane C. M. Moura, Ricardo de O. Schmidt, John Heidemann, Wouter B. de Vries, Moritz Müller, Lan Wei, and Christian Hesselman. Anycast vs DDoS: Evaluating the November 2015 root DNS event. In *Proceedings of the ACM Internet Measurement Conference*, November 2016.

[6] Jon Porter. Amazon says it mitigated the largest ddos attack ever recorded. https://www.theverge.com/2020/6/18/21295337/amazon-aws-biggest-ddos-attack-ever-2-3-tbps-shield-github-netscout-arbor, 2021. [Online; accessed 24-October-2021].

[7] LANDER project. Lander:b root anomaly-20170306. https://ant.isi.edu/datasets/readmes/B_Root_Anomaly-20170306.README.txt, 2019. [Online; accessed 27-April-2020].

[8] ASM Rizvi, Joao Ceron, Leandro Bertholdo, and John Heidemann. Anycast agility: Adaptive routing to manage ddos. *arXiv preprint arXiv:2006.14058*, 2020.

[9] Alethea Toh. Azure DDoS protection—2021 q1 and q2 ddos attack trends. https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q1-and-q2-ddos-attack-trends/, 2021. [Online; accessed 23-October-2021].