OARnet

An OH·TECH Consortium Member

The Quilt Winter Member Meeting 2018
DDoS Protection and Cisco Umbrella // OpenDNS

Paul Schopis – Interim Executive Director;
Chief Technology Officer

Meeting Members' Needs and Expectations

OARnet

An OH·TECH Consortium Member

DDoS

Need and Expectation

- Members and clients need a DDoS solution that is
  - Scalable
  - Affordable

- Historically had looked at distributing scrubbers in a number of our POPs
  - Very costly
- Solutions that entailed rerouting via tunnels or hybrid device/tunnel
  - Offerings not scaling to our needs
  - Hybrid had limited success due to boots on the ground at scale problems

How we got where we are with DDoS

- AT&T had a solution that was the GRE tunnel type of arrangement requiring an access port from them. Original offer was 10G.
  - Not big enough, had already seen 20 Gbps attacks
- AT&T also wanted internet business; we expressed what a minimum threshold was for serious discussion.
- Came back with an offer that hit threshold both in price and minimum commitment and included DDoS
- To meet procurement requirements we put it out to bid, and much to our surprise CenturyLink came back with a similar offer.

- 100G CenturyLink : Akron and Dayton
- 100G AT&T : Cleveland and Columbus
- 400Gb/s aggregate capacity, ~ 4x increase
- 11/1/2017 – all circuits up and in production. Legacy 10G transit circuits ordered out by end of 2017

OARnet Cloud Based DDoS

- Service provided by AT&T and CenturyLink
- Inclusive to all customers purchasing Internet service from OARnet.
- On-Demand, or customer initiated mitigation service is available now. Both AT&T and CenturyLink services have been enabled. Proactive ready for initial customer testing.
- Working through internal processes to operationalize the service – mitigation will be handled by our tier2 group. Supported now through escalations to senior engineering staff.
- Customers load-sharing with other carriers will not be fully protected by OARnet DDoS service. Might require disabling other carrier in the event of a DDoS.

OARnet Cloud Based DDoS (On-Demand)

- Expands filtering of protocols, ports, and IP addresses to application filtering. Increases capacity of DDoS filtering from 10's of Gb/s to Tb/s. In the past, using black-hole routes to signal upstream transit carriers to drop all traffic to a destination. Black-hole routes used to protect the infrastructure from volumetric attacks has the side effect of denying service to the target server.

- Now Cloud service allows for much more granular application level filtering to enable mitigation of DDoS without loss of application service.

- Now have the aggregate carrier capacity for simple port/protocol filters (Tb/s) plus hundreds of Gb/s across distributed scrubbing centers for more complex application level filters.

OARnet Cloud Based DDoS (Monitored)

- Provides an “always-on” level of protection. Cloud providers use automated tools to inspect traffic and initiate DDoS mitigation.
- Tools require a learning period to help minimize false positives.
- Much faster level of response. On-Demand mitigation usually requires notifying OARnet of the issue before any intervention is taken.
- Offered as a premium service with OARnet Commodity Internet.
- OARnet tier2 group is notified of events and has access to reporting tools. Monitored DDoS service is active, working through internal processes and procedures.

OARnet
An OH·TECH Consortium Member

OpenDNS/Cisco Umbrella

How we got where we are with OpenDNS/Umbrella

- K-12 and state customers needed malware and content filtering. Campuses have shown some interest as well.
- K-12 and state customers have tried appliance based in-line solutions with limited success.
  - Scalability issues
  - Boots on the ground
- OpenDNS/Umbrella offers a scalable approach that is cloud based i.e. on in-line appliance to maintain.

Cisco Umbrella – Malware Command & Control

- Command and Control Servers (also known as C2's) are used by malicious actors to control infected computers.
- C2's can send a "heartbeat" that acts as a keep alive and check-in as well.
- As long as the Malware can communicate with the C2, the malware can either be controlled, ordered to propagate, etc.
- Common C2 channels we see are through HTTP // HTTPS, however some C2 channels utilize other network protocols such as DNS.

Cisco Umbrella – Stopping Malware

- Cisco's new Umbrella Product utilizes OpenDNS and Threat intelligence from their Talos team to stop Malware.
- Umbrella offers DNS and IP-Layer enforcement to stop malware from contacting known malicious command and control servers.
- Umbrella also blocks communication with known websites that commonly distribute malware.
- Example:
  - maliciousdomain.com is serving malware to hosts via ads. Umbrella blocks the connection to maliciousdomain.com , preventing the site from serving malware to our endpoint.

Cisco Umbrella – Content Filtering

- A huge bonus of the Umbrella product is that our clients will gain the ability to filter content at the DNS level.
- Umbrella can filter based on:
  - Site Type:
    - Blocks based on Social Media, Gambling, Adult Content, Violence, etc.
  - DNS VPN Tunneling
    - Blocks VPN services that can be used to bypass corporate / academic policy.
  - Custom Destination Lists
    - Example: If OARnet sees malicousdomain.com is malicious before TALOS / Umbrella, we could block this connection via a destination list.

Perks of Cisco Umbrella for OARnet Clients

- Ability to remove traditional in-line solutions.
- Ability to place the Umbrella Client on a machine, and that machine keeps the security policy no matter what network the machine is connected to.
- HTTPS traffic is also filtered by Umbrella natively, opposed to traditional in-line solutions that typically require more work to intercept this traffic.

Cisco Umbrella – Where we are at

- OARnet is currently testing the Cisco Umbrella product.
- OARnet is in the process of obtaining enrollment numbers from OARnet Customers to get a rough number of those interested for bargaining purposes. Initial quotes suggest OARnet would receive >70% discount for Umbrella Services.
- OARnet could offer the product in three different ways:
  - Client is hands off (Just point to our DNS Forwarders // C2 and Malware Protection)
  - OARnet is the master, Clients have their own dashboard (Custom policies, access, and content filtering.)
  - OARnet is only a contract mechanism. (Think OARnet's VMware contract)

OARnet
An OH·TECH Consortium Member

For more information, Contact.

Paul Schopis
Email: pschopis@oar.net