DoS and DDoS Attack Prevention

DoS and DDoS attacks are on the rise, and they are getting more sophisticated and intense every year.

OneNeck® IT Solutions takes these potential attacks very seriously and have numerous preventative measures in place to ensure the safety of our customer's data. In truth, DDoS attacks alone are an annoyance to online users and can cost a company lost business during the time they deny access to customers, but rest assured OneNeck is working diligently to mitigate the risks associated with these attacks.

One Size Fits One

When OneNeck helps our customers plan for potential Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, we do not believe that "one size fits all." Our various customers have very different needs. Some customers provide a web-based service to their clients, requiring security filtering at the web application layer; others provide Internet-scale products to their clients requiring high-bandwidth, low-latency connectivity to the Internet; and other customers host high-value private applications such as VDI or ERP, which connect to the Internet primarily for secure VPN-based access. OneNeck works with each customer to build an appropriate defense against Internet-based attacks.

The Capacity to Deliver

Depending on customer need, the customer-specific gateway to the Internet could be anything from a virtual firewall with 100 Mbps capacity, to a clustered hardware firewall solution with 1 Gbps of capacity, or even a web-scale security perimeter which can filter multiple Gbps in ASICs. For all our Internet customers, OneNeck's Internet infrastructure is designed to deliver full-speed connectivity from that customer's environment to the Internet. Each OneNeck data center with ReliaCloud® is served by 10 Gbps or more of Internet connectivity. This connectivity reliably delivers Internet traffic, large or small, to the customer's deployment, allowing the customer's security perimeter to do its job.

Intelligent Internet Delivery

No matter what capacity a customer's security perimeter may support, there will be DoS attacks which are even bigger. OneNeck's Internet infrastructure must discard some of the traffic, in order to fit the remaining traffic into the service contracted by our customer. In such cases, OneNeck separates the traffic into several traffic groups, and looks for any group which may have excessive amounts of traffic. For example, during a Web Syn flood to a customer with a OneNeck 1 Gbps Internet service, there may be 2 Gbps of Web Syn packets, along with normal amounts of other types of traffic. In this case, OneNeck's router will discard as much of the Web Syn traffic as necessary, to fit the remaining traffic onto the 1 Gbps service. Other traffic types, including non-Syn web traffic, DNS, VPN tunnels, SSH/RDP etc. will be largely unaffected by the Web Syn flood.

Optional Sub-gigabit Service

For colocated customers with security services which cannot filter a full 1 Gbps of abusive traffic, OneNeck can limit the amount of traffic allowed from the Internet to an appropriate amount. For example, if a colocated customer has a security perimeter which can safely filter up-to 500 Mbps of abusive traffic, OneNeck can limit downstream Internet traffic to roughly 500 Mbps, to allow the customer's firewall to do its job effectively.

OneNeck® IT SOLUTIONS
a TDS® Company

Protected DNS Service

In recent years, Domain Name Server (DNS) reflection attacks have grown to comprise the majority of volumetric DDoS attacks. During a DNS reflection attack against a OneNeck data center or customer, customers in that data center may experience significant packet loss of DNS replies from outside servers. Because working DNS resolution is a critical foundation for many applications, OneNeck provides a protected DNS service to our Internet customers: customers who use OneNeck's Anycast DNS servers for DNS resolution will enjoy continued DNS resolution, even when they or another data center customer is subject to a DNS reflection attack.

Protected Infrastructure

In the case of extremely large DDoS attacks, even large data center infrastructure links may become saturated with abusive traffic. To preserve the quality of Internet service for the entire data center, in these extreme situations, OneNeck will block all traffic for the affected target IP address. This ensures that other IP addresses in the data center continue to receive a high-quality Internet service.

In Summary

- OneNeck has QoS protections built into our network to prevent a DDoS attack against one customer from affecting other customers.
- We also can lower the rate of traffic we send to the customer, so if, for example, their firewall would tip-over at 250 Mbps, we can limit their downstream traffic to somewhere around 250 Mbps, so that their firewall is able to handle the attack traffic. This accomplishes 90% of what a traditional scrubber box would do.
- In regards to appliance solutions, these have a side-effect that when there are small/modest DoS attacks, which fit within a data center's pipes (e.g., 5 Gbps), we discard the attack traffic first. So, if the customer has a 1 Gbps cable and 100 Mbps of legitimate traffic, that 100 Mbps gets through to them, and their firewall can stop the rest. For attacks larger than OneNeck's Internet pipes, then no Arbor appliance can filter them anyway.

About OneNeck® IT Solutions

OneNeck IT Solutions LLC offers hybrid IT solutions including cloud and hosting solutions, managed services, enterprise application management, advanced IT services, IT hardware and top-tier data centers in Arizona, Colorado, Iowa, Minnesota, New Jersey, Oregon and Wisconsin. OneNeck's team of technology professionals manage secure, world-class, hybrid IT infrastructures and applications for businesses around the country. Visit oneneck.com.

OneNeck is a subsidiary of Telephone and Data Systems, Inc. [NYSE: TDS]. TDS provides wireless; cable and wireline broadband, TV and voice; and hosted and managed services to approximately six million customers nationwide through its businesses U.S. Cellular, TDS Telecom, OneNeck IT Solutions LLC, and TDS Broadband Service LLC. Visit tdsinc.com.

Part #2.7.4_SSDOS_0617_v1

OneNeck® IT SOLUTIONS a TDS®Company

Call 855.ONENECK | Visit OneNeck.com