Benefits of Hardware Bypass in Anti-DDoS Solution

Background

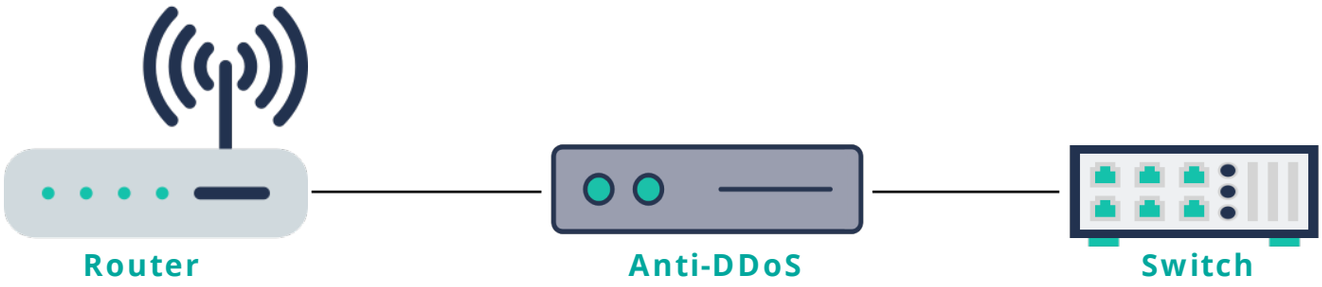
DDoS (Distributed Denial of Service) attacks have become a common occurrence thanks to the availability of DDoS-as-a-Service tools on the dark web. With increased botnet activity arising primarily from vulnerability in billions of IoT devices, DDoS attacks have never been as common, powerful, or sophisticated making DDoS mitigation a necessity in implementing secure network. An organization has four key options: a completely on-premises solution, DDoS Protection as a Service (DDPaaS) from an Internet Service Provider (Clean-Pipe), a cloud-based mitigation service, or a hybrid combination of on-premises with cloud scrubbing for attacks that exceed the Internet link capacity.

Cloud-based mitigation is necessary to defend against DDoS attacks that are larger than your internet bandwidth - the kind that result in the infamously huge, overwhelming, floods of traffic to an unsuspecting organization. However, on-demand cloud mitigation is not, and can never be, truly real-time, so cannot deliver protection without at least some degree of downtime. This can be from minutes, to tens-of-minutes, depending on the chosen provider. Haltdos research also shows that many DDoS attacks are short (less than ten minutes) and sub-saturating (over 75% are less than 1Gbps) so the typical time to swing traffic to cloud scrubbing means the attack is often already over.

In contrast to cloud-based mitigation, always-on on-premises DDoS solutions are perfect for defending against the vast majority of attacks a typical organization is likely to experience, as these are non-saturating and can just be dealt with locally. On-premises, always-on, solutions can deliver this local protection instantaneously, preventing any amount of downtime for the applications and services being protected.

On-Premise Anti-DDoS Deployment

On-premise DDoS solutions typically work in Transparent Layer 2 mode. A Layer 2 network device communicates with its peer using MAC address without the need for assigning any IP address to the device. A transparent Layer 2 solution, on the other hand, acts like a bump in the wire where it does not modify IP address or MAC address when packets traverse through the device - making it invisible to its peers. Consider the diagram below of typical Anti-DDoS solution deployment:



The On-Premise Anti-DDoS solution above is placed between the external router and the next hop - in this case a switch. As the Anti-DDoS solution is deployed inline in Transparent Layer 2 mode, the router assumes all packets it is receiving are coming from the switch and vise-versa. Hence, neither the router nor the switch is aware of the presence of another network device and assume they are directly connected to each other - making the Anti-DDoS device invisible.

Benefits of Hardware Bypass in Anti-DDoS Solution

Cost of DDoS Protection

While both Cloud scrubbing and on-premise, always-on DDoS protection have their advantages and disadvantages, it is a combination of the two that offers the ultimate protection against the whole spectrum of attacks for organizations. Furthermore, to implement a good network architecture, requires ensuring no single point of failure in the network. This means, every network element - including on-premise Anti-DDoS solution must be implemented in High Availability.

Hardware Bypass

Given the mode of operation of Anti-DDoS as being inline Transparent Layer 2, there is a respite for organizations wanting to implement comprehensive DDoS protection without incurring prohibitive costs by avoiding High Availability deployments with Hardware Bypass capable Anti-DDoS solutions.

When an Anti-DDoS solution has built-in hardware bypass capability, it can fail gracefully in Fail-Open mode without breaking network connectivity - therefore, no single point of failure. With reference to the previous diagram, as the router and the switch do not have any knowledge of Anti-DDoS device, they continue to operate as usual. Of course, for the duration the Anti-DDoS device is down, there will not be any protection either.

Benefits of Hardware Bypass

A good network design must anticipate and accommodate for possible events that can result in downtime - however remote. Hardware Bypass capability help address continuity of business despite various failures:

Hardware Failures
Like any network appliance, there is always a possibility of hardware failure. Hardware Bypass ensures that despite such events, the network continues to operate without downtime.

Power Failures
Another common downtime scenario in Data Centers is when there is power failure in the rack. Like in the case of hardware failures, Hardware Bypass ensures network continuity even when there is no power in the device.

Software Failures
All networking devices run software and software have bugs - after all they are developed by humans. A good software also must cater to gracefully handle catastrophic failures by incorporating continuity in its design - especially when it comes to inline network device. Programmatically controlled Hardware Bypass provide software to handle catastrophic failures gracefully and ensure continuity of service.

Haltdos Anti-DDoS Solution

Haltdos is a network security company providing enterprise grade multi-layer, multi-vector DDoS protection to ensure that your IT network stays online and always accessible to your customers. All Haltdos on-prem solutions have built-in hardware bypass capability that is programmatically controlled to ensure continuity and availability of service and operation.

To know more visit www.haltdos.com or email us at sales@haltdos.com