Cloud Based DDoS Protection

KEY BENEFITS:

- Focuses on the customer edge.
- Ensures application availability
- Provides immediate protection from threats
- Provides complete DDoS protection within a single user interface.
- Provides advanced DDoS blocking.
- Prevents volumetric DDoS attacks by signalling upstream ISPs
- Prevents emerging botnet and application-layer attacks.
- Provides real-time and historical traffic forensics and reports.

INTRODUCING HYBRID DDOS PROTECTION:

There is an ever-increasing number of DDoS attacks that directly target specific applications or organisations. Despite these assaults being smaller in scale, by using application knowledge they are able to strain edge servers lowering availability. In order to detect attacks of this nature organisations require packet-level visibility. This is something that is often neither possible nor cost effective within a service provider network.

Through the deployment of the RedSpam on-premise solution you are able to achieve visibility into packet-level data. As it is located close to the customer edge it has the functionality to detect new attacks without the constraints associated with the service provider level. This model allows RedSpam to detect and block lower-bandwidth attacks that target enterprise organisations.

With cloud signalling RedSpam can automatically divert traffic to its scrubbing centres when traffic breaches a predetermined threshold ensuring ISP links don't get saturated, blocking volumetric attacks before they affect service.

DATA CENTRE AVAILABILITY:

Despite the clear benefits of adopting a cloud-based DDoS solution its use in isolation cannot guarantee 100 percent availability. Instead it must be deployed in tandem with an on-premise DDoS solution, ensuring protection from all attacks that threaten availability.

RedSpam covers both areas by providing both customer-edge mitigation of application-layer attacks and upstream mitigation of volumetric attacks. With other security solutions focusing on the confidentiality and integrity of data RedSpam has a sole focus of ensuring that these cloud based data centres remain available. Offering guaranteed protection against volumetric and application layer DDoS attacks.

PRAVAIL APS DEPLOYMENT:

- Pravail APS is deployed at the data centre premises
- It is positioned external to other security devices in order to protect them from direct and indirect attacks
- The device is deployed in layer 2 without an IP address associating with either the inbound or outbound interface
- It can be deployed inline our out-of-line through a span port or network tap
- Pravail APS can be deployed either upstream or downstream from the router
- To ensure cloud signalling integrity a separate out-of-bound management network is provisioned between the data centre and the cloud service provider

REDSPAM:
RedSpam provide fully managed global 24x7x365 DDoS protection and mitigation solutions that prevent targeted malicious attacks from reaching your customers' infrastructure. RedSpam offer a breadth of solutions, services and technologies and a wealth of experience that helps protect and secure your business.

CUSTOMISED TO MEET YOUR NEEDS:

RedSpam tailor's protection and mitigations bespoke to customer requirements ensuring availability and optimised protection. Profiles can be created per application all managed and maintained by RedSpam's dedicated 24/7 SOC team.

THREAT DETECTION AND MITIGATION:

RedSpam's customer portal reports traffic statistics in real time, giving a brief overview report as well as detailed statistics both in an easy to understand format. Providing you with the information you need to decide whether a threat needs to be mitigated or not. You can also view where traffic is coming from, including URLs, domains or countries that might need blocking.

When monitoring an ongoing attack RedSpam helps you to assess the mitigations effectiveness. You can quickly see which traffic is passed and which traffic is blocked, and you can determine which protection categories are responsible for the mitigation. You can also view the source hosts that have been blocked.

THREAT PROTECTION MODEL: