DDoS Protection

For businesses and organisations that are dependent on the Internet for their operations, it's crucial that systems and functions remain online. DDoS Protection prevents attacks from reaching the Internet facing assets, ensuring a secure environment and continuous service delivery to users.

Key Benefits

- No policies to create - automated policy generation
- Machine learning-driven
- Protect your entire network infrastructure against DDoS
- Attacks are mitigated automatically.
- Several Deployment methods to suit your needs, including always-on or always-available
- Also available in Routed Proxy mode, allowing for Layer 7 modules to be used on selected assets
- Can be implemented in under one day.

The DDoS threat

Distributed Denial of Service (DDoS) attacks typically include a full-stack attack, involving malicious packets targeting the network, layer (L3 and L4) with volume-based attacks, and L5, L6 and L7 application attacks.

Network-based DDoS attacks

L2 and L3 attacks target networks and transport layers. Generally, such attacks are volumetric. An attacker overwhelms target IP addresses with large amounts of data resulting in a loss of service for legitimate users. While at the lower end of the threat spectrum, these attacks can include single packets used to target known and unknown vulnerabilities in TCP/IP stacks that bring down network-based equipment and cause denial of service.

Application-based DDoS attacks

Application-based DDoS attacks target application protocols and applications running those protocols. Targeted applications may include web, mail and FTP servers, and tend not to be volumetric attacks. Examples of application-based attacks include, HTTP Get Flood Attacks, HTTP Post Flood Attacks, SSL Renegotiation Attacks and DNS NXDOMAIN Attacks.

Key features

- Detect and mitigate volumetric DDoS Attacks (e.g. SYN Flood, UDP Flood and ICMP Flood)
- Detect and mitigate application DDoS attacks (e.g. HTTP(S)-based, DNS-based, SIP-based)
- Support for all major protocols
- Protocol security, (HTTP, SMTP, FTP, DNS, SSH)
- Protocol optimization for all major protocols (compression and HTTP pipelining)
- Protocol convergence, (HTTP 2.0, SPDY)
- Server load balancing, (advanced SLB methods to monitor CPU, memory usage on SLB members)
- Automated key and certificate management for SSL and TLS traffic
- Proxy and/or routed mode

How we combat DDoS attacks

Baffin Bay Networks apply powerful machine learning and adaptive defense that detect new and existing DDoS threats with measures which are easy to implement and rapidly deliver results. Combined with the world's leading service providers, our mitigation capacity makes our solution highly effective.

We provide the adequate capacity and functionality to consume and block network- and/or application-based attacks. Virtually all mitigation in our TPCs™ is carried out in hardware, which makes it suitable for dealing with low-and-slow and volumetric attacks at several hundred gigabits per second.

The advanced fingerprint function allows us to identify every device behind a request, and subsequently block individual devices behind a single source IP mounting an application-based DDoS attack. We extract hundreds of parameters from connecting clients and their web browsers to safely identify individual attackers.

Threat Protection Centers™ (TPC)

Amsterdam, New York, Los Angeles, Singapore, Stockholm, Frankfurt, Dubai, Tokyo (2019), London (2019), Miami (2019)

RiverView Portal™

Our RiverView™ portal monitors attacks in real-time. It provides statistics on all traffic and attempted attacks and a comprehensive reporting function allows clients to create daily, weekly and monthly reports.

You receive the best possible protection from fresh attacks with our Security Operation Center which monitors the constantly evolving threat landscape around the clock.

Regardless of where your assets are located – on premises, in cloud-based platforms, third party hosts – our Threat Protection Platform is equipped to provide multi-vector threat protection to all deployed assets.