BAFFIN BAY NETWORKS

# DDoS Protection
DATA SHEET

*We have Europe's best and largest Threat Protection Network™.*

*We consume, identify and mitigate volume metric DDoS attacks.*

*Capacity and capability; mitigate and monitor.*

## The DDoS threat

Distributed Denial of Service (DDoS) attacks today typically include a full stack attack, meaning it involves malicious packets targeting Layer-3 and -4, (L3 and L4), volume-based attacks, and L5, L6 and L7 application attacks. This data sheet outlines the threat these attacks pose, and how Baffin Bay Networks provides a unique level of protection against such attacks.

## Network-based DDoS attacks

L2 and L3 attacks refer to attacks targeting networks and transport layers. As a rule, such attacks are volume-based, also known as volumetric attacks. An attacker overwhelms target IP addresses with large amounts of data causing service outage for legitimate traffic.

While at the lower end of the threat spectrum, these attacks can include single packets used to target known and unknown vulnerabilities in the TCP/IP stack to bring down network-based equipment causing denial of service.

## Application-based DDoS attacks

Application-based DDoS attacks target application protocols as well as applications running those protocols. Applications typically targeted include web, mail and FTP servers, and tend not to be volumetric attacks. Examples of application-based attacks include:

- HTTP Get Flood Attack – server capacity is exhausted by requests submitted at abnormally high rates making the server unavailable to respond to legitimate requests as memory and CPU is allocated for malicious requests.
- HTTP Post Flood Attack – over allocation of webserver session resources (memory) by posting small packages over a long period of time to keep a session open. This type of low-and-slow attack prevents legitimate sessions being established.
- SSL Renegotiation Attack - that drain CPU capacity of the target machine by requesting an abnormal number of key renegotiations.
- DNS NXDOMAIN Attacks - where the attacker requests content that is outside the scope of a given DNS server, or for a non-existing subdomain if the DNS Server is configured to be a recursive DNS server, an attacker's goal can be to consume available resources or pollute the cache with NXDOMAIN results.

## How we combat DDoS attacks

Baffin Bay Networks provides complete protection from more than 250 different types of DDoS attacks – all with measures that are easy to implement and deliver results from day one. With a mitigation capacity of 3tbps and transit capacity of 500gbps, we operate an unrivalled Threat Protection Network™ (TPN), with Europe's leading service providers.

We offer sufficient capacity and functionality to consume and block network- and/or application-based attacks detected by our deep learning and machine learning components. Each Threat Protection Center™ (TPC) is equipped with functionality to deal with both clear-text data and encrypted data.

Our unique approach to offer free SSL/TLS Certificate through “Let’s Encrypt” makes it easy to set up a robust certificate management policy with short-lived keys to ensure a high degree of privacy.

Close to all mitigation in a TPC is done in hardware that makes it suitable for dealing with both low-and-slow attacks and volumetric attacks at several hundred gbps.

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

All attacks can be monitored as they occur in real-time through our RiverView™ portal. Statistics on all traffic is available, and a comprehensive reporting engine allows you to manage daily, weekly and monthly reports.

Our Security Operation Center continuously monitors the dynamic threat landscape to offer the best possible protection for new attacks.

## Key features

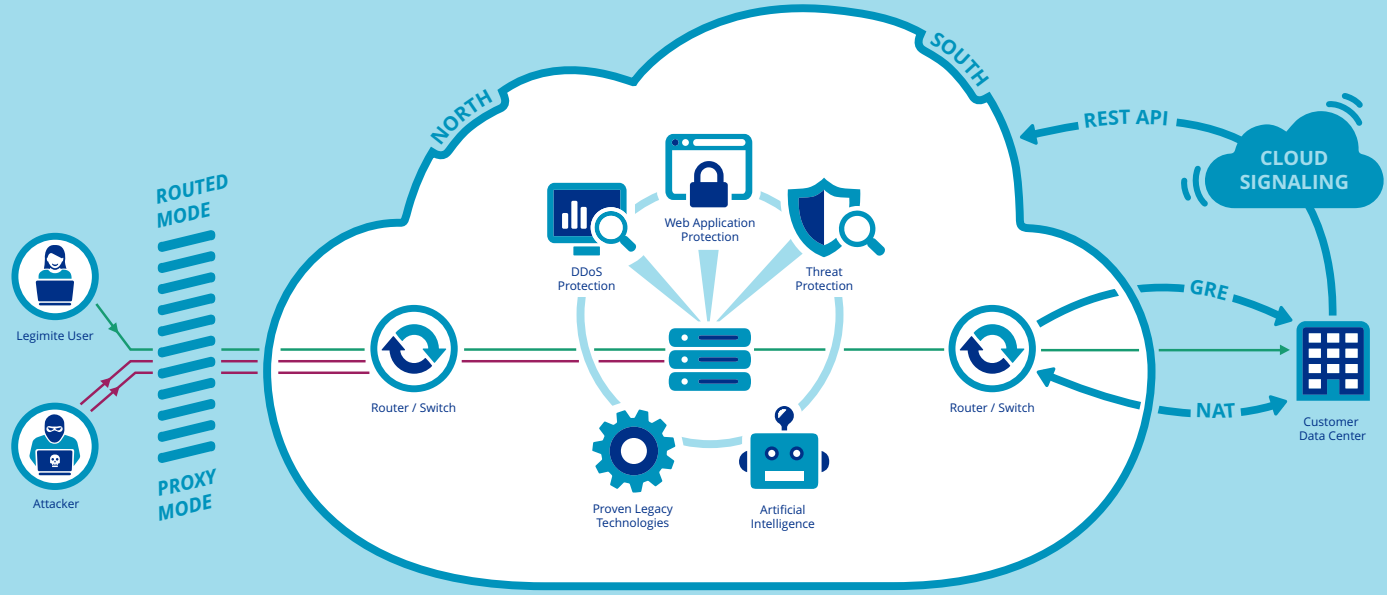
- Detect and mitigate volumetric DDoS attacks (e.g. SYN Flood, UDP Flood and ICM Flood)
- Detect and mitigate application DDoS attacks (e.g. HTTP(S)-based, DNS-based, SIP-based)
- Support for all major protocols
- Protocol security (HTTP, SMTP, FTP, DNS, SSH)
- Protocol optimization for all major protocols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

**Threat Protection Centers ™ (TPC)**

Amsterdam, East and west coast US, Singapore, Stockholm and Tokyo

**Internet Exchange Points**

Amsterdam, Copenhagen, Dubai, Frankfurt, Gothenburg, Helsingfors, Prague, London, Oslo and Stockholm




MARCH 8, 2017 - REV 1.0.1 EN

**Baffin Bay Networks AB**

Regeringsgatan 65, 111 56 Stockholm, Sweden
info@baffinbaynetworks.com
baffinbaynetworks.com