FortiDDoS Solution Sheet

Organizations looking to defend their businesses from potentially catastrophic DDoS attacks, often consider leveraging the combination of on-site equipment for detection with cloud-based mitigation to create a hybrid DDoS solution. The cooperation between Baffin Bay Networks and Fortinet provides a total solution to address this need. By integrating Riverview, the cloud-based solution from Baffin Bay Networks, and the Fortinet FortiDDoS on-premise solution, your networks will be protected against all types of Denial of Service attacks. The combined solution enables cloud-based mitigation for attacks that are larger than your available Internet bandwidth, ensuring clean traffic without filling the pipes of the on-premise solution, and in doing so improving efficiency. In the scenario of an ongoing, large scale DDoS-attack hitting your network, Riverview can automatically divert network traffic through Baffin Bay Networks Threat Protection Centers (TPC) and prevent the attack from impacting your business. By leveraging the strengths in both the solutions, deployed in a concert, provide a complete DDoS mitigation solution, continually improving by communicating, interacting and learning from each other.

The ideal DDoS Solution for

- Organizations with an on-premise solution from Fortinet, looking to expand and complement with a cloud-based DDoS protection, for an interworking hybrid security solution.
- Enterprises with strong Internet dependency, for example Finance, Gaming, Gambling, Government and Healthcare.
- Service Providers, Hosting Companies and MSSPs who would like to quickly provide cloud-based services to their customers without upfront investments and competence ramp-up

Hybrid Cloud DDoS Solution Description

Enabling the hybrid solution is easy -- A connection is established between Riverview and your on-premise FortiDDoS appliance in a few clicks. Events from your FortiDDoS device are then sent to Riverview. These events are analyzed for trigger conditions you define, such as 95% bandwidth utilization. When one or more condition is met, your traffic can be routed through the cloud service automatically for the duration of the attack.
The cloud services function via globally distributed Threat Protection Centers (TPC), allowing Riverview to block the attack as close to the source as possible. Additionally, the TPC network is designed with continuous service availability in mind, providing redundancy, high availability and flexibility.
Riverview learns your traffic patterns by analyzing flow data from your existing network infrastructure and applying advanced machine learning to generate a custom traffic model for your organization. This means when the FortiDDoS on-premise solution signals an attack Riverview's artificial intelligence can determine who is an attacker and who is a valid user. Thanks to this automation, you never need to create a complicated set of policies to protect your network. Even when you aren't under attack, the Riverview portal delivers continuous value by providing visibility into both traffic and threat data.

Key Benefits and Highlights

1+1=3 We create a hybrid solution by combining on-premise FortiDDoS appliances and cloud-based mitigation by Riverview

NO BAD TRAFFIC COST Save your Internet capacity from bad traffic

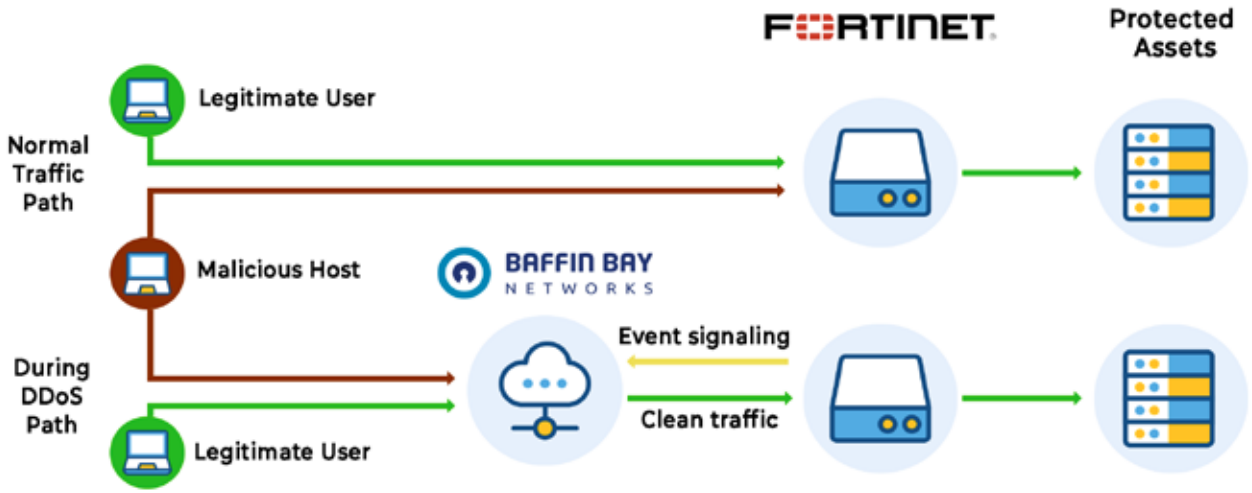
WHEN YOU NEED IT Deploy the cloud-based DDoS on-demand. Automated redirection of attack traffic to cloud-based Threat Protection Centers

REAL TIME MONITOR Full visibility of traffic status and threats in the Riverview portal

MACHINE LEARNING Shares traffic data from FortiDDoS to train Machine Learning function for improved Threat Mitigation

You need

1. Subnets bigger than /24
2. Router or firewall capable of GRE decryption of the entire normal traffic load for the largest subnet under attack. All traffic that is diverted to us is returned to you via GRE tunnels.
3. Some means of signaling to us.



How does it work?

1. Traffic destined to your network is analyzed by the FortiDDoS appliance, Mitigating DDoS attacks at up to line speed.

2. When attack traffic exceeds the user defined thresholds the FortiDDoS signals via API to Riverview. Riverview will then begin announcing the affected prefix(es) from your Autonomous System Number (AS) from the TPC network.

3. Riverview leverages both Threat Intelligence and learned traffic patterns to block malicious traffic inbound to your network. Traffic is learned by sending flow data into Riverview, where it is analyzed to determine normal traffic and behaviors for your network. When mitigation is activated Riverview already understands what signifies abnormal traffic

4. The Riverview portal provides the customer with visibility and can share information with the customers on-premise monitoring function (SIEM)