SOLUTION BRIEF

FortiDDoS and Baffin Bay Networks Riverview Cloud DDoS Protection Service

Executive Summary

Distributed denial-of-service (DDoS) attacks continue to be a prevalent threat to networks and applications around the world.[1] Fortinet FortiDDoS appliances offer industry-leading DDoS detection and mitigation for all types of Layer 3, 4, and 7 DDoS attacks. FortiDDoS can mitigate any DDoS attack up to the maximum limit of available bandwidth. Yet, even with a strong mitigation approach, pervasive DDoS attacks can still saturate incoming links, causing upstream routers to overflow buffers and discard packets at random. This type of link saturation can render the good traffic unusable. By combining FortiDDoS mitigation appliances with cloud-based Baffin Bay Networks Riverview DDoS Protection Service, customers gain the confidence of a truly unified approach to DDoS attack remediation with actionable, shared threat intelligence.

A Joint Approach for High-volume DDoS Mitigation

FortiDDoS and Baffin Bay Networks work in tandem to detect and mitigate high-volume DDoS attacks. The FortiDDoS on-premises appliance works to transmit real-time threat information to the cloud-based partner solution, Baffin Bay Networks. When the FortiDDoS on-premises appliance detects an attack that approaches the capacity of a customer's bandwidth links, it automatically alerts Baffin Bay Networks via the FortiDDoS open API. Notifications include detailed information on the types and sizes of attacks FortiDDoS has detected, along with the attacked subnets or IP addresses. This attack information is used to automatically configure attack filters at Riverview Threat Protection Centers (TPCs) and to process Border Gateway Protocol (BGP) diversion of the customer-bound traffic to the TPCs. Once scrubbed, clean traffic is returned to the customer site, usually via a Generic Routing Encapsulation (GRE) tunnel. FortiDDoS continuously inspects traffic inside the GRE tunnel, searching for new potential threat vectors.

With Baffin Bay Networks, customers benefit from both a cloud-based service and a team of security experts who can continuously monitor customer attacks, block malicious traffic near its source, and transport clean traffic back to the customer to maintain normal business functions. Baffin Bay Networks leverages its globally distributed TPCs to protect against multivector Layer 3 and Layer 4 volumetric attacks as well as Layer 7 attacks. FortiDDoS works to continuously monitor returned clean traffic for all parameters to maintain graphing, logging, and reporting.

Solution Benefits

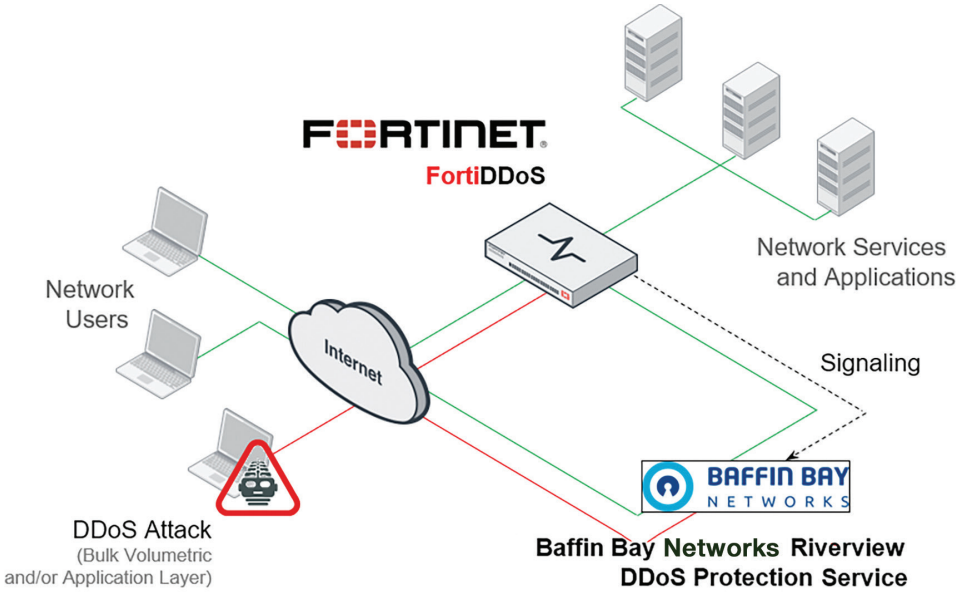
- Always-on DDoS defense delivered via the FortiDDoS on-premises appliance(s)
- Rapid and wide-ranging DDoS mitigation from single-packet scans to full-link line-rate attacks
- Superior cloud mitigation for saturating volumetric attacks that exceed network capacity
- Utilization of a joint on-premises and cloud-based solution to create massive scalability
- Minimized operational involvement with attack redirection to cloud, based on customer-defined thresholds and automated BGP diversion
- DDoS event reporting and analytics on-premises, coupled with visibility of attack countermeasures applied in the cloud
- Next-generation technology, built to grow with the needs of a customer's business
- FortiDDoS open API integration with Baffin Bay Networks Riverview DDoS Protection Service provides scalable mitigation protection

FortiDDoS Mitigation Appliances

FortiDDoS appliances detect and prevent DDoS attacks while providing real-time network visibility. FortiDDoS helps protect internet-facing infrastructures from threats and service disruptions by finding and mitigating network and application-layer DDoS attacks. It defends critical on-premises and cloud infrastructures from attacks while relying on sophisticated filtering technologies to allow secure traffic to continue to flow. These scalable, high-performance appliances deliver proven DDoS defenses, are completely interoperable with a customer's existing security technologies and network infrastructure, and seamlessly integrate with other Fortinet Security Fabric products.

Cloud Signaling

FortiDDoS and Baffin Bay Networks have agreed to use the FortiDDoS cloud signaling open RESTful API that enables interoperability with Fortinet Security Fabric partners. FortiDDoS on-premises devices automatically generate alerts based on predefined attack thresholds and sends them to Baffin Bay Networks to begin mitigation services, providing customers with the combined benefits of both on-premises and cloud-based DDoS protection services. Alerts generated from the FortiDDoS appliances and delivered to Baffin Bay Networks can be viewed by customers on the Baffin Bay Networks customer portal.



FortiDDoS detects a link-saturating DDoS attack and sends an alert with attack information to the cloud DDoS service provider. Traffic is then redirected via BGP to the cloud DDoS scrubbing sites.

Figure 1: FortiDDoS and Baffin Bay Networks Riverview DDoS Protection Service working together to mitigate an attack.

[1] Brad Puckett, "DDoS Is Still a Threat and It Matters How You Handle It," Global Knowledge, July 18, 2018.

About Baffin Bay Networks
Baffin Bay Networks was founded in 2017 by cybersecurity experts who believe no company or organization should be defenseless against advanced cyber threats. Baffin Bay Networks' cybersecurity experts have backgrounds from major U.S. security enterprises, as well as from the largest banks in the Nordics. The company's goal is to build and deliver a Threat Protection Platform that helps customers mitigate cyber threats. Headquartered in Stockholm, Sweden, with a global network of Threat Protection Centers, Baffin Bay Networks protects secures customers worldwide.

About Fortinet
Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad, high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments, whether virtualized, cloud, or physical. More than 210,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at www.fortinet.com.

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 21, 2019 9:30 PM
401729-0-0-EN
D:\Fortinet\Work\May\052119\Task 5- FortiDDoS and Baffin\sb-fortiddos-and-baffin-bay-networks