SOLUTION BRIEF

FortiDDoS and Nexusguard Cloud DDoS Protection Service

The Best of Both Worlds Solution: On-premises and in the Cloud DDoS Prevention

Executive Summary

Increasingly disruptive, frequent, and sophisticated, distributed denial-of-service (DDoS) attacks can cost enterprises huge sums of money for every hour their networks and applications are unavailable or underperforming. Organizations seeking to safeguard their businesses from potentially catastrophic DDoS attacks often consider combining on-premises equipment for detection and local mitigation with cloud-based mitigation to create an interworking "hybrid" solution. The amalgamation between Fortinet FortiDDoS mitigation appliances with Nexusguard's cloud-based Origin Protection service provides a comprehensive and unified solution to address this need.

Challenges

When employing a hybrid solution, DDoS attack detection and mitigation starts immediately and automatically using the on-premises appliances or virtual machines (VMs) that stop application attacks from curtailing the availability of the online services. In the event that an attack surpasses the capacity of the internet uplink, the hybrid solution activates the cloud mitigation and offloads traffic to the cloud, where it is scrubbed before being returned to the enterprise. Cloud diversion will only be engaged when required, as small attacks can be mitigated via the on-premises appliances.

Joint Solution

The Fortinet and Nexusguard partnership delivers an industry-leading security solution to address the vast scope of DDoS attacks posed to enterprise infrastructures and networks. The integration of the Nexusguard Origin Protection service and Fortinet FortiDDoS appliances, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers rapid, always-on, on-premises protection for minor attacks and on-demand cloud offload protection for major attacks.

Upon detection of DDoS attack threats, FortiDDoS appliances relay attack data to the Nexusguard FortiDDoS Cloudshield App. All incoming traffic is routed through Nexusguard's scrubbing network using Border Gateway Protocol (BGP) announcements. Clean traffic will then be routed through Generic Routing Encapsulation (GRE) tunnels back to the protected network.

FortiDDoS is a purpose-built line of DDoS appliances and VMs with class-leading performance and mitigation parameters. FortiDDoS' unique architecture analyzes 100% of passing packets for more than 230,000 possible attack vectors. No signature services are required and no manual operator intervention is needed during attacks. FortiDDoS operates fully autonomously, mitigating and reporting in real time.

Joint Solution Components

- Cloudshield for FortiDDoS App integrates with FortiDDoS on-premises appliances
- Cloud Diversion App facilitates route diversion for under-attack IP prefixes to Nexusguard cloud
- Nexusguard Origin Protection (OP) service mitigates volumetric attacks and delivers clean traffic to the customer's network

Joint Solution Benefits

- The fastest and best quality DDoS mitigation
- Fully automatic traffic diversion requires no human intervention
- Immediate detection by on-premises appliance
- Cloud mitigation of terabit-scale attacks
- Comply with regulations by keeping traffic in-region

FORTINET FABRIC-READY

Joint Solution Integration

Setup consists of a few simple steps via the Nexusguard Customer Portal. The FortiDDoS on-premises appliance automatically generates alerts based on predefined DDoS attack thresholds and relays the attack details to the Nexusguard Cloudshield for FortiDDoS App.

In order to establish peering and authenticate the exchange of threat information between FortiDDoS appliances and the Cloudshield for FortiDDoS App, Nexusguard and Fortinet use a documented, open, secure, attack signalling REST API.

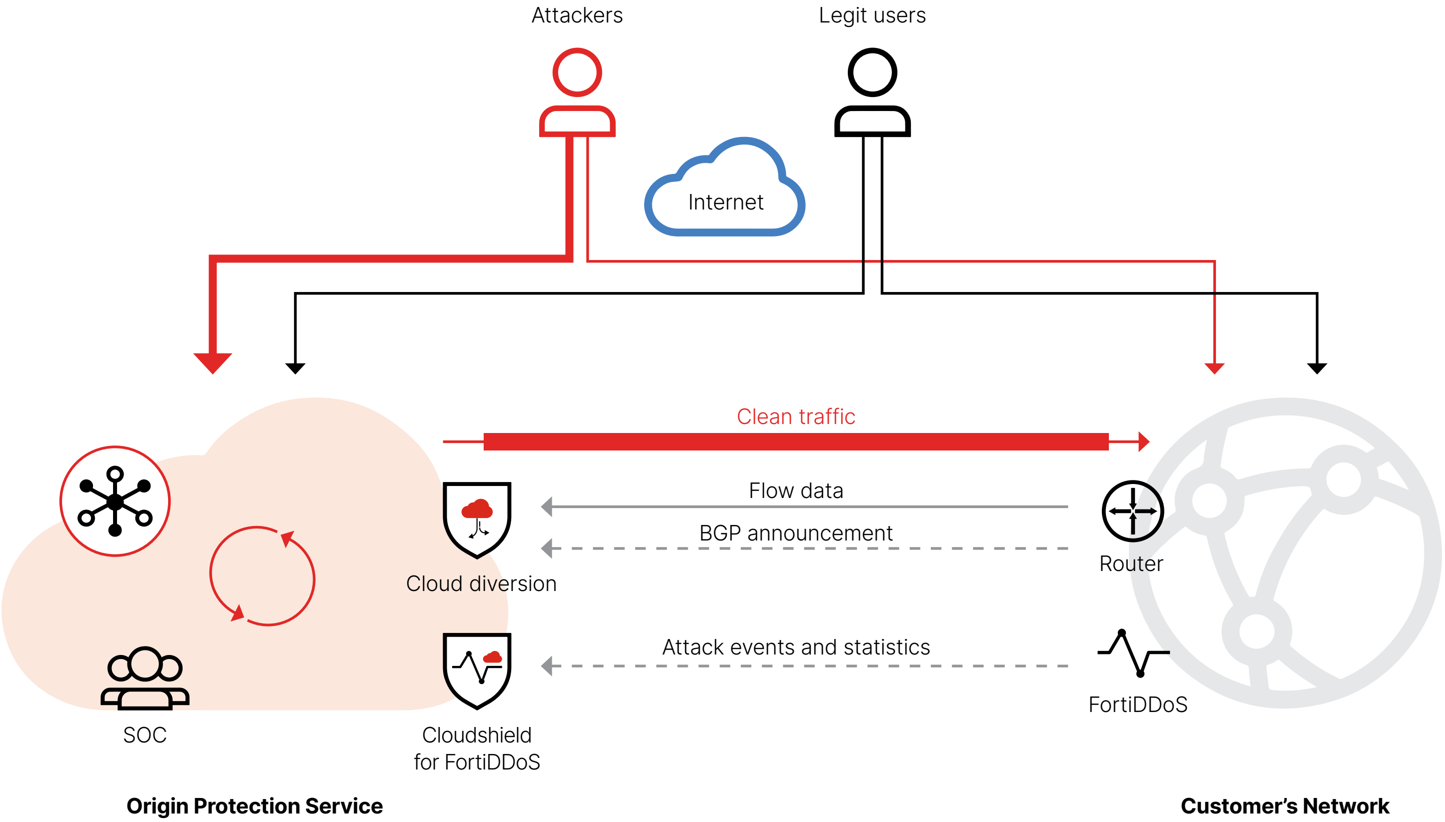

Figure 1: Nexusguard–Fortinet hybrid solution.

Joint Use Cases

Use Case 1

If a DDoS attack is smaller than the total internet link capacity, it is handled locally by the FortiDDoS appliance or VM. Traffic will only be diverted to the cloud for mitigation by Nexusguard Origin Protection service if an attack exceeds the total internet link capacity or a customer-defined threshold.

Use Case 2

Application attacks will be mitigated by either the FortiDDoS appliance or Nexusguard's Origin Protection cloud service depending on the size of the attack.

About Nexusguard

Founded in 2008, Nexusguard is the leading managed security service provider (MSSP) specialized in combating DDoS attacks, leveraging its purpose-built, high-performance scrubbing centers and a growing partner network around the world. We simplify DDoS for communications service providers (CSPs), large enterprises and organizations to maintain uninterrupted access to websites, applications, networks and DNS servers. Visit www.nexusguard.com for more information.

www.fortinet.com

September 11, 2021 12:50 AM
1270490-0-0-EN