Datasheet

Nexusguard InfraProtect

Protect Large Networks & Downstreams

With the rise of DDoS attacks, many Communication Service Providers (CSPs) such as ISPs and Managed Security Service Providers (MSSPs) have begun to offer anti-DDoS services, often referred to as “clean pipe”, to their downstream customers. Whereas in the past, blackholing the traffic to the IP address of victim network was the only option. This protected everyone else on the carrier infrastructure and helped avoid a collateral damage, but at the expense of the victim.

Nexusguard InfraProtect offers CSPs the ability to leverage Nexusguard's globally distributed infrastructure to be used as an off-site sandbox to perform traffic analysis, shaping and DDoS mitigation so that traffic that reaches CSPs' network are always clean.

“More scalable protection and deployment options that go beyond legacy CleanPipe”

Typical approaches CSPs use to the handling of network-layer DDoS attacks at a carrier level rely on two classes of network devices.

Considered to be more advanced are flow-aware devices, such as firewalls, load-balancers, IDS/IPS and the likes, despite the fact that they are oftentimes the bottleneck themselves in the face of volumetric attacks and risk collateral damage.

The second, less effective mitigation method relies on routers (and switches). Unfortunately, routers are high throughout devices designed to handle packet in stateless manner and base on well-defined fields in packet headers. They do not have enough CPU power to perform DDoS detection.

To address the shortcomings of these legacy anti-DDoS techniques, Nexusguard is introducing InfraProtect to provide more scalable and agile DDoS protection to CSPs committed to meeting their SLAs.

For CSPs looking for detection capability

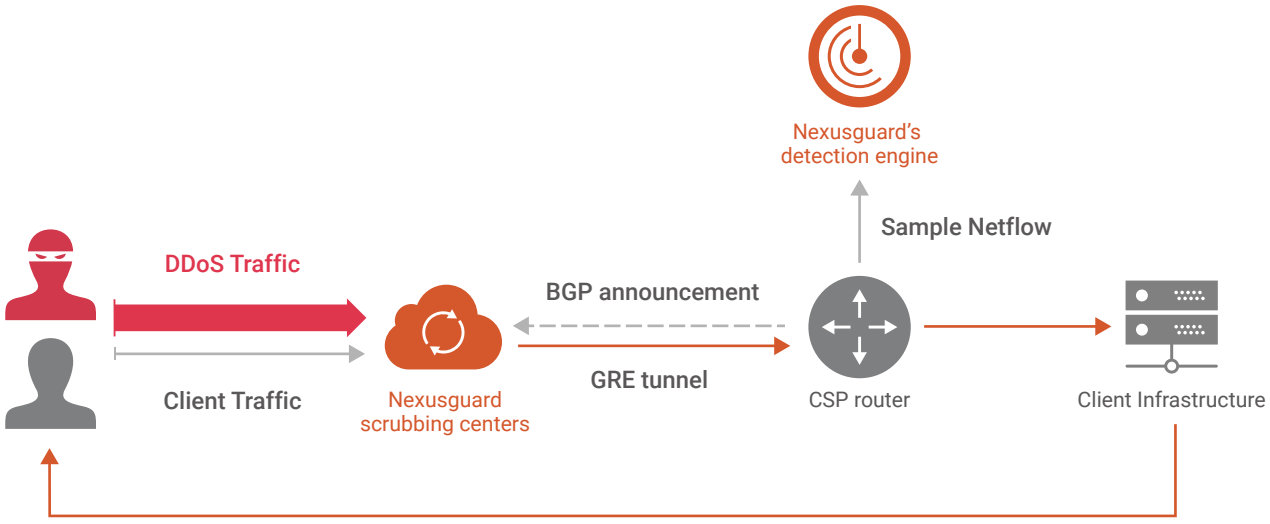
Detection + Mitigation

CSPs without local flow-analysis capability to send traffic flow to a centralised collector at Nexusguard's scrubbing cloud can rely on Nexusguard's detection engine.

Sample Flow data will be fed to Nexusguard's detection engine. Detection of malicious traffic will automatically trigger traffic redirection via BGP announcement to Nexusguard's scrubbing cloud, while clean traffic will be returned to the CSP network via a GRE tunnel after scrubbing.

The detection engine is comprised of flow-based traffic analyzer and collector that supports NetFlow, JFlow and limited versions of Netstream. Based on threshold anomaly detection, the engine is capable of continuously monitoring hundreds of thousands of IP addresses in real time.

At the core of Nexusguard's scrubbing cloud, the mitigation engine, NetShield, defends against known, unknown and evolving DDoS attacks against the network layer.



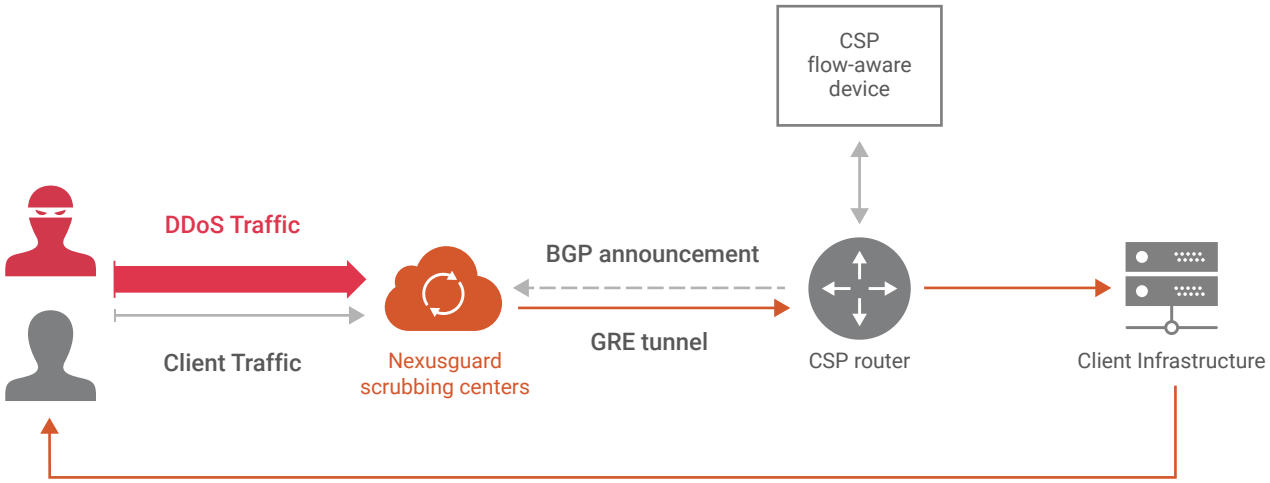
For CSPs with flow-analysis capability

Mitigation Only

This deployment is ideal for CSPs deployed with flow-aware devices or anti-DDoS appliances on the edge of their network as a way to offer clean pipe service.

When a DDoS attack is detected by the on-premise devices, the CSP can start announcing its IP range to divert all traffic to this IP range to Nexusguard's scrubbing centres without first reaching the CSP network.

After traffic scrubbing, clean traffic will be forwarded back to the CSP network via a GRE tunnel.



Visibility and control

Through a Portal, the CSP will have access to an integrated Dashboard and automated tools to:

- Monitor aggregate network traffic.
- Configure network-level security policies.
- Monitor and audit mitigation activities.
- View event alerts, logs and reports.
- Carry out null-routing (blackhole) to a Host.

Global scrubbing centres

Nexusguard's globally located scrubbing centers are equipped with over 1.44Tbps of core mitigation capacity, strategically deployed in main internet intersections, i.e. San Jose, L.A., Miami, London, HK (x2), Taiwan and Singapore, to mitigate attacks closest to their sources. This architecture ensures high resiliency, scalability and availability at all times, and minimizes latency even under a massive volumetric attack.

Key features

Protect large networks including downstreams

Regardless of mitigation effectiveness, InfraProtect is capable of provisioning for and protecting large networks of /16 and smaller within the same AS or across multiple AS's, as long as they have the same traffic return point.

Automatic abnormality detection and mitigation

As a DDoS mitigation solution intended for a large network, the mitigation engine is based on auto-mitigation templates built on top of a parent detection and mitigation profile.

Self-service/Managed mitigation platform as a service

The CSP will have access a Portal that functions as a single-point management and reporting by consolidating data received from flow-analysis devices or Nexusguard's detection engine as well as Nexusguard's mitigation platform.

One-button blackhole

Customer can perform null-routing (blackhole) via the Portal. Null-routes can only be performed every two hours. This action drops all traffic to a Host when attacks are so overwhelming that they might cause collateral damage.

Intelligence-based Detection Engine

Nexusguard Threat Intelligence collects and analyzes traffic data from multiple sources, including our mitigation platform, Security Operation Center (SOC), industry research, IP reputations and external intelligence exchanges to identify threats, proactively mitigate them, and enable preventive security postures.

Feature specs

Network size

Since the traffic of the CSP network is diverted to Nexusguard's scrubbing cloud using BGP, the CSP client needs to be in control of an Autonomous System (AS) in order to be able to control the announcement of the IP range that the CSP client uses.

The smallest prefix we accept is a /24 range in the case of IPv4. We are able to provision for up to 256 x /24s in a single Site Profile, via a range or individual entry. All prefixes in this Parent Site profile will inherit the same configurations including Flow, GRE tunnel, detection, mitigation and auto-mitigation templates.

Profile anomaly detection

In our context, a mitigation profile defines the scope and configurations of how Networks within a Site a protected. The IPs under protection can therefore be systematically grouped by Networks, allowing you to define and customize rule-sets for resources of similar nature more effectively.

Profile anomaly detection is recommended only for Networks that have a predictable traffic pattern. Larger subnets are usually more predictable.

Mitigation template

A mitigation template contains a set of mitigation rules that are activated by default upon detection of threats. In other words, these rules are automatically enforced when the threshold values defined by Detection policies are reached.

A mitigation template has four core rule-sets, including Anti-Flood, FlexFilter, Zombie and Traffic Policing. You can customize up to five mitigation templates via the Portal.

More options beyond InfraProtect

If you are looking for other solutions that provide a higher level of security policy customization down to the host level, end-customer protection and upselling opportunities, you will find our Origin Protection (OP) and becoming our partner are a better choice.

Origin Protection

OP is designed to protect the CSP network infrastructure as well as the downstream customers. It is complete with an Admin Portal for granular, real-time traffic visibility, detailed event logs, flexible policy configuration and customer management in a multi-tenant environment. CSP can capitalize on reselling opportunities offered by OP.

Transformational Alliance Partner (TAP) Program

Down the journey, CSPs can extend partnership with us by joining the Transformational Alliance Partner (TAP) program. This partner program enables them to offer complete DDoS mitigation services by leveraging Nexusguard's three-pillar Cybersecurity Platform comprised of Application Protection (AP), Origin Protection (OP) and DNS Protection (DP).

contact@nexusguard.com
www.nexusguard.com

NEXUSGUARD®