SOLUTION BRIEF

Fortinet and NoviFlow Partner to Deliver a Carrier-Grade Network Address Translation Solution

Executive Overview

Carrier-grade network address translation (CG-NAT) offers a way to mitigate IPv4 address exhaustion. CG-NAT is an approach to IPv4 network design where end sites are configured with private network addresses that are then translated into public IPv4 addresses. This enables the sharing of small pools of public addresses among many end sites by shifting translation function and configuration from on-premises to the internet service provider (ISP) network. NoviFlow and Fortinet have partnered to deliver high throughput and dynamically scalable CG-NAT services in a programmable software-defined network (SDN) environment.

Mapping CG-NAT Requirements

The vast proliferation of mobile and connected devices, streaming video-based applications, and cloud-based services is causing problems when it comes to delivering data capacity and ensuring quality. This has precipitated a global depletion of public IPv4 addresses, which strains existing IPv4 infrastructures while increasing demand for CG-NAT IPv4 services to compensate for the exhausted supply.

CG-NAT must be deployed to provide key capabilities such as:

- Enablement of IP-address expansion by relying on the CG-NAT to overcome the IPv4 address exhaustion
- Enhanced threat prevention by hiding subscribers' and infrastructures' IP addresses from the internet
- High scalability to support the rapid growth in the number of subscribers and devices to substantially increase revenue

Solution Highlights

- Provides cost-effective, dynamically scalable, multiple-terabit CG-NAT services
- Efficiently addresses even the largest deployments via dynamic scaling to target capacity for even the most highly variable demand
- NoviFlow CyberMapper provides line-rate traffic filtering, steering, and load balancing to the Fortinet CG-NAT tool farm and ensures that return packets of the public IP address assigned by Fortinet is steered back to that same device

Despite the launch of IPv6 in 2012, IPv4 continues to account for the majority of online traffic.[1]

A joint solution from Fortinet and NoviFlow combines NoviFlow's CyberMapper software-defined network (SDN) forwarding plane with the Fortinet FortiGate CG-NAT service. This combined solution delivers high throughput and dynamically scalable CG-NAT services in a programmable SDN networking environment that helps reduce both capital (CAPEX) and operating (OPEX) network expenses for customers.

Delivering Dynamically Scalable and Affordable CG-NAT Services

A Security Fabric-ready partner, NoviFlow solutions ensure SDN integration via Fortinet SDN Connectors and APIs. NoviFlow enables elastic scaling of FortiGate CG-NAT services to stay ahead of both exponentially growing demand and an ever-expanding network attack surface. It is designed to help large network operators affordably scale CG-NAT into the terabit range.

NoviFlow's forwarding plane solutions (NoviWare and CGNmapper) provide complex flow processing, massive throughput, and scalability. By implementing traffic-handling and load-balancing functions in the forwarding plane, traffic directed to each FortiGate CG-NAT device is optimized so that the capacity of a Fortinet CG-NAT tool farm can be dynamically scaled to meet network demand.

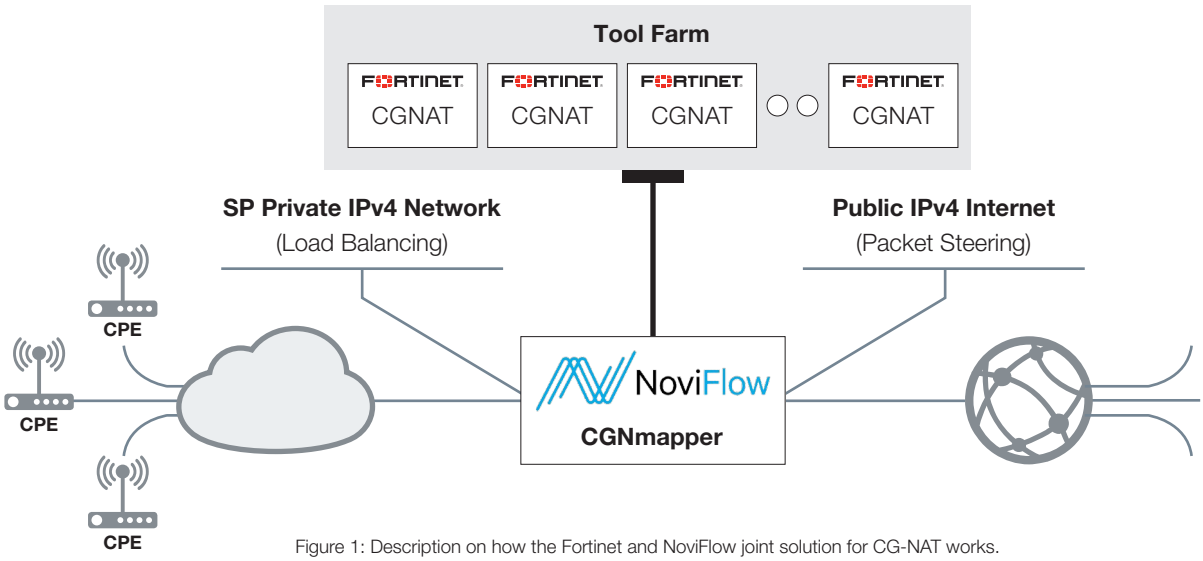

Figure 1: Description on how the Fortinet and NoviFlow joint solution for CG-NAT works.

The Fortinet and NoviFlow joint solution includes:

1. A FortiGate tool farm of devices or VMs
2. Tofino switch(es) running the NoviWare OpenFlow NOS
3. NoviFlow CGNmapper Controller

NoviFlow also significantly simplifies configuration and management of flows to tools and fully automates the assignment and management of address spaces. CGNmapper even provides a feedback channel that enables Fortinet cybersecurity applications to adjust network behavior in real time.

Other key solution features include:

- Terabit load balancing from the private (customer premises equipment) side.
- Terabit traffic steering from the public (internet) side.
- Proprietary algorithms that are pinned to a specific CGN tool for the life of a private flow and its public internet response. This enables the NAT mapping of flows and the associated database to be divided and isolated to specific tools within the farm.
- Operational dashboard to visualize tool state and loads.

Physical or Virtual Network Function

Flexible deployment options are available with FortiGate next-generation firewalls. Physical appliances include high availability and the highest proven scalability. Fortinet custom security processors deliver unparalleled hardware acceleration. The same capabilities are also provided by FortiGate virtual machines (VMs) acting as security VNFs for specific interfaces and protocols.

A Collaboration for Transparent Connectivity

As network attack surfaces continue to grow, threats become more sophisticated, and the global depletion of public IPv4 addresses strains existing infrastructures, customers must address both carrier-grade security and NAT capabilities. The joint CG-NAT solution offered by Fortinet and NoviFlow helps reduce operating costs while increasing reliability by significantly simplifying network architectures.

[1] "State of IPv6 Deployment 2018," Internet Society, June 6, 2018.

March 19, 2019 9:58 AM

361953-0-0-EN

D:\Fortinet\Work\March\031719\sb-fortinet-and-noviflow