Executive Summary

The Fortinet and Pluribus Networks solution uniquely addresses both perimeter security as well as network traffic analysis, a multilayer approach critical for today’s threat environment.

Challenges

The evolving threat landscape requires enterprises to address both perimeter and interior security, with the “hard shell and soft underbelly” architecture cast by the wayside. FortiGate, deployed within the public address pool (POD), offers both north-south and east-west protection closely integrated to the data forwarding path. But this is only part of the solution.

Joint Solution

Pluribus Networks and Fortinet have partnered to deliver an industry-leading security solution to address these challenges. The integration of the Pluribus Netvisor and Fortinet FortiGate NGFW, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers the industry’s first and only bare-metal, distributed network hypervisor operating system, Netvisor, for the convergence of compute, network, storage, and virtualization based on open compute and open networking technologies.

Pluribus has integrated FortiGate VM into the Netvisor environment, providing Pluribus customers with an industry-leading firewall solution. FortiGate powered by Netvisor runs at full bandwidth, and the user experience is no different than when running it on a standalone server. However, FortiGate is now more tightly integrated with the network, supports Netvisor-driven network virtualization, and is optimized for evolving east-west traffic patterns in addition to more traditional north-south flows, avoiding any traffic hairpinning.

Joint Solution Components

- Fortinet FortiGate Next-Generation Firewall (NGFW)
- Pluribus Networks Netvisor

Joint Solution Benefits

- Optimize infrastructure investment and offer security programmability to both DevOps and NetOps
- Integrated proactive security solution with deep analytics for perimeter and interior protection
- Native support for network virtualization and east-west traffic patterns—deploy FortiGate on true TOR or spine switch
- Software-defined networking (SDN) at scale and with interoperability
When deployed, Pluribus Netvisor forms a fabric-cluster across multiple switches, offering a single point of management, in-line analytics, network virtualization (a.k.a. microsegmentation), and full Layer 2/Layer 3 interoperability with currently deployed networking hardware. The platform now supports the FortiGate virtualized firewall, offering a multilayer approach to today’s threat landscape, securing both the perimeter and the interior.

**Joint Solution Components**

- Pluribus Networks F64-M/L/XL Network Computing Appliance. Number of FortiGate instances and performance will depend upon model number and memory. Suggestion is to deploy the XL if deploying multiple virtual instances.
- Pluribus Networks Netvisor ASDF license for F64.
- Fortinet FortiGate VM64-KVM. Throughput will depend upon license purchased – 01/02/04/08.

**Joint Solution Integration**

The Pluribus Netvisor fabric-cluster uniquely provides visibility across the network for all traffic, down to the application, host, and virtual machine (VM), and even supports full packet capture. In conjunction with Netvisor vFlow functionality and FortiGate, it permits proactive security management that addresses both infiltration and exfiltration. For example, the ability to identify inbound and outbound traffic anomalies, and then take immediate action with Netvisor programmability. The addition of the SanDisk/Fusion-io flash drive enables “time-machine” functionality to track network intrusions back in time. This multilayer security is top of mind for many enterprises if one looks at visibility fabric/network packet broker deployments. The combination of Fortinet and Pluribus offers enterprises a unique integrated capability.

A typical deployment consists of hosts connected “inside the firewall” on PN switch ports or connected via an intermediate switch. The PN switch also has ports connected directly/indirectly to the “outside” network or to the internet. For example, a bare-metal server may be connected on VLAN 200, while VMs belonging to VLAN 100 on a second server may both be connected through the virtual firewall. They both then point to internet-facing VLAN 300. In addition, VMs belonging to VLAN 101 on the same second server may connect to the PN switch and not firewalled, connecting directly to the internet. The architecture scales for traffic entering the POD, or the FortiGate may be deployed at each TOR or spine switch for east-west protection.

---

Figure 1: Visibility into “syn” attack—timing and severity.
The FortiGate virtual appliance, a standard KVM image, runs within a high-performance Netvisor VM, and acts as if it is running on a standard server. Both routed and transparent modes are supported. Because Netvisor is virtualization-aware, the IT manager may install multiple instances of FortiGate on the platform, each mapped to a separate microsegment. As part of an OpenStack deployment leveraging the Pluribus Cloud Controller, separate FortiGate instances will map to and be manageable by different tenant networks. The Cloud Controller enables a “cloud in a rack” by integrating both the OpenStack controller and networking, leveraging the Pluribus Centos-based distribution or the Red Hat Enterprise Linux OpenStack Platform (RHEL OSP).

---

**FortiGate on Netvisor**
- Standard KVM edition deployed on Pluribus Network Computing Appliance with Netvisor
- Same user experience as on a server, but now closely tied to the network

**Multilayer Security**
- Enhance perimeter security with “inside the firewall” real-time analytics
- IT is now proactive, addressing both infiltration and exfiltration—exterior and interior protection

**DevOps and NetOps**
- True SDN security, offering both the network and service team a programmatic approach to security
- More responsive and agile

**Virtualization-aware**
- Solution maps to virtualized networks/microsegmentation
- Tenant security for OpenStack

**Evolving Data Center Designs**
- Optimized for evolving spine and leaf deployments
- Both north-south and east-west traffic profiles

**Open Standards**
- Open architectures and no vendor lock-in
- Compute hypervisor-agnostic—virtualized and bare-metal deployments

---

**About Pluribus Networks**
Pluribus Networks delivers industry-leading open networking solutions featuring a unique next-generation software-defined networking (SDN) fabric for modern single-site data centers, multi-site data centers, and distributed cloud edge compute environments. Learn more at [https://www.pluribusnetworks.com/](https://www.pluribusnetworks.com/).