SOLUTION BRIEF

Fortinet and Pluribus Networks Security Solution

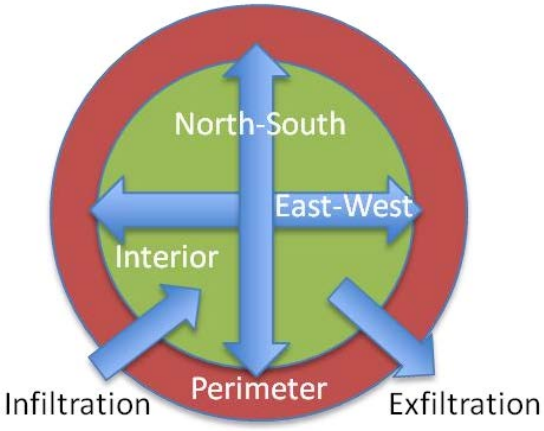
Integrated Solution Paves Way for Scalable and Interoperable SDN Deployments

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

FORTINET Fabric-Ready

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

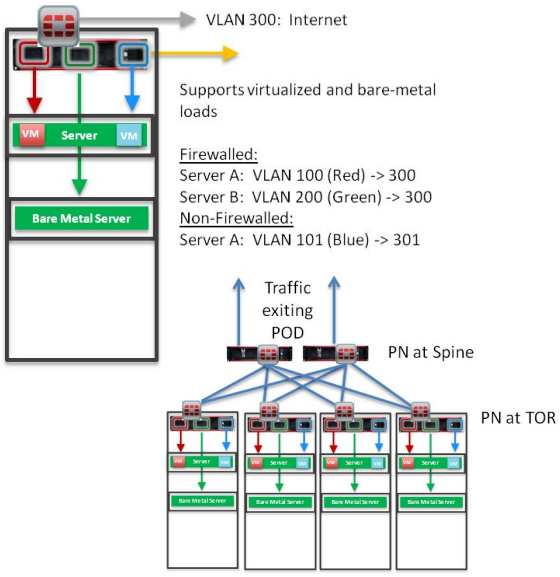
The Pluribus Netvisor fabric-cluster uniquely provides visibility across the network for all traffic, down to the application, host, and virtual machine (VM), and even supports full packet capture. In conjunction with Netvisor vFlow functionality and FortiGate, it permits proactive security management 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.

client-ip	server-ip	server-port	syn	total-bytes	last-seen-ago
10.9.10.189	192.168.1.6	8060	209K		1d23h26m53s
10.9.99.20	169.254.2.1	23398	139K		1s
10.9.99.16	10.9.11.30	8084	100K		1s
10.9.9.136	10.20.3.9	8084	77.0K	81.8M	2s
10.9.18.55	10.20.3.9	8084	76.8K	87.8M	12s
10.9.9.136	10.20.3.9	8443	72.5K	1.06G	1s
10.9.18.55	10.20.3.9	8443	72.1K	1.17G	12s
10.9.18.89	10.20.3.9	8084	46.9K	89.7M	4s
10.9.18.89	10.20.3.9	8443	42.2K	1.21G	4s
10.9.10.168	192.168.1.148	8008	38.2K		1d17h6m36s
10.9.10.189	192.168.1.12	8008	25.6K		2d19h45m29s
10.9.99.20	10.20.3.9	8084	25.1K	68.7M	6s
10.9.9.186	173.164.164.42	ssh	19.7K	16.8G	2m38s
10.9.99.20	10.20.3.9	8443	19.4K	933M	5s
10.9.18.153	10.20.100.2	nfs	18.2K	918M	2d3h33m13s
192.168.20.112	192.168.20.122	23398	14.1K	1.17M	1d18h59m17s
192.168.20.3	192.168.20.122	23398	13.5K	2.17M	1d19h3m18s
192.168.2.41	192.168.20.122	23398	13.5K	1.38M	1d19h1m54s
192.168.20.118	192.168.20.122	23398	13.4K	1.19M	1d19h2m56s
192.168.2.31	192.168.20.122	23398	13.3K	2.75M	1d19h7m44s
192.168.20.114	192.168.20.122	23398	13.1K	642K	1d19h2m8s
192.168.2.11	192.168.20.122	23398	12.9K	2.06G	1d19h7m39s
192.168.2.61	192.168.20.122	23398	12.7K	1.10M	1d19h16s
10.9.9.21	10.9.9.136	https	11.8K	7.42G	2d20m14s
10.9.10.65	174.129.132.8	http	11.5K	4.47M	2d3h49m36s
10.9.9.151	10.20.9.79	nfs	10.1K	8.98G	5m3s
10.9.10.65	10.9.10.1	53	9.23K		1d18h27m55s
10.9.18.65	10.20.9.79	nfs	8.72K	13.2G	8m36s
10.9.18.177	10.20.3.9	8084	8.66K	60.8M	24s
10.9.9.21	10.20.9.137	http	8.54K	4.83G	2d2m6s
10.9.10.90	10.9.10.1	53	7.41K		2d1h10m4s
192.168.20.117	192.168.20.122	23398	7.30K	2.52G	1d19h3m2s
10.9.9.117	10.9.9.9	8080	6.87K		18m11s
192.168.20.121	192.168.20.116	23398	6.68K	87.0M	1d18h59m52s

Figure 1: Visibility into "syn" attack—timing and severity.

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.

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	Multilayer Security	DevOps and NetOps
■ 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	■ Enhance perimeter security with "inside the firewall" real-time analytics ■ IT is now proactive, addressing both infiltration and exfiltration—exterior and interior protection	■ True SDN security, offering both the network and service team a programmatic approach to security ■ More responsive and agile
Virtualization-aware	**Evolving Data Center Designs**	**Open Standards**
■ Solution maps to virtualized networks/ microsegmentation ■ Tenant security for OpenStack	■ Optimized for evolving spine and leaf deployments ■ Both north-south and east-west traffic profiles	■ 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/.

FORTINET®

www.fortinet.com

December 10, 2020 7:38 AM

861797-0-0-EN

D:\Fortinet\Solution Brief\Grey Solution Brief\Pluribus\sb-FA-pluribus-netvisor-for-fortinet-fortigate-12102020\sb-FA-pluribus-netvisor-for-fortinet-fortigate-12102020