A Comprehensive Approach to Fabric Security Through Macro-Segmentation

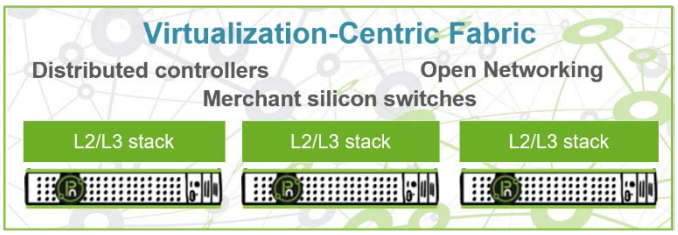
The Need For a Comprehensive Approach To Fabric Security

Today's data center environments are subject to immense amounts of security threats – and no perimeter is impervious. Hardware-based firewall solutions in the DMZ only handle North-South traffic. But the largest security breaches we see in the news have gotten past the firewall and lingered in the East-West traffic amongst applications and infrastructure.

Instead, why not segment your network with private virtual networks, isolating each application or department from each other, allowing fine-grained policy for traffic flow and access to L4-7 services while simultaneously alleviating unnecessary load on your existing firewall?

Pluribus ToolKit for East-West Fabric Security

The Pluribus Fabric unlocks the built-in power of today's Open Networking hardware, to deliver a comprehensive approach to secure the East-West fabric and insert security appliances on the traffic patch of selected applications.



There are three pillars of the Pluribus Fabric Security Architecture:

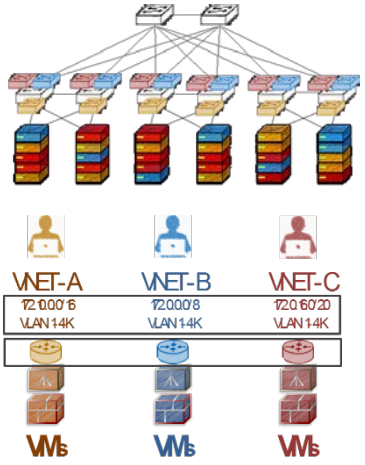
Secure Multi-tenancy – Virtual Private Networks with completely independent and isolated network resources (VLANs, subnets, L2 tables, vRouters) and traffic.

Per application conditional Security Service Insertion – granular, line-rate flow control for conditional security insertion policies.

East-West End-point behavior Visibility – gain insight into the behavior and connections of every end point without sampling. Track the connection state of each TCP connection to identify application misbehavior or security threaths. No need for a separate monitorning fabric; visibility and analytics are built-in with the Pluribus Fabric.

Secure Multi-tenancy with Netvisor® Private Virtual Networks

Pluribus can rapidly provision private virtual networks (VNETs) as virtual pods (VPODs) with management, control and data plane isolation.



Independent tenant networks

- Overlapping subnets (VLANs and IP prefixes)
- End-to-end, fabric-wide autoprovisioning of virtual networks resources.

Management Plane Isolation

- Multi-tenant management plane, with dedicated switch OS containers, for provisioning the tenant network.
- Per tenant visibility of flows, services and VMs.

Control Plane Isolation

- Tenant vRouters run in dedicated containers of the switch OS.

Data Plane Isolation

- Automatic orchestration of VLAN, VRF and VXLAN VNI space to prevent leaking between tenants.
- Anti-spoofing mechanism to prevent servers belonging to a logical tenant from sourcing IP traffic with illegitimate prefixes. Enforce servers to use consistent VLAN/IP addresses.

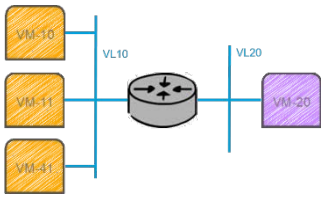
Per application conditional Security Service Insertion

With the Pluribus vFlow technology, security service insertion can be executed at line-rate and with granular, per application control for each tenant network (VNET).

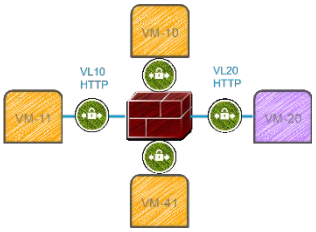
Redirect East-West Traffic

For example, a default behavior of a network fabric (on the left) would be to bridge and route East-West traffic without inspection.

But with configurable Security Service Insertion, the Fabric can be controlled to redirect instead to a security appliance for selected traffic based on, e.g., configurable L1-L4 parameters – and all at line rate.



Default Behavior, no inspection, all traffic bridged and routed

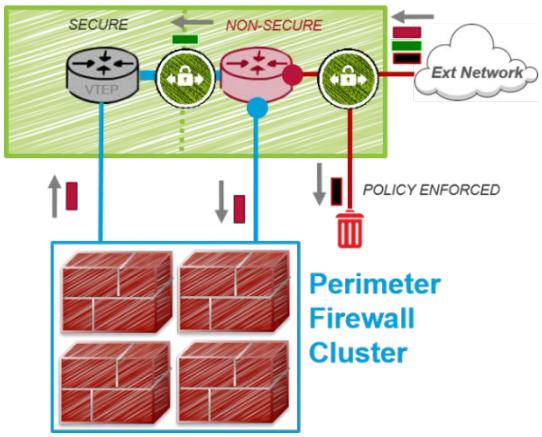


Configured Security Insertion introduces security service for (e.g.) each VM

Control Traffic Flow and Routing based on your Security Policy

With conditional security service insertion from Pluribus vFlow, you can select which traffic from external networks needs to pass through your perimeter firewall cluster, and which routes directly from one side of the fabric to the other – or gets dropped.

Save considerably by not oversizing your firewall, optimizing your traffic flow.

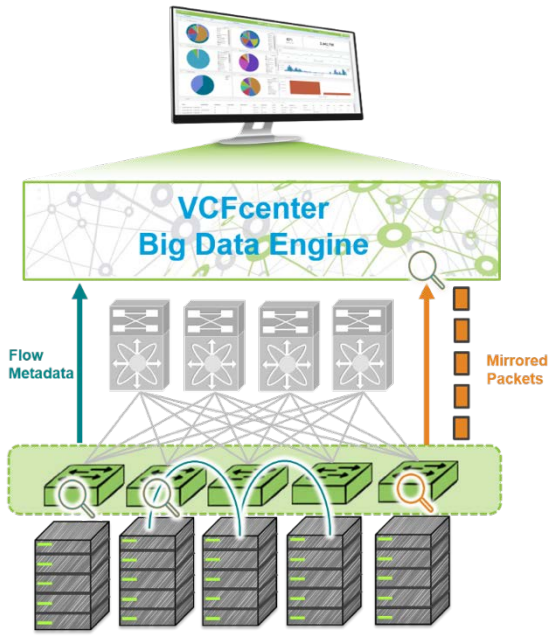


East-West End-point Behavior Visibility

Leverage our built-in visibilty and analytics with our Insight Analytics™ Flow and Packet analytics solutions for continual policy improvements.

With Insight Analytics, each tenant can have its own analytics and visibility tool, built right into its private virtual network to:

- Detect Rogue Attacks
- See E-W (or N-S) traffic capacity
- Detect and Block DDoS Traffic
- Detect Port Scan Attacks
- Improve your Server Security Posture
- Verify Access Compliance



Award-winning Insight Analytics™ platform receives and analyzes packet and flow information with an intuitive dashboard for virtually any security and network investigation

About Pluribus Networks

Pluribus Networks provides fabric networking and analytics solutions that transform existing network infrastructures from being rigid, costly and complex, into a foundation for modern digital-centric businesses. Our Fabric provides unprecedented insight, agility and security to create the industry's only combined SDN and Network Performance Monitoring (NPM) offering.

Learn more at **www.pluribusnetworks.com** and **@pluribusnet**.

Pluribus Networks, Inc., 2455 Faber Place, Suite 100, Palo Alto, CA 94303
1-855-GET-VNET / +1 650-289-4717

April 2017