Solution Overview

Highlights

- Distributed overlay Fabric inserts segmentation, filtering and security services over existing networks
- Granular network segmentation to secure wired, wireless, multi-cloud and untrusted traffic
- Isolate IoT, Operational Technology (OT), and Industrial Control System (ICS) traffic over shared networks
- Implement centralized policy definition with distributed enforcement and control across existing networks
- Transparently interconnect and dynamically share security resources and tools
- Gain visibility to improve situational awareness, support remediation and speed incident response

Enabling Segmentation, Centralized Policy, Service Insertion and Visibility with the Adaptive Cloud Fabric

With increasing numbers of high profile breaches, focusing on securing the perimeter is no longer sufficient; requiring organizations to re-evaluate their approaches to securing the network. New traffic types and the proliferation of new diverse end-points along with increased mobility and wireless access fuels a dramatic increase in untrusted traffic entering the network. In addition, the growth of multi-cloud environments and cloud services requiring access to enterprise resources pose challenges that require new approaches to gain control oversight and visibility for all traffic traversing the enterprise network.

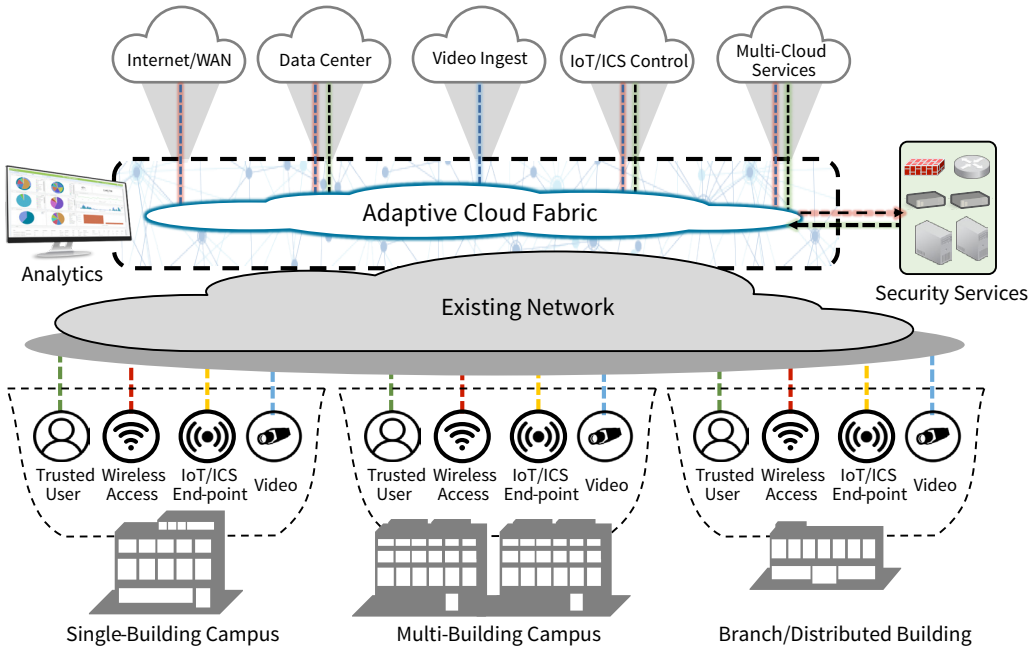
As mixed-use networks continue to grow and Internet of Things (IoT) traffic is introduced to the network, IT organizations need a more dynamic approach to address the significant increase of unsecure and untrusted traffic being introduced into the network. Despite significant investments in perimeter defense, many existing networks lack the intelligence and ability to segment and control traffic. In addition, as traditional perimeter defense and inspection technologies such as Next Generation Firewall (NGFW), Next Generation Intrusion Protection Systems (NGIPS) and Data Loss Prevention (DLP), are being more widely deployed to protect the network interior, security operations is faced with the cost and complexity of deploying these devices across the network to protect against internal threats and mitigate risks from lateral attacks and data exfiltration.

Adaptive Cloud Fabric Enables Network Control

The Pluribus Adaptive Cloud Fabric™ addresses the challenges of segmenting and controlling diverse traffic types needed to close the security gaps unaddressed by legacy networks. The Adaptive Cloud Fabric features an intelligent distributed control plane that integrates and orchestrates multiple security functionalities to improve internal security protections. These capabilities include:

- Traffic segmentation with granular, wire-speed filtering
- Centralized policy with distributed enforcement
- Security services pooling and resource sharing
- Integrated network and application visibility

The Adaptive Cloud Fabric enables the security team to establish an independent, transparent and secure control layer from which to segment and control all traffic flowing across the enterprise without dealing with the complexity of the underlying physical network infrastructure. This empowers the security team to assert direct oversight with highly granular controls for all traffic to reduce risk, and contain infiltrations to prevent attack proliferation.



Featuring a scale-out architecture to stretch across the entire enterprise, the Adaptive Cloud Fabric is inserted as an overlay to existing networks and orchestrates and automates granular traffic segmentation and filtering with service interconnection across the data center, campus, branch office and edge devices. The Fabric can be used to manage traffic to and from any number of multi-cloud services and can be extended to parallel or interconnected networks such as Internet of Things (IoT) environments, Operational Technology (OT), and Industrial Control Systems (ICS).

The Adaptive Cloud Fabric is a programmable, software-defined distributed architecture that can be inserted as an overlay to existing networks. With full interoperability with existing networks, the Fabric architecture is simple to operate, leverages open standards and common protocols, and does not require changing the underlying network architecture, or operational model.

Simple, Distributed Architecture Across the Enterprise

To meet the challenges of complex, distributed networks, the Adaptive Cloud Fabric features a unique distributed control plane to decouple network resources from the underlying hardware. This enables the Fabric to be deployed in a single physical location, across a multi-building campus or geographically stretched across distributed locations over any existing Layer 2 or Layer 3 core or WAN network.

The distributed characteristics enable a holistic Fabric that can span across a distributed campus with many buildings, such as a university or healthcare facility, or be stretched geographically across many cities and countries to support multiple data centers, campuses and branch offices.

Highly Resilient for Mission-Critical Protections

The Adaptive Cloud Fabric is deployment-proven in production mission-critical enterprise and carrier networks and is designed to meet the most stringent performance requirements with maximum levels of security, reliability and flexibility at scale without compromise. To meet high availability requirements, the Adaptive Cloud Fabric architecture has no single-point-of-failure and delivers fabric-wide resiliency with sub-second failover. Control plane traffic protection and auto-quarantine host-hog prevention protects the CPU from excessive traffic volumes and provides fine-grained control over different types of control plane classes and automatically quarantines offending host traffic in hardware.

Fabric Security Services

The Adaptive Cloud Fabric simplifies the process of defining and enforcing security policy while improving control and delivering consistent protection of virtualized or bare metal applications and services. The Adaptive Cloud Fabric uses a policy-based approach, combined with fabric-wide automation and distributed enforcement to protect against internal and external threats.

Segmentation addresses the risk from untrusted and unsecure traffic being introduced into the network and helps prevent lateral movement within the enterprise should an attack breach perimeter defenses.

Granular Network Segmentation with Adaptive Policy

Network segmentation isolates traffic into separate operational domains to segregate trusted and untrusted traffic, prevent lateral movements making it more difficult for an attacker to perpetrate an attack across the network, and protect sensitive company data to comply with regulatory mandates such as HIPAA and PCI standards. In addition, network segmentation significantly reduces system attack surfaces so that end-points only see the resources and services necessary to perform their tasks, limiting reachability and mitigating risk.

The Adaptive Cloud Fabric combines transparent network overlay tunnels and adaptive policy to enable fine-grained, wire-speed filtering and control over all network traffic traversing the Fabric layer. This empowers the security team to assert omni-directional traffic segmentation with centralized policy controls for any traffic, trusted or untrusted, across the enterprise to prevent the proliferation of malicious activity.

Any number of secure segments can be defined based upon any parameter such as service, application, traffic type, traffic source or user class. Policy can be applied on a per-user and per-flow basis to filter, isolated and redirect untrusted traffic onto the overlay fabric. Security services can be dynamically applied to segments or specific traffic classes from pooled security appliances such as NGFW and NGIPS. Traffic can be directed to specific resources such as a company-controlled IoT collection points or external cloud services. In addition, to protect against potential DDoS attacks and other malicious activities targeting the Fabric, each appliance maintains its own separate control and data plane from other appliances across the Fabric.

Security Service Insertion and Resource Sharing

Dynamic security service insertion enables the efficient sharing of physical or virtual security resources such as NGFW, NGIPS and DLP across the Fabric layer. This reduces the number of appliances needed, eliminates appliance sprawl, allows the centralization of policy management and enables the dynamic application of inspection and security services across the Fabric regardless of end-point location or origin of unsecure traffic to be inspected.

Resource pooling significantly reduces the expense and complexity associated with deploying and managing distributed security policy and services.

Centralization simplifies appliance integration and administration, as all traffic across the Fabric dynamically shares access to pooled resources. In addition, availability and resiliency for security appliances is improved as multiple appliances can be shared to meet service demands across the Fabric. Leveraging the Adaptive Cloud Fabric for service insertion enables new appliances and services to be quickly added and provisioned into existing networks without requiring the network operations team to reconfigure and redefine policy changes for the underlying network—reducing deployment time from days to minutes.

Integrates the Packet Broker Layer

In addition to delivering integrated monitoring metrics, the Adaptive Cloud Fabric can deliver groomed traffic flows to distributed performance and security monitoring tools – eliminating the need for a separate network packet broker layer. Advanced filtering capabilities enable dynamically directing specific traffic flows to specific tools. In addition, the Fabric can distribute targeted traffic flows across multiple tools and optimize speed conversions to preserve the usable life of low-speed tools deployed in a high-speed network. Groomed traffic can be delivered from anywhere to anywhere across the distributed fabric assuring the right information gets to the right tool at the right time. This greatly improves resource sharing and utilization and reduces the need to add expensive duplicate monitoring probes or security tools to different areas of the network.

Integrated Network Visibility

The Adaptive Cloud Fabric features embedded flow and packet-based telemetry to monitor every port across the Fabric at the speed of the network. This enables pervasive visibility across the Fabric without requiring expensive packet broker devices or dedicated network probes. The integrated telemetry monitors every TCP connection and flow at wire-speed, including traffic within overlay tunnels orchestrated by the Adaptive Cloud Fabric, to expose important network and application behavior characteristics.

Visibility is provided on a per-segment basis with complete separation of data for compliance requirements. Performance metrics are stored within the fabric and delivered as lightweight metadata which can be viewed using CLI from the Fabric or can be delivered via APIs or IPFIX to other monitoring systems, Security Information and Event (SIEM) platforms or the Pluribus Insight Analytics™ monitoring platform. Enabling a comprehensive view of the enterprise, the integrated visibility greatly improves situational awareness while eliminating the costs and complexity associated with independent monitoring tools.

Insight Analytics Improves Situational Awareness

Insight Analytics is an integrated monitoring platform that leverages the metadata from the embedded Fabric telemetry to visualize all traffic traversing the Fabric layer. This enables a comprehensive, real-time end-to-end view of network activity and interactions to improve operational intelligence, enhance situational awareness, support remediation activities, and speed incident response. Insight Analytics is application-aware and integrates with network services platforms such as Active Directory, Aruba ClearPass and Office365 to track user and device location and related characteristics. Real-time monitoring can provide early warning for volumetric anomalies and historical data supports granular back-in-time replay for forensic analysis activities. Insight Analytics will help the security operations team quickly identify:

- Anomalous volumetric traffic to expose emerging zero-day or DDoS attacks
- Rogue protocol activities
- Port scan attacks
- Non-authorized server access
- Rogue users and devices

Automation Simplifies Operations

The virtualized Adaptive Cloud Fabric architecture is highly programmable with integrated automation for exceptional operational agility. There are no external SDN or management controllers required – eliminating complexity and simplifying operations. The Fabric is provisioned and managed through any member device via Command Line Interface (CLI) or RESTful APIs and can be seamlessly integrated into many popular automation platforms. To support diverse operational groups, the Fabric also supports a wide array of traditional interfaces for SNMP, Syslog, and Linux scripting tools to enable cross-functional operations across SecOps, NetOps and DevOps.

The automated Fabric architecture dynamically maintains state knowledge of all member devices and implements Fabric-wide configurations, services and policies with a single atomic command. This significantly reduces configuration times by up to 90% over traditional box-by-box management. Workflow automation simplifies operations and enables service and policy changes to be dynamically updated and rolled-out across the Fabric in real-time to improve agility, responsiveness and security service velocity. To mitigate potential configuration errors, the Fabric offers dynamic configuration rollback, allowing the operator to instantaneously restore a previous configuration across the entire Fabric to prevent unwanted disruptions.

Leverages Open Networking Hardware

The Fabric supports a diverse range of network interface speeds including 1, 10, 25, 40 and 100 gigabit connections, and can scale-out to support many thousands of ports and millions of concurrent connections with multi-terabit capacity and performance and latency predictability. Enabling freedom from the constraints of legacy networks, the Pluribus Adaptive Cloud Fabric runs on many Open Compute Project (OCP), and Open Network Install Environment (ONIE) hardware compliant Open Networking switch platforms built with deployment-proven high-performance switching silicon technology.

Adopting an Open Networking strategy eliminates the lock-in associated with proprietary, closed systems and appliances and leverages white box, bare metal hardware economics to reduce Capex and Opex. This flexibility allows the choice of open networking hardware platforms to build a scale-out security fabric with the flexibility to support high-density, multi-speed connections, while providing operational consistency and simplified sparing strategies to improve efficiency and lower TCO.

Summary

The Adaptive Cloud Fabric architecture enables security teams to efficiently meet the security challenges of today's complex and distributed networks to address the need for more granular control over network traffic to support the growth of untrusted traffic and services. Using the Adaptive Cloud Fabric enables the blending of intelligent network segmentation, dynamic policy, interconnection of next-generation detection and response systems, and pervasive visibility to address the significant gaps unaddressed by legacy networks. The Adaptive Cloud Fabric empowers the security team to assert isolation with independent granular controls over network traffic and enables a more synchronized end-to-end attack response to mitigate damage and effect.

Pluribus Networks, Inc.
6001 America Center Dr.
Suite 450
San Jose, CA 95002

+1-650-289-4717
+1-855-438-8638
www.pluribusnetworks.com