USING PLEXXI SOFTWARE-DEFINED NETWORKING TO SECURE PRIVATE CLOUD TRAFFIC

SOLUTION BRIEF

Overview

Network security is top-of-mind for most CIOs and their IT staffs. It's a major challenge they face today and will continue to face far into the future. Part of their challenge is in setting up a network security model that is: flexible enough to react to constant growth and change, and efficient enough to reduce capital and operating expenses. Plexxi’s Infrastructure Network Fabric enables customers to easily implement a network security model that links together physical and virtual security services to meet specific network security goals. With Plexxi’s control software, administrators have the flexibility to configure, manage, reconfigure, and expand network fabric security services to cost-effectively meet the security requirements of their ever-changing private cloud infrastructure.

The Challenge

Many globally distributed enterprises employ an internal private cloud to deliver information technology resources across the organization. Many of these enterprises have two main struggles:

» Managing and auditing a large number of policies both centrally at the cloud and at every remote site.

» Providing fine-grain (per-workload) policy control cost effectively.

The cloud not only serves compute and data resources to applications and users at corporate headquarters, but extends cloud access to remote/branch office sites.
This not only creates a large amount of manual work and increases the chance for security lapses, but also greatly increases the scope of any audit processes mandated by corporate governance policies. At the central data center, another problem persists.

Most current private clouds are built on a traditional leaf/spine networking architecture that segments the resources based on network L2/L3 boundaries and forces policy control onto high-bandwidth inter-subnet spine links. This so-called, “macro-segmentation” provides only coarse level security that is not aligned with actual workload criticality and policy needs. The result is an unneeded burden and over-reliance on expensive stateful appliances, such as firewalls and load balancers, that can be deployed on these high-bandwidth links without an increase in security coverage. The hard-wired, static nature of the leaf/spine network limits the network’s flexibility to implement a more granular, workload-centric, software-defined approach to network security.

**The Solution**

Plexxi offers a more agile and cost-effective approach to delivering security to private clouds and distributed enterprise networks. Unlike traditional, leaf/spine networking architectures, Plexxi’s software-defined network fabric enables network administrators and cloud builders to set up specific secure paths (“Flow Entries”) that define policy actions for both corporate and remote user traffic to and from cloud resources. Plexxi’s centralization and simplification of policy, combined with the powerful workload-centric capabilities, lowers operational costs while increasing security coverage and reducing the scope of audits.

**USING PLEXXI’S FLEXIBLE FLOW ENTRIES FOR SERVICE CHAINING AND REMOTE OFFICE POLICY MANAGEMENT**

Plexxi’s innovative Flow Entry capabilities allow network administrators to create explicit policies that dictate how traffic is directed through the network. This allows administrators to solve these two specific security challenges. By deploying Plexxi at remote sites, administrators can force all traffic through the central cloud location for processing. Similarly, within the cloud data center infrastructure, the administrators can leverage flow entries to enforce specific treatment of traffic by 3rd-party security devices and other services appliances. All of these capabilities are easy to automate, providing customers simple, error free mechanisms to ensure the highest levels of security.

**SERVICE CHAINING**

Using Flow Entries in a network service chaining approach, the Plexxi administrator can explicitly define specific types of flows that need to be directed through various network services such as firewalls, load balancers, etc.. For example, the Plexxi administrator can define a flow entry that specifies that all traffic destined to a specific IP address must be serialized through any number of service devices such as: Deep Packet Inspection (DPI), Intrusion Detection Services (IDS), Network Address Translation (NAT), and Firewalls. Administrators can create these flow entries to match on Layer 1 through Layer 4 header information, and define the specific policies for traffic steering, such as drop, forward, and local redirect actions. Using these policies, specifically the redirect policy, the administrator can control how network traffic is automatically steered through the service chain. This level of service granularity and automation is key to Plexxi’s ability to reduce cost and complexity.
REMOTE SITE POLICY MANAGEMENT

Administrators can also leverage the Plexxi flow entry capability to enforce traffic redirection at local sites. By forcing all traffic through the main cloud site, security personnel can focus on managing policies only at the main site and not at every remote location. This approach helps organizations reduce the amount of managed equipment, drastically reducing operating costs, and more importantly standardizing policy to a single location, where it can be more easily managed for change control. It also reduces the amount of coverage required for security audits, greatly reducing overall security costs.

Example Secure Plexxi Configuration

The following diagram illustrates how a Plexxi Network Fabric can secure traffic flows based on the source, destination, or type of network traffic. In this configuration, the Plexxi network fabric is supported by three physical Plexxi switches. Using Plexxi Control software, the administrator defines a security policy with two flow entries: one between Web Clients and Web Servers (Zone 1), and another between Web Clients and Databases (Zone 2). If the flow header information matches one of these flow entries, the pre-configured action determines how network traffic is automatically routed through the Plexxi fabric instead of the default routing or switching information:

» The first entry defines that traffic from Web Clients to Web Servers is always allowed. The Plexxi switches make this determination based on the administrator-defined policy defined in the flow entries.

» The second entry defines that traffic from Web Clients to Zone 2 is never allowed to flow directly, but should flow through the service chain, in this example a firewall, which then makes the determination of whether to let traffic pass through to Zone 2 or quarantine.
This simple example is easily scalable to support much more extensive security scenarios that include many more flow entries and service chaining with additional value added services. The key difference between Plexxi and traditional network architectures is the ability to use software to define flow entries, which Plexxi uses to secure and control network traffic flow.

**SOLUTION SUMMARY**

The Plexxi network enables organizations to secure network traffic paths using a combination of user-defined flow entries and service chaining. Flow entries define policy-based forwarding rules that identify workload traffic and then trigger the appropriate drop, forward, and local redirect actions based on the workload’s characteristics. These actions can be linked in a service chain to value-added services, such as firewalls, to leverage additional security capabilities. The administrator can configure and reconfigure all of this, across all Plexxi switches, using a Plexxi’s software-defined network controller from a single management console. Plexxi Control has visibility of all the links and paths that make up the Plexxi fabric.

**Increasing Efficiency—Lowering Costs**

Plexxi’s software control plane delivers the agility needed to quickly respond to change and make more efficient use of physical, stateful devices like firewalls. With Plexxi’s security service chaining, organizations can preserve performance for legitimate network traffic, while enabling the tightest security controls for any suspicious traffic. Plexxi administrators can align security inspection mechanisms with the nature of the threat, rather than being forced to a “one-path-fits-all” approach, or worse yet, disabling certain security controls to maintain only minimum compliance standards.

The economic advantages of Plexxi security service chaining are most realized in network topologies that have many remote points of access, remote/branch offices or remote point-of-sales systems, where potential security threat levels are high.

One straightforward approach to mitigate these remote threats could be to deploy a stateful firewall at each remote edge location to monitor and control all traffic flow between the edge and the core private cloud. While effective from a security perspective, this deployment and operation of remote office firewalls is a very inefficient and costly proposition.

A better, more cost-effective approach is to deploy stateful firewalls at the core of the private cloud, and use a security service chaining approach to evaluate network traffic coming from edge locations, and then steer only suspicious traffic through to the stateful firewall(s) at the core. For example, by creating a Plexxi affinity group policy, which designates that traffic from an edge office user to the parts list database hosted at the core, can bypass the core firewall and steer such traffic directly to the database. Conversely, another affinity group policy for traffic originating from any POS location must go through the core firewall. This approach not only consolidates firewalls in the core of the private cloud, but also reduces the reliance on the firewall(s) to process all remote site network traffic. Consolidation of firewalls at the core also reduces the security audit domain and narrows the scope of audit for security.
Benefits Summary

Plexxi’s infrastructure network fabric delivers significant benefits to organizations that require a dynamic security model for specific workloads in the cloud.

» Ease-of-Use: Plexxi’s network fabric is simple to configure and manage. Unlike traditional leaf/spine networks, which are hardwired and inflexible, the Plexxi fabric is a Software-Defined Network (SDN) under software control. Administrators can easily define specific actions for a given network workload to match corporate policies, and the Plexxi fabric dynamically manages them.

» Operational Efficiency: Because the Plexxi network fabric is under software control, it is much more flexible than traditional leaf/spine networks. The Plexxi solution offers much better agility to react to change, and administrators can incrementally scale network resources as needed.

» Reduced Capital Costs: A Plexxi solution is much less complex than traditional network architectures, requires considerably fewer cables, and does not require the administrator to over provision network bandwidth at initial setup. As a result, Plexxi is much less expensive to deploy and maintain. Also, by controlling traffic flow using flexible flow entries and service chaining, there is less of a reliance on expensive firewalls, routers, and load balancers to secure network traffic.

» Reduced Operational Costs: The Plexxi fabric, including all member switches, is managed and controlled from a single management console. Administrators can easily define flow entries via Plexxi Control, and easily chain together flow entries and value added services, such as firewalls, to secure specific traffic throughout the cloud infrastructure.

Learn More

To learn more about Plexxi networking solutions and Plexxi Connect Integration Packs for Nutanix Enterprise Cloud Platform and VMware send an email to info@plexxi.com.

The information contained herein is subject to change without notice. Plexxi, the Plexxi logo, LightRail, and Flexx Ports are trademarks of Plexxi Inc. Other company, product or service names may be trademarks or service marks of their respective owners.