SOLUTIONS BRIEF

PENSANDO

Guardicore Integration with Pensando Distributed Services Cards

Data Center Challenges

As the number and types of applications companies deploy accelerates, security risks continue to grow exponentially. In the past, it was considered sufficient to control external access to the data center—essentially a perimeter or North/South firewall—as most flows were between end users and an application backend.

With the growth of distributed applications, virtualization, and containerization, 70-80% of the traffic in a data center is now East/West, creating more complex security challenges within the data center itself.

Addressing East/West security introduces two fundamental challenges:

- **Security must scale** alongside application growth without increasing latency, decreasing throughput, or adding complexity to network design.
- The proper security rules between each application need to be determined and implemented, simply and accurately. Given the complexity and frequency of this task, **automation is key**.

The combination of the *Pensando Distributed Services Platform* and the *Guardicore Centra Security Platform* uniquely addresses both of these problems:

- The Pensando platform provides network services that efficiently scale with your enterprise, transparently offloading and isolating critical functions from your server hardware and software.
- Guardicore Centra automatically discovers applications and flows— including process-to-process communications—and creates contextual maps that make understanding activity and creating policies simple. This allows for all East/West firewall rules to be created in an automated fashion, which can then be implemented, agent-free, on the Pensando platform.

The integration of these two groundbreaking platforms delivers unprecedented security to match the increasing risks in leading-edge application deployments.

Security at Scale

Security monitoring and protection has traditionally been implemented by hardware appliances or VM hosted firewalls. In either case, the shift from simple North/South traffic patterns to a virtualized/distributed application environment creates the need to "trombone" traffic—either physically or logically—to the firewall before it reaches its destination workload. This complexity has historically created several challenges:

- Inserting security now requires modification to the networking layers;
- Workload mobility requires the re-establishment of security as an element of any relocation—either on a new appliance or by tracking to a new inline VM;
- Latency is increased, both by security processing and by additional network hops;
- Security is now a multi-dimensional problem, as each firewall needs to be sized for the bandwidth of the workloads it is protecting. A simple application update can change traffic volumes and invalidate

© 2021, Pensando Systems. All rights reserved

firewall scaling. Workload mobility can create firewall "hot spots", leading to dropped flows and impacting application performance.

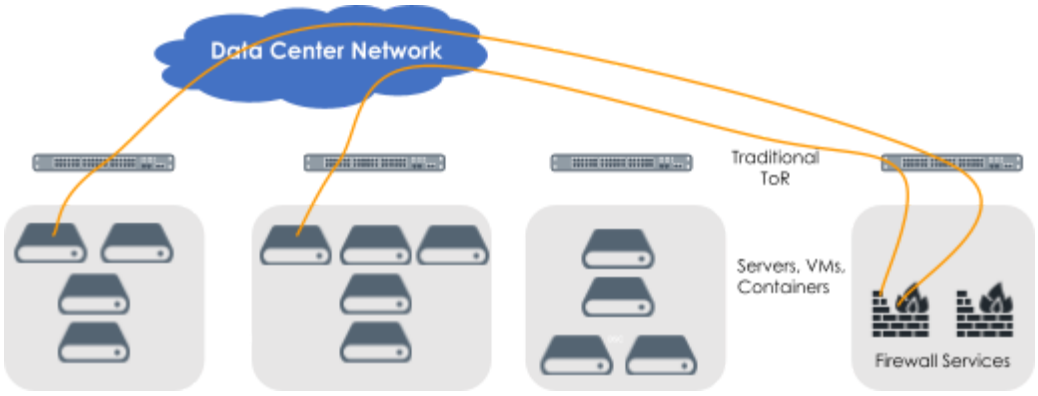

Figure 1. Traditional firewall appliances require E/W traffic to be tromboned between source and destination, increasing complexity and introducing performance issues.

The Pensando platform solves this problem architecturally, by separating security functions from the x86 environment, operating system, or hypervisor, and delivering the advantages of a dedicated security appliance at the server edge, for optimal scale and efficiency.

The Pensando Distributed Services Card (DSC) is a custom, fully programmable processor optimized to deliver cloud, compute, networking, storage and security services wherever data is located. It is a tamper proof, anti-counterfeit DPU that can provide workload security and protect hypervisor or bare metal operating systems as well. By hosting security functions outside of the x86 hardware/software stack, any compromise in the kernel or user space cannot affect security policy enforcement.

Since all traffic to or from each server already passes through the DSC acting as its network interface, enabling firewall functionality on the DSC delivers security at scale. Each server has a DSC, so security capabilities scale with each new server added to the data center. Each DSC delivers firewall services (supported in bare metal, virtualized (Microsoft Hyper-V, Linux KVM) and containerized environments) at full line rate for each server; firewall bandwidth is automatically dimensioned for the data center's needs. Since services are isolated from the x86 hardware/software stack, every server can protect all workloads without any performance impact. Network tromboning is no longer a concern: any flow between workloads will traverse DSCs without any redirection needed, further simplifying the data center architecture.

© 2021, Pensando Systems. All rights reserved

Security Simplified

With security services now a scalable function of the data center fabric, the second challenge to address is to determine the proper firewall rules to be enforced.

Guardicore Centra is able to automatically determine the proper rules between applications in the data center by monitoring the traffic logs between applications and learning the proper rules to support these flows and block any other attempts to access these workloads. The Pensando platform provides the raw data, with each DSC monitoring all flows and passing that log information to Guardicore. Centra analyzes these flows, learns how the workloads communicate, and then creates a set of firewall rules to enforce these flows. These rules are then passed back to the Pensando Policy and Services Manager (PSM), the centralized management component of the Pensando platform, which then establishes and maintains the appropriate policies on each DSC. Once these rules are in place, Guardicore Centra can continue to monitor application flows (both those blocked and those that pass through the firewall) to verify that proper application policies are being enforced and update them as services are added or modified.

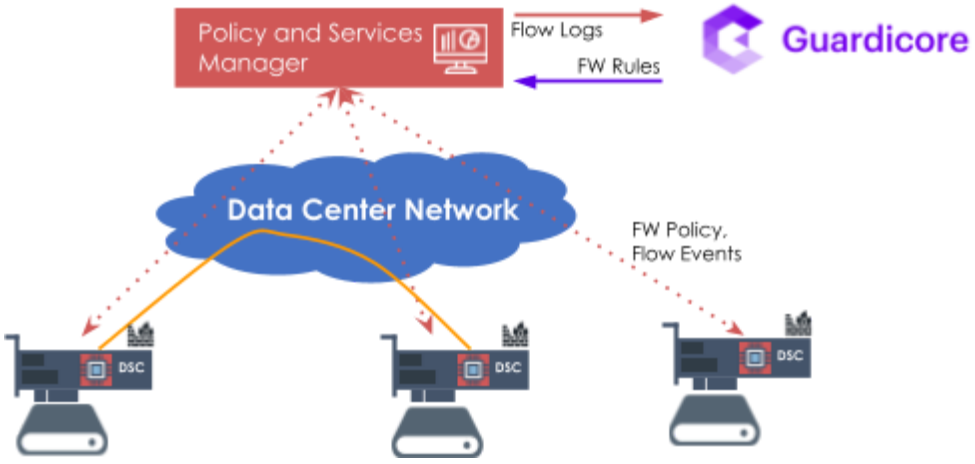

Figure 2.The Pensando platform's distributed stateful services implement a flexible, centrally-managed firewall and flow monitoring solution that scales with applications and eliminates the need for tromboning..

Conclusion

Security is one of many infrastructure services that the Pensando Distributed Services Platform can deliver at the server edge. Together, Guardicore and Pensando address the two most challenging problems in securing next-generation application architecture: scale and automation. By making firewall services a pervasive, scalable part of the data center fabric and automating application firewall rules, effective security does not impact workload performance or scalability. East/West security can now scale with applications, and update as the services themselves are updated—enabling an easy-to-provision and secure data center, and at the same time freeing expensive x86 hardware/software resources.

© 2021, Pensando Systems. All rights reserved