SOLUTION BRIEF

PENSANDO

Guardicore Integration with Aruba CX 10000 with Pensando

Data Center Challenges

As the number and types of applications companies deploy in their data centers 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 the applications themselves.

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 *Aruba CX 10000 Series Switch with Pensando* and the *Guardicore Centra Security Platform* uniquely addresses both of these problems:

- The Aruba CX 10000 is the industry's first *distributed services switch* (*DSS*), providing network services that efficiently scale with application workloads, transparently offloading and isolating critical functions from server hardware and software. In short, security becomes part of the fabric, not just an add-on function.
- 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 products delivers unprecedented security, to match the increasing risks in leading-edge application deployments.

Security as Part of the Fabric

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

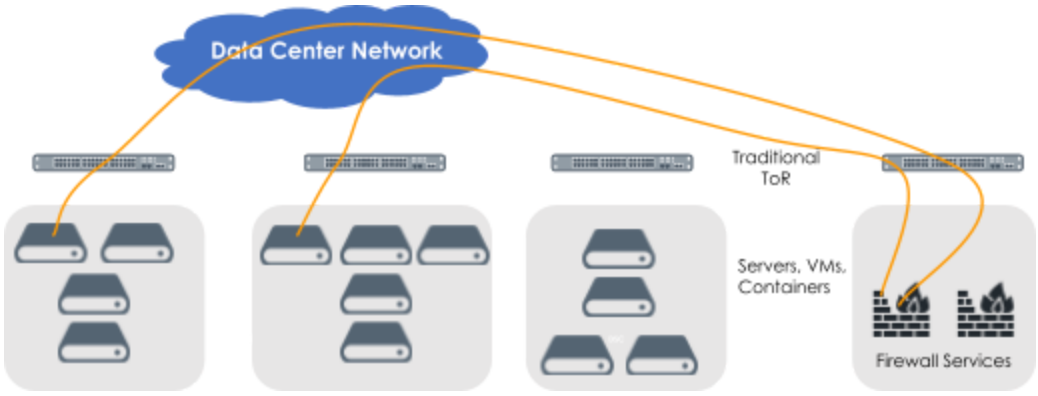

Figure 1. Traditional firewall appliances require E/W traffic to be tromboned between source and destination, increasing complexity and introducing performance issues.

The Aruba CX 10000 DSS solves this problem architecturally, by distributing security functions within each switch. Any server connected to the DSS can have specific security policies applied. The firewall function is now simply part of the fabric.

Network tromboning is no longer a concern: any flow between workloads will traverse DSSes and can be secured without any redirection needed, further simplifying the data center architecture. In short: Flows are secured as they enter the fabric, removing any inappropriate traffic from the data center backbone at the network edge.

Security Simplified

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

Guardicore Centra is able to automatically determine the proper rules between applications in the data center by monitoring the traffic logs between applications, determining what is necessary to support valid flows, and blocking any other attempts to access workloads. The Pensando platform provides the raw data, with each DSS 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 CX 10000. 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.

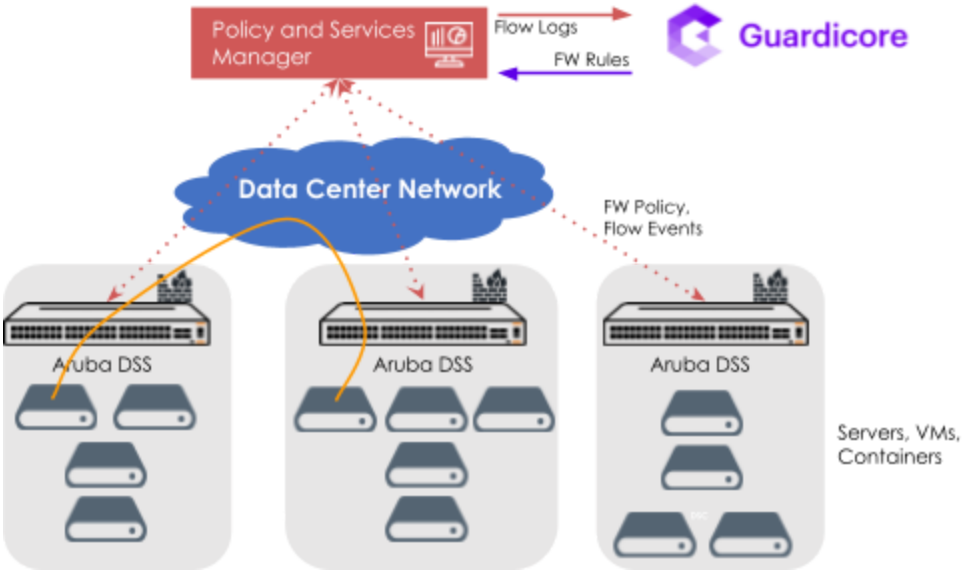

Figure 2. The Aruba CX 10000's distributed stateful services implement a flexible, centrally-managed firewall and flow monitoring solution that scales with applications and eliminates the need for tromboning..

Conclusion

Security is one of many infrastructure services that the Pensando Distributed Services Platform can deliver at the server edge. Together, Guardicore, Aruba, and Pensando address the two most challenging problems in securing next-generation application architecture: scale and automation.

For enterprises implementing the Aruba CX 10000 Series Switch with Pensando, security is now part of the fabric. All flows that enter the fabric are now secured. The integration of Guardicore Centra provides unprecedented ability to determine the required East/West security rules between these applications, further automating the overall process.

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 host hardware/software resources.