HPE aruba networking

HPE Aruba Networking CX 10000

Akamai Guardicore security integration

HPE GreenLake

Data center challenges

As the number and type of data center applications deployed accelerate, 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.
- 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 HPE Aruba Networking CX 10000 Series Switch with AMD Pensando and Akamai Guardicore Segmentation uniquely addresses both problems:

- The HPE Aruba Networking CX 10000 is the industry's first distributed services switch (DSS) that provides network services that efficiently scale with application workloads, transparently offloading and isolating critical functions from the server hardware and software. In short, security becomes part of the fabric, not just an add-on function.
- Akamai Guardicore Segmentation automatically discovers applications and flows - including process-to-process Communications - and creates contextual maps that make understanding activities and creating policies. This allows the automatic creation of all east-west firewall rules, which you can then implement, agent-free, on the Pensando platform. The integration of these two groundbreaking products delivers unprecedented security, matching the increased risks in leading-edge application deployments.

Security as part of the fabric

VM-hosted firewalls or hardware appliances have traditionally implemented security monitoring and protection. 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 modifying 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 bandwidth sizing 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.

The HPE Aruba Networking CX 10000 solves this problem architecturally by distributing security functions within each switch. Any server connected to the CX 10000 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 CX10000 switches and be secured without needing redirection, 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.

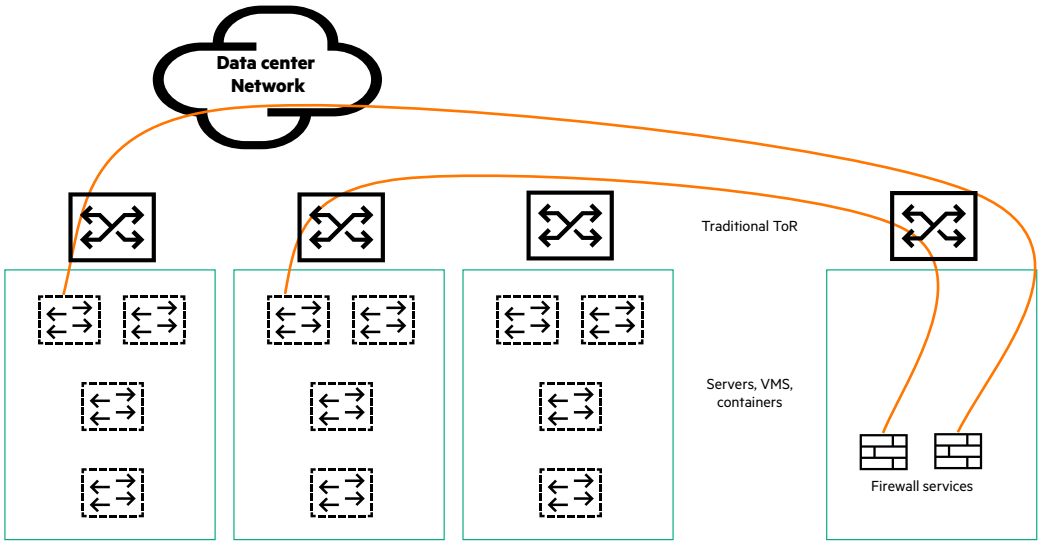

Figure 1. Traditional firewall appliances require east-west traffic to be tromboned between source and destination, increasing complexity and introducing performance issues.

Security simplified

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

Akamai Guardicore Segmentation can 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 Akamai Guardicore Segmentation. 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 **HPE Aruba Networking Fabric Composer** Policy and Services Manager (PSM), the centralized management component of the solution, which then establishes and maintains the appropriate policies on each HPE Aruba Networking CX 10000. After these rules are in place, Akamai Guardicore Segmentation continues monitoring application flows (both those blocked and those that pass through the firewall) to verify that proper application policies are enforced and updated as services are added or modified.

Conclusion

Security is one of many infrastructure services that the HPE Aruba Networking CX 10000 Distributed Services Platform can deliver at the server edge. Together, Akamai and HPE Aruba Networking address the two most challenging problems in securing next-generation application architecture: scale and automation.

For enterprises implementing the HPE Aruba Networking CX 10000 Series Switch with AMD Pensando security is now part of the fabric. All flows that enter the fabric are now secured. The integration of Akamai Guardicore Segmentation 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 up expensive x86 host hardware/software resources.

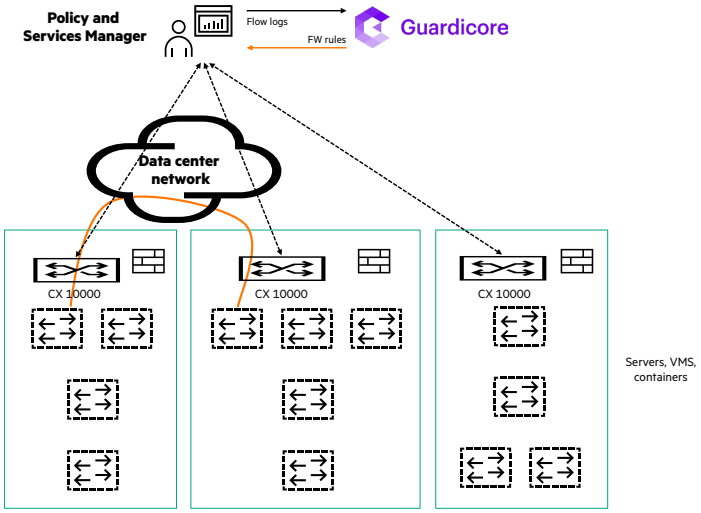

Figure 2. The HPE Aruba Networking CX 10000's distributed stateful services implement a flexible, centrally managed firewall and flow monitoring solution that scales withapplications and eliminates the need for tromboning.

Make the right purchase decision.
Contact our presales specialists.

Contact us

Visit **ArubaNetworks.com**

SO_HPEANWCX10000withAMDPensando_RVK_041024 a00138695ENW

Hewlett Packard
Enterprise