SOLUTION BRIEF

Building Secure Data Centers Using the Aruba CX 10000 with Pensando

Introduction

The *Aruba CX 10000 series switch with Pensando* delivers **stateful software-defined services** inline, at scale, with wire-rate performance and orders of magnitude scale and performance improvements over traditional data center L2/3 switches, at a fraction of their TCO. It represents a new category of data center switches, combining best-of-breed Aruba data center L2/3 switching with Pensando Elba, the industry's only fully-programmable data processing unit (DPU).

By integrating stateful service capabilities within a data center switch, the CX 10000 moves security closer to where applications and workloads are processed, without changing existing hardware or software configurations. This introduces significant opportunities for any organization to improve their data center security posture, while reducing cost of acquisition and simplifying operations.

This document will compare the CX 10000-based solution for security within the data center itself, contrasting its opportunities with legacy firewall, software agent, and classic switch implementations.

Zero Trust Security For Data Centers

The cybersecurity threat landscape has changed dramatically in recent years. Today, adversaries are more motivated than ever to penetrate enterprise data centers and steal valuable information.

Therefore, adopting the concept of *zero trust* is the number one trend in enterprise security practice today. For the data center, this means by default trusting no entity on the network, and distrusting all traffic unless a security policy explicitly allows it. According to NIST SP 800-207, "*Zero trust security models assume that an attacker is present in the environment*" and that a zero trust architecture is "*designed to prevent data breaches and limit internal lateral movement.*"

Segmentation is key to preventing unwanted lateral movement, by inspecting all East-West traffic in the data center and applying policies that stop bad actors from moving through the internal network. Several approaches have been tried to achieve segmentation in the past, but with very limited success:

- Hardware **next-generation firewall** appliance-based segmentation
- **Virtualized firewall appliance**-based segmentation
- **Software agent**-based segmentation
- **Network switch** (stateless ACL)-based segmentation

The following section will compare the architectural advantage of the Pensando/Aruba solution compared with each of the above approaches.

Solutions From Pensando/Aruba

The CX 10000's stateful services allows operators to extend the capabilities of the data center leaf-spine fabric to natively provide 800G of **distributed stateful firewall** for East-West traffic, zero-trust **segmentation**, and pervasive **telemetry**. These built-in security services are meant to minimize the attack surface within the data center, stop lateral movement, and achieve PCI compliance.

The flexibility of the CX 10000 platform allows additional security services such as stateful NAT, encryption, and advanced DDoS protection to be added in the future via a simple software upgrade.

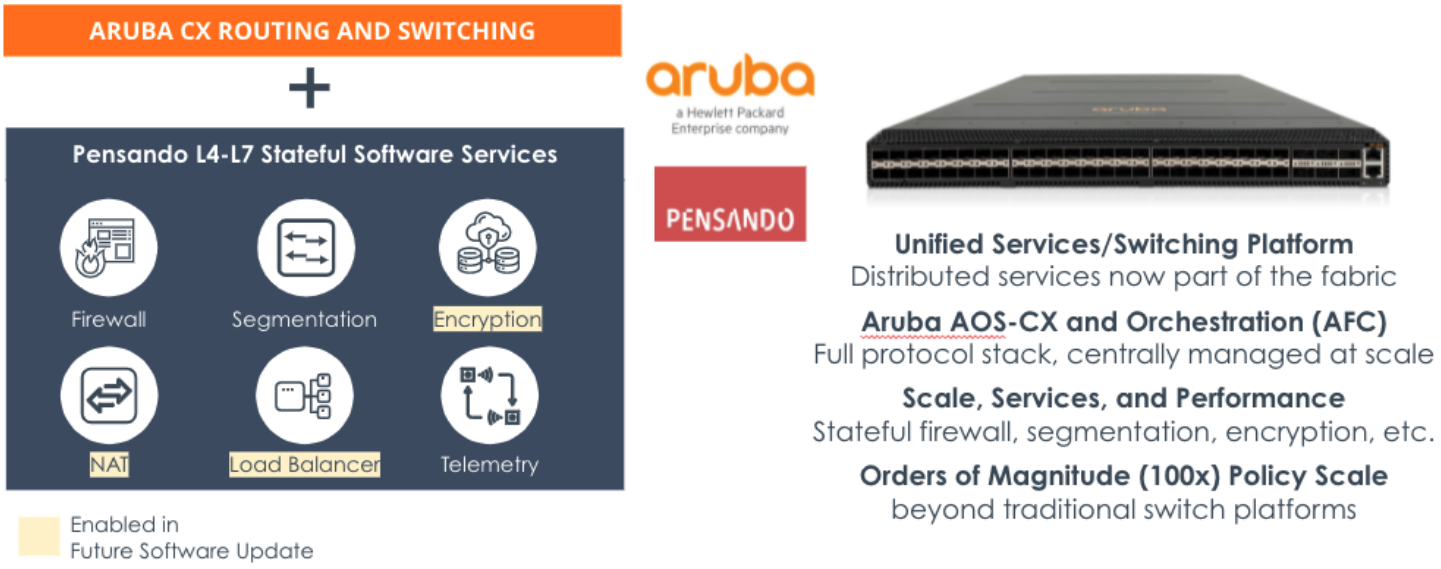

Figure 1. The Aruba CX 10000 introduces a new switching category: the Distributed Services Switch

Compared With Traditional Firewall

A solution based on traditional ("next-generation") firewalls would appear to be ideally suited to stopping East-West lateral movement, even though they are originally designed to inspect North-South traffic. Whether physical or virtual appliances, they were repurposed by many organizations to serve as internal East-West firewalls to segment the network. However, there are several key problems with this approach.

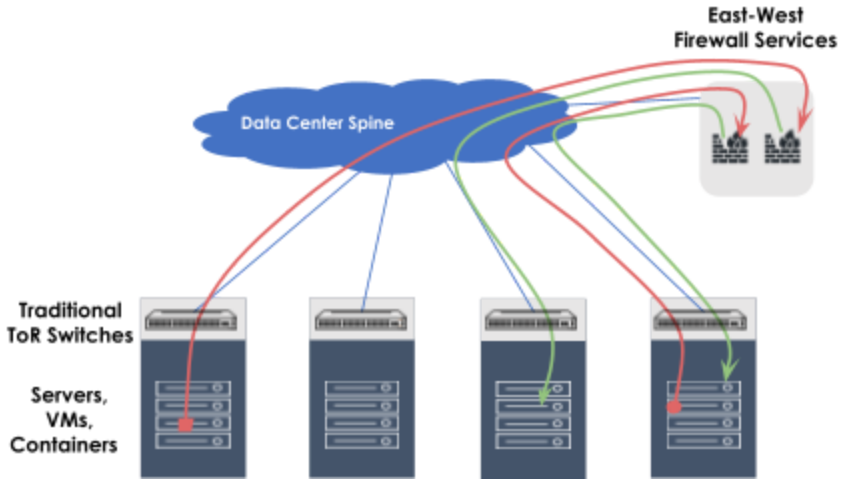

Figure 2. Traffic tromboning with firewall appliances

- **Complexity:** As shown in Figure 2, traffic tromboning is a big issue when inserting appliances in modern data center fabrics. Getting traffic to and from them symmetrically is challenging, requiring techniques like policy-based routing (PBR), and is close to impossible when dealing with overlays, as they do not natively speak VXLAN. Today next-generation firewalls are typically installed at the VRF boundary, with a leg in each VRF or as the default gateway between VLANs. This makes the appliance firewall a network choke point, and adds to the application latency and unnecessary use of network bandwidth.

- **Capacity and Cost:** Using next-generation firewalls for East-West traffic can be cost prohibitive. Such firewalls quickly run into capacity problems if trying to inspect all internal data center traffic, creating the need for multiple firewalls that must be periodically upgraded to deal with traffic increases. As a result, most organizations choose to inspect only a small amount of East-West traffic, if any.

- **Static Policies:** Next-gen firewalls don't explicitly consider data center application architecture in their design. They remain blind to the relationship between workloads and applications. Today an application may comprise multiple workload types, microservices, and containers that run in the data center or in the public cloud. In a virtual environment, workloads can be spinned on and off any minute and they can be moved around dynamically within the data center. As the workloads come and go, the same IP address can be reused. All these make traditional firewalls very ineffective as an internal firewall to enforce policies for East-West traffic.

- **Blind Spots:** The traditional model has blind spots and lack of visibility for intra-VLAN traffic.

- **Only Broader Segmentation:** It is only possible to do broader inter-VLAN network segmentation, with no option to do granular application segmentation, which is needed to protect organizations from East-West lateral movement within the data center.

On the other hand, the CX 10000 solution removes all of these limitations and challenges, providing a more robust, scalable and flexible solution. Advantages of using the CX 10000 solution include:

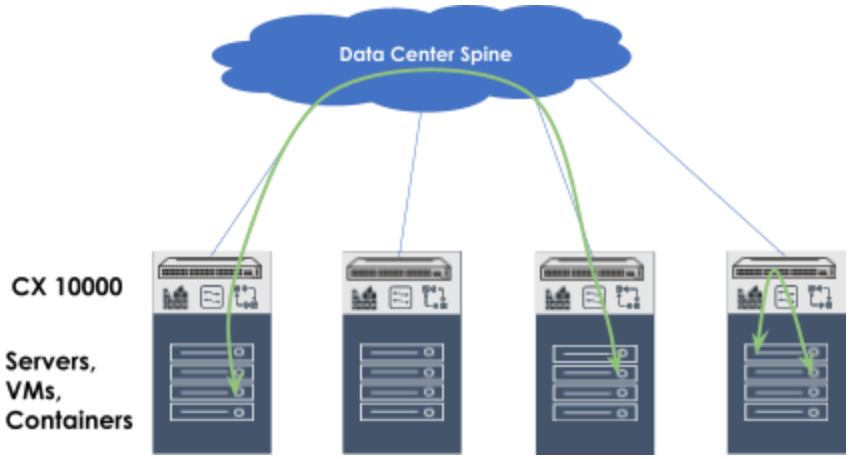

Figure 3. Firewall functions are integrated into the data center fabric, at the ToR.

- **Distributed and Scalable Architecture:** The distributed architecture inspects traffic right at the Top Of Rack (ToR) switches, removing the need to hairpin traffic to traditional centralized appliances and reducing network congestion and complexity. Aggregate East-West inspection capacity scales as additional server racks are added into the pod.
- **Cost Effective:** All stateful services including firewall come built into each and every leaf switch in the data center, priced optimally within range of the TCO of a typical standard data center incumbent platform.
- **Context-Aware Policies:** The CX 10000 solution allows context-aware segmentation policies to accommodate the dynamic nature of data center virtualization. Segmentation rules can be configured based on the virtual workloads' tags or names. As virtual workloads are spun up, deactivated, or relocated, their associated policies remain effective without any manual reconfiguration required.
- **More visibility and granular segmentation:** Because the CX 10000 switch sits at the top of the server rack, it sees all workload-to-workload communication, no matter if they are inside the same server, on different servers, within the same rack or across different racks. This deeper visibility allows the CX 10000 solution to provide more granular segmentation across the entire data center fabric.

Compared With Software Agents

The typical software agent-based solution consists of two components: an agent and an orchestrator. The agent resides inside the virtual machine, the pod or the physical server, and enforces security policies distributed to it by the orchestrator. While this approach allows for very granular control over the interaction between workloads inside a data center, there are several challenges associated with it.

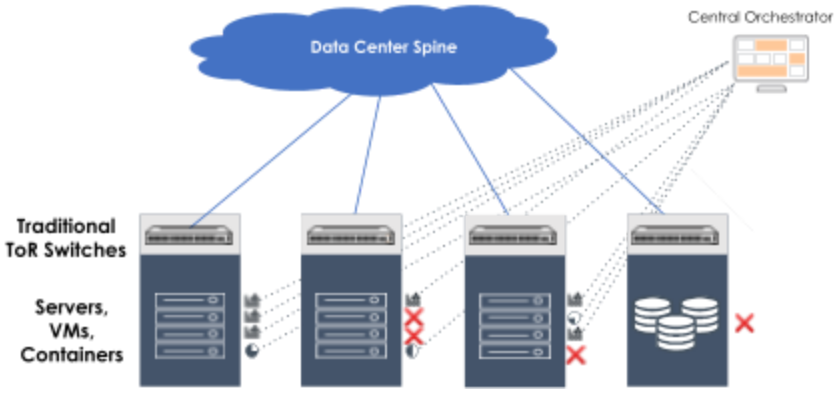

Figure 4. Software agents may not be supported on all hosts/VMs or appliances.

- **Manageability and Scalability:** This approach requires installation of the software agent in every workload. In a large enterprise data center environment with 10,000+ workloads, maintaining this huge amount of agents will soon put significant pressure on the support organization, affecting the solution's manageability and scaling. Additionally, getting approval to install agent software on machines can be challenging within some organizations, and in some cases run up against policies that strictly forbid their use (government agencies, critical infrastructure, etc.).

- **Server Resources:** All traffic enforcement and filtering is done in the software. No matter how small the percentage of CPU and memory a vendor claims to consume for its solution, in the real world the agents sap compute resources and impede performance, wasting precious resources that otherwise could be used for business applications.

- **Cost:** Customers usually have to purchase a subscription license on a per-agent per-year basis. In a large deployment, these annual subscription costs become exorbitant at enterprise scale.

- **Vulnerability:** Proliferation of agents is also becoming a security issue: as a user-level process that runs inside the host operating system, if the host is compromised, these agents can be stopped or bypassed, which effectively stops segmentation.

- **Protection Coverage:** Any component in the data center that cannot support the installation of a software agent will remain unprotected. This may include assets such as the hypervisor itself, storage servers, or a memory copy of VMotion™ traffic.

In contrast, the CX 10000 solution provides a more robust, scalable and secure solution. Advantages include:

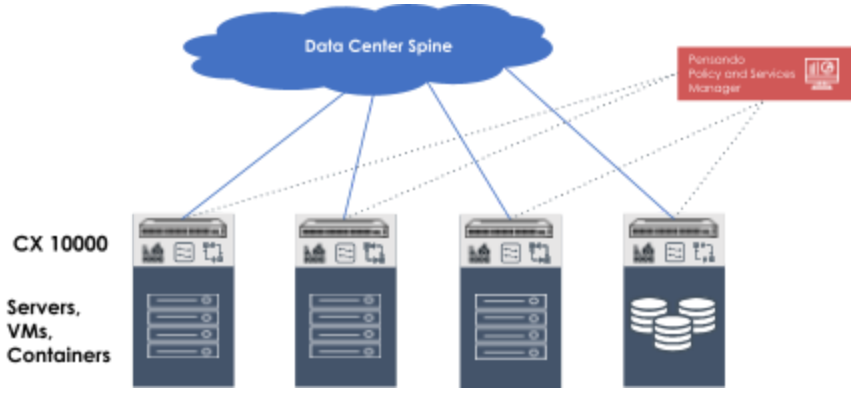

Figure 5: CX 10000 "protects the unprotected", providing full coverage for any data center asset; firewall resources scale with data center growth.

- **Manageable and Scalable Architecture:** The CX 10000 solution is managed centrally with a single pane of glass. The total East-West inspection capacity scales out as more server racks are added into the pod.
- **Zero impact on server resources:** All traffic inspection happens on the CX 10000 switch with hardware acceleration outside of the rack servers, with minimal latency.
- **Cost Effective:** The stateful firewall is built into each and every ToR switch (CX 10000) without any additional cost. The standard CX 10000 package includes the East-West firewall license.
- **Secure Platform:** Security enforcement happens on the CX 10000 switch outside of the workload servers. In cases where one or more servers are compromised, the segmentation policy will remain effective and stop any potential lateral movement.
- **Complete Protection Coverage:** the CX 10000 solution provides complete protection coverage for any connected data center asset, such as bare metal servers, hypervisors, virtual machines, storage servers, independent of operating system type or version.

Compared With Network Switches (Stateless ACLs)

This approach simply leverages the standard stateless ACL feature supported in most network switching platforms to filter East-West traffic within the data center. Stateless ACL-based filtering merely leverages generic access lists and checks if a packet matches the source and destination address and port numbers in the header to make a permit/deny decision. Irrespective of whether they receive a single packet or thousands, each packet is treated individually and the switch doesn't track the ordering of packets in a TCP session, or maintain or understand connection state.

This approach will quickly run into many restrictions for a large data center deployment.

- **Stateless:** Its stateless nature provides no session tracking for traffic flows. Lack of session tracking requires the policy to explicitly include rules for the return traffic of each flow, which effectively opens all ports to the server and provides zero protection for clients.
- **No application-layer gateway (ALG) support:** Applications that use multi-channel protocols such as FTP, MSRPC etc, require data channels to be created dynamically on the fly. These dynamic channels have

known significant difficulties in association with stateless ACLs.

- **Lack of security:** A standard ACL solution does not provide any security checks for TCP sessions, such as handshake validation, half-open session checking, etc. This means application servers are vulnerable to DDoS attacks.
- **Scale limitation:** Standard ACLs in network switches are usually implemented in the switch's TCAM table for faster speed. However, TCAM table size is limited in most switch products, which results in a limited number of ACL entries that can be supported. In addition, lack of support of group-based policy makes it even less scalable.
- **Manageability:** Standard ACLs are difficult to manage at scale. By design, ACLs are configured at each port level for each switch. Enterprise data centers can easily deploy thousands, even tens of thousands of switch ports. Implementing a right set of ACL entries at the right port can quickly become a nightmare for network administrators.
- **Static rules:** By design, standard ACL rules are implemented by simply using layer 3/4 IP addresses and ports. They remain blind to the relationship between workloads and applications. In a virtual environment, workloads can be spun up or down at any point, and dynamically migrated within the data center, which makes standard ACLs very limited and cumbersome when it comes to enforcing policies for East-West traffic.

The stateful firewall embedded natively as part of the CX 10000 platform provides a full suite of traditional firewall functions normally only found in dedicated appliances, which include:

- **Stateful connection and ALG support:** The CX 10000 solution intrinsically supports stateful connection tracking. Return traffic of existing flows is automatically allowed. ALG support is also built in, including FTP, TFTP, and MSRPC.
- **TCP security checking:** Comprehensive TCP session security checking—such as TCP handshake validation, half-open session tracking, and DDoS protection—is included as part of the stateful firewall feature set.
- **Highly scalable rules:** The policy rules in the CX 10000 solution are implemented in data plane DRAM, instead of TCAM, with the support of a highly efficient lookup algorithm. This method removes the TCAM size limitations while maintaining line-speed traffic filtering. The CX 10000 security policy has practically unlimited scaling, up to millions of rules,
- **Easy to manage and deploy:** By design, CX 10000 security policy is configured at the entire cluster level. Sites need only consider who is allowed to talk to who inside the data center when configuring the security policy, without worrying how policies will be deployed: which CX 10000 switch and which port is automatically determined by the management plane, which will apply these policies for optimized deployment.
- **Context-Aware Policies:** The CX 10000 solution implements context-aware segmentation policies to accommodate the dynamic aspect of data center virtualization. Segmentation rules can be configured based on the virtual workloads' tags or names. Even as virtual workloads are spun up, deactivated, or migrated, the policies can remain untouched and still effective.

Summary

As enterprise data centers continue to grow, both in size and sophistication, it is increasingly important to protect lateral (East-West) traffic. At the same time, it's increasingly impractical to implement security solutions that require routing traffic to a centralized policy enforcement point, or deal with the management and resource overhead of software agent-based implementations.

The Aruba CX 10000 solution delivers a unique blend of performance, scale, and automation for distributing advanced networking and security services at the network access layer edge, providing scalable coverage where the applications are running, with simplified dynamic management at low cost.

About Pensando

Founded in 2017, Pensando Systems is pioneering distributed computing designed for the New Edge, powering software-defined cloud, compute, networking, storage and security services to transform existing architectures into the secure, ultra-fast environments demanded by next generation applications. For more information, please visit pensando.io .