IDC

SPOTLIGHT

Sponsored by: Hewlett Packard Enterprise

A rising tide of modern applications and data demands a new approach to datacenter fabrics. Automation is a given, but the network must deliver fast provisioning, agile operations, zero trust network security, and proactive visibility — with no trade-off between speed and security control.

Meeting the Need for High Performance and Security Through a Modern Datacenter Fabric

April 2023

Written by: Brad Casemore, Research Vice President, Datacenter and Multicloud Networks

Introduction

As modern applications require more east-west traffic, organizations must enhance their datacenter infrastructure to meet the new requirements. Modern datacenter architectures are designed to provide the agility, availability, and security that modern workloads require to support an organization's digital objectives amid the rise in cybersecurity attacks. As per IDC's *Future of Digital Infrastructure 2022 Global Sentiment Survey*, around 57% of respondents were moving to more flexible software-defined networking infrastructure to meet emerging edge computing, distributed data, and mobile/hybrid work strategies.

AT A GLANCE

KEY TAKEAWAYS

- Digital business means that applications and data have never been so important to commercial success and competitive advantage.
- Datacenter networks, which provide essential connectivity and security for the servers that host modern applications and rising tides of east-west data traffic, must be revamped to meet the need for both unprecedented performance and uncompromised security.

Increased Data Volumes and Modern Apps Place New Requirements on the Datacenter Network

At the same time, modern application architectures and increased data volumes require better control and visibility at the network edge, where the network and compute merge, to optimize resource usage efficiently. This includes managing CPU, memory, network fabric, inline firewalls, load balancers (ADCs), racks, and power. Technologies like performance-intensive computing (PIC) support complex workloads such as modeling, forecasting, and scenario planning, enabling faster business decisions. IDC predicts that 35% of the G2000 will benefit from investments in PIC by 2026. With server densities and processing power increasing, the need for edge control and visibility grows, and network bandwidth also increases with server adapters and top-of-rack (ToR) switches moving to 25/100Gbps and 100/400Gbps becoming prevalent in cloud datacenter networks.

Growing Wave of East-West Traffic Redefines Security Requirements

The speed and volume of east-west traffic in virtualized and containerized application environments require new security requirements, especially in multitenant scenarios where zero trust security is imperative. Automated and policy-based network segmentation and microsegmentation are necessary, and centralized security appliances are inefficient for expanding traffic flows. Hairpinning of traffic to hardware appliances at the datacenter edge impairs application performance, restricts scalability, increases costs, and adds latency. The datacenter network is critical in enabling or hindering digital objectives, and modernization is necessary to optimize server and storage performance. Failure to modernize compromises the integrity and performance of critical applications.

A Simple, Scalable, Secure Approach to Datacenter Network Automation

Unfortunately, many organizations with dedicated or private cloud environments find themselves hindered by fragmented and inflexible traditional network architectures and infrastructure. These complexities can lead to impaired digital business agility and increased security risks. Traditional network architectures were not designed to handle the highly dynamic east-west traffic volumes of modern applications, and operational models tend to be manual and inefficient.

To address these challenges, a simpler, scalable, and consistent approach to network automation is necessary. Such an approach should be aligned with cloud agility and streamlined operations, allowing organizations to unify, automate, and secure overlay and underlay networking across their distributed application landscape. This unified approach can significantly reduce operational costs and increase business agility by ideally providing a common and unified network fabric across switches and hosts that support heterogeneous infrastructure comprising multiple hypervisors, Kubernetes, and bare metal workloads. In addition, this fabric should encompass distributed security services, eliminating the inefficient and costly clutter of appliance sprawl.

In the past, customers were compelled to choose between performance (speed and throughput) or control and security. However, with increasingly important workloads critical to digital business running on datacenter networks, customers are now rightfully demanding both performance and security from their datacenter networks. With a unified and automated approach to datacenter network automation, organizations can achieve both performance and security, without sacrificing one for the other.

Benefits

A modern datacenter network fabric, with an architecture and operational model that extends all the way to the server, provides a range of benefits such as:

- **Faster provisioning:** Improved fabric automation and orchestration allows for greater provisioning agility and speed, including better adaptability and flexibility of IT operational models. Extensive automation mitigates the delays entailed by manual interactions involving siloed IT operations teams.
- **Simplified, agile network and security operations:** Policy-based network automation and orchestration over a unified fabric simplifies the entire life cycle of network operations, from day 0 through day 2/N. Not only is provisioning simplified and accelerated but so is troubleshooting and remediation of issues that can affect application availability and performance.
- **Zero trust network security:** By delivering advanced services at the network-server edge, infrastructure operations teams can provide protection throughout the network, putting a distributed stateful firewall at every switch port. The result is a reduction in coverage gaps, as well as a diminution of the costly and complex sprawl associated with firewall hardware and software appliances.
- **Actionable, proactive insights:** Real-time telemetry provides ubiquitous visibility across all east-west datacenter traffic, enabling network operators to detect potential issues before they become serious problems that can affect application performance and availability. The result is a more proactive approach to datacenter operations, resulting in highly performant and optimized applications and digital services.
- **No compromise between performance and security:** This approach to automating a modern datacenter network fabric solves the dilemma of having to choose between performance and network speed on one hand and fine-grained control and security on the other. Enterprises can now have both, with no compromise to either.

How Hewlett Packard Enterprise Addresses Automation and Security in the Modern Datacenter

Hewlett Packard Enterprise (HPE) offers a datacenter networking portfolio featuring HPE Aruba CX switches, including the HPE Aruba X 10000 Series Switch, the industry's first distributed services switch (DSS). The HPE Aruba CX switches provide robust and scalable hardware and intuitive management tools with a cloud-native operating system designed for modern datacenters. The HPE Aruba CX 10000 is an essential component of the HPE Aruba datacenter fabric, delivering advanced network and security services at the datacenter edge. It integrates with the HPE Aruba Fabric Composer, an API-driven software-defined network orchestration platform that simplifies and accelerates network provisioning, security management, and day-to-day operations. It orchestrates datacenter switches as a single network fabric throughout an automated network life cycle, supporting workflows that abstract and streamline otherwise complex and manual processes associated with datacenter infrastructure.

The HPE Aruba CX 10000 provides a simple spine-leaf underlay overlay network, offering 3.6Tbps of switching capacity, 48 ports of line rate 10/25GbE (SFP/SFP+/SFP28), and 6 40/100GbE ports (QSFP+/QSFP28). It is supported by the Pensando Elba programmable DPU, which provides distributed stateful firewall, zero trust segmentation, and pervasive telemetry for east-west traffic, as well as forthcoming capabilities for stateful NAT and encryption services. In addition, it integrates with various third-party network and security products and tooling, including those for advanced security and performance management. The HPE Aruba Fabric Composer centrally configures switch configurations and distributes firewall policies.

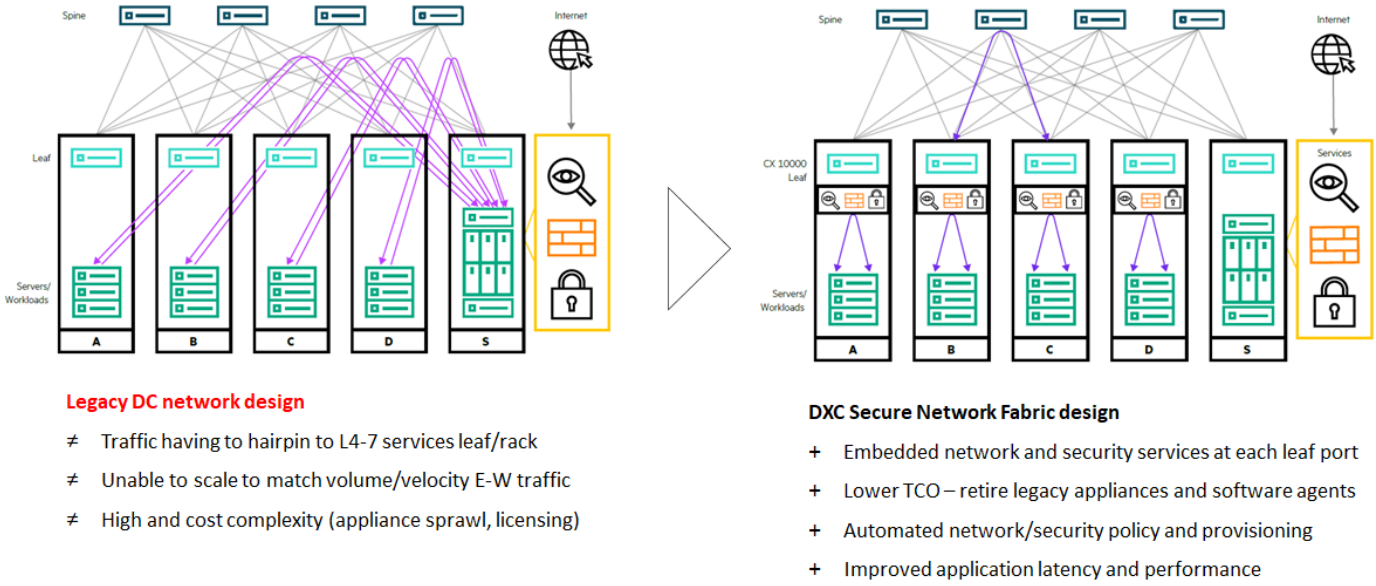
DXC Secure Network Fabric Offering Powered by HPE Aruba CX 10000 Series Switch

Hewlett Packard Enterprise has partnered with DXC Technology, a global service integrator with 130,000+ employees and more than 240 Fortune 500 customers across 70 countries. As part of the go-to-market (GTM) relationship, DXC designs, validates, and delivers to customers a range of use cases for the HPE Aruba CX 10000 through its DXC Secure Network Fabric offering. Customers can take advantage of DXC's expertise in designing, deploying, and managing next-generation datacenter network fabrics utilizing HPE Aruba CX10000, orchestration, and automation capabilities. This partnership enables a symbiotic relationship where DXC provides knowledge of customer requirements to HPE Aruba 's product development, ensuring alignment in providing solutions.

East-West Segmentation Use Case

DXC Technology utilizes the HPE Aruba CX 10000 and HPE Aruba Fabric Composer in its 40+ global datacenters to enhance its security posture with micro-segmentation and improve operations through automation. The Distributed Services Switch architecture enables granular control over the interactions between customer-facing tools and applications, enhancing traffic visibility and security across the entire datacenter fabric. Traffic is inspected directly at the ToR switches, eliminating the need to hairpin traffic to traditional centralized appliances while reducing network congestion and complexity. As additional server racks are added to the pod, aggregate east-west inspection capacity scales accordingly, enabling active/active stateful firewalling with state-sync via VSX. In addition, the HPE Aruba CX 10000 solution includes all stateful services, including firewall, built into every leaf switch in the datacenter, improving the TCO profile relative to a traditional datacenter platform (see Figure 1).

FIGURE 1: ***DXC Technology East-West Segmentation Use Case***



Legacy DC network design

≠ Traffic having to hairpin to L4-7 services leaf/rack

≠ Unable to scale to match volume/velocity E-W traffic

≠ High and cost complexity (appliance sprawl, licensing)

DXC Secure Network Fabric design

\+ Embedded network and security services at each leaf port

\+ Lower TCO – retire legacy appliances and software agents

\+ Automated network/security policy and provisioning

\+ Improved application latency and performance

Source: Hewlett Packard Enterprise, 2023

Context-aware segmentation policies accommodate the dynamic nature of datacenter virtualization, enabling segmentation rules to be configured based on the virtual workloads' tags or names. This approach ensures that segmentation policies remain effective, even as virtual workloads are spun up, deactivated, or relocated, without requiring manual reconfiguration. The HPE Aruba CX 10000 has visibility to all workload-to-workload communication, enabling granular segmentation across the entire datacenter fabric. Furthermore, all traffic inspection occurs on the switch with hardware acceleration outside the rack servers, ensuring that there is no impact on server resources and minimal latency.

HPE Aruba CX 10000 also includes stateful connection and ALG support, with comprehensive TCP session security checking and DDoS protection as part of the stateful firewall feature set. The policy rules in the solution are implemented in data plane DRAM, removing the TCAM size limitations while maintaining line-speed traffic filtering. This approach allows the switch security policy to scale up to a million rules. By design, HPE Aruba CX 10000 security policy is configured at the entire cluster level, simplifying policy and management. Sites only need to consider who is allowed to talk to whom inside the datacenter when configuring the security policy, and the management plane automatically determines which switch and port must be configured to implement policies for optimized deployment.

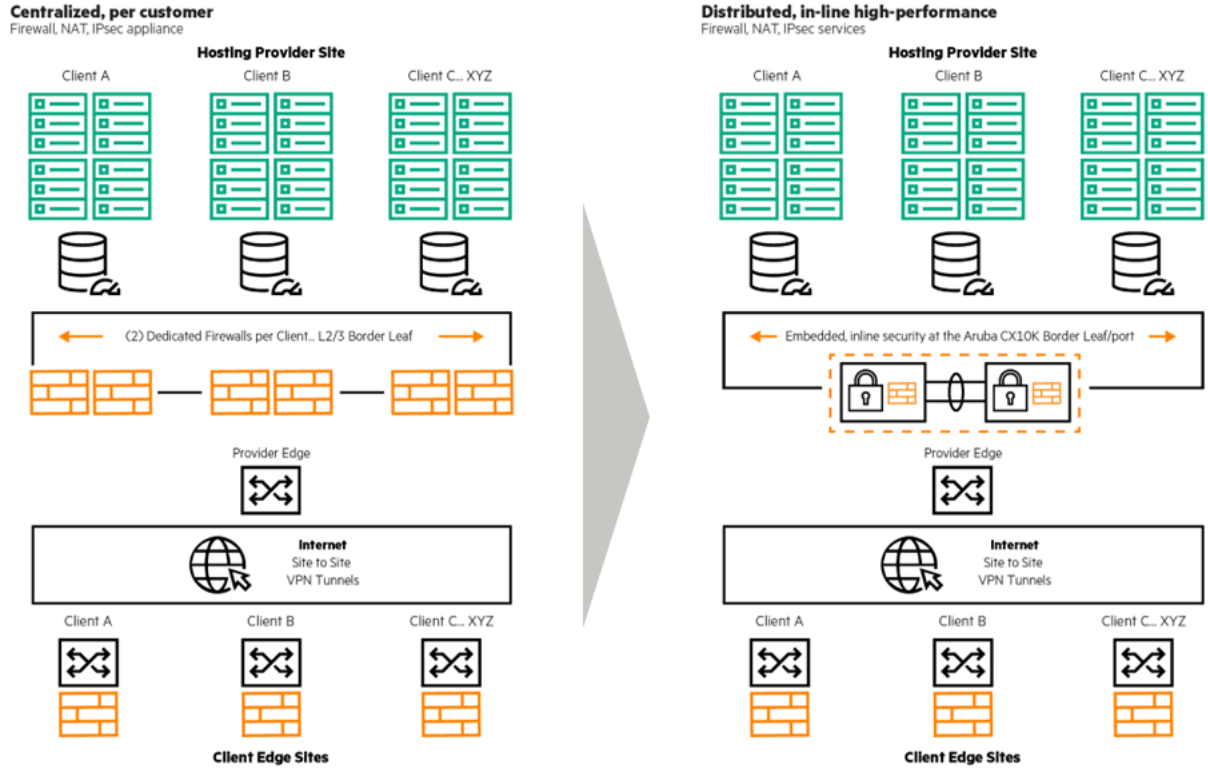
The centralized orchestration and automation provided by HPE Aruba Fabric Composer, along with the Pensando Policy and Services Manager (PSM), facilitates the combination of each datacenter switch environment into a single secure fabric with centralized policy management. This integration reduces capital and operational expenses, helping to make the solution cost-effective.

Security Appliance Replacement Use Case

In addition to simplifying its security architecture through microsegmentation, DXC Technology has utilized the NAT and encryption services provided by the HPE Aruba CX 10000 to reduce the number of security appliances and associated licenses required at the network border.

Traditionally, DXC has utilized numerous logical or physical appliances at the network border for each tenant. By replacing these with the Distributed Services Switch, DXC can significantly reduce the number of security appliances required, resulting in cost savings (see Figure 2).

FIGURE 2: ***Security Appliance Replacement Use Case***



Source: Hewlett Packard Enterprise, 2023

To further streamline DXC's security architecture, Hewlett Packard Enterprise and DXC Technology are working together to develop enhancements for the Distributed Services Switch, including NAT and encryption services. These services will help DXC reduce its security appliance footprint even further, while also providing additional security measures for ingress and egress traffic.

Challenges

The Distributed Services Switch is a departure from traditional datacenter network architecture and deployment. While the product is positioned to offer compelling benefits across several use cases and application environments, some customers might be inclined to perceive the inconvenience of change before they grasp the benefits that accrue from the modernization of datacenter architecture and infrastructure. Consequently, Hewlett Packard Enterprise and DXC

Technology must ensure that customers understand the value and utility of the offering. Hewlett Packard Enterprise and DXC Technology must also demonstrate that the product is easy to provision, deploy, and operate.

Indeed, Hewlett Packard Enterprise asserts the technology can be integrated easily into existing environments, providing benefits that traditional architected network fabrics were not designed to deliver. The limitations of prior approaches become apparent with the substantial increase in speed and density of compute resources, requiring security policy to be closer to applications and workloads.

Conclusion

Applications are the lifeblood of a successful digital business, and they are becoming more numerous and data intensive as application architectures are modernized and enterprises seek to leverage artificial intelligence (AI) and torrential data streams for competitive advantage. These developments place new responsibilities on datacenter networks, which must be extensively automated and architecturally streamlined to provide the speed, performance, scalability, and security that are integral to effective and reliable datacenter fabrics.

If Hewlett Packard Enterprise, in conjunction with its partners such as DXC Technology, is successful in overcoming the challenges cited previously, IDC believes the HPE Aruba CX 10000 Series Switch is well placed to meet the datacenter fabric requirements and use cases that are becoming increasingly important for digital enterprises worldwide.

About the Analyst

Brad Casemore, *Research Vice President, Datacenter and Multicloud Networks*

Brad Casemore is IDC's Research Vice President, Datacenter and Multicloud Networks. He covers datacenter network hardware, software, IaaS cloud-delivered network services, and related technologies, including hybrid and multicloud networking software, services, and transit networks. Mr. Casemore also works closely with IDC's Enterprise Networking, Server, Storage, Cloud, and Security research analysts to assess the impact of emerging IT and converged and hyperconverged infrastructure.

MESSAGE FROM THE SPONSOR

Data-First Modernization Requires a New Generation of Data Center Network Fabrics

The shift is on from centralized legacy data center architectures to emerging, distributed "Centers of Data." A data-first modernization strategy must consider how the network needs to evolve to provide the secure connectivity and automated agility that ensures an exceptional experience for enterprise applications and workloads regardless of where they live, on-premises, at the edge, in colocations or a public cloud. This next wave of data center connectivity requires higher performing 100/200/400GbE fabrics, simplified IT orchestration and intelligent distributed services to support next-gen app architectures running on increasingly powerful compute, across hybrid-cloud infrastructures. Learn more about how Hewlett Packard Enterprise can help your organization simplify, secure, and accelerate your Data-First Modernization journey.

https://www.arubanetworks.com/solutions/data-center-modernization/

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com