HPE aruba networking

Business white paper

Pervasive encryption and security from edge to cloud with the HPE Aruba Networking CX 10000 Distributed Services Switch

Radically reduced TCO, simplified operations, and enhanced performance

HPE

Introduction

Technology architectures are ever evolving, but rarely do we see a major development that redefines the architecture of the modern enterprise network. Today we are in the midst of the era of data as cited by many technologists and industry analysts: not data that is generated in the cloud or the data center, but rather data that is generated where for application performance, latency, or data gravity reasons makes most sense—the edge—where users, devices, and applications all come together.

Gartner has been predicting for many years that the majority of enterprise-generated data will be created and processed outside a traditional data center or cloud.

It's fundamental that the network deployed at the edge can meet the mission-critical availability, scale, and security requirements customers now demand for hybrid multicloud architectures which extend far beyond ensuring reliable connectivity site to site and site to cloud.

Next-generation fabric for data centers and edge deployments

The category creating HPE Aruba Networking CX 10000 with AMD Pensando™ has unique characteristics that make it particularly suitable to address a diverse set of these demanding use cases across data center, edge, and cloud. This includes functionality typically delivered by enterprise class services appliances, in addition to foundational, best-in-class networking enabled through the HPE Aruba Networking CX Operating System Operating System platform. In this solution paper, we'll look at unique capabilities the HPE Aruba Networking CX 10000 distributed services architecture provides for edge and cloud security.

This paper will detail several multicloud, edge, and colocation connectivity use cases that highlight the HPE Aruba Networking CX 10000's market-leading security and TCO advantages.

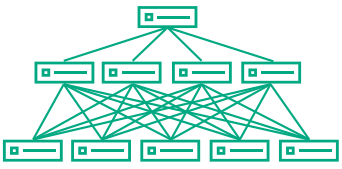
HPE Aruba Networking CX 10000 core capabilities

L4 stateful software services

- Firewall
- DDoS
- Telemetry
- NAT
- Encryption

Native security in the data center

Data center

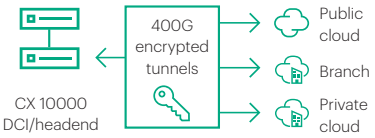


CX 10000 DC Leaf

- Zero trust microsegmentation,
- Stateful firewall w/DoS, ALGs
- Logging/telemetry/IPFix
- Turnkey orchestration with HPE Aruba Networking Fabric Composer and HPE Aruba Networking Central

Encryption for hybrid multicloud

Data center/colocation/PoP



- Secure 400G encryption to anywhere
- Site to SIG, site to site or site to cloud, site to branch
- Large scale NAT (500K rules)

Figure 1. HPE Aruba Networking CX 10000 with AMD Pensando

Use case 1: Managed cloud provider secure client onboarding

By integrating the CX 10000 into their cloud hosting architecture, a large global service provider is realizing significant TCO savings (more than 60%) over their incumbent approach for securing client connections from the internet[1], which today uses dedicated hosted virtual firewall VPN clusters to peer with the customer managed firewall in edge sites.

The CX 10000 deployed at the data center interconnect (DCI) role replaces these virtual appliances, allowing multitenant encrypted client connection onboarding utilizing high bandwidth (more than 400G) IPSec VPN encryption tunnels, 800G L4 stateful firewalling capacity, and Network Address Translation (NAT) inline for all traffic ingressing/egressing the cloud availability zone.

The solution provides secure, encrypted multitenant access for customers to their hosted workloads and shared services over the internet, at a significantly lower cost for the provider.

The platform is additionally deployed as the fabric leaf foundation in the data center pods, providing stateful microsegmentation, and NAT for address translation for tenants accessing shared services in the data center.

The architecture is orchestrated using the HPE Aruba Networking suite of products:

HPE Aruba Networking Fabric Composer for the data center and HPE Aruba Networking Central for the campus/WAN fabric.

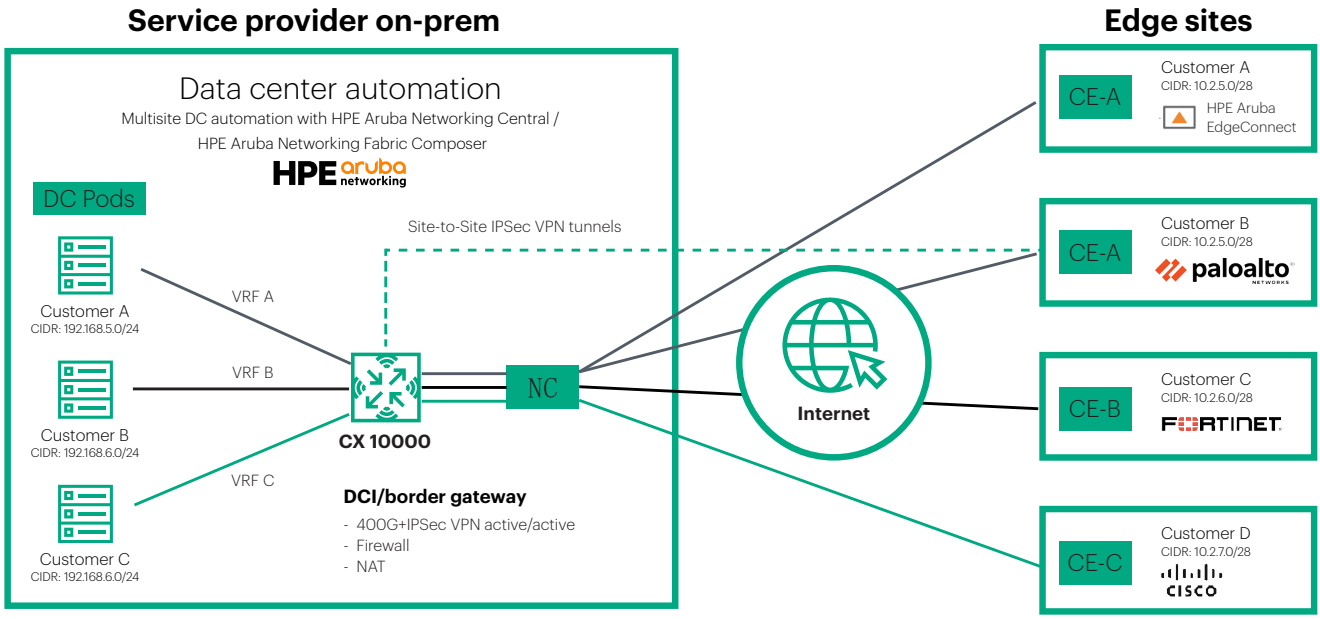


Figure 2. Service provider secure client onboarding

Benefits

— End-to-end encryption to secure sensitive data in flight, between customer and provider

— Native secure and encrypted multitenant infrastructure, with VPN tunnels mapped per customer VRF

— Support for overlapping IPs, to easily onboard new customers even if there are IP addressing scheme conflicts

— Provide stateful zero trust segmentation and isolation between hosted customers, extending all the way to their data center applications.

— Flow and packet level visibility of customer traffic using IPFIX/ERSPAN for SecOps and NetOps teams to address both analytics/threat detection and accelerated diagnosis of network issues

— Easily insert/redirect to next-gen firewalls between customers and their on-prem hosted workloads, for deep packet inspection or IDS/IPS

— Simplified operational model for customers not burdened with complex VPN and NAT configuration

— Per-network QoS mapped to VPN tunnels, helping ensure fair bandwidth allocation across tenant customers

[1] Based on internal HPE analysis.

Use case 2: Secure multicloud networking connectivity

In their quest for agility, flexibility, and TCO optimization, enterprise data center customers are increasingly adopting the flexibility of multicloud to meet their accelerating business demands. The boundaries of data centers are effectively getting erased from geographically large site locations to distributed edge, with hybrid multicloud being the norm. A majority of HPE data center customers are beginning to transition to higher performing network connectivity (100/200/400G).

Customers are challenged with ensuring reliable secure access to hybrid multicloud resources for their applications while also delivering on the TCO required for the business. In an era of tightening CapEx and OpEx budgets, this is specifically where the CX 10000 enables significant value for enterprise customers.

Enterprise financial services cloud on-ramp security

Financial services customers with significant investment in hybrid multicloud architectures have purchased expensive dedicated connectivity to the public cloud using AWS Direct Connect or Azure Private Link 40/100G circuits to ensure reliable performance for critical PAAS applications.

Specifically, some firms use large-scale public cloud VPC/VNet instances for capacity expansion for applications running complex financial modeling simulation jobs in distributed hybrid cloud architectures. These consume vast compute resources but are also highly confidential and have compliance mandates requiring on-prem-to-cloud end-to-end encryption, without impacting job processing times or causing unnecessary latency.

Regulatory compliance is a critical mandate and network infrastructure teams don't want to solely trust application-based TLS; they also want to enforce it end to end at the network infrastructure level using IPSec.

Today this can involve utilizing some variant of a large chassis appliance firewall with the necessary line cards for 100G IPSec VPN, firewalling, and NAT, which are extremely cost prohibitive, complex to manage and have a large blast radius if a node in a cluster has an outage. These are typically deployed in on-prem DMZs where the traffic is back-hauled, which also negatively impacts application latency and performance.

These customers are seeking to deploy the CX 10000 in a distributed services architecture in their regional colocation facilities to secure the cloud on-ramp more effectively and meet their compliance mandates at a significantly reduced CapEx and OpEx cost.

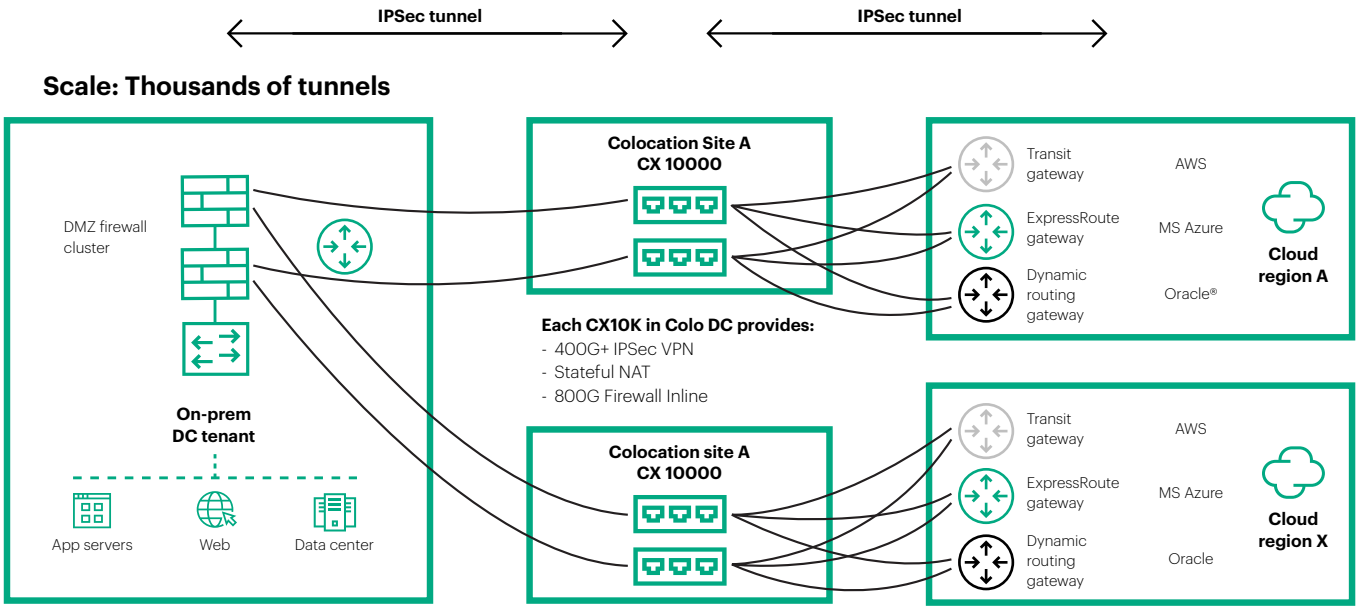


Figure 3. Customer colocation on-ramp encryption to public cloud

Benefits

High performance IPSec encrypted access to cloud VPC/VNet resources:

While some vendors offer MACsec to secure direct access to cloud resources, this exposes data in the clear at every router hop in the datapath, and with a direct connection that ends at the cloud provider peering router.

Using IPSec provides end-to-end encryption with the performance offered with the CX 10000 at more than 400G speeds across thousands of tunnels, provides better security connecting to hybrid multicloud resources than MACsec alone. While MACsec operates at the link layer, with point-to-point encryption, IPSec enables the construction of encrypted IP tunnels that traverse multiple unencrypted hops between router enabling line-rate strong encryption across third party infrastructure for WAN or DCI deployments.

Data remains encrypted even as it travels through third-party routers which customers don't own or control. Packets intercepted or spanned at an intermediate router hop cannot be decrypted as only the IPSec tunnel end devices will have access to the keys, data will be useless to whoever sees it.

Lower cost: High-end firewall appliances and router service modules tend to be built from large numbers of x86 CPUs or network processors (NPUs), which offer limited throughput with high latency in large, expensive, power-hungry form factors. In contrast, the CX 10000 replaces expensive legacy networking appliances and routers by moving these critical services directly into the network at wire speed.

Scale-out security architecture: Easily horizontally scale as bandwidth demands increase, add additional platforms to peer with public cloud transit gateways or VPN, and secure access to additional VNets/VPCs.

Highly available: Distributed architecture, where VPN secured access to VPCs/VNets from colocation is distributed across a fabric of CX 10000 platforms, helps ensure failure domain is much more isolated, compared to routing all traffic through a single point of failure in a firewall appliance chassis cluster.

Optimized performance: Security is closer to cloud on-ramp point, with less back hauling to on-prem DMZs, which improves bandwidth to applications and performance, and allows customers to utilize expensive cloud circuits and resources more effectively.

Overlapping addressing: With hybrid cloud deployments, overlapping, and conflicting IP CIDR ranges is increasingly likely; this is especially true after mergers and acquisitions. NAT on the CX 10000 makes it straightforward to address these complex IP conflict scenarios.

Key capability summary

The multifunctional CX 10000 is typically deployed to offload functions delivered by expensive services and network appliances, such as firewalling and security policy enforcement, VPN tunnel termination, network address translation onto the platform at reduced cost in a variety of network roles for enterprise data center, cloud, and edge deployments.

Security: Comprehensive segmentation and firewall functionality to protect the unprotected in the data center and edge that horizontally scales on-demand:

— Zero trust macro/microsegmentation for any workload, tenant, or device

— Layer 4 stateful firewalling, with DDoS protection and ALG support

— High availability through active/active clustering architecture using state sync with VSX

— DDoS protection against network infrastructure level (Layer 3 and 4) TCP/UDP attacks using session limits, alerting, and policing

— Dynamic workload groups with orchestrator integration, to simplify policy provisioning.

IPSec encryption: End to end for site to site and site to cloud

— High bandwidth: more than 400G of IPSec VPN throughput

— Interoperable: Encrypt to any standards compliant IKEv2 capable IPSec VPN router, firewall or cloud

VPN gateway

— Multitenant: Native inbuilt using network VRF constructs tied to VPN tunnels

— High availability: Flexible models for IPSec HA, using either BGP over active-active tunnel, or active/standby tunnel failover

— Large scale: Support for thousands of tunnel peering connections to cloud or site VPNs.

NAT: Stateful NAT for dual stack IPv4/IPv6 deployments

— Large scale: Up to 250K NAT translation rules

— Standard functionality: As offered by firewall appliances or routing platforms.

TCO analysis and assumptions

Comparison includes the cost of deploying/supporting 400G of IPSec VPN encryption and NAT connecting three remote locations, with 1000 tunnels per site over three years. Configuration includes two firewall/VPN appliances or two CX 10000 per site for redundancy. Pricing includes all hardware and software licensing cost and three-year support discounted at 70% off MSRP.

The HPE Aruba Networking CX 10000 provides dramatically lower total cost of ownership (~89%)[2] vs. a design configured with a traditional next-generation firewall/VPN appliances.

Results

Next-gen firewall/VPN appliance 400G site-to-site IPSec VPN design

$1407M
Total 3-year costs

$3518
Average cost per Gbps of IPSec encryption

HPE Aruba Networking CX 10000 400G site-to-site IPSec VPN design

$149,148
Total 3-year costs

$372
Average cost per Gbps of IPSec encryption

$1258M

Table 1. HPE Aruba Networking CX 10000 ordering information

Product SKU	Description
R8P13A	R8P13A 10000-48Y6C Front-to-Back switch bundle
R8P14A	R8P14A 10000-48Y6C Back-to-Front switch bundle
R9H25AAE	R9H25AAE HPE Aruba Networking CX 10000 Advanced Services E-LTU: (Firewall, Segmentation, DDoS protection, telemetry)
R9H26AAE[3]	HPE Aruba Networking Premium Svcs for CX 10000 Premium Services E-LTU (IPSec Encryption/NAT/ Advanced DDoS protection)

[2] TCO analysis is based on hypothetical examples, using specific industry assumptions. Individual customer configurations will vary based on specific designs and configurations.

[3] Note purchasing Premier services package, additionally provides entitlement to all functionality included in Advanced tier I license.

Learn more at

HPE.com/us/en/aruba-networking-cx-10000-switch-series.html

Visit HPE.com

Chat now

a00129289ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com