



HPE aruba
networking

Crittografia pervasiva e sicurezza dall'edge al cloud con gli switch per servizi distribuiti HPE Aruba Networking CX 10000

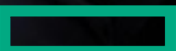
Drastica riduzione del TCO, semplificazione delle operazioni
e aumento delle prestazioni

HPE 
GreenLake



Sommario

- 3 **Introduzione**
- 3 **Fabric di nuova generazione per data center e distribuzioni all'edge**
- 4 **Caso d'uso 1: onboarding sicuro dei client per provider di cloud gestito**
- 5 **Caso d'uso 2: connettività di rete multicloud sicura**
- 7 **Riepilogo delle funzionalità chiave**



Introduzione

Le architetture tecnologiche sono in costante evoluzione, ma raramente assistiamo a uno sviluppo importante che ridefinisce l'architettura della moderna rete aziendale. Oggi viviamo nell'era dei dati, come sostengono molti esperti di tecnologia e analisti del settore: non si tratta però di dati generati nel cloud o nel data center, ma piuttosto di dati creati nel luogo più indicato per ragioni di prestazioni delle applicazioni, latenza o data gravity, ovvero l'edge, dove interagiscono utenti, dispositivi e applicazioni.

Gartner da molti anni prevede che la maggior parte dei dati generati dalle aziende sarà creata ed elaborata all'esterno di un data center o di un cloud tradizionale.

È essenziale che la rete distribuita all'edge sia in grado di soddisfare i requisiti mission-critical in termini di disponibilità, scalabilità e sicurezza definiti dai clienti per le architetture multicloud ibride, che vanno ben oltre la garanzia di una connettività affidabile da sito a sito e da sito a cloud.

Fabric di nuova generazione per data center e distribuzioni all'edge

HPE Aruba Networking CX 10000 with AMD Pensando™ ha introdotto una categoria con caratteristiche esclusive, particolarmente adatte per affrontare una serie diversificata di casi d'uso complessi tra data center, edge e cloud. Sono incluse funzioni generalmente fornite da appliance di servizi di livello enterprise e opzioni di rete essenziali, le migliori della categoria, supportate dalla piattaforma HPE Aruba Networking AOS-CX. In questa presentazione della soluzione, analizzeremo le funzionalità esclusive offerte dall'architettura di servizi distribuiti HPE Aruba Networking CX 10000 per la sicurezza del cloud e all'edge.

Il documento descriverà in dettaglio numerosi casi d'uso di connettività multicloud, edge e in colocation che evidenziano i vantaggi in tema di sicurezza e TCO della soluzione leader di mercato HPE Aruba Networking CX10000.

Funzionalità principali di HPE Aruba Networking CX 10000

HPE aruba
networking



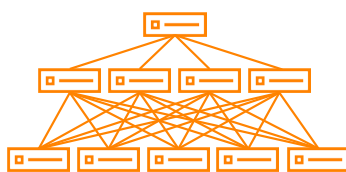
Servizi software stateful L4

- Firewall
- DDoS
- Telemetria
- NAT
- Crittografia

Sicurezza nativa nel data center



Data center



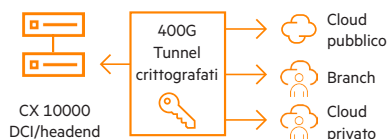
Leaf DC CX10000

- Microsegmentazione zero trust
- Firewall stateful con DoS, ALG
- Registrazione/telemetria/IPFix
- Orchestrazione chiavi in mano con HPE Aruba Networking Fabric Composer e HPE Aruba Networking Central

Crittografia per multicloud ibrido L4



Data center/colocation/PoP



- Crittografia 400G sicura ovunque
- Da sito a SIG, da sito a sito o da sito a cloud, da sito a filiale
- NAT su vasta scala (500.000 regole)

Figura 1. HPE Aruba Networking CX 10000 with AMD Pensando



Caso d'uso 1: onboarding sicuro dei client per provider di cloud gestito

Integrando CX 10000 nella propria architettura in hosting nel cloud, un grande service provider di livello globale registra significativi risparmi in termini di TCO (oltre il 60%) rispetto all'approccio in uso per la protezione delle connessioni dei client da Internet¹, che oggi sfrutta cluster VPN dedicati con firewall virtuali in hosting per il peering con il firewall gestito dal cliente nelle sedi all'edge.

Il sistema CX 10000 distribuito nel ruolo DCI (Data Center Interconnect) sostituisce queste appliance virtuali, consentendo l'onboarding di connessioni client crittografate multitenant che utilizzano tunnel di crittografia IPsec VPN a elevata larghezza di banda (oltre 400G), capacità di firewall stateful L4 da 800G e Network Address Translation (NAT) in linea per tutto il traffico in ingresso/uscita dalla zona di disponibilità del cloud.

La soluzione garantisce ai clienti un accesso multitenant sicuro e crittografato ai carichi di lavoro in hosting e ai servizi condivisi su Internet, a un costo nettamente inferiore per il provider.

La piattaforma viene inoltre distribuita come base leaf del fabric in data center con prestazioni ottimizzate, fornendo microsegmentazione stateful e NAT per la conversione degli indirizzi per i tenant che accedono ai servizi condivisi nel data center.

L'orchestrazione dell'architettura viene eseguita tramite la suite di prodotti HPE Aruba Networking:

HPE Aruba Networking Fabric Composer per il data center e HPE Aruba Networking Central per il fabric di campus/WAN.

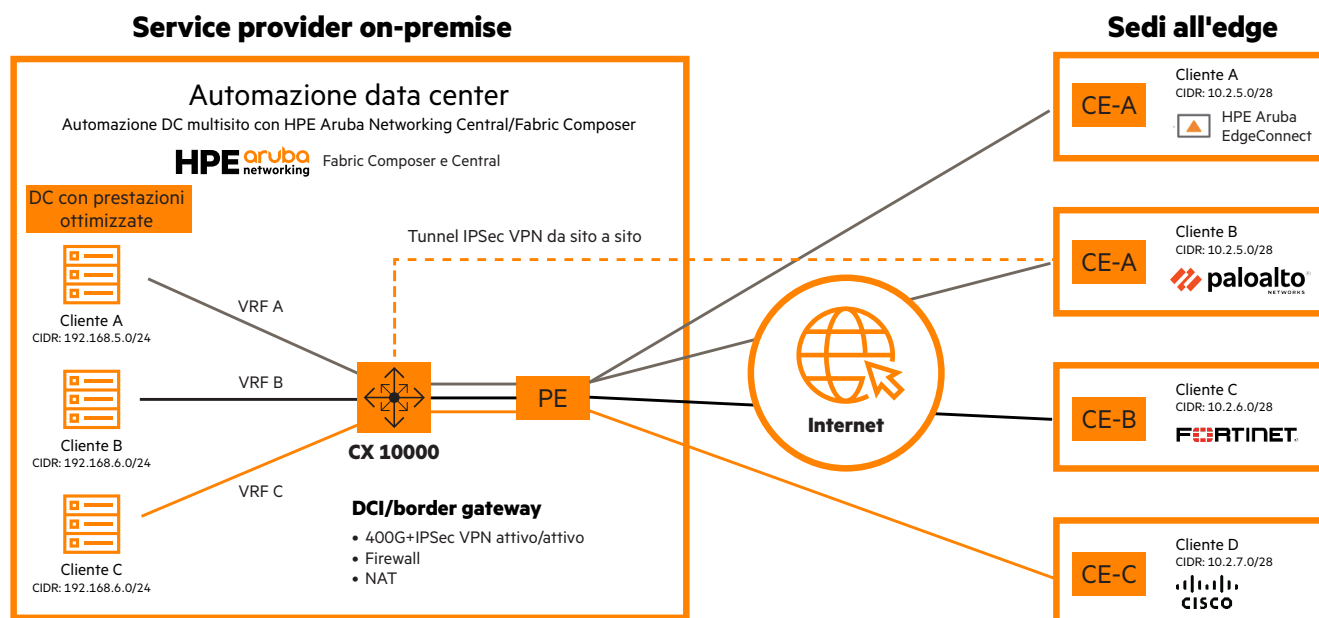


Figura 2. Onboarding sicuro dei client per service provider

Vantaggi

- Crittografia end-to-end per la protezione dei dati sensibili in transito, tra cliente e provider
- Infrastruttura multitenant nativa sicura e crittografata, con tunnel VPN mappati per ogni VRF del cliente
- Supporto di IP sovrapposti, per facilitare l'onboarding di nuovi clienti anche in caso di conflitti tra gli schemi di creazione degli indirizzi IP
- Segmentazione zero trust e isolamento stateful tra i clienti in hosting, estesi fino alle applicazioni del data center
- Visibilità a livello di flusso e di pacchetto del traffico dei clienti mediante IPFIX/ERSPAN per permettere ai team SecOps e NetOps di gestire l'analisi/il rilevamento delle minacce e la diagnosi accelerata dei problemi di rete
- Facile inserimento/reindirizzamento a firewall di nuova generazione tra i clienti e i loro carichi di lavoro in hosting on-premise, per l'ispezione approfondita dei pacchetti o IDS/IPS
- Modello operativo semplificato per i clienti che non devono sostenere il peso di complesse configurazioni VPN e NAT
- QoS per singola rete mappata ai tunnel VPN, per contribuire a garantire un'allocazione equa della larghezza di banda tra i clienti tenant

¹ In base ad analisi interne di HPE.



Caso d'uso 2: connettività di rete multicloud sicura

Nella costante ricerca di agilità, flessibilità e ottimizzazione del TCO, i clienti dei data center aziendali adottano sempre più spesso la flessibilità del multicloud per rispondere alle loro esigenze di business in crescita. I confini dei data center si stanno di fatto dissolvendo, con il passaggio da sedi geograficamente estese a edge distribuiti e con il multicloud ibrido che diventa la norma. La maggior parte dei clienti dei data center HPE sta avviando la transizione a una connettività di rete con prestazioni superiori (100/200/400G).

I clienti devono affrontare due problematiche: garantire un accesso sicuro e affidabile alle risorse multicloud ibride per le loro applicazioni e rispettare contemporaneamente il TCO richiesto per l'azienda. In un'epoca di budget CapEx e OpEx sempre più limitati, è proprio in questo ambito che CX 10000 assicura un valore significativo per i clienti aziendali.

Sicurezza del cloud on-ramp dei servizi finanziari aziendali

I clienti dei servizi finanziari che hanno effettuato investimenti significativi in architetture multicloud ibride hanno acquistato costose opzioni di connettività dedicata al cloud pubblico tramite circuiti 40/100G AWS Direct Connect o Azure Private Link per garantire prestazioni affidabili delle applicazioni PAAS essenziali.

In particolare, alcune aziende utilizzano istanze VPC/VNet di cloud pubblico su larga scala per espandere la capacità delle applicazioni che eseguono simulazioni di complessi modelli finanziari in architetture di cloud ibrido distribuite. Queste applicazioni consumano grandi quantità di risorse di elaborazione, ma sono anche estremamente riservate e presentano imperativi di compliance che prevedono la crittografia end-to-end da on-premise a cloud, senza influire sulle tempistiche di elaborazione dei progetti o causare inutili casi di latenza.

La compliance normativa è un requisito fondamentale e i team dell'infrastruttura di rete preferiscono non fidarsi solo del protocollo TLS basato sulle applicazioni, ma vogliono anche applicarlo end-to-end a livello di infrastruttura di rete utilizzando IPSec.

Oggi tutto questo può comportare l'impiego di una variante di un firewall di appliance con chassis di grandi dimensioni e le necessarie schede di linea per IPSec VPN 100G, firewalling e NAT, soluzioni proibitive dal punto di vista dei costi, complesse da gestire e con un ampio raggio d'azione in caso di interruzione di un nodo in un cluster. In genere vengono distribuite in DMZ on-premise dove viene eseguito il backhaul del traffico, con un impatto negativo sulla latenza e le prestazioni delle applicazioni.

Questi clienti desiderano distribuire CX 10000 in un'architettura di servizi distribuiti nelle loro strutture in colocation regionali per proteggere il cloud on-ramp in modo più efficace e soddisfare gli obblighi di compliance a un costo CapEx e OpEx nettamente inferiore.

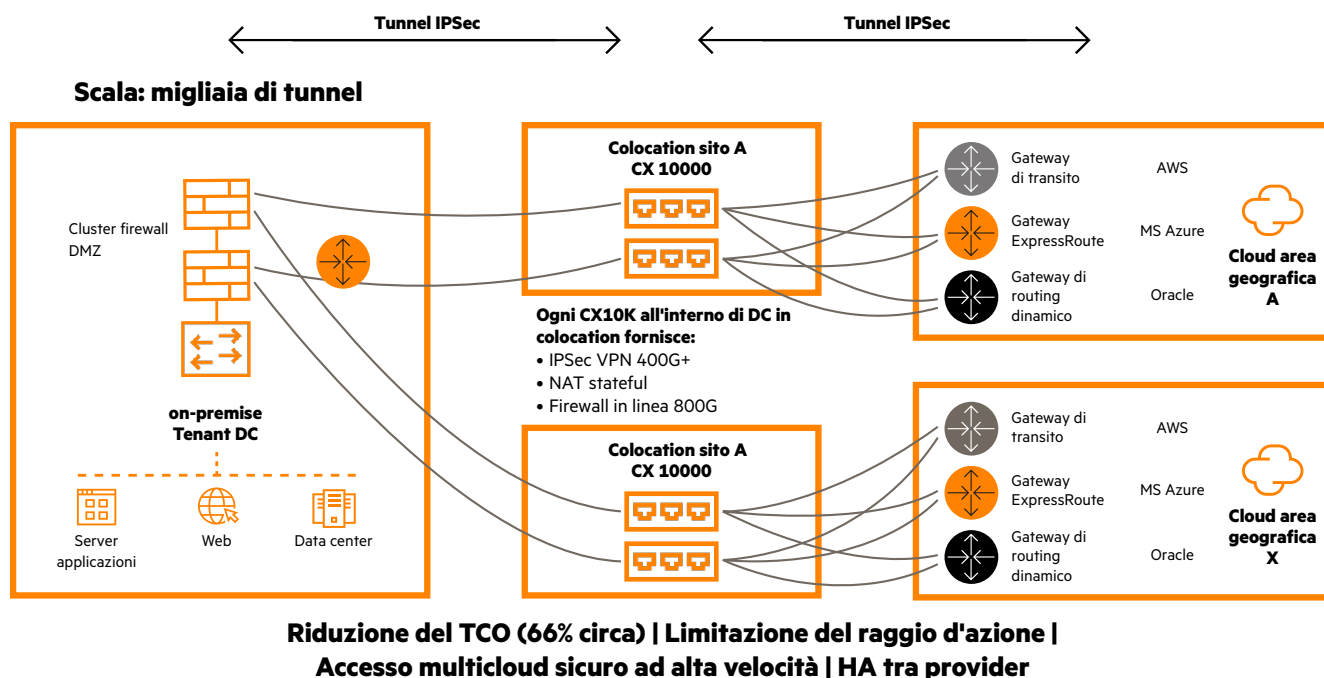


Figura 3. Crittografia on-ramp delle strutture in colocation del cliente verso il cloud pubblico





Vantaggi

Accesso crittografato IPSec ad alte prestazioni alle risorse VPC/VNet nel cloud:

sebbene alcuni fornitori offrano MACsec per proteggere l'accesso diretto alle risorse cloud, questo espone i dati in chiaro a ogni hop di router nel percorso dati e con una connessione diretta che termina al router di peering del provider cloud.

L'utilizzo di IPSec fornisce crittografia end-to-end con le prestazioni offerte da CX 10000 a velocità superiori a 400G su migliaia di tunnel, garantendo una maggiore sicurezza nella connessione a risorse multicloud ibride rispetto al solo standard MACsec. Mentre quest'ultimo opera a livello di link, con una crittografia da punto a punto, IPSec consente di realizzare tunnel IP crittografati che attraversano più hop non crittografati tra router, abilitando una solida crittografia a velocità di linea all'interno di infrastrutture di terzi per le distribuzioni WAN o DCI.

I dati rimangono crittografati anche quando transitano attraverso router di terzi che i clienti non possiedono né controllano. I pacchetti intercettati o diffusi in un hop di router intermedio non possono essere decrittografati, poiché solo i dispositivi finali del tunnel IPSec avranno accesso alle chiavi, quindi i dati saranno inutilizzabili per chiunque li visualizzi.

Costi ridotti: tendenzialmente le appliance firewall di fascia alta e i moduli di servizio per router vengono realizzati con un elevato numero di CPU x86 o processori di rete (NPU), che offrono un throughput limitato con un'alta latenza in fattori di forma di grandi dimensioni, costosi e a elevati consumi energetici. Al contrario, CX 10000 sostituisce le costose appliance di rete e i router legacy, trasferendo questi servizi essenziali direttamente nella rete con prestazioni wire-speed.

Architettura di sicurezza a scalabilità orizzontale: è possibile scalare orizzontalmente seguendo l'aumento delle richieste di larghezza di banda, aggiungere ulteriori piattaforme per il peering con gateway di transito del cloud pubblico o VPN e proteggere l'accesso a ulteriori VNet/VPC.

Alta disponibilità: l'architettura distribuita, in cui l'accesso protetto da VPN a VPC/VNet dalla struttura di colocation è distribuito su un fabric di piattaforme CX 10000, contribuisce a garantire un dominio di guasto molto più isolato, rispetto all'instradamento di tutto il traffico attraverso un singolo punto di guasto in un cluster di chassis di appliance firewall.

Prestazioni ottimizzate: la sicurezza è più vicina al punto di connessione diretta al cloud, con meno backhauling verso le DMZ on-premise; questo migliora la larghezza di banda per le applicazioni e le prestazioni e permette ai clienti di utilizzare in modo più efficace i costosi circuiti e le risorse cloud.

Creazione di indirizzi sovrapposti: con le distribuzioni di cloud ibrido, è sempre più probabile che si verifichi la sovrapposizione e il conflitto degli intervalli IP CIDR, soprattutto dopo fusioni e acquisizioni. La tecnica NAT su CX 10000 consente di affrontare con semplicità questi complessi scenari di conflitti IP.



Riepilogo delle funzionalità chiave

Gli switch CX 10000 vengono in genere distribuiti per l'offloading di funzioni fornite da costosi servizi e appliance di rete, come firewall e applicazione di policy di sicurezza, terminazione dei tunnel VPN e NAT sulla piattaforma, a un costo ridotto, in un'ampia gamma di ruoli di rete per data center aziendali, cloud, e distribuzioni all'edge.

Sicurezza: funzionalità complete di segmentazione e firewall per proteggere gli elementi non protetti nel data center e all'edge, con scalabilità orizzontale on demand:

- macro/microsegmentazione Zero Trust per qualsiasi carico di lavoro, tenant o dispositivo
- firewalling stateful di livello 4, con protezione DDoS e supporto ALG
- elevata disponibilità grazie all'architettura di clustering attivo/attivo che utilizza la sincronizzazione di stato con VSX
- protezione DDoS contro gli attacchi TCP/UDP a livello di infrastruttura di rete (livello 3 e 4) tramite limiti di sessione, avvisi e policing
- gruppi dinamici di carichi di lavoro con integrazione dell'orchestrator, per semplificare il provisioning delle policy.

Crittografia IPsec: end-to-end per il collegamento da sito a sito e da sito a cloud

- Elevata larghezza di banda: più di 400G di throughput VPN IPsec
- Interoperabilità: crittografia verso qualsiasi router, firewall o cloud IPsec VPN compatibile con IKEv2 e conforme agli standard

Gateway VPN:

- multitenant: integrazione nativa tramite costrutti VRF di rete legati ai tunnel VPN
- elevata disponibilità: modelli flessibili per IPsec HA, attraverso BGP su tunnel attivo/attivo o failover di tunnel attivo/standby
- vasta scala: supporto per migliaia di connessioni di peering tunnel verso cloud o VPN di siti.

NAT: NAT stateful per distribuzioni IPv4/IPv6 dual stack

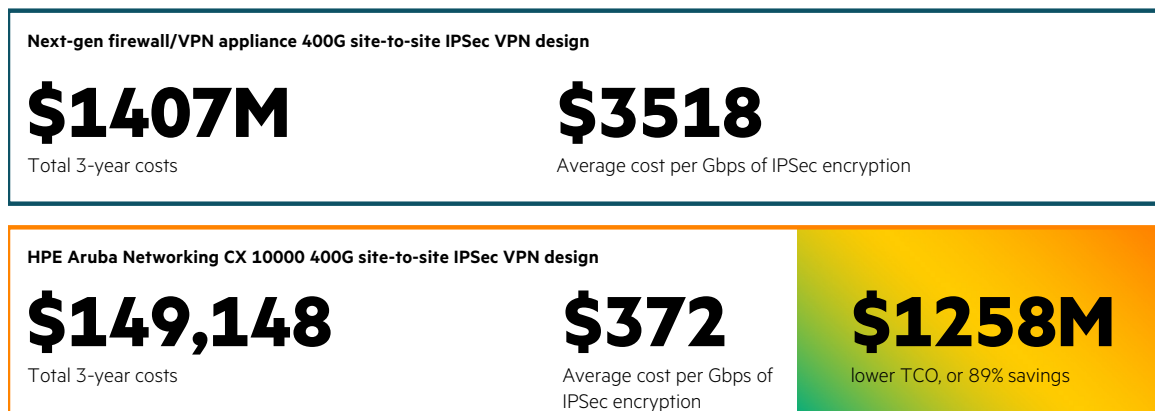
- Vasta scala: fino a 250.000 regole di conversione NAT
- Funzionalità standard: come quelle offerte da appliance firewall o piattaforme di instradamento.

Analisi del TCO e ipotesi

Il confronto include il costo di distribuzione/supporto di 400G di crittografia IPsec VPN e NAT per il collegamento di tre sedi remote, con 1.000 tunnel per sito in tre anni. La configurazione comprende due appliance firewall/VPN o due switch CX 10000 in ogni sito per ridondanza. Il prezzo include tutti i costi di licenza hardware e software e il supporto triennale scontato del 70% rispetto al prezzo di vendita al dettaglio suggerito.

HPE Aruba Networking CX 10000 assicura una drastica riduzione del TCO (89% circa)² rispetto a una tradizionale architettura configurata con appliance firewall/VPN di nuova generazione.

Results



² Le analisi del TCO precedenti sono basate su esempi ipotetici, con presupposti specifici del settore. Le configurazioni dei singoli clienti varieranno in base ad architetture e configurazioni specifiche.



Tabella 1. Informazioni per gli ordini di HPE Aruba Networking CX 10000

SKU prodotto	Descrizione
R8P13A	R8P13A bundle switch da fronte a retro 10000-48Y6C
R8P14A	R8P14A bundle switch da fronte a retro 10000-48Y6C
R9H25AAE	R9H25AAE licenza elettronica HPE Aruba Networking CX 10000 Advanced Services: (firewall, segmentazione, protezione DDoS, telemetria)
R9H26AAE ³	Licenza elettronica HPE Aruba Networking Premium Svcs per CX 10000 Premium Services (crittografia IPSec/NAT/protezione DDoS avanzata)

Ulteriori informazioni alla pagina

ArubaNetworks.com/products/switches/distributed-services-switches

³ L'acquisto di un pacchetto di servizi Premier dà anche diritto a tutte le funzionalità incluse nella licenza Advanced livello I.

**Prendi la decisione d'acquisto giusta.
Contatta i nostri specialisti della prevendita.**

Visita HPE.com



Contattaci

**Hewlett Packard
Enterprise**

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i servizi e i prodotti Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni ed errori tecnici o editoriali contenuti nel presente documento.

AMD è un marchio di Advanced Micro Devices, Inc. Oracle è un marchio registrato di Oracle e/o delle sue affiliate. Azure è un marchio o un marchio registrato di Microsoft Corporation negli Stati Uniti e/o in altri paesi. Tutti i marchi di terzi appartengono ai rispettivi titolari.
a00129289ITE