CLOUDFLARE

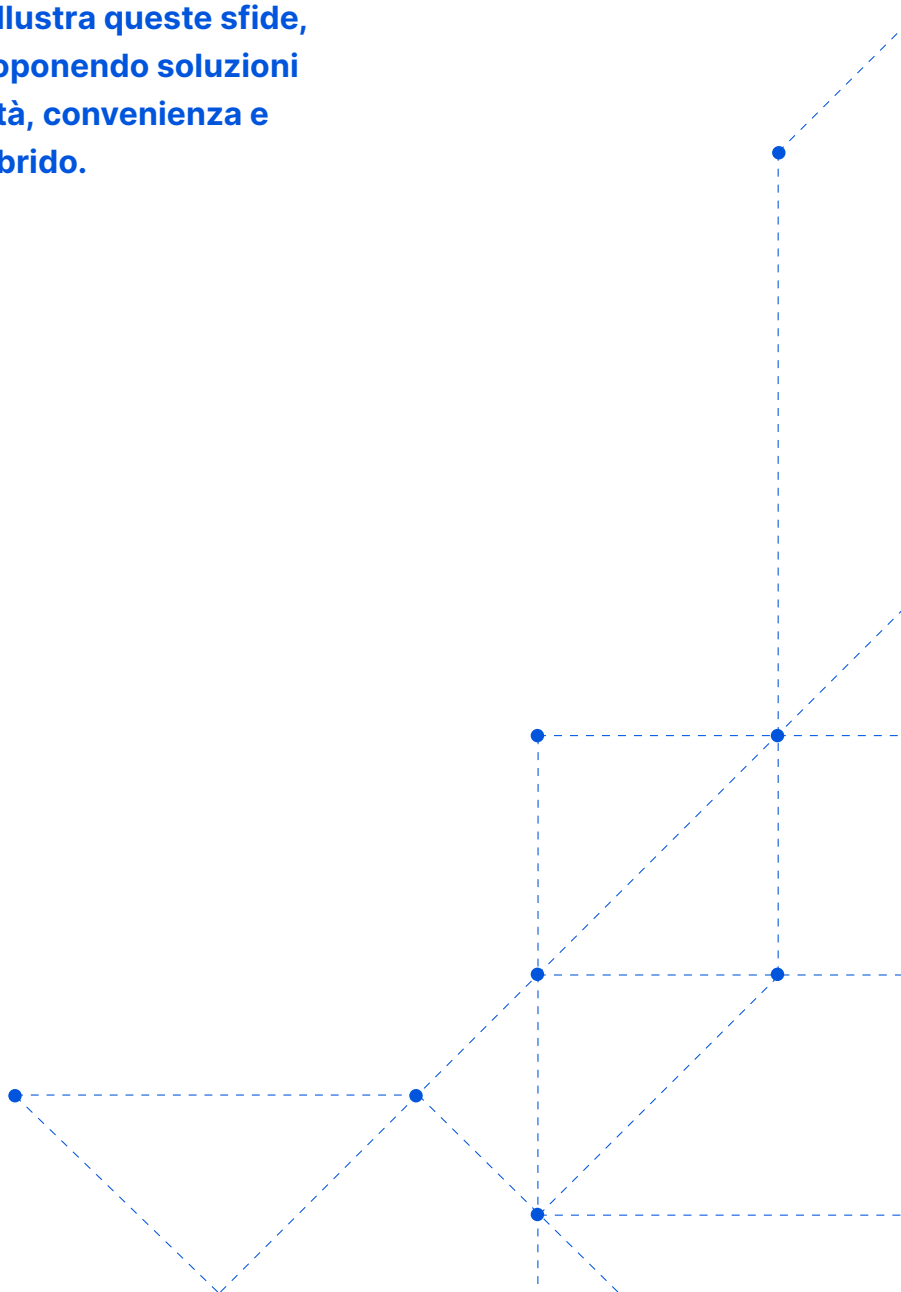
WHITEPAPER

La Scomparsa Delle Appliance Hardware di Rete

Perché è giunto il momento di liberarsi dall'hardware di rete

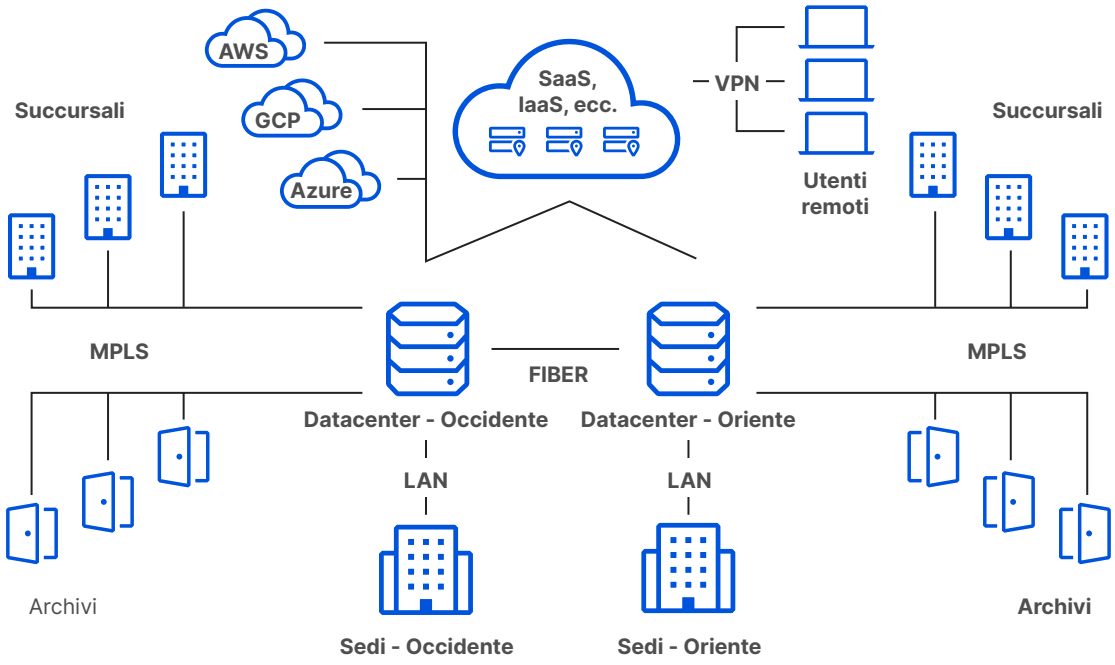
Riepilogo

Sebbene l'archiviazione e l'elaborazione siano passate al cloud, molte funzioni di rete rimangono on-premise, generando limitazioni di capacità, costi totali di proprietà elevati, problemi di supporto e lacune nella sicurezza. Le organizzazioni stanno lottando per garantire capacità adeguate e sicurezza effettiva con il lavoro ibrido che sta diventando la norma. Molti progetti di trasformazione si sono bloccati a causa di arretrati hardware in esecuzione da oltre un anno. Questo documento illustra queste sfide, quantificandone le conseguenze e proponendo soluzioni basate sul cloud per migliorare velocità, convenienza e sicurezza dell'infrastruttura di cloud ibrido.



Introduzione

La migrazione al cloud si è dimostrata una strategia efficace per ridurre i costi dell'infrastruttura, migliorare la disponibilità di dati e applicazioni e incrementare l'agilità operativa. Tuttavia, tale migrazione di rado si verifica in un colpo solo. Molte grandi organizzazioni si ritrovano oggi con una complessa combinazione di infrastruttura multi-cloud e on-premise.



Tale infrastruttura ibrida non è necessariamente negativa in sé, ma presenta delle complicazioni. In particolare, crea situazioni in cui diverse funzioni di rete, quali la mitigazione dei DDoS, il bilanciamento di carico, il firewall e la VPN, rimangono on-premise.

Le apparecchiature hardware di rete legacy non sono all'altezza del compito di proteggere e accelerare l'infrastruttura critica in un mondo incentrato sul cloud. Da sempre sono una seccatura: un groviglio costoso, e spesso indisciplinato, di attrezzature e ragOnce you add the cloud to the picture, security gaps, performance penalties, and additional support challenges quickly emerge.natele di cavi messe insieme. Dopo aver aggiunto il cloud all'immagine, emergono rapidamente lacune di sicurezza, riduzione delle prestazioni e altri problemi di supporto.

Questo documento descrive i rischi e le insidie della manutenzione dell'hardware di rete in un mondo che sta passando al cloud e offre strategie per costruire una rete più sicura ed efficace.

I rischi dell'hardware in un mondo cloud

Le apparecchiature hardware di rete riuniscono una varietà di funzioni specifiche e vengono utilizzate in modo alquanto diverso da un'organizzazione all'altra.

Alcuni esempi comuni:

Sicurezza

- Protezione da attacchi DDoS
- Firewall
- Rete privata virtuale (VPN)
- Criteri configurabili

Prestazioni e affidabilità

- Bilanciamento di carico
- Accelerazione del traffico/ Ottimizzazione della WAN
- Filtro dei pacchetti
- Analisi del traffico

Quando questo hardware viene distribuito in sede, l'architettura risultante presenta generalmente cinque categorie di rischi: **stress della supply chain, limiti di capacità, costo totale di proprietà elevato, problemi di supporto** e **lacune nella sicurezza.**

Le prime tre categorie hanno sempre creato problemi anche ai team di sicurezza e di rete più sofisticati. Gli altri due sono esacerbati dalla migrazione al cloud.

Stress della supply chain

Come qualsiasi tipo di prodotto fisico, l'hardware di rete è vulnerabile a una serie di difficoltà della supply chain. Quando i costi dei materiali aumentano, alcuni materiali e componenti sono più difficili da ottenere o i fornitori di servizi di spedizione sono sovraccarichi, l'hardware di rete diventa più difficile da acquistare e sostituire.

Purtroppo, tali difficoltà sono state comuni negli ultimi tempi, in gran parte a causa degli effetti della pandemia di Covid-19. Secondo la Gartner Research, "i tempi di consegna pre-pandemia di 4-6 settimane erano la norma. Ora, si arriva a 200-300 giorni, fino anche a più di 430 giorni riportati dai clienti".

Questi ritardi derivano da molteplici fattori:

- **Difficoltà logistiche:** i modelli storici della supply chain hanno molteplici punti di errore, forza lavoro minima e una forte dipendenza da tecnologie che possono essere o meno sicure, problemi che di recente sono arrivati anche qui. Durante la pandemia, molte fabbriche hanno chiuso, le società di spedizione hanno iniziato a subire ritardi e molti tipi di lavoratori della supply chain sono diventati più difficili da assumere e mantenere. Tutti questi problemi richiedono più tempo per la produzione e la consegna dell'hardware. Forse l'aspetto più impegnativo da ricordare di qualsiasi logistica è che è paragonabile a una staffetta: solo perché la tua organizzazione individuale potrebbe non avere problemi non significa che non sarai influenzato da un anello interrotto più a monte della catena.
- **Costi dei materiali più alti:** le apparecchiature hardware di rete si basano su una varietà di materie prime. A causa dell'elevata domanda e dell'offerta limitata, i prezzi dei materiali sono saliti alle stelle, il che significa che non solo le aziende aspettano più a lungo per ottenere ciò di cui hanno bisogno per la loro rete, ma lo pagano anche molto di più. Sfortunatamente, a causa di questi problemi, Gartner prevede che i tempi di consegna delle apparecchiature hardware rimarranno elevati fino all'inizio del 2023 (fonte).

Tutti questi problemi hanno delle conseguenze. Continuare a concentrarsi sull'acquisto, la manutenzione e la sostituzione di hardware significa maggiori costi generali, più tempo dedicato alla pianificazione piuttosto che all'esecuzione e maggiori problemi di sicurezza relativi alla protezione di una supply chain fisica durante periodi di incertezza. Invece di concentrarsi su logistica, tempi di consegna, approvvigionamento e stoccaggio di hardware, le organizzazioni potrebbero invece concentrarsi sulla soddisfazione delle esigenze dei propri clienti.

Limitazioni di capacità

Non dovrebbe sorprendere che, per loro stessa natura, gli apparecchi hardware di rete possano sovraccaricarsi durante imprevisti sbalzi di traffico, a prescindere dal fatto che il traffico sia legittimo o meno. Ma recentemente diverse tendenze indicano che il raggiungimento di questi limiti è una preoccupazione condivisa.

Prendi in considerazione la mitigazione DDoS (Distributed Denial of Service). Il più grande attacco DDoS della storia è avvenuto nel novembre del 2021, secondo Microsoft, e si dice che abbia raggiunto un volume massimo di 3,47 Tbps (fonte). Gli attacchi DDoS sovraccaricano molte volte l'hardware di mitigazione DDoS più avanzato sul mercato, che in genere fornisce una frazione della capacità richiesta per mitigare tali attacchi.

Nel novembre del 2021, si dice che il più grande attacco DDoS della storia abbia raggiunto un volume massimo di 3,47 Tbps.

Non tutte le organizzazioni attireranno attacchi di tale portata — ma non tutte le organizzazioni possono implementare o implementano l'hardware di mitigazione DDoS più avanzato. Un rapporto di Cloudflare ha rilevato che gli attacchi volumetrici sono aumentati nel primo trimestre del 2022. Infatti, gli attacchi superiori a 10 Mpps (milioni di pacchetti al secondo) sono cresciuti di oltre il 300% su base trimestrale e gli attacchi oltre i 100 Gbps sono cresciuti del 645% su base trimestrale (fonte). Non solo il forte aumento degli attacchi DDoS è allarmante, ma questi tipi di attacchi sovraccaricano molte soluzioni di mitigazione basate su hardware presumibilmente ad alta capacità.

Inoltre, il volume di attacco non tiene conto del traffico legittimo che potrebbe raggiungere contemporaneamente il tuo datacenter.

Se dovesse arrivare un attacco minore durante un periodo di traffico intenso, come il weekend dello shopping del Black Friday, quando le visualizzazioni di pagina giornaliere dell'e-commerce raddoppiano in media durante la notte (fonte), il conseguente aumento del traffico potrebbe essere ancora sufficiente per spingere l'hardware di sicurezza oltre il suo punto di rottura.

La mitigazione degli attacchi DDoS è solo un esempio delle limitazioni di capacità dell'hardware on-premise.

Altri esempi:

Bilanciatori di carico: i singoli bilanciatori di carico on-premise possono essere facilmente sovraccaricati da picchi improvvisi di traffico legittimo. In questo caso, il provisioning e l'installazione di hardware aggiuntivo può richiedere molto tempo. L'alternativa consiste nel mantenere una capacità sufficiente per lo scenario peggiore, ma questo approccio richiede all'organizzazione di eseguire continuamente molti dispositivi hardware a un costo elevato.

Virtual Private Network (VPN): l'uso delle VPN è diventato molto più difficile da prevedere in anticipo. Per molte organizzazioni, il lavoro completamente remoto e ibrido è la nuova normalità, ma l'approccio VPN tradizionale richiede un'attenta pianificazione, manutenzione e gestione, poiché molte VPN non sono state progettate per l'uso continuo da parte di un'intera organizzazione. Quando troppi dipendenti utilizzano una VPN, la connettività e l'affidabilità ne risentono. Inoltre, possono emergere problemi di sicurezza, proprio per la natura di come sono state progettate le VPN senza alcun controllo Zero Trust. Inoltre, se una VPN viene sovraccaricata, le organizzazioni possono "dividere in tunnel" il traffico in modo che il traffico verso il Web non passi attraverso la VPN, il che rende difficile tracciare e gestire l'attività Web dei dipendenti.

Di fronte a questi problemi, una risposta può essere quella di acquistare hardware più recenti e con maggiore capacità. Questo approccio, tuttavia, introduce tutta una serie di altri problemi.

Costi di proprietà

Come nel caso delle limitazioni di capacità, non dovrebbe sorprendere che l'hardware del datacenter abbia un costo elevato. Ad esempio, l'hardware necessario per raggiungere circa 100 Gbps di capacità di mitigazione DDoS potrebbe costare tra i 400.000 e i 500.000 dollari.

In aggiunta, questi costi sono solo una parte del costo totale di proprietà di un apparecchio hardware.

Si considerino le seguenti spese:

- Costi dei team: l'acquisto, la gestione e la manutenzione dell'hardware per difendersi dalle minacce a ogni livello del modello OSI, e per fornire il livello di prestazioni e affidabilità attesi dai siti web moderni e dalle applicazioni Internet, richiedono membri del team esperti in ognuna di queste funzioni di rete. Costruire una squadra con questa ampiezza e profondità di competenze è una proposta costosa, specialmente durante uno dei mercati del lavoro più ristretti che il mondo abbia mai visto. Un sondaggio ISACA del 2022 ha rilevato che su 2.000 professionisti della sicurezza informatica che hanno partecipato al sondaggio annuale, il 63% ha posizioni di sicurezza informatica non occupate, in aumento dell'8% rispetto all'anno precedente (fonte).
- Costi di manutenzione: l'hardware di rete locale medio ha una durata di conservazione compresa tra 3 e 5 anni, tuttavia le garanzie per quegli interi periodi spesso richiedono spese aggiuntive. Se si tiene conto del ritmo dell'innovazione tecnologica, è inevitabile che queste scatole on-premise continueranno a ridursi nella durata. L'alternativa sono le riparazioni inaspettate, e quindi senza budget, dal produttore originale o da terzi. I malfunzionamenti dell'hardware possono anche causare tempi di inattività del datacenter, che hanno un costo opportunità medio di oltre $ 8.800 al minuto (fonte).
- Costi di sostituzione: la sostituzione di un dispositivo hardware ogni tre anni richiede alle organizzazioni non solo di pagare nuovamente l'investimento iniziale, ma di dedicare risorse alla spedizione e all'installazione del nuovo hardware. Il ritardo nelle sostituzioni comporta spesso malfunzionamenti più frequenti e, di conseguenza, costi di manutenzione aggiuntivi.

Si confronti questo modello con i servizi di rete forniti dal cloud. Questi sono attrezzati per operare con un team più agile, non hanno costi di manutenzione e spedizione, e non costringono le organizzazioni a scegliere tra costosi aggiornamenti e un aumento dei malfunzionamenti.

I malfunzionamenti dell'hardware possono causare tempi di inattività del datacenter con un costo opportunità medio di oltre 8.800 dollari al minuto.

Problemi di supporto

Il supporto per le apparecchiature hardware di rete non solo è una proposta costosa, ma rappresenta anche una sfida in termini di logistica. L'hardware richiede frequenti patch per rimanere al passo con le ultime vulnerabilità e tattiche di attacco, processo che spesso si basa sull'implementazione manuale, e quindi soggetto a errore umano.

Più dispositivi hardware utilizzano un'organizzazione, maggiori sono le possibilità che alla fine si trascuri una patch a causa della disattenzione o delle preoccupazioni sull'influenza dei sistemi vitali. In una recente consulenza congiunta sulla sicurezza informatica, la National Security Agency (NSA), la Cybersecurity and Infrastructure Agency (CISA) e il Federal Bureau of Investigations (FBI) hanno riferito che 16 difetti noti pubblicamente nei dispositivi di rete senza patch sono stati sfruttati in campagne diffuse (fonte). Gli exploit hanno un impatto su vari dispositivi locali, dai router per piccole imprese alle VPN aziendali e potenzialmente offrono agli aggressori la possibilità di manipolare il traffico di rete ed esfiltrare i dati dalle reti di destinazione.

Nonostante la maggior parte dei 16 difetti elencati siano classificati come critici, l'applicazione di patch e la riparazione non sono un compito semplice. In effetti, l'applicazione di patch all'hardware può essere così complessa che esiste un'intera categoria di software per aiutare le aziende a tenersi aggiornate (fonte).

Le conseguenze di un'unica patch non installata possono essere gravi. Non solo l'hardware rimane vulnerabile, ma una volta rilasciata una patch, la vulnerabilità associata diventa un obiettivo di profilo superiore per gli aggressori opportunistici. Si confronti questa situazione con i servizi di sicurezza basati sul cloud, in cui la correzione delle vulnerabilità e l'installazione degli aggiornamenti avviene automaticamente per impostazione predefinita e la propagazione può richiedere solo trenta secondi, a seconda della velocità di rete del provider cloud.

Altri problemi di manutenzione dell'hardware includono:

- **Risoluzione dei problemi:** In uno scenario solo hardware, la risoluzione dei problemi spesso costringe i team IT a passare attraverso l'arduo processo di scollegamento di bilanciatori del carico, firewall e altri dispositivi locali uno alla volta per scoprire dove si trova il problema.

  Questo processo è ulteriormente complicato dall'uso simultaneo di servizi cloud. Le organizzazioni che dipendono dall'hardware spesso gestiscono l'accesso a tali servizi tramite il datacenter centralizzato e tutte le sue singole apparecchiature. Quando i dipendenti non sono in grado di accedere a un particolare servizio, i team IT hanno un posto aggiuntivo da controllare per diagnosticare i problemi. Se si considera un recente rapporto di Productiv che mostra che il 56% di tutte le applicazioni SaaS rientra nella categoria Shadow IT, o applicazioni non approvate e non gestite acquistate all'insaputa dell'IT, questo problema cresce rapidamente sia in termini di portata che di scala (fonte).
- **Manutenzione fisica:** Quando un'appliance hardware si rompe, i team IT devono scollegarla fisicamente, ordinarne una sostitutiva, testare la sostituzione e reinstallarla, un altro processo arduo. Se si considerano le dimensioni di molte imprese globali, questi dispositivi che necessitano di attenzione potrebbero trovarsi dall'altra parte del mondo.

Falle nella sicurezza

Anche se un'organizzazione avesse le risorse necessarie per eseguire continuamente il provisioning e la manutenzione dell'hardware on-premise più recente e con la massima capacità, l'infrastruttura risultante soffrirebbe comunque gravi carenze di sicurezza, specialmente in un mondo che tende al cloud.

Si consideri la gestione degli accessi dei dipendenti. Anche se l'hardware VPN è in grado di stabilire tunnel crittografati tra i dispositivi dei dipendenti in remoto e le applicazioni ospitate in un datacenter interno, non può monitorare e proteggere l'attività dell'utente dopo aver creato questo tunnel.

Se il dispositivo del dipendente viene compromesso da malware o se un attacco di phishing compromette le sue credenziali VPN, un utente malintenzionato potrebbe essere in grado di utilizzare tale accesso VPN per accedere a un'ampia varietà di informazioni riservate. Sia il phishing che il malware continuano a rappresentare seri rischi e generano guadagni monetari significativi per gli attori delle minacce. Nel 2021, secondo l'FBI, sono stati persi 6,9 miliardi di dollari a causa della criminalità informatica. In particolare, il Business Email Compromise (BEC) è costato alle aziende 2,4 miliardi di dollari di perdite (fonte).

Se il dispositivo di un dipendente venisse compromesso da un malware, o se un attacco di phishing dovesse compromettere le sue credenziali VPN, un utente malintenzionato potrebbe essere in grado di utilizzare l'accesso VPN per accedere a un'ampia varietà di informazioni sensibili.

I servizi cloud e le applicazioni SaaS complicano ulteriormente la sicurezza di una infrastruttura basata sull'hardware. In un modello di cloud ibrido, ad esempio, un'organizzazione gestisce una combinazione di infrastruttura on-premise e cloud. L'organizzazione non può semplicemente inviare hardware di sicurezza a un provider cloud. Se desidera continuare a utilizzare hardware on-premise per il proprio datacenter, diverse parti della sua infrastruttura saranno protette in modi diversi, offrendo ai team di sicurezza meno visibilità e controllo sugli attacchi in arrivo.

I servizi basati sul cloud possono superare entrambe queste sfide unificando i datacenter e i servizi cloud in un unico livello definito dal software.

Una spiegazione dettagliata di questo approccio esula dallo scopo del presente documento. Per maggiori informazioni, consultare i seguenti articoli:

- Cos'è una rete Zero Trust?
- Cos'è Secure Access Service Edge?

Servizi di sicurezza e prestazioni basati sul cloud: vantaggi e problemi

La distribuzione dei servizi di rete attraverso il cloud evita molti dei problemi associati all'hardware: limitazioni di capacità, costi, problemi di supporto e lacune nella sicurezza.

- **Supply chain:** molti provider di rete basati su cloud sono progettati per adattarsi alle moderne architetture globali, rendendo meno acuti i problemi della supply chain.
- **Capacità:** in ragione della natura distribuita del cloud e definita dal software, le organizzazioni possono eseguire facilmente il provisioning di capacità aggiuntiva in base alla scalabilità aziendale.
- **Costo:** i costi aggiuntivi dell'hardware sono nulli o più agevoli da pianificare anticipatamente. Inoltre, i servizi cloud vengono generalmente classificati come spese operative, non come spese in conto capitale, il che offre vantaggi fiscali e contabili per molte aziende.
- **Supporto:** le esigenze logistiche e di risorse vengono gestite dal provider di servizi. In più, non c'è più il rischio di perdere una patch, in quanto gli aggiornamenti vengono eseguiti automaticamente.
- **Sicurezza:** i servizi di rete definiti dal software possono unificare infrastrutture diverse sotto un unico livello di protezione.

Tuttavia, i servizi di rete cloud presentano i propri rischi se non vengono implementati in modo accurato:

Rischio	Descrizione
Latenza	Alcune funzioni di rete basate su cloud si basano su datacenter specializzati basati su cloud, ad esempio scrubbing center per la mitigazione DDoS. Il backhauling del traffico verso quei datacenter può aggiungere una latenza significativa a seconda della sua posizione rispetto al server di destinazione. Questo problema si aggrava quando un'organizzazione utilizza provider diversi per diverse funzioni di rete. Quando il traffico deve passare da un provider all'altro, la latenza può essere misurata in centinaia di millisecondi.
Sup-porto	Quando un'organizzazione utilizza provider diversi per funzioni diverse, la risoluzione dei problemi rimane un problema. Può essere difficile stabilire quale provider sia la causa della congestione o dei disservizi.
Costi	Quando un'organizzazione utilizza provider diversi per funzioni diverse, l'investimento di tempo (e quindi di denaro) per gestirli può essere comunque elevato.

Per evitare questi problemi bisogna prendere in considerazione le seguenti strategie:

- **Ricerca di provider che funzionano sia con l'infrastruttura cloud che on-premise.** questa funzionalità consente ai team IT e di sicurezza di impostare controlli coerenti e monitorare il traffico globale da un'unica posizione. Aiuta anche a costruire un'architettura più resiliente, una in cui i tuoi team possono ruotare rapidamente in risposta alle fluttuazioni delle condizioni di mercato.
- **Ricerca provider cloud che offrono più funzioni di rete che funzionano insieme.** questo spesso riduce il numero di salti di rete che il traffico deve effettuare, con conseguente riduzione della latenza e quindi una migliore esperienza per l'utente finale. La risoluzione dei problemi di rete è anche più semplice quando si dispone di un'azienda da chiamare anziché di molte. Inoltre, il raggruppamento di più funzioni insieme spesso comporta costi inferiori.
- **Cercare provider cloud in grado di eseguire più funzioni di rete da ogni posizione della loro rete.**
  I provider che ampliano i propri portafogli di servizi mediante acquisizione non sempre integrano completamente questi nuovi servizi, il che significa che alcune funzioni possono essere erogate solo attraverso determinati datacenter. Prendere in considerazione i provider che offrono queste funzioni su tutta la loro rete per evitare gli stessi problemi elencati sopra.
- **Cercare provider cloud con ampia presenza a livello globale.**
  Questa funzionalità supporta la precedente, assicurando che gli utenti finali siano sempre vicini alla rete, indipendentemente da dove si trovino. Crea anche un'estesa superficie di rete con cui assorbire il traffico DDoS e svolgere altre funzioni di rete che richiedono una grande capacità.

In che modo Cloudflare può essere d'aiuto

In che modo le organizzazioni possono accelerare la trasformazione della propria rete, senza attendere l'arrivo dell'hardware e senza investire più denaro in box che dureranno solo una manciata di anni?Con Cloudflare.

Cloudflare ha creato una piattaforma cloud globale che offre un'ampia gamma di servizi, rendendo le organizzazioni più sicure, migliorando le prestazioni delle loro applicazioni ed eliminando i costi e la complessità di gestione delle singole apparecchiature hardware di rete. Questa piattaforma opera come piano di controllo unificato, scalabile e facile da usare per garantire sicurezza, alte prestazioni e affidabilità a livello di applicazioni locali, ibride, cloud e SaaS (Software-as-a-Service).

Fondamentalmente, ogni datacenter nella rete globale di oltre 270 città di Cloudflare può fornire ognuno di questi servizi, riducendo la latenza che può complicare le implementazioni del cloud. Semplifica il tuo stack di rete, accelera la trasformazione e prepara la tua rete per ciò che verrà dopo.

Per saperne di più, visita il sito www.cloudflare.com.

> “Dropbox è recentemente diventata un'organizzazione 'virtual first'. Abbiamo esplorato l'impatto di questa strategia aziendale sul nostro approccio alla sicurezza e sull'architettura di rete. Apprezziamo il supporto di Cloudflare nell'aiutare noi e altre organizzazioni remote come la nostra a imparare come adattarsi a questa "nuova normalità".
>
> Konstantin Sinichkin
> **Engineering Manager, Dropbox**

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

REV:BDES-3313.2022JUN10