Cosa cercare in una soluzione SD-WAN sicura per ambienti multi-cloud

Sommario

Panoramica preliminare

L'introduzione del cloud sta diventando una parte sempre più consistente dei budget dei CIO, al punto che alcune aziende stanno utilizzando molti ambienti cloud diversi per costruire la loro infrastruttura IT. Un modello multi-cloud comporta la selezione personalizzata di più servizi cloud per servire funzioni specifiche. Oggi le aziende hanno praticamente adottato il multi-cloud per la sua flessibilità; attualmente il 93% ha una strategia multi-cloud.[1] Tuttavia, collegare carichi di lavoro su più cloud alla periferia della WAN del data center crea varie sfide, tra cui distribuzione complessa, prestazioni di rete incostanti e maggior costo della connettività.

Una soluzione SD-WAN (Software-Defined Wide-Area Networking) può contribuire a facilitare l'adozione di distribuzioni multi-cloud, semplificando al contempo l'infrastruttura WAN e riducendo i costi della connettività. Per ottenere i risultati desiderati, tuttavia, la SD-WAN deve essere mantenuta sicura.

Secondo le proiezioni, il mercato globale delle IaaS (Infrastructure-as-a-Service) cloud dovrebbe registrare un tasso di crescita annuo composto (CAGR) quasi pari al 28% raggiungendo 101,56 miliardi di dollari entro il 2023.[2]

Perché le aziende stanno adottando rapidamente il multi-cloud

Una strategia multi-cloud consente alle organizzazioni di evitare il vendor lock-in e selezionare i migliori servizi cloud disponibili per una particolare applicazione o uno specifico carico di lavoro. Il multi-cloud non equivale al cloud ibrido, in cui si integrano cloud pubblici e privati per ottimizzare le prestazioni, la sicurezza e la flessibilità. Multi-cloud significa semplicemente che le organizzazioni hanno la flessibilità di selezionare il miglior fornitore di cloud per ciascuna delle loro varie esigenze a livello di infrastrutture e applicazioni.

Le organizzazioni possono scegliere servizi ottimizzati in base ai costi e sfruttare cloud geograficamente dispersi ad esempio per il disaster recovery o per soddisfare i requisiti di sovranità dei dati e migliorare l'esperienza dell'utente.

Il modello multi-cloud assicura inoltre ridondanza, riducendo così il rischio di inattività operativa. Anche se le interruzioni del servizio da parte del provider non sono così comuni e pervasive come una volta, il potenziale rischio, con conseguente compromissione dell'azienda, è ancora notevole. Infatti, poiché le organizzazioni continuano a trasferire in cloud carichi di lavoro mission-critical, un'interruzione o un degrado delle prestazioni può avere un forte impatto sulla continuità delle loro attività aziendali o sulla qualità complessiva dell'esperienza.

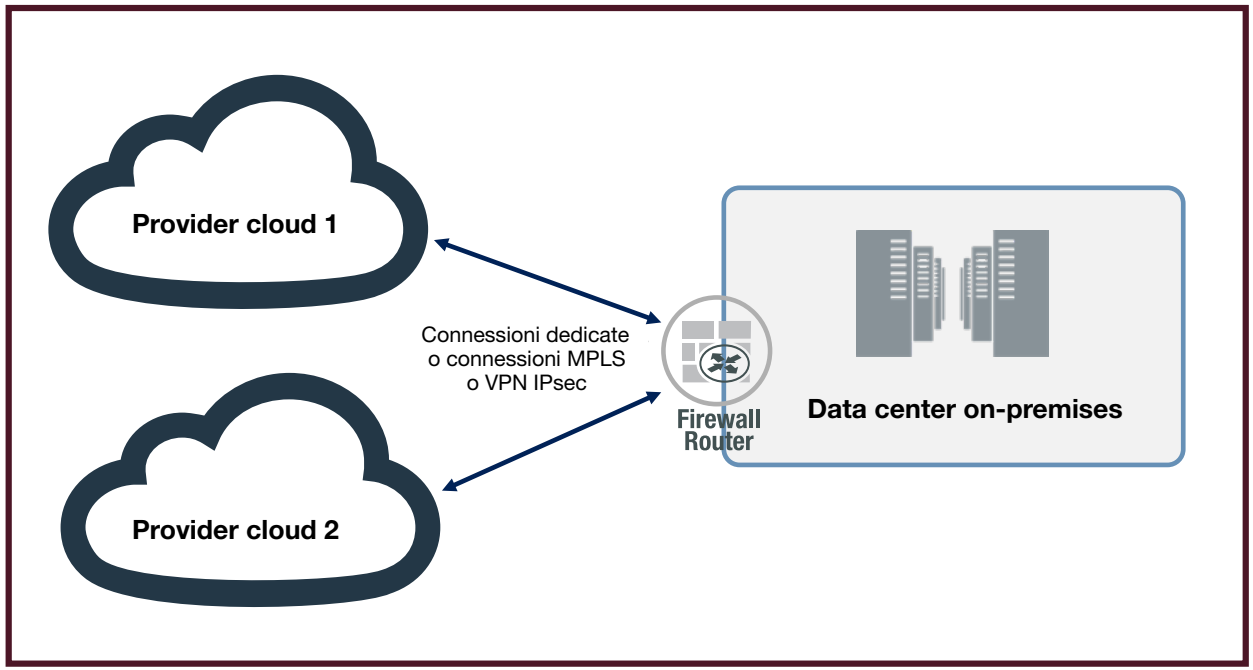
Più cloud significa più complessità

Nonostante i numerosissimi vantaggi, l'adozione del multi-cloud aggiunge indubbiamente ulteriori livelli di complessità gestionale, soprattutto se l'aggiunta di servizi cloud avviene in modo puntuale anziché essere pianificata dall'inizio.[3] Tale complessità crea sfide gestionali e operative, dalla distribuzione alle prestazioni di rete, passando per i costi di esercizio. Pochi team IT hanno l'esperienza necessaria per gestire una distribuzione mista di più ambienti con cloud pubblici, cloud privati e on-premises, soprattutto se si considera la persistente carenza di competenze IT (in particolare nel campo della sicurezza informatica). Le organizzazioni che dispongono di risorse limitate faranno fatica a tenere il passo.

Per mantenere il controllo e la visibilità centralizzati con le tradizionali infrastrutture di rete a stella, il backhaul del traffico delle applicazioni da ogni cloud è generalmente eseguito dai provider su un data center on-premises utilizzando costose connessioni MPLS (Multiprotocol Label Switching), il che aumenta i costi di esercizio e può incidere sull'esperienza applicativa a causa di colli di bottiglia a livello di sicurezza.

Poiché le organizzazioni continuano a utilizzare sempre più il cloud per l'hosting delle applicazioni, l'accesso diretto con prestazioni elevate è fondamentale.[4]

Inoltre, le organizzazioni che non stanno introducendo una gestione e un monitoraggio centralizzati sono poi appesantite da policy di sicurezza frammentate in più ambienti cloud e non hanno visibilità end-to-end della loro infrastruttura, il che aumenta il rischio di violazioni, perdita di dati, sanzioni per non compliance e altri danni all'azienda. Fortunatamente, esiste un modo migliore per strutturare tutto questo.



- Complessità di distribuzione
- Degrada le prestazioni delle applicazioni
- Costi di connessione elevati

Figura 1: Attuali distribuzioni IT multi-cloud.

Più cloud richiedono una gestione e una sicurezza unificate

Per massimizzare i vantaggi e la flessibilità di una strategia multi-cloud, sono necessarie tecnologie di sicurezza e rete in grado di offrire i seguenti vantaggi:

- Utilizzare connessioni ottimali per instradare il traffico delle applicazioni in modo da garantire affidabilità e prestazioni
- Sfruttare le connessioni Internet a banda larga in modo da ridurre i costi
- Ottenere visibilità su tutta l'infrastruttura di rete
- Bilanciare i carichi di lavoro tra i vari cloud pubblici e privati
- Applicare policy di sicurezza e rete coerenti ai vari cloud

Grazie alle sue capacità di automazione e alla posizione strategica che occupa nella rete, la SD-WAN è diventata la soluzione preferita per le innovazioni in rapida evoluzione delle rete in cloud (anche in multi-cloud).[5] La SD-WAN consente alle aziende di aumentare o sostituire le costose connessioni MPLS con una serie application-aware di opzioni di connettività Internet più convenienti in termini di costi. Questo a sua volta compensa il degrado delle prestazioni che sta diventando un problema crescente a causa della quantità di traffico derivante dai carichi di lavoro delle applicazioni in cloud di tutta l'azienda.

Le applicazioni ospitate nel cloud pubblico possono utilizzare gateway SD-WAN avanzati basati su cloud per dirigere il traffico tra le applicazioni.[6]

Cosa cercare in una soluzione SD-WAN

Le soluzioni SD-WAN variano notevolmente in termini di capacità. Le aziende dovrebbero pertanto analizzare attentamente tutti i costi associati, sia le spese in conto capitale (CapEx) che le spese di esercizio (OpEx), così come i requisiti di gestione, prestazioni e soprattutto sicurezza.

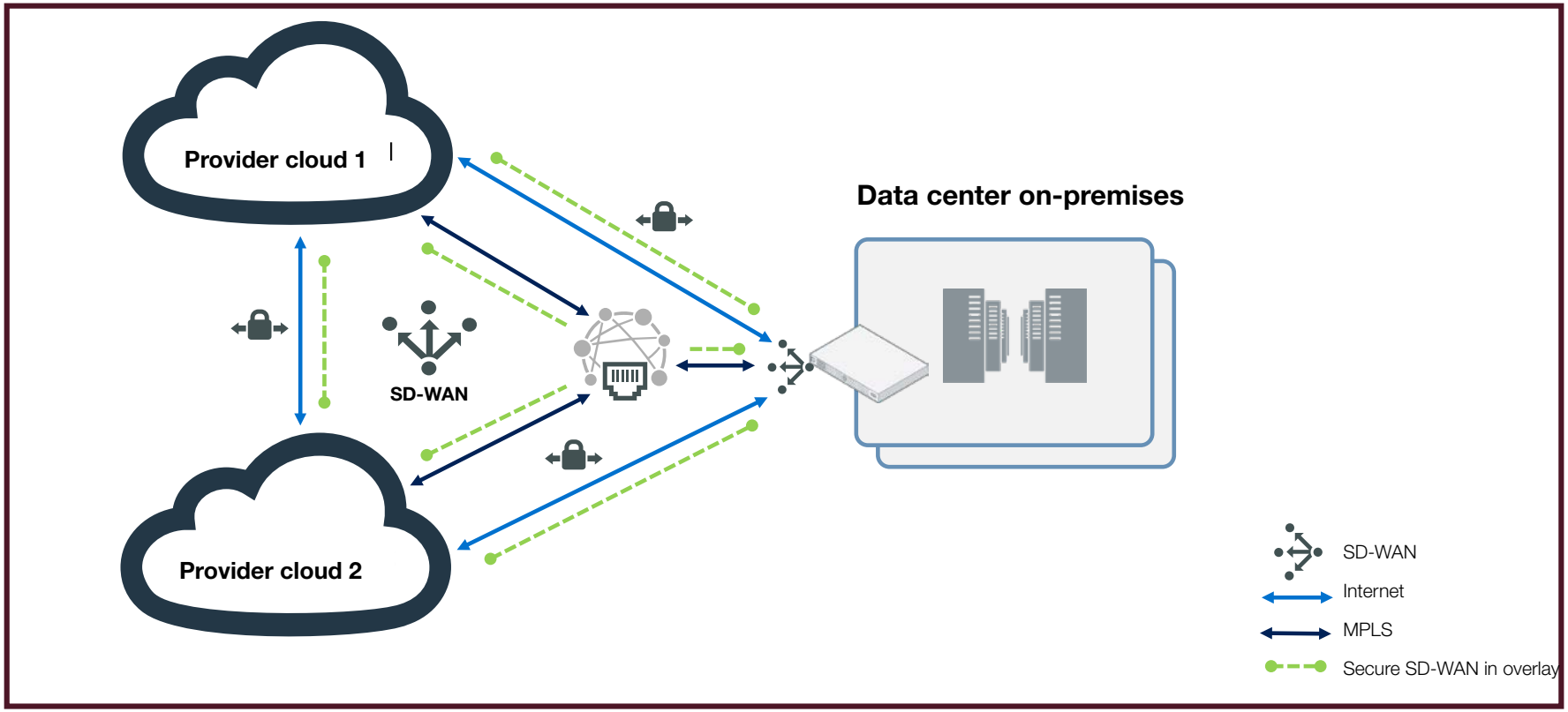


Figura 2: Collegamento di più cloud tramite SD-WAN.

- **SD-WAN sicura e consolidata.** Un approccio frammentario alla SD-WAN comporta investimenti in più dispositivi per creare tutte le capacità di rete e sicurezza necessarie al fine di costituire una soluzione perfettamente funzionale. Tuttavia, questo approccio frammentario presenta lacune intrinseche a livello di sicurezza che possono essere sfruttate dagli attacchi informatici. Un'unica soluzione che integri capacità di rete SD-WAN avanzate all'interno di un firewall di nuova generazione (NGFW) può invece eliminare tali lacune, riducendo al contempo i costi di investimento CapEx complessivi.
- **Distribuzione e gestione semplificate.** Una SD-WAN frammentaria comporta anche un aumento dei costi OpEx in termini di tempo dedicato dal personale alla distribuzione, all'orchestrazione e alla gestione della soluzione. Una soluzione SD-WAN consolidata centralizza questi processi. Un'interfaccia **unica** comune semplifica le operazioni e alleggerisce il carico che grava su un personale ridotto. Va dunque ricercata una soluzione che abbia **profonde integrazioni cloud-native e da un ampio supporto del cloud** per contribuire a semplificare le fasi iniziali di impostazione e configurazione.
- **Prestazioni.** Una soluzione SD-WAN con capacità di **riconoscimento delle applicazioni** intelligente può risolvere i problemi di larghezza di banda e prestazioni. La soluzione dovrebbe fare riferimento a un ampio database di applicazioni conosciute e utilizzare firme personalizzate che le consentano di dare priorità al traffico e gestire automaticamente le connessioni in base alla esigenze in tempo reale dell'azienda.
- **Visibilità e controllo.** Il monitoraggio delle vulnerabilità su più cloud distribuiti può essere difficile. Una SD-WAN con gestione centralizzata e integrazione a livello di supporto con i costrutti di sicurezza del provider del cloud come il tagging, può assicurare una visibilità end-to-end attivabile su tutte le iterazioni del cloud per garantire capacità di rilevamento e prevenzione avanzate, nonché per l'applicazione automatica di controlli basati su policy. Ciò a sua volta può contribuire a garantire la compliance alle leggi sulla privacy dei dati e alle normative di settore, indipendentemente dal luogo in cui vengono archiviati i dati sensibili.

Una soluzione SD-WAN efficace semplifica le sfide del multi-cloud

Una soluzione SD-WAN efficace può fornire un'infrastruttura di rete application-aware che si estende in più ambienti cloud, eliminando le incoerenze attraverso un'infrastruttura definita da policy uniforme, semplificando la gestione e riducendo i costi infrastrutturali, oltre a migliorare l'agilità delle distribuzioni e l'esperienza applicativa in tutta l'azienda. Infine, le funzionalità di sicurezza integrate offerte da una soluzione SD-WAN robusta e consolidata possono ridurre i rischi e applicare controlli sulle infrastrutture aziendali basate su ambienti multi-cloud.

Per valutare la capacità di una soluzione SD-WAN di ottimizzare la funzionalità del multi-cloud e migliorare la sicurezza, possono essere utili le seguenti domande:

- ☐ La soluzione consolida la sicurezza e la funzionalità di rete?
- ☐ La soluzione garantisce una visibilità end-to-end e un controllo capillare di tutti gli ambienti cloud?
- ☐ La soluzione offre una console di gestione centralizzata (interfaccia unica) con la possibilità di applicare policy globali?
- ☐ Esistono test per convalidare le prestazioni, l'affidabilità o il valore (TCO) della soluzione in ambienti cloud?
- ☐ La soluzione supporta l'ampia gamma di ambienti cloud pubblici e privati?

[1] Kim Weins, "Cloud Computing Trends: 2020 State of the Cloud Report," Flexera, 21 maggio 2020.

[2] "Global Infrastructure as a Service (IaaS) Market 2019-2023," Business Wire, 23 ottobre 2019.

[3] Charles McLellan, "Multicloud: Everything you need to know about the biggest trend in cloud computing," ZDNet, 1° luglio 2019.

[4] Sasha Emmerling, "The Network Edge: Stretching the Boundaries of SD-WAN," Network Computing, 7 agosto 2019.

[5] Ibid.

[6] Ibid.

www.fortinet.com

719125-0-0-IT

novembre 19, 2020 12:05 PM

eb-FA-what-to-look-for-in-a-secure-sdwan-7112020_IT