FORTINET

Worauf Sie bei einer Secure SD-WAN-Lösung für Multi-Cloud-Umgebungen achten sollten

Inhaltsverzeichnis

Zusammenfassung

Die Cloud-Einführung gewinnt in CIO-Budgets immer mehr an Gewicht. Einige Unternehmen bauen sogar ihre gesamte IT-Infrastruktur auf vielen verschiedenen Cloud-Umgebungen auf – und 93 % der Unternehmen verfolgen bereits eine Multi-Cloud-Strategie, um von mehr Flexibilität zu profitieren.[1] Die Dienste solcher Multi-Cloud-Modelle müssen jedoch genau auf das Unternehmen abgestimmt sein, um bestimmte Funktionen zu erfüllen. Auch bringt das Verbinden von Workloads aus mehreren Clouds am WAN-Edge des Rechenzentrums einige Probleme mit sich, wie z. B. komplexe Implementierungen, hohe Verbindungskosten und eine schwankende Netzwerk-Performance.

Ein softwaredefiniertes Wide Area Network (SD-WAN) kann die Multi-Cloud-Implementierung und die WAN-Infrastruktur vereinfachen sowie die Konnektivitätskosten senken. Diese Rechnung geht jedoch nur auf, wenn das SD-WAN richtig geschützt wird. Kurz: Die Security ist entscheidend.

Es wird erwartet, dass der globale IaaS-Markt für Cloud-Infrastrukturen mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von über 28 % wächst und bis 2023 ein Marktvolumen von 85,65 Milliarden € erreicht.[2]

Warum Unternehmen Multi-Clouds so schnell einführen

Mit einer Multi-Cloud-Strategie vermeiden Unternehmen die Bindung an einen bestimmten Anbieter und können Cloud-Dienste optimal auf Anwendungen oder bestimmte Workloads abstimmen. Multi-Cloud-Umgebungen sind nicht dasselbe wie Hybrid Clouds, die Public und Private Clouds für mehr Leistung, Sicherheit und Flexibilität miteinander kombinieren. „Multi-Cloud“ bedeutet einfach, dass Unternehmen flexibel den besten Cloud-Anbieter je nach Infrastruktur- und Anwendungsanforderung auswählen können.

Für relativ wenig Geld lassen sich geografisch verteilte Clouds für das Disaster Recovery nutzen, um z. B. Anforderungen an die Datenhoheit zu erfüllen oder die Nutzererfahrung zu verbessern.

Das Multi-Cloud-Modell bietet außerdem eine Redundanz, die das Risiko von Betriebsausfällen verringert. Obwohl Service-Provider-Ausfälle nicht mehr so oft vorkommen wie früher, besteht weiterhin ein hohes Ausfallrisiko, das Geschäftsabläufe empfindlich stören kann.

Durch die Verlagerung von immer mehr kritischen Workloads in die Cloud können Ausfälle oder Performance-Verluste den kontinuierlichen Geschäftsbetrieb gefährden oder die allgemeine Nutzererfahrung erheblich beeinträchtigen.

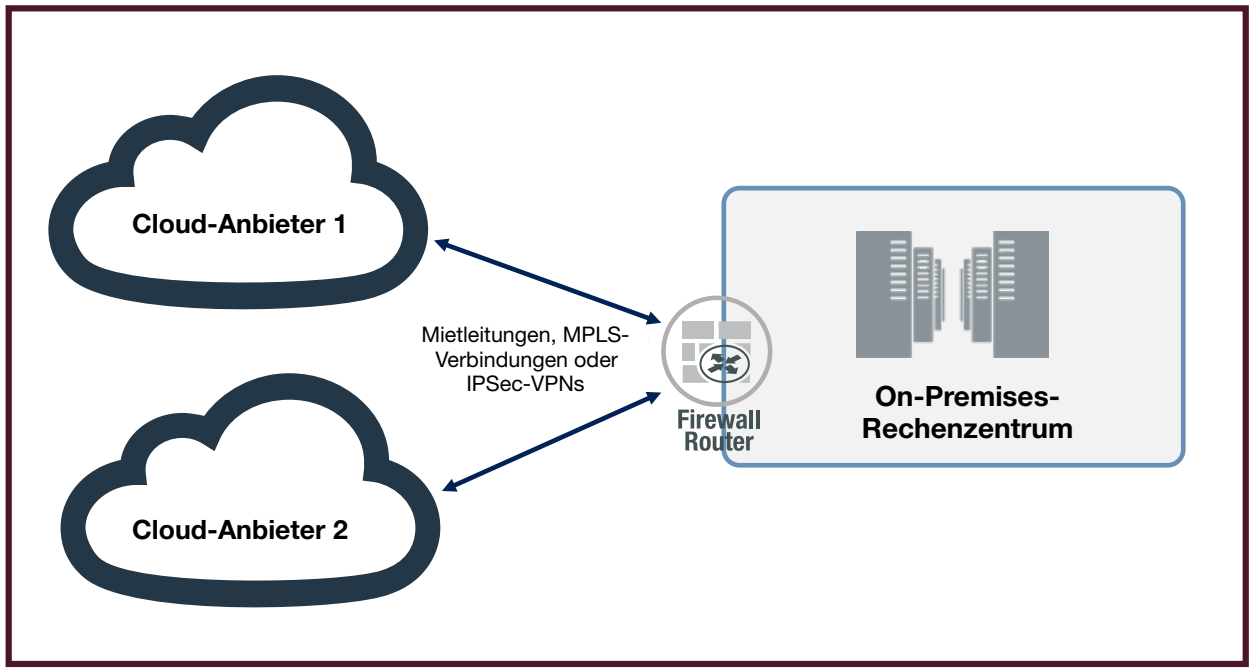
Mehr Clouds bedeuten mehr Komplexität

Trotz der unzähligen Vorteile wird das Management durch Multi-Clouds immer komplexer, insbesondere, wenn Cloud-Dienste nicht nach Plan, sondern Ad-hoc bei Bedarf hinzugefügt werden.[3] Diese Komplexität schafft neue Management- und Betriebsprobleme in allen Bereichen – von der Implementierung über die Netzwerk-Performance bis hin zu den Betriebskosten. Nur wenige IT-Teams haben das Know-how, um eine gemischte Implementierung mit mehreren Public Clouds, Private Clouds und On-Premises-Umgebungen zu verwalten. Verschärft wird dieses Problem noch durch den anhaltenden Fachkräftemangel im IT-Bereich speziell bei Cyber-Security-Experten. Unternehmen mit begrenzten personellen Ressourcen dürften daher Schwierigkeiten haben, diese Komplexität in den Griff zu bekommen.

Um eine zentralisierte Kontrolle und Transparenz mit herkömmlichen „Hub-and-Spoke“-Netzwerk-Infrastrukturen zu gewährleisten, wird der Anwendungsverkehr aus jeder Cloud oft über teure MPLS-Verbindungen (Multiprotocol Label Switching) zu einem On-Premises-Rechenzentrum zurückgeleitet. Das führt jedoch zu höheren Betriebskosten und Security-Engpässen, die die Anwendungserfahrung beeinträchtigen.

Da Unternehmen die Cloud immer häufiger zum Hosten von Anwendungen nutzen, ist ein direkter, leistungsstarker Cloud-Zugriff von entscheidender Bedeutung.[4]

Ohne ein zentrales Management und Monitoring werden Unternehmen zusätzlich durch uneinheitliche Sicherheitsrichtlinien in verschiedenen Cloud-Umgebungen belastet. Dazu kommt eine fehlende, lückenlose Transparenz über die eigene Infrastruktur, was das Risiko von Sicherheitsverletzungen, Datenverlusten, Compliance-Bußgeldern und anderen Schäden für das Unternehmen erhöht. Zum Glück muss das nicht so sein – es gibt bessere Alternativen.



- Komplexe Implementierung
- Schlechtere Anwendungs-Performance
- Hohe Verbindungs-kosten

Abbildung 1: Heutige Multi-Cloud-IT-Implementierungen

Mehrere Clouds erfordern eine einheitliche Verwaltung und Security

Um maximal von den Vorteilen und der Flexibilität einer Multi-Cloud-Strategie zu profitieren, sollten Security- und Netzwerk-Technologien folgende Vorteile bieten:

- Auswahl der optimalen Verbindung, um Anwendungsverkehr mit der besten Zuverlässigkeit und Leistung zu übertragen
- Nutzung von Internet-Verbindungen mit hoher Bandbreite, um Kosten zu senken
- Transparenz über Ihre gesamte Netzwerk-Infrastruktur
- Verteilung von Workloads auf separate Public und Private Clouds
- Durchsetzung einheitlicher Netzwerk- und Sicherheitsrichtlinien in mehreren Clouds

Aufgrund seiner Automatisierungsfunktionen und strategischen Position im Netzwerk ist ein SD-WAN ideal für Cloud-Netzwerke (einschließlich Multi-Cloud) mit kurzen Innovationszyklen.[5] Mit einem SD-WAN können Unternehmen kostspielige MPLS-Verbindungen durch mehrere anwendungsorientierte, günstige Verbindungsoptionen über das Internet erweitern oder komplett ersetzen. So lassen sich auch Leistungsverluste vermeiden, die sonst durch die hohen Verkehrsaufkommen von unternehmensweit genutzten Cloud-Anwendungen zum Problem werden.

Werden Anwendungen in Public Clouds gehostet, kann der Traffic zwischen diesen Anwendungen über ein intelligentes, cloudbasiertes SD-WAN-Gateway gelenkt werden.[6]

Worauf Sie bei einer SD-WAN-Lösung achten sollten

SD-WAN-Lösungen unterscheiden sich stark bei der Funktionalität. Unternehmen sollten alle damit verbundenen Kosten – sowohl Investitions- als auch Betriebskosten – sowie Management-, Leistungs- und insbesondere die Sicherheitsanforderungen sorgfältig prüfen.

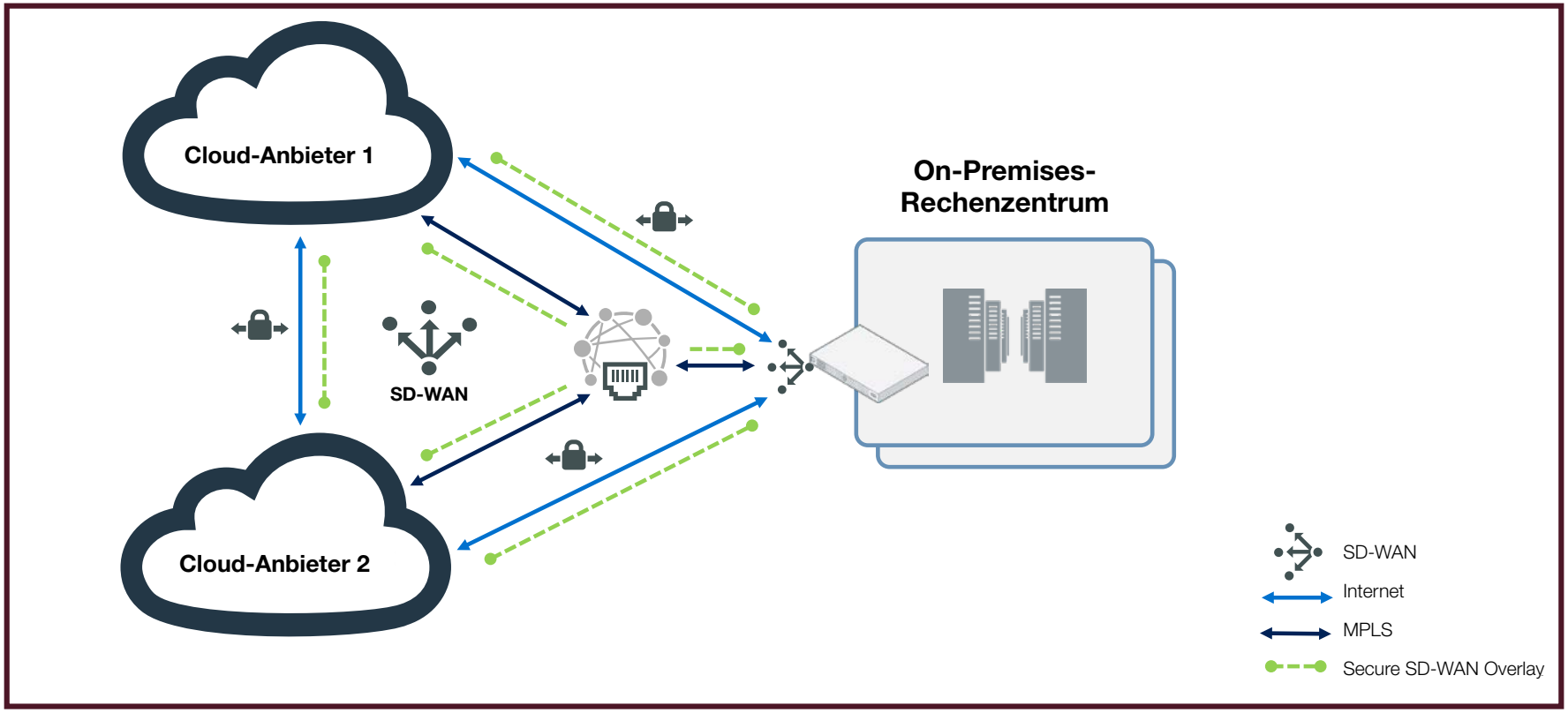


Abbildung 2: Verbinden mehrerer Clouds über ein SD-WAN

- **Konsolidiertes Secure SD-WAN:** Bei einem disaggregierten SD-WAN-Ansatz ist die Anschaffung zahlreicher Einzelgeräte notwendig. Nur so lassen sich alle benötigten Netzwerk- und Security-Funktionen bereitstellen, um eine vollfunktionsfähige Lösung zu erhalten. Durch viele Einzelprodukte entstehen jedoch neue Sicherheitsprobleme, die Cyber-Angreifer ausnutzen können. Eine Komplettlösung, die intelligente SD-WAN-Netzwerk-Funktionen in eine Next Generation Firewall (NGFW) integriert, kann diese Sicherheitslücken schließen und zugleich die Gesamtinvestitionskosten senken.
- **Einfachere Implementierung und Verwaltung:** Ein disaggregiertes SD-WAN erhöht auch die Betriebskosten, da der Personalaufwand für die Implementierung, Orchestrierung und das Management der Lösung steigt. Eine konsolidierte SD-WAN-Lösung zentralisiert dagegen diese Prozesse: Eine einzige Konsole sorgt für **Transparenz**, was den Betrieb vereinfacht und personell begrenzte Teams entlastet. Achten Sie bei einer Lösung darauf, dass diese **tiefe cloudnative Integrationen und einen umfassenden Cloud-Support** bietet, um die Einrichtung und Konfiguration zu beschleunigen.
- **Performance:** Eine SD-WAN-Lösung mit intelligenten Funktionen für die **Anwendungserkennung** kann Bandbreiten- und Leistungsprobleme aus der Welt schaffen. Die Lösung sollte auf eine umfassende Datenbank bekannter Anwendungen referenzieren und benutzerdefinierte Signaturen verwenden, um den Datenverkehr zu priorisieren und Verbindungen automatisch – je nach Echtzeit-Anforderungen des Unternehmens – zu steuern.
- **Transparenz und Kontrolle:** Das Verfolgen von Schwachstellen in mehreren dezentralen Cloud-Implementierungen kann schwierig sein. Ein SD-WAN mit einem zentralen Management und Support, das in die Sicherheitskonzepte von Cloud-Anbietern (z. B. Tagging) integriert wird, bietet eine durchgängige, praxisnahe Transparenz über alle Cloud-Iterationen hinweg. Unternehmen erhalten damit einen erweiterten Bedrohungsschutz und intelligente Funktionen für die Bedrohungserkennung. Auch lassen sich richtlinienbasierte Sicherheitskontrollen automatisch durchsetzen, um Datenschutzgesetze und Branchenvorschriften unabhängig vom Speicherort der Daten zu erfüllen.

Ein effektives SD-WAN vereinfacht Multi-Cloud-Herausforderungen

Eine effektive SD-WAN-Lösung kann eine anwendungsorientierte Netzwerk-Infrastruktur bereitstellen, die mehrere Cloud-Umgebungen umfasst. Unternehmen erhalten damit eine einheitliche, richtliniendefinierte Infrastruktur mit Vorteilen wie ein einfacheres Management, geringere Infrastrukturkosten sowie unternehmensweit flexiblere Implementierungen und bessere Anwendungserfahrungen. Zudem können integrierte Security-Funktionen in einer robusten, konsolidierten SD-WAN-Lösung Risiken verringern und Kontrollen in Unternehmensinfrastrukturen mit mehreren Cloud-Umgebungen durchsetzen.

Bei der Evaluierung einer SD-WAN-Lösung zur Optimierung der Multi-Cloud-Funktionalität und zur Verbesserung der Sicherheit können die folgenden Fragen hilfreich sein:

- ☐ Konsolidiert die Lösung die Security- und Netzwerk-Funktionalität auf effektive Weise?
- ☐ Bietet die Lösung eine durchgehende Transparenz und granulare Kontrolle in allen Cloud-Umgebungen?
- ☐ Gibt es eine zentralisierte Management-Konsole (eine „Schaltzentrale“), mit der sich globale Richtlinien durchsetzen lassen?
- ☐ Wurden Leistung, Zuverlässigkeit oder Wert der Lösung (TCO) in Cloud-Umgebungen durch Tests bestätigt?
- ☐ Unterstützt die Lösung die breite Palette von Public- und Private-Cloud-Umgebungen?

[1] Kim Weins: „Cloud Computing Trends: 2020 State of the Cloud Report“. Flexera, 21. Mai 2020.

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

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

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

[5] Ebd.

[6] Ebd.

www.fortinet.com/de

719125-0-0-DE

7. Dezember 2020, 14:00 Uhr