SOLUTION BRIEF

Fortinet – Sichere Hybrid Cloud

Zusammenfassung

Hybrid Clouds sind eine Mischung aus lokalen und Public Cloud-Diensten, deren Nutzung immer mehr zunimmt. Die Sicherheit über diese erweiterte Umgebung hinweg wird in der Regel nicht konsequent durchgesetzt und ist komplex zu verwalten – und Verbindungen sind oft unsicher. Die Fortinet Security Fabric löst diese Herausforderungen durch die native Integration mit großen Cloud-Anbietern, die zentrale Durchsetzung einheitlicher Sicherheitsrichtlinien und die Einrichtung einer schnellen und sicheren Konnektivität.

Sicherer Hybrid Cloud-Schutz von Fortinet:

- Security Management über zentrale Konsole
- Konsequentes Durchsetzen der Sicherheitsmaßnahmen über alle Umgebungen hinweg
- Sichere Verbindungen ohne Leistungseinbußen

Fragmentierte, inkonsistente Sicherheit zwischen lokalen Rechenzentren und Clouds

Viele Unternehmen verlassen ihre lokalen Rechenzentren, um die Public Cloud als zusätzliche Infrastruktur für die Entwicklung und Bereitstellung von IT-Lösungen zu nutzen. Häufig entwickeln sie neue Anwendungen in der Cloud und pflegen alte Anwendungen im lokalen Rechenzentrum. Die Nutzung von Hybrid Clouds nimmt zu: 81 % der Unternehmen verfügen über Multi Cloud-Strategien, und die globalen Ausgaben für Hybrid Clouds werden sich voraussichtlich von 45 Milliarden USD im Jahr 2018 bis zum Jahr 2023 auf 98 Milliarden USD mehr als verdoppeln.[1]

Trotz zunehmender Dynamik verlangsamen mehrere Hürden die Nutzung von Hybrid Clouds. Insbesondere sehen 77 % der Unternehmen die Sicherheit von Hybrid Clouds als Problem.[2] Unterdessen argumentiert jeder Cloud-Anbieter für die speziellen Vorteile seiner eigenen Cloud Security-Funktionen. Die Realität ist jedoch, dass sich Hybrid Cloud-Nutzer einer Vielzahl von unterschiedlichen Security-Technologien, Plattformen und Management-Tools gegenübersehen. Das Sicherheitsprofil zwischen den lokalen Rechenzentren und den einzelnen Cloud-Implementierungen ist uneinheitlich. Darüber hinaus ist die Netzwerktransparenz schlecht und das Security Management komplex.

Fehlende Security-Konnektivität zwischen Cloud-Implementierungen und über sie hinweg führt zu zusätzlichen Sicherheitslücken.

Zentralisiertes Security Management über eine zentrale Konsole mit Fortinet

Die Fortinet Security Fabric stellt sich diesen Herausforderungen. Sie bietet über die gesamte digitale Angriffsfläche hinweg breite Transparenz, sowohl On-Premises als auch in mehreren Clouds. Sie nutzt native Integration mit allen großen Cloud-Anbietern und ermöglicht die automatisierte, zentralisierte Verwaltung der gesamten Security-Infrastruktur über eine zentrale Konsole.

Im Folgenden finden Sie die wichtigsten Fortinet-Elemente, die Hybrid Clouds schützen und zu starken Infrastrukturkomponenten machen:

FortiGate Next-Generation Firewalls (NGFWs) bieten sichere Konnektivität, Netzwerksegmentierung und Anwendungssicherheit für Hybrid Cloud-basierte Implementierungen. Sie tragen dazu bei, eine zentralisierte

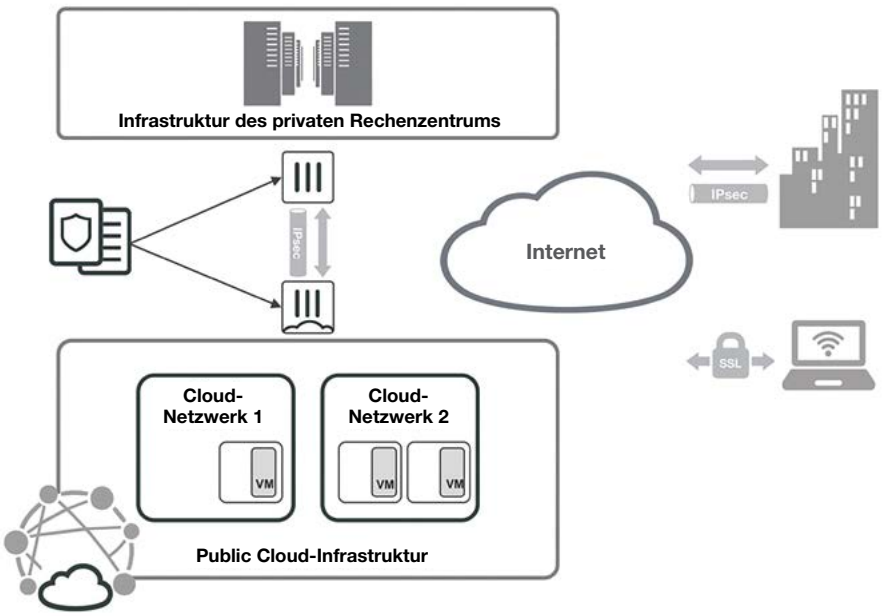

Abbildung 1: Security muss über Rechenzentrums- und Cloud-Umgebungen hinweg einheitlich sein. Typische Hybrid Cloud-Umgebungen erhöhen das Risiko durch mangelnde Transparenz, uneinheitliche Sicherheitsrichtlinien und komplexes Security Management.

und konsequente Durchsetzung der Sicherheitsrichtlinien zu gewährleisten und eine Verbindung über einen schnellen VPN-(Virtual Private Network-)Tunnel herzustellen. Letzterer schützt Daten ohne Abstriche bei der Leistung.

Fortinet NGFWs haben auch bei externen Tests das beste Preis-Leistungs-Verhältnis unter allen 10 teilnehmenden Anbietern erzielt.[3] In Tests blockierten sie 100 % der Umgehungen und verzeichneten nur minimale Leistungseinbußen bei der Prüfung von verschlüsseltem Datenverkehr (im Vergleich zu Lösungen von Wettbewerbern). Dies ist entscheidend, da über 72 % des gesamten Netzwerkverkehrs inzwischen verschlüsselt sind, was einem Anstieg von 20 Prozent gegenüber dem dritten Quartal 2017 entspricht.[4]

FortiGate-VMs sind virtualisierte Instanzen von FortiGate NGFWs. FortiGate VMs können sicher kommunizieren und einheitliche Richtlinien mit FortiGate NGFWs aller Formfaktoren austauschen, die in einem lokalen Rechenzentrum bereitgestellt werden.

FortiManager bietet über das gesamte Unternehmen hinweg eine Verwaltung über eine zentrale Konsole – einschließlich Fortinet NGFWs, Switches, WLAN-Infrastruktur und Endgeräte.

FortiManager vereinfacht das Security Management für Unternehmen und ermöglicht es Security-Experten, Richtlinien und Objekte mit einem konsolidierten Drag&Drop-fähigen Editor zu erstellen und zu ändern. Sie können auch Geräte in einer Security Fabric-Gruppe so verwalten, als wären sie ein einzelnes Gerät, um sicherzustellen, dass Sicherheitsrichtlinien über alle Umgebungen hinweg konsequent durchgesetzt werden. Schließlich können Security-Experten Änderungen vereinfachen und verfolgen und durch die Integration mit ITSM-(IT Service Management-) Anwendungen wie ServiceNow auditierbar machen.

FortiAnalyzer ermöglicht es Unternehmen, Sicherheitsereignisse, Netzwerkverkehr, Web-Inhalte und Messaging-Daten zu analysieren, zu melden und zu archivieren. Eine umfassende Suite von einfach anpassbaren Berichten vereinfacht die Prüfung und Dokumentation der Compliance.

Schutz – und umfassende Nutzung – von Hybrid Clouds

Hybrid Clouds geben Unternehmen neue Flexibilität. Die virtuellen und physischen Komponenten der Fortinet Security Fabric arbeiten zusammen, um die resultierende dynamische Infrastruktur zentral zu schützen und kritische Daten vom Kunden bis zur Cloud und zurück zu sichern.

[1] Chaitanya Atreya, „A Closer Look At Hybrid-Cloud And Multi-Cloud Approaches“, Forbes, 26. November 2018.

[2] Gary Thome, „Survey Says: Cost and Security are Top Hybrid Cloud Concerns“, CIO, 28. September 2018.

[3] „Fortinet Receives Recommended Rating in Latest NSS Labs NGFW Report, Delivers High SSL Performance Suited for Encrypted Cloud Access“, Fortinet, 17. Juli 2018.

[4] John Maddison, „Encrypted Traffic Reaches A New Threshold“, Network Computing, 28. November 2018.

September 10, 2019 10:46 vorm.

356355-0-1-DE

E:\PRACE\ARGOS\2019\09 2019\A-344888-924139\de-DE\Cloud\sb-secure-hybrid-cloud-A4_de-DE\sb-secure-hybrid-cloud-A4_de-DE