FORTINET

WHITEPAPER

Security für Hyperscale-Rechenzentren: Kein Buch mit 7 Siegeln

Wie sich eine bessere Performance mit leistungsstarken Netzwerk- und Sicherheitsfunktionen erreichen lässt

Zusammenfassung

Hyperscale Computing wird heute in vielen Branchen für unterschiedlichstes Anwendungsfälle eingesetzt: Großunternehmen realisieren mit hybriden IT-Architekturen ultraschnelle Übertragungen zwischen physischen und virtuellen Ressourcen, um neue Anwendungen in kürzester Zeit einzuführen. Moderne Einrichtungen der Spitzenforschung – z. B. im Bereich Gentechnik oder Luft- und Raumfahrt – nutzen Hyperscale Computing, um riesige Datenmengen in Netzwerken zu übertragen. Und E-Commerce-Unternehmen wie Online-Händler mit hohen Umsatzgeschwindigkeiten bewältigen mit Hyperscale-Architekturen sprunghaft ansteigende Verbindungszahlen (Connection Bursts) zu umsatzstarken Zeiten wie im Weihnachtsgeschäft oder stark schwankende Kundenaktivitäten während der Corona-Pandemie.

Ein Problem bei Hyperscale-Rechenzentren ist jedoch die mangelnde Sicherheit. Das liegt daran, dass die Aktivierung von Sicherheitsfunktionen oft zu Netzwerk-Engpässen führt. Schuld sind falsch segmentierte IT-Infrastrukturen oder veraltete Security-Lösungen, die mit hohen Durchsätzen nicht mithalten können. Um Engpässe durch ungeeignete Netzwerk-Firewalls zu vermeiden, umgehen viele Netzwerk-Verantwortliche die Sicherheitsfunktionen – mit verheerenden Folgen für das Unternehmen: Fehlt ein breiter Bedrohungsschutz, können Angreifer grundlegende Geschäftsfunktionen manipulieren und massiv behindern.

Deshalb erfordert der Schutz von Hyperscale-Rechenzentren eine moderne Strategie, die mit einer geeigneten Technologie umgesetzt wird.

Einleitung

Digitale Innovationen (DI) und neue Geschäftsanforderungen haben die Funktion von Rechenzentren verändert – und auch die Erwartungen an ihre Performance. Um von neuen Netzwerk-Funktionen zu profitieren, wird daher verstärkt auf das Hyperscale Computing gesetzt.

Ein Hyperscale-Rechenzentrum bietet eine effiziente Skalierbarkeit und dynamische Funktionalität, um steigende Geschäftsanforderungen zu erfüllen. Damit lassen sich extreme Kapazitäten bewältigen und eine ungeahnte Performance bereitstellen. Welche Anforderungen eine Hyperscale-Architektur erfüllen soll, hängt allerdings stark von der Branche ab:

- **Große Unternehmen (z. B. Cloud-Anbieter):** Unternehmen, die mit Virtualisierung massiv skalierbare virtuelle Netzwerke erstellen, benötigen umfangreiche Netzwerk-Segmentierungen auf VXLAN-Basis (Virtual Extensible Local Area Networks) sowie eine schnelle Kommunikation zwischen Diensten, die auf physischen und virtuellen Plattformen gemeinsam gehostet werden.
- **Dynamischer E-Commerce (z. B. Online-Händler mit hohen Umsatzgeschwindigkeiten):** Um einen sprunghaften Anstieg der Verbindungen – sogenannte „Connection Bursts“ – an umsatzstarken Tagen wie im Weihnachtsgeschäft zu bewältigen, muss eine sehr hohe Anzahl von Benutzerverbindungen pro Sekunde unterstützt werden können.[1]
- **Moderne Forschung (z. B. Pharma, Öl, Gas, Luft-/Raumfahrt):** Führende Forschungseinrichtungen arbeiten mit Big-Data- und ML-Algorithmen für maschinelles Lernen – Technologien, die eine schnelle Übertragung großer Datenmengen (auch als „Elephant Flows“ bezeichnet) mit 40 und 100 Gbit/s erfordern.[2]
- **Börsen:** Marktdaten müssen mit geringstmöglichen Latenzzeiten in elektronische Handelsinfrastrukturen gespeist werden.[3]
- **Hyperscaler (internationale Technologiekonzerne):** Ultraschnelle Verbindungen zwischen Cloud-Rechenzentren zur Datenreplizierung für DR-Standorte (Disaster Recovery) erfordern Hochgeschwindigkeitsschnittstellen und IPSec-Tunnel mit hohen Durchsätzen, um den Datenschutz zu gewährleisten und sensible Informationen zu schützen.[4]

Viele Unternehmen aus diesen Branchen haben bereits in die erforderliche Netzwerk-Infrastruktur investiert. Doch die Implementierung geeigneter Security-Lösungen für derart hohe Geschwindigkeiten ist nach wie vor ein Problem. Vorhandene Next Generation Firewalls (NGFWs) können die massiven Skalierungs- und Performance-Anforderungen von Hyperscale-Architekturen nicht erfüllen – schon gar nicht, wenn Unternehmen Millionen von Benutzerverbindungen pro Sekunde unterstützen müssen oder die Verbreitung von DDoS-Angriffen (Anti-Distributed Denial-of-Service) im Netzwerk durch eine grundlegende Layer-4-Firewall verhindern wollen. Solche Sicherheitsmaßnahmen beeinträchtigen die Netzwerk-Performance derart, dass viele Unternehmen die Security-Funktionen einfach deaktivieren. Dahinter steckt die Befürchtung, dass die Security das Netzwerk so stark ausbremst, dass der Geschäftserfolg darunter leidet und die Optimierung von Durchsätzen und Latenzzeiten verhindert. Dies ist jedoch ein gefährlicher Kompromiss: Verzichtet ein Unternehmen zugunsten schnell steigender Geschäftsanforderungen auf angemessene Security-Controls, gefährdet es damit seine gesamte Existenz – ähnlich wie beim Russisch Roulette.

Herausforderungen bei Hyperscale-Architekturen

Welche Probleme bei der Hyperscale-Security gelöst werden müssen, hängt von der Implementierungsumgebung ab.

Probleme beim Ausführen von massiv skalierbaren, virtualisierten Diensten

Unternehmen brauchen maximale Agilität bei der Einführung neuer Dienste, um die Produktivität und den Umsatz zu steigern. Für eine maximale Kapitalrendite (ROI) müssen Dienste für physische und virtuelle Ressourcen deshalb zusammenarbeiten.

Mit massiv skalierbaren Technologien wie VXLAN können Unternehmen alle virtualisierten Dienste segmentieren – in einem Umfang, der mit einem VLAN nicht möglich ist. Up- und Down-Scaling ist kein Problem: Virtualisierte Dienste können ohne nennenswerten Betriebsaufwand erweitert, eingestellt oder an anderer Stelle eingesetzt werden. Solche Dienste dienen oft für die Kommunikation mit anderen Diensten in der vorhandenen physischen Infrastruktur. Die meisten heutigen Lösungen haben jedoch Defizite bei der Performance und den Latenzzeiten und bieten nicht die nötige Layer-4-Security, um den Sitzungsstatus zu verfolgen und Zugriffsrechte von Benutzern zu kontrollieren. Auch fehlt eine bessere Layer-7-Security für die Bedrohungserkennung und Durchsetzung von Richtlinien, um Compliance-Vorgaben zu erreichen und Risiken zu kontrollieren.

Unflexible Security bei sprunghaftem Anstieg der Verbindungen

In einigen Branchen zählt nicht so sehr das übertragene Datenvolumen pro Verbindung, sondern die Gesamtzahl der Verbindungen, die ein Unternehmen in kürzester Zeit bewältigen kann. An gewissen Tagen wie dem Black Friday oder Cyber Monday sowie in saisonal umsatzstarken Zeiten wie dem Weihnachtsgeschäft verzeichnen E-Commerce-Websites innerhalb von 24 Stunden gewaltige Kundenzahlen – manchmal bis zu 1,5-mal mehr als an Einkaufstagen mit dem zweithöchsten Umsatz im Jahr.[5]

Ähnliche ereignisbasierte Spitzenwerte gibt es bei Abgabeterminen von Steuererklärungen, zu Beginn von Ticket-Verkäufen für Großveranstaltungen, an Feiertagen wie dem asiatischen Mond-Neujahrsfest oder auch beim Online-Gaming – insbesondere bei beliebten Multiplayer-Spielen oder Gaming-Turnieren mit Hunderten von Spielern, die gleichzeitige Connection Bursts von 30 Minuten verursachen können.

Mit Hyperscale-Architekturen können Online-Portale von Finanzämtern, Online-Händler und Game-Hosting-Anbieter Millionen eingehende Verbindungen pro Sekunde akzeptieren und effizient verarbeiten. Der Grund für Investitionen in Hyperscale-Architekturen liegt auf der Hand: Abgebrochene oder zu langsame Verbindungen können zu Umsatzverlusten und zur Schädigung des Marken-Images führen. Wird z. B. eine Webseite nur ein bis drei Sekunden langsamer geladen, verlassen im Durchschnitt 32 % der Besucher die Website.[6]

Große Datenflüsse im Netzwerk sind anfällig für Angriffe

Anwendungen, die mit künstlicher Intelligenz (KI) und maschinellem Lernen (ML) arbeiten, erfordern riesige Datenmengen. Oft sind mehrere Terabyte für das Training und Testen von Algorithmen notwendig.[7] Besonders Pharma-, Biotech-, Gentechnik- und Öl-/Gas-Unternehmen benötigen für die Forschung gewaltige Datenmengen, deren Verarbeitung und Analyse sich ohne effiziente Netzwerk-Übertragungen nicht realisieren lässt. Dafür sind jedoch Netzwerk-Bandbreiten von bis zu 100 Gbit/s notwendig, um schnell massive Datenvolumen (sogenannte „Elephant Flows“) zu übertragen.

Theoretisch sollten Forschungseinrichtungen diese Bandbreite über Hyperscale-Netzwerk-Architekturen mit Routern und Switchen bereitstellen können. Aber Router und Switche verfolgen weder den Sitzungsstatus noch bieten sie eine grundlegende Layer-4-Security – und sie sind anfällig für die steigende Anzahl von DDoS-Angriffen.

Darüber hinaus müssen Daten, die über diese Verbindungen übertragen werden, häufig geheim gehalten werden und unterliegen Datenschutzgesetzen wie der Datenschutz-Grundverordnung (DSGVO) der EU oder Vorschriften im Gesundheitswesen wie HIPAA, die verschiedene Zugriffskontrollen erfordern. Das bedeutet, dass der Netzwerk-Traffic über Security-Technologien wie Firewalls geleitet werden muss und der Nachrichtenfluss zu verschlüsseln ist. Die meisten NGFWs können jedoch keine Verbindungsbandbreiten von mehr als 10 Gbit/s verarbeiten. Dies verlangsamt nicht nur die Forschung erheblich, sondern verhindert auch eine maximale Kapitalrendite (ROI) mit vorhandenen WAN-Verbindungen, die extra für Datenübertragungen mit 40 Gbit/s und 100 Gbit/s angeschafft wurden. Schuld daran ist ein einziger Engpass: Die vorhandenen NGFWs können nur 10 Gbit/s unterstützen, ohne abzustürzen.

Firewall-Latenzzeiten können zu Millionenverlusten führen

Für den Börsenhandel, Gaming-Turniere und ähnliche Branchen ist eine geringe Netzwerk-Latenz äußerst wichtig. Selbst kleine Verzögerungen in der Roundtrip-Time (RTT) des Netzwerk-Verkehrs können die Rentabilität oder Performance empfindlich beeinträchtigen.

Deshalb investieren die meisten Finanzunternehmen in eine Netzwerk-Infrastruktur, die sich durch extrem geringe Latenzzeiten im Rechenzentrum auszeichnet. Beispielsweise toleriert die elektronische Handelsinfrastruktur höchstens eine Latenzzeit von 5 µs.[8] Ist die Latenz derart wichtig, entscheiden sich viele Unternehmen gegen die Sicherheit und konfigurieren NGFWs nur im Überwachungsmodus. Damit wird jedoch in Kauf genommen, dass der Netzwerk-Durchsatz nicht ausreichend geschützt ist.[9]

Hochgeschwindigkeitsverbindungen zum Rechenzentrum erfordern einen hohen IPSec-Durchsatz

Für Cloud-Anbieter und Betreiber von Content Distribution Networks (CDNs) ist entscheidend, dass sich Daten über mehrere regionale Standorte hinweg replizieren lassen. Unternehmen hosten komplette Kopien aller gespeicherten Daten auf lokalen Websites, um von einer höherer Ausfallsicherheit, geringerer Latenz bei Kundenanfragen und einer Entlastung des primären Rechenzentrums zu profitieren.

Dafür sind DCIs (Data Center Interconnects) notwendig – Verbindungen mit hoher Bandbreite zwischen regionalen Standorten, die die Synchronisierung des Netzwerks unterstützen.[10] Da Cloud-Anbieter und CDNs häufig vertrauliche oder proprietäre Daten übertragen, werden diese Verbindungen oft als IPSec-Tunnel implementiert. Gleichzeitig erfordert die Layer-4-Netzwerk-Security, dass NGFWs den IPSec-Traffic mit demselben Durchsatz wie die Netzwerk-Verbindungen verarbeiten können. Da die meisten vorhandenen NGFWs jedoch keinen IPSec-Durchsatz von mehr als 10 Gbit/s erreichen, kann der NGFW-Schutz dieser Verbindungen die Gesamtübertragung großer Datenmengen zwischen Rechenzentren verlangsamen.

Fazit

DI-Initiativen zur Verbesserung der Effizienz und der Kundenerfahrung erfordern eine Weiterentwicklung der Netzwerk-Infrastruktur. Hyperscale-Rechenzentren sind speziell für die Unterstützung massiver Netzwerk-Datenflüsse, sprunghafter Verbindungsanstiege (Connection Bursts) und zahlreiche andere Anwendungsfälle ausgelegt.

Obwohl viele Unternehmen eine Hyperscale-Netzwerk-Architektur implementiert haben, bleibt die Hyperscale-Security eine größere Herausforderung. Werden NGFWs komplett ausgeschaltet oder nur im Überwachungsmodus betrieben, um Netzwerk-Engpässe zu vermeiden, wird das Unternehmen anfällig für Angriffe und kann womöglich Datenschutzbestimmungen nicht mehr erfüllen. Werden Anwendungen und IT-Infrastruktur nicht segmentiert, kann ein erfolgreicher Angreifer vom Netzwerk-Rand aus auf das gesamte Netzwerk zugreifen. Diese gefährlichen Folgen potenzieren sich um ein Vielfaches, wenn Angriffe von internen und vertrauenswürdigen Benutzern ausgehen.

Hyperscale-Rechenzentren erfordern einen radikalen Ansatz bei Sicherheitslösungen, damit die Security jederzeit mit schnell steigenden Geschäftsanforderungen mithalten kann. Eine Hyperscale-Sicherheitslösung muss für eine sehr große Anzahl Benutzerverbindungen skalierbar sein sowie mehrere Millionen Verbindungen pro Sekunde verarbeiten, gewaltige Datenmengen mit 100 Gbit/s übertragen, große virtuelle Umgebungen effizient segmentieren, den Netzwerk-Rand mit einer leistungsstarken, grundlegenden Layer-4-Security schützen und DDoS-Angriffe verhindern können. Kann die Hyperscale-Security diese Anforderungen nicht erfüllen, bleiben Angreifer im Vorteil und können mit unterschiedlichsten Cyber-Attacken Geschäftsprozesse empfindlich stören, den guten Ruf des Unternehmens schädigen oder schlimmstenfalls den gesamten Betrieb zum Erliegen bringen.

1 Marisa Sanfilippo: „The Best Days for Holiday Sales: A Guide for Businesses“. Business News Daily, 2. Dezember 2019.

2 Rajiv Kohli und Nigel P. Melville: „Digital innovation: A review and synthesis“. Information Systems Journal, 29. Januar 2018.

3 „Deterministic Communications for Secure High-speed Performance: Fortinet Protects Connections to Electronic Trading Platforms with the Industry's Lowest Latency and Jitter Rates“. Fortinet, 23. September 2019.

4 „What is DCI?“ Ciena, 16. Mai 2019.

5 Marisa Sanfilippo: „The Best Days for Holiday Sales: A Guide for Businesses“. Business News Daily, 2. Dezember 2019.

6 „Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed“. Google, März 2017.

7 Mohammad Shaikh und Harsha Gurukar: „Machine Learning and HPC in Pharma Research and Development“. Super Computing 2019, November 2019.

8 „Deterministic Communications for Secure High-speed Performance: Fortinet Protects Connections to Electronic Trading Platforms with the Industry's Lowest Latency and Jitter Rates“. Fortinet, 23. September 2019.

9 Jason Pappalexis: „The NGFW Today: A Staple of Network Security in Spite of Challenges“. NSS Labs, 11. März 2019.

10 „What is DCI?“ Ciena, 16. Mai 2019.

FORTINET

www.fortinet.com/de

7. Dezember 2020, 14:20 Uhr

744553-A-1-DE