FORTINET

WHITEPAPER

Hindernisse bei der WAN-Transformation verstehen

Security, Performance und Gesamtbetriebskosten (TCO)

Zusammenfassung

Netzwerk-Verantwortliche entscheiden sich zunehmend für SD-WANs (Software-Defined Wide Area Networks), um den Anstieg beim Datenverkehr und die zunehmende Fülle neuer Anwendungen zu unterstützen, die die digitale Transformation (DX) mit sich bringt. Diese Anwendungen steigern die Mitarbeiterproduktivität und eröffnen neue Geschäftschancen, verändern aber auch die Netzwerk- und Sicherheitsanforderungen eines Unternehmens.

Als Reaktion überdenken viele Unternehmen herkömmliche WAN-Architekturen und entscheiden sich für ein SD-WAN. Jedoch gehen mit vielen SD-WAN-Implementierungen auch große Herausforderungen einher – von unzureichender Sicherheit bis hin zu hohen Gesamtbetriebskosten (TCO). Das Verständnis dieser Probleme ist entscheidend, um sich in dem zunehmend komplexen Markt für WAN-Edge-Technologien zurechtzufinden.

IDC rechnet bis 2022 beim SD-WAN-Markt mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von über 40 %.[1]

„Das Aufkommen der SD-WAN-Technologie war eine der schnellsten Transformationen in der Branche seit Jahren. Unternehmen jeder Größe modernisieren ihre WANs, um eine bessere Nutzererfahrung für zahlreiche Cloud-Anwendungen zu bieten.“[2]

– Rohit Mehra
VP, Network Infrastructure
IDC

Wie sich die digitale Transformation (DX) auf Unternehmensnetzwerke auswirkt

Unternehmen setzen mit breit gefächerten DX-Initiativen verstärkt auf die digitale Transformation – von der zunehmenden Verbreitung von Videokonferenzen und Voice-over-IP (VoIP) für die Zusammenarbeit, das Projektmanagement und die Geschäftsentwicklung bis hin zur schnelleren Bereitstellung neuer Web-Anwendungen durch DevOps-Teams und den Einsatz von IoT-Geräten (Internet der Dinge) zur Datenerfassung und Sammlung von Telemetriedaten.

Für Filialen und Niederlassungen bringen diese DX-Initiativen jedoch neue Herausforderungen mit sich. Netzwerk-Verantwortliche müssen eine verlässliche Performance und Security gewährleisten – vom Rechenzentrum auf dem Unternehmensgelände bis hin zum Netzwerk-Rand. Das Problem ist jedoch, dass herkömmliche WANs (Wide Area Networks) nicht für das hohe Traffic-Volumen und die schnellen Übertragungen ausgelegt sind, die eine sinnvolle Einbindung von Filialen erfordert. Das liegt daran, dass klassische WAN-Lösungen ein MPLS-basiertes Netzwerk (Multiprotocol Label Switching) verwenden, bei dem der gesamte Netzwerk-Traffic zum Filtern und für Sicherheitsprüfungen zurück an das zentrale Rechenzentrum des Unternehmens geht. Diese „Hub-and-Spoke“-Architektur führt schnell zu Engpässen am Netzwerk-Rand, wodurch Netzwerk-Verbindungen von Endanwendern als quälend langsam empfunden werden.

Dies ist jedoch nicht das einzige Problem mit herkömmlichen WAN-Lösungen. Zudem sind MPLS-Verbindungen teuer und werden schnell zur Kostenspirale – insbesondere, wenn das Traffic-Aufkommen von Filialen rasch wächst.

Typische Probleme mit herkömmlichen WANs

Infolgedessen setzen viele Unternehmen auf SD-WANs, um eine bessere Netzwerk-Performance zu erzielen. Doch angesichts der Fülle an SD-WAN-Angeboten auf dem Markt mit unterschiedlichstem Funktionsumfang lässt sich oft nur schwer beurteilen, welche Lösung die wichtigsten Geschäftsanforderungen erfüllt. Bevor Netzwerk-Verantwortliche die verfügbaren Optionen bewerten können, müssen zuerst die Anforderungen des Unternehmens an ein SD-WAN geklärt werden.

Unzureichende Sicherheit: Kein umfassender Bedrohungsschutz

Trotz des langsamen Durchsatzes, wenn ein WAN den gesamten Traffic durch das Rechenzentrum leitet, gelten MPLS-basierte WANs im Allgemeinen als ausreichend sicher. Im Gegensatz dazu ist bei vielen SD-WAN-Lösungen die erweiterte Sicherheit nicht oder nur unzureichend integriert: So decken die Sicherheitsfunktionen der meisten SD-WAN-Lösungen nicht die gesamte erweiterte Security von Layer 3 bis Layer 7 ab, da es weder eine integrierte IPS-Technologie (Intrusion Prevention System) noch einen Web-Filter oder die Überprüfung von verschlüsselten Übertragungen per SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) gibt.

Um diese Sicherheitsanforderungen in Filial- und Remote-Netzwerken zu erfüllen, müssen Netzwerk-Verantwortliche dedizierte Security-Appliances in das SD-WAN integrieren. In der Praxis bedeutet das mindestens eine Firewall pro Standort – manchmal aber auch mehr (da nicht jede Firewall auf dem Markt eine SSL/TLS-Inspektion bietet). Das erhöht nicht nur die Komplexität, sondern auch die Gesamtbetriebskosten (TCO) – angefangen bei den Investitionskosten für die zusätzliche Appliance bis hin zu den höheren Betriebskosten, da das IT-Team durch das Management einer zusätzlichen Firewall und weiterer Geräte zeitlich stärker belastet wird.

Aber auch SD-WAN-Lösungen mit modernen Technologien können Sicherheitslücken aufweisen. Beispielsweise bietet nicht jede SD-WAN-Lösung Sicherheitsfunktionen, die von unabhängigen Experten wie den NSS Labs gründlich überprüft wurden. Dieser objektive Vergleich ist jedoch notwendig, um zu wissen, welche SD-WAN-Lösungen die Geschäftsanforderungen am besten erfüllen.

Kompromiss zwischen Leistung und Sicherheit

Die direkte Connectivity und die Lastverteilung von SD-WAN-Lösungen bringen eine höhere Leistung verglichen mit herkömmlichen WANs. Aber genau wie bei der Security ist dies ein weiterer Bereich, in dem sich SD-WAN-Lösungen stark unterscheiden. So kann nicht jede SD-WAN-Lösung den Traffic pro Anwendung erkennen und klassifizieren oder detaillierte Routing-Richtlinien durchsetzen. Eine Priorisierung bestimmter Anwendungen ist somit unmöglich. Unter einer „Pauschallösung“ für den gesamten Datenverkehr von Applikationen leidet dann die Performance kritischer Anwendungen – wie VoIP oder Videokonferenzen – und damit die Produktivität der Endanwender.

Weiter gibt es SD-WAN-Lösungen mit integrierter Security, bei denen einige Sicherheitseinstellungen zu Lasten der Netzwerkleistung gehen. Beispielsweise kann das Aktivieren einer tiefgehenden Inspektion von verschlüsseltem SSL/TLS-Traffic den Durchsatz erheblich drücken. Andererseits sind Unternehmen, die diese Option deaktivieren, einem erhöhten Risiko ausgesetzt: Heutzutage werden 72 % des Netzwerk-Traffics verschlüsselt übertragen – und 60 % der Angriffe gehen auf Malware zurück, die versteckt in verschlüsselten SSL- und TLS-Paketen ins Unternehmensnetzwerk gelangte.[4]

Kosten und Ressourcen: Anhaltend hohe Gesamtbetriebskosten (TCO)

Durch den dramatischen Anstieg bei Volumen und Geschwindigkeit des Netzwerk-Traffics – bedingt durch VoIP-, Video- und SaaS-Anwendungen – explodieren die Bandbreitenkosten vieler Unternehmen. Angesichts der um das Vier- oder Fünffache steigenden MPLS-Kosten eröffnet ein SD-WAN erhebliche die Kosteneinsparungen, da hier der Datenverkehr über das öffentliche Internet läuft.

Trotzdem sind führende Netzwerk-Verantwortliche nach der SD-WAN-Implementierung oft überrascht, wenn die Gesamtbetriebskosten (TCO) höher als erwartet ausfallen. Insbesondere das Hinzufügen mehrerer Appliances für verschiedene Funktionen erhöht die Investitions- und Betriebskosten. Denn hierdurch steigt der administrative Aufwand für Netzwerk-Teams, da Protokollinformationen für das Bedrohungsmanagement manuell überwacht und kompiliert werden müssen. Das ist nicht nur zeitaufwändig, sondern auch äußerst ineffizient.

„72 % der Befragten [basierend auf einer Gartner-Umfrage] gaben an, dass ihnen die WAN-Sicherheit die größten Sorgen bereitet.“[3]

Viele Unternehmen, die auf ein SD-WAN umsteigen, erzielen erhebliche Einsparungen bei der Bandbreiten-Connectivity – in einigen Fällen bis zu 40 %.[5]

72 % des Netzwerk-Traffics wird verschlüsselt – und 60 % der Angriffe nutzen diese Verschlüsselung aus.

Die Gesamtbetriebskosten (TCO) für SD-WAN-Lösungen betragen umgerechnet 4,6–458 € pro Mbit/s. Unternehmen sollten die kurz- und langfristigen Gesamtbetriebskosten der ins Auge gefassten SD-WAN-Lösung sorgfältig prüfen, um zu wissen, welche Lösung die meisten Funktionen zu den geringsten Gesamtbetriebskosten bietet.[6]

Die Bereitstellung mehrerer Einzelprodukte für jedes Remote-Büro und jede Filiale – von Routern, Firewalls und Security-Web-Gateways bis hin zur WAN-Optimierung – ist für das IT-Team mit einem erheblichen Management-Aufwand verbunden, da jedes dieser Geräte mit eigenen Protokollen und Benutzerschnittstellen arbeitet. Transparenz, eine zentralisierte Kontrolle und die Einhaltung verschiedener behördlicher Vorgaben und Branchenvorschriften sowie der Nachweis von Sicherheitsstandards lassen sich nur mit gewaltigem Zeitaufwand erreichen, weil Netzwerk-Teams sämtliche Daten manuell aus Einzelgeräten abrufen und abgleichen müssen. Angesichts des Fachkräftemangels kann dies sehr kostspielig werden, da technische und operative Netzwerk-Teams sich um eine personelle Aufstockung bemühen werden, um diese Anforderungen zu erfüllen.

Ineffizienzen treten in verteilten Netzwerken auf, in denen für das Management von Netzwerk- und Sicherheitslösungen Mitarbeiter an entfernte Standorte reisen müssen. Insbesondere wenn SD-WAN-Lösungen weder eine virtuelle Alternative noch eine Zero-Touch-Bereitstellung bieten, können die Installation, Implementierung und laufende Wartung schnell einen enormen Zeitaufwand verursachen.

Fazit: Worauf man bei einer SD-WAN-Lösung achten sollte

Bei der Bewertung des großen Angebots an SD-WAN-Lösungen sollten Netzwerk-Verantwortliche sich zu jeder enger ins Auge gefassten Lösung folgende Fragen stellen:

- Welche Ergebnisse zeigen die Praxistests von unabhängigen Dritten wie den NSS Labs?
- Wie wurde die Lösung in Analystenberichten von Drittanbietern wie dem Gartner-Magic-Quadrant bewertet?
- Angenommen, die Lösung bietet eine integrierte Security: Gehören dazu auch erweiterte Funktionen wie Sicherheitskontrollen auf Layer 3 bis 7: 1) IPS, 2) Web-Filter und 3) tiefgehende Überprüfung des SSL/TLS-verschlüsselten Traffics?
- Sollte die Lösung eine SSL/TLS-Inspektion haben: Welche Leistungseinbußen treten auf, wenn diese Option aktiviert wird?
- Ist die Lösung anwendungsbezogen und verwendet sie automatisierte Pfadinformationen für das optimierte Routing und die Priorisierung geschäftskritischer SaaS-Anwendungen, VoIP-Anrufe und Videos? Kann die Lösung in unternehmensweite Sicherheitselemente und in verschiedene Security-Bereiche (z. B. E-Mail, Cloud, Endpunkte) für die integrierte und automatisierte Weitergabe von Bedrohungsinformationen eingebunden werden?

[1] „SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022“. IDC, 7. August 2018.

[2] Ibid.

[3] Naresh Singh: „Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth“. Gartner, 12. November 2018.

[4] John Maddison: „More Encrypted Traffic Than Ever“. Fortinet Blog, 10. Dezember 2018; Omar Yaacoubi: „The hidden threat in GDPR's encryption push“. PrivSec Report, 8. Januar 2019.

[5] Paul Ruelas: „Catching the SD-WAN wave: the cost savings hype and MPLS misconceptions need more explanation“. Network World, 18. April 2018.

[6] Thomas Skybakmoen: „SD-WAN Comparative Report“. NSS Labs, 8. August 2018.

FORTINET

www.fortinet.com/de

5. Mai 2020, 15:41 Uhr

376872-0-1-DE