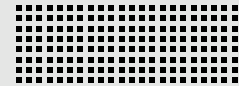


TIPPS VON FORTINET

Versteckte LAN-Kosten vermeiden: Bestehen Sie auf Einfachheit bei Betrieb und Lizenzierung



Zusammenfassung

LANs und Wireless LANs bilden das IT-Kernnetzwerk und ermöglichen Next-Gen-Anwendungen und mehr Produktivität. Wie gut diese kabelgebundenen und drahtlosen Netzwerke funktionieren, hat entscheidenden Einfluss auf die Benutzererfahrung – und auch auf die Sicherheit.

Heutige IT-Administratoren müssen Next-Gen-Netzwerke mit Schwerpunkt auf eine sichere, nahtlose Nutzererfahrung gestalten. Zwar gehören Ethernet-Switching und Wi-Fi zu den ausgereiftesten Technologien im IT-Markt, aber mit den wachsenden Netzwerk-Anforderungen sind auch die versteckten Kosten durch die „Tricks unter der Haube“ gestiegen, mit denen viele Anbieter ihre Kerntechnologien am Laufen halten.

Trends, die die Betriebskosten erhöhen

Das Multivendor-Problem: Komplexität durch mehrere Anbieter

Es gibt viele Gründe, warum Unternehmen für LANs und Wireless LANs unterschiedliche Anbieter kombinieren. Upgrade-Zyklen, Vertrautheit mit bestimmten Lösungen, neue Entscheidungsträger im Management, veränderte Anbietervorlieben, Kostengründe oder auch die Lieferbarkeit können zu einem Mix vieler unterschiedlicher Einzelprodukte führen. Das Ergebnis ist jedoch immer das gleiche: Multivendor-LANs verursachen zusätzliche Komplexität und damit tendenziell höhere Betriebskosten.

Da jeder Anbieter eigene Schnittstellen hat, ist die Problembeseitigung für IT-Teams extrem arbeitsaufwendig. Ständig muss zwischen diversen Einzelprodukten hin- und hergewechselt werden, um die eigentliche Fehlerursache zu finden. Dazu kommt die zeitraubende Kommunikation mit den einzelnen Support-Teams jedes Anbieters, die meistens kein Interesse an der Zusammenarbeit mit einem fremden Support haben. Dieser begrenzte Informationsaustausch erschwert rückblickende Problemanalysen zusätzlich.

Zu viele Lizenzen

Die Grundelemente eines LANs sind Ethernet-Switches und Wireless Access Points (AP). Noch vor geraumer Zeit fielen für die meisten LAN- und Wireless-LAN-Komponenten lediglich Investitionskosten an: Ein Ethernet-Switch wurde gekauft und vielleicht kam noch ein Supportvertrag zu den Hardware-Kosten hinzu. Ähnlich verhielt es sich bei Wireless APs, bis Wireless-LAN-Controller (WLC) auf den Markt kamen. Nun wurden Lizenzen pro Access Point erstellt, häufig gebündelt mit den WLC-Kosten. In beiden Fällen konnte ein IT-Administrator aber dennoch die Ausgaben für die Wireless-LAN-Lösung als anfängliche Investitionskosten budgetieren.

„78 % der IT-Entscheidungsträger gaben an, dass sie lieber auf eine einzige Marke für Netzwerk-Hardware standardisieren würden, statt Lösungen von mehreren Anbietern zu kombinieren.“¹

Heutzutage müssen sich IT-Administratoren bei LAN- und Wireless-LAN-Geräten (und deren Management) in einem wahren Dschungel aus Lizenzen und Abonnementgebühren zurechtfinden. Diese Lizenzen und Lizenzgebühren können für so grundlegende Dinge wie das Betriebssystem oder sehr komplexe Features wie Transparenz über Anwendungen anfallen. Es ist mittlerweile üblich, dass eine Bestellung für ein kleines Niederlassungsnetzwerk mehrere Seiten mit schwer verständlichen Lizenzbedingungen für Funktionen umfasst, die früher beim Kauf der Hardware inbegriffen waren. Auch diese Entwicklung trägt zu erheblich höheren Betriebskosten bei.

„69 % der Unternehmen haben mehr IoT-Geräte als Computer in ihren Netzwerken.“²

Drei vermeidbare Fehler bei der Lizenzierung

Management

Die meisten Wireless LANs und LANs werden heute über die Cloud verwaltet. Das hat den großen Vorteil, dass das Wireless-LAN- und LAN-Management überall und jederzeit erledigt werden kann. Ein echter Effizienzgewinn – wären da nicht die oft undurchsichtigen, teuren Abonnementlizenzen.

Kosten und Funktionsumfang dieser Lizenzen variieren zwar, aber in einigen Fällen kann die angeschaffte Hardware ohne die Lizenz gar nicht verwendet werden. Unser Tipp: Sehen Sie sich vor einer Investition in eine Cloud-Management-Lösung die Lizenzbedingungen genau an, damit sich die Betriebskosten später in Grenzen halten. Wichtig ist auch, dass ein Anbieter On-Premises-Optionen vorsieht, sollte das IT-Team die Cloud weniger oder nicht mehr nutzen wollen – und zwar ohne Vertragsstrafen.

Endpunkt-Transparenz

Es ist schwierig, ein Netzwerk zu verwalten, ohne alle bestehenden Verbindungen zum Netzwerk zu kennen. Authentifizierungssysteme können IT-Administratoren mitteilen, welche Benutzer sich im Netzwerk befinden, aber nicht welche Geräte. Also muss das IT-Team Letzteres manuell herausfinden – ein zeitaufwendiger und fehleranfälliger Prozess, der hohe laufende Kosten verursacht. Viele Anbieter benötigen eine Lizenz und/oder ein Abonnement für eine transparente Endpunkt-Überwachung, die oft nicht einmal ein sicheres Onboarding (das Einbinden der Geräte im Netzwerk) umfasst. Solche grundlegenden Funktionen sollten eigentlich inbegriffen sein und nichts extra kosten.

Security

Viele Sicherheitsvorfälle beginnen am LAN- und Wireless-LAN-Edge – also am Netzwerk-Rand bei den Verbindungen, über die Anwender und Geräte auf das Unternehmensnetzwerk zugreifen. Bei vielen LAN- und Wireless-LAN-Lösungen fehlt jedoch eine integrierte Security, die dann später ergänzt werden muss. Das wiederum führt zu noch mehr Komplexität durch isolierte Funktionen und schwächt die Sicherheitseffektivität. Auch kostet dieser Verzicht auf integrierte Sicherheitsfunktionen die für das LAN zuständigen IT- und Security-Teams erheblich mehr Zeit bei der Problemerkennung und -behebung. Bei Sicherheitsvorfällen können die Betriebskosten dann erheblich steigen – und oft kann ein Angriff wegen der langsamen Abwehrreaktion mehr Schaden verursachen.

So finden Sie die richtige integrierte LAN-Edge-Lösung

Klassische LAN-Lösungen, bei denen die Hardware die Hauptkosten ausmachen (und nicht die Abonnement-Lizenzen) gibt es weiterhin. Unser Tipp: Suchen Sie nach Anbietern, bei denen wichtige Grundfunktionen inklusive sind und nicht extra zugekauft werden müssen. Eine gute LAN-Edge-Lösung sollte mindestens Folgendes bieten:

- einheitliches Management für LAN und Wireless LAN, das On-Premises und über die Cloud möglich ist
- Hardware, die auch nach Ablauf einer Lizenz funktioniert
- intelligente Funktionen, die erkennen, was mit dem LAN verbunden ist, und Maßnahmen gegen unautorisierte Geräte ergreifen können
- integrierte, wirksame Sicherheit

Um die LAN-Edge-Bereitstellung und -Verwaltung zu vereinfachen und die niedrigsten Gesamtbetriebskosten zu erzielen, muss eine Lösung Netzwerk- und Sicherheitsfunktionen zusammenführen. Unternehmen erhalten damit eine sichere, einfach zu verwaltende Architektur mit allen notwendigen Funktionen, die nicht nur die Betriebskosten senkt, sondern auch die Performance verbessert.

¹ „Networking Technology Trends in 2020 and Beyond“. Spiceworks Ziff Davis, abgerufen am 1. Februar 2022.

² „How Prepared Is Your IT Department for Attacks on IoT Devices?“. Virginia Business Systems, abgerufen am 1. Februar 2022.