SONICWALL

KURZDARSTELLUNG: SCHUTZ FÜR DIE NÄCHSTE WIRELESS-WELLE

Zusammenfassung

In der mobilen, globalen Wirtschaft ist Wireless-Konnektivität eine Selbstverständlichkeit. Wohin man auch schaut, drahtlose Geräte sind heute überall präsent – angefangen bei Smartphones und Laptops bis hin zu Sicherheitskameras und Virtual Reality-Headsets. Erfolgreiche Unternehmen müssen sich heute darüber Gedanken machen, wie sie eine hohe Qualität, Performance und Sicherheit für ihre drahtlosen Netzwerke und Endpunkte bereitstellen können.

Die neue Wireless-Welt

Drahtlose Highspeed-Verbindungen sind in der heutigen Welt kein Nice-to-have mehr, sondern eine Notwendigkeit. Sie ermöglichen es Unternehmen, ihren Kunden einen höheren Mehrwert zu bieten und die Produktivität ihrer Mitarbeiter mit BYOD-Initiativen und dem zunehmenden Einsatz bandbreitenintensiver Apps zu verbessern. Andere Organisationen wie Schulen und Universitäten nutzen WLAN, um ihren Schülern und Studenten eine besser vernetzte Bildungsumgebung zu bieten. Und Anwender erwarten drahtlose Konnektivität unabhängig von Standort oder Gerätetyp. Hinzu kommt, dass am Arbeitsplatz, im Unterricht, in Krankenhäusern und im täglichen Leben immer mehr Geräte eingesetzt werden, die nur noch drahtlos funktionieren.

Wireless-IoT

Diese Entwicklung wird von mehreren entscheidenden Faktoren vorangetrieben. Erstens sind sowohl private als auch von der IT bereitgestellte WLAN-fähige Geräte weiterhin auf dem Vormarsch. Laut ABI Research werden zwischen 2016 und 2021 voraussichtlich über 20 Milliarden WLAN-Chipsätze ausgeliefert. Außerdem geht man davon aus, dass über 95 % der 2021 ausgelieferten Geräte 5 GHz unterstützen. Zweitens wächst das Internet der Dinge (Internet of Things, IoT) ständig weiter, da Geräte, die man bisher nicht mit drahtloser Konnektivität in Verbindung gebracht hatte wie Autos, Smart Home-Geräte (z. B. Kühlschränke, Sicherheitskameras) etc. sich jetzt per WLAN mit dem Internet verbinden können. Mehrere Analystenhäuser haben vorausgesagt, dass es bis 2020 50 Milliarden IoT-Geräte geben wird.

Drittens wächst nicht nur die Zahl der WLAN-fähigen Geräte, sondern auch der Einsatz zunehmend im Netzwerk gehosteter, bandbreitenintensiver Anwendungen wie HD Multimedia, Cloud- und Mobil-Apps. Und schließlich konnte sich der neueste Wireless-Standard 802.11ac Wave 2 gut etablieren, da immer mehr Anwender von den Multi-Gigabit-Wireless-Geschwindigkeiten profitieren möchten. All dies zeigt: Organisationen müssen einen Weg finden, Kunden, Mitarbeitern sowie Schülern und Studenten eine Highspeed-Wireless-Lösung zu bieten, die das Benutzererlebnis deutlich verbessert.

Zuhause im Unternehmen

Laut Wi-Fi Alliance wird das Zuhause immer mehr zu einem Firmennetzwerk. Das liegt vor allem an den alltäglichen vernetzten Geräten, persönlichen Assistenten und kabellosen Virtual Reality-Gadgets. WLAN ist nicht nur im Alltag der Benutzer angekommen, sondern auch bei Unternehmen wie Amazon, Facebook, Netflix und großen Fluggesellschaften. Diese setzen bei täglichen Prozessen wie Versand am gleichen Tag, mobilem Zugriff auf soziale Medien, Streaming Media-Services und sogar pünktlichen Abflügen auf WLAN. Und mit der Einführung neuer Standards und Protokolle wird sich das WLAN zweifellos noch weiterentwickeln und verbessern.

Drahtlose Servicequalität

Für Netzwerkumgebungen ist nicht nur die Geschwindigkeit wichtig, sondern auch die Qualität der drahtlosen Verbindung in Umgebungen mit hoher Dichte wie Außenbereiche, in denen raue Bedingungen herrschen können. Häufig verbinden sich mehrere Geräte mit dem gleichen Access Point und konkurrieren um Bandbreite. Dieser „Gerätestau“ verursacht Interferenzen, die zu einer Verschlechterung der Signalqualität und letztendlich zu schlechter Performance führen können. Zusätzliche Faktoren wie physische Objekte (z. B. Gebäude, Mauern, Bäume) und weitere Geräte, die den gleichen Kanal oder die gleiche Frequenz nutzen (z. B. Mikrowellengeräte, kabellose Telefone), können die Funkstrecke stören und so das WLAN-Signal beeinträchtigen. All diese Faktoren können sich negativ auf Anwendungen wie Video-Streaming auswirken, wenn Datenpakete zeitverzögert übertragen werden und die Bildqualität schlecht bzw. die Videoübertragung langsam ist, weil zwischengespeichert werden muss.

Eine wachsende Bedrohung für die Sicherheit

Gleichzeitig muss der drahtlose Verkehr vor bösartigen Bedrohungen und Internetschwachstellen geschützt werden. Viele der heute erhältlichen Wireless-Netzwerkprodukte bieten Schutz vor unberechtigten Access-Points oder Access Point Mapping, damit Eindringlinge nicht ins Netzwerk gelangen und auf kritische Ressourcen zugreifen können. Häufig bieten sie jedoch keine Deep Packet Inspection-Prüfung von verschlüsseltem Verkehr im WLAN, sodass sie für Organisationen ein Sicherheitsrisiko darstellen. Darüber hinaus fehlen diesen Produkten oft zusätzliche Sicherheitsfeatures wie Erkennung unberechtigter Access Points und Funktionen, um den externen und den internen Benutzerzugriff zu trennen. Neben diesen Sicherheitsrisiken gestalten sich Implementierung, Überwachung und Verwaltung meist recht zeitaufwändig. Darüber hinaus enthalten diese Produkte nicht immer Supportfeatures zur automatischen Konfiguration und zentralisierten Verwaltung, die für die Erstellung und Wartung einer umfangreichen Wireless-Netzwerkinfrastruktur wichtig sind.

Fazit

Organisationen erwarten heute mehr von ihrem Wireless-Netzwerk als nur eine schnelle Verbindung. Sie brauchen eine Lösung, die mehr Durchsatz, eine höhere Signalqualität und eine verbesserte Benutzererfahrung für die vielen drahtlosen Clients in extrem dichten Umgebungen. Darüber hinaus muss die Lösung in der Lage sein, verschlüsselte wie unverschlüsselte Bedrohungen im Wireless-Verkehr aufzuspüren und zu beseitigen, um das Netzwerk zu schützen und gleichzeitig die Implementierung und laufende Verwaltung zu vereinfachen.

Erfahren Sie mehr. Besuchen Sie www.sonicwall.com/en-us/products/firewalls/wireless-security.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, Kalifornien 95035, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com