GARANTIRE LA SICUREZZA NELLE NUOVE COMUNICAZIONI WIRELESS

Abstract

Nell'economia mobile e globale di oggi la connettività senza fili è onnipresente. Smartphone, laptop, telecamere di sicurezza e headset per la realtà virtuale sono tutti dispositivi wireless. Le aziende devono riconoscere e soddisfare le proprie esigenze in termini di alta qualità, elevate prestazioni e sicurezza tra diverse reti wireless e molteplici endpoint.

Fare business oggi in un mondo wireless

La connettività wireless ad alta velocità non è più un optional per le reti informatiche di oggi. È divenuta una necessità, ora che le imprese puntano ad aumentare il valore offerto alla clientela e la produttività dei dipendenti tramite misure di BYOD, e considerando l'uso crescente di app ad alto consumo di banda. Altre organizzazioni come gli istituti scolastici e universitari usano la tecnologia wireless per fornire agli studenti un ambiente di apprendimento più connesso. L'utente, dal canto suo, si aspetta di poter usufruire della connettività wireless indipendentemente dal luogo in cui si trova e dal dispositivo che utilizza. Inoltre cresce la tendenza a utilizzare dispositivi "wireless only" sul luogo di lavoro, nelle aule didattiche, negli ospedali e nella vita di tutti i giorni.

L'IoT wireless

Diversi fattori chiave sono alla base di questa evoluzione. Innanzitutto la continua proliferazione di dispositivi che supportano il Wi-Fi, sia personali che forniti dall'IT aziendale. Secondo ABI Research, tra il 2016 e il 2021 verranno prodotti più di 20 miliardi di chipset Wi-Fi, e oltre il 95% dei device messi in commercio nel 2021 dovrebbe supportare i 5 GHz. In secondo luogo, anche l'Internet delle cose (IoT) ha preso piede. Dispositivi finora ritenuti non capaci di un funzionamento wireless, come le automobili o gli apparecchi domestici intelligenti (ad es. frigoriferi, telecamere di sicurezza, ecc.), sono ora in grado di connettersi a Internet in modalità wireless. Diverse società di analisi hanno previsto che entro il 2020 ci saranno 50 miliardi di dispositivi IoT.

In terzo luogo, la diffusione di apparecchi dotati di Wi-Fi è accompagnata dall'uso di applicazioni ad alto consumo di banda, come servizi multimediali in alta definizione e app per dispositivi mobili e il cloud, che sono sempre più spesso ospitate in rete. Infine lo standard wireless più recente, l'802.11ac Wave 2, ha ormai raggiunto una vastissima diffusione, con gli utenti in attesa di poter utilizzare il wireless con velocità multi-gigabit. La combinazione di questi elementi mette aziende e organizzazioni nella condizione di dover fornire a clienti, collaboratori e studenti una soluzione wireless ad alta velocità che offra loro una migliore esperienza d'uso.

A casa come in azienda

Secondo Wi-Fi Alliance, anche l'ambiente domestico sta assumendo le caratteristiche di una rete aziendale. Ciò è dovuto principalmente alla comparsa di oggetti d'uso quotidiano connessi, assistenti personali e dispositivi cordless per la realtà virtuale. L'impatto del Wi-Fi è percepibile nella vita di tutti i giorni non solo dagli utenti, ma anche da aziende come Amazon, Facebook, Netflix e le grandi compagnie aeree. Anch'esse dipendono dal Wi-Fi per svolgere operazioni quotidiane quali spedizioni con consegna in giornata, accesso mobile ai social media, gestione di servizi di streaming multimediale e per garantire la partenza puntuale dei voli aerei. Con l'introduzione di nuovi standard e protocolli, il Wi-Fi è destinato a evolversi e potenziarsi ulteriormente.

Assicurare la qualità del servizio wireless

La velocità è sempre importante su qualsiasi rete, ma anche la qualità della connessione wireless in ambienti ad alta densità, compresi i luoghi esterni con condizioni talvolta difficili, è altrettanto importante. In molti casi più dispositivi si connettono allo stesso punto di accesso e competono per la larghezza di banda. Questa "congestione di dispositivi" causa interferenze, con possibili effetti negativi come un peggioramento del segnale e modeste prestazioni. Ulteriori fattori come gli oggetti fisici (edifici, pareti, alberi) e altri apparecchi che condividono la stessa frequenza o canale (microonde, telefoni cordless) possono interferire con il segnale wireless, ostacolando la trasmissione della radiofrequenza. Tutto questo può ripercuotersi su applicazioni come lo streaming video, che possono peggiorare in caso di trasmissione ritardata di pacchetti di dati e scarsa qualità delle immagini o subire un rallentamento dei filmati a causa del buffering.

Una minaccia crescente per la sicurezza

Alla base di tutto questo vi è la necessità di proteggere il traffico wireless dalle minacce e dalle vulnerabilità di Internet. Molti degli attuali prodotti wireless connessi in rete offrono protezione da attività come i punti di accesso non autorizzati o la mappatura degli access point, per impedire a utenti non autorizzati di accedere alla rete e quindi a risorse critiche. Questi prodotti, però, spesso non consentono una scansione DPI del traffico crittografato nella LAN wireless ed espongono quindi le organizzazioni a rischi. Inoltre potrebbero non disporre di funzionalità di sicurezza aggiuntive come il rilevamento di punti di accesso rogue o la capacità di segmentare gli accessi degli utenti esterni da quelli interni. Oltre ai rischi in termini di sicurezza, questi prodotti possono richiedere molto tempo per l'implementazione, il monitoraggio e la gestione. A volte sono privi di funzioni di supporto per l'auto-configurazione e la gestione centralizzata, funzioni che risultano essenziali quando occorre creare e gestire una grande infrastruttura di rete wireless.

Conclusioni

Oggi le organizzazioni non hanno solo bisogno di una maggiore velocità di connessione per la propria rete wireless. Necessitano di una soluzione che fornisca un throughput superiore, una maggiore qualità del segnale e una migliore esperienza utente per una grande varietà di client wireless in ambienti ad alta densità. Una soluzione che riesca anche a individuare ed eliminare le minacce nel traffico wireless, crittografato o meno, per proteggere la rete e semplificarne al contempo l'utilizzo e la gestione.

Maggiori informazioni. Visita www.sonicwall.com/en-us/products/firewalls/wireless-security.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com