



Cos'è Secure SD-WAN e in che modo mi fa risparmiare?

Per qualunque tipologia di organizzazione, grande o piccola, pubblica o privata, tagliare i costi è sempre una priorità. Dopo tutto, ridurre le spese operative fa sempre un bell'effetto sul bilancio e consente all'azienda di investire in altre attività importanti.

Un costo imprescindibile è quello della connettività internet. L'accesso a internet è indispensabile per le comunicazioni, l'hosting dei siti web, la condivisione dei file, la fornitura di applicazioni e molte altre attività, ma può essere costoso – specialmente per le organizzazioni che hanno più sedi, filiali o punti vendita.

Oggi gli utilizzatori della banda larga, dipendenti o clienti che siano, valutano la propria esperienza in termini di prestazioni piuttosto che di disponibilità. Non si aspettano solo di accedere alle applicazioni e ai video, ma anche di usufruirne in tempo reale. Ogni ritardo comporta lamentele e richieste di più banda, con un conseguente aumento delle spese.

Come collegare in sicurezza sedi remote alla rete

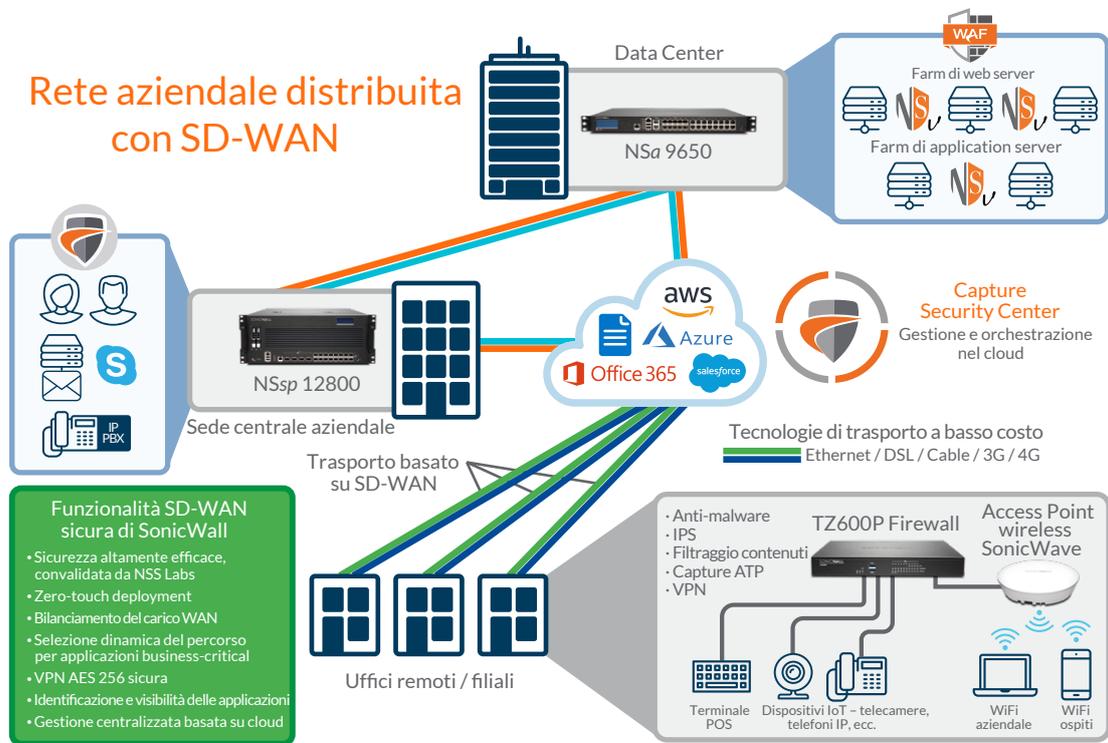
In una rete distribuita con diverse filiali e sedi remote, è necessario che queste siano collegate in modo sicuro tra loro e con la sede centrale dell'azienda. Questo obiettivo può essere raggiunto utilizzando diverse tecniche. Un metodo ampiamente diffuso è l'MPLS (Multiprotocol Label Switching), che consente alle organizzazioni di creare una rete WAN (Wide Area Network) privata per trasmettere i dati in modo sicuro tra le varie sedi attraverso il percorso più breve disponibile senza passare per la rete internet pubblica.

L'MPLS supporta diversi tipi di connessione, tra cui T1 e frame relay. Il problema è che queste connessioni devono supportare un numero crescente di dispositivi connessi e applicazioni ad alto consumo di banda che richiedono velocità più elevate e, di conseguenza, sono costose. Ecco perché molte aziende distribuite stanno passando all'SD-WAN (Software-Defined Wide Area Networking).

Affinché SD-WAN sia un'alternativa valida alle WAN private, le aziende devono garantire di avere, presso le filiali e nei siti remoti, lo stesso livello di ispezione e applicazione che hanno nel data center" ha dichiarato Mike Fratto, analista di 451 Research, [nell'annuncio ufficiale del lancio](#).

“Le funzionalità di sicurezza integrate con SD-WAN sono la vera posta in gioco per la maggior parte delle aziende che adottano questa tecnologia.”

Mike Fratto
Analyst
451



Ridurre i costi con Secure SD-WAN

Per aiutare le organizzazioni a ridurre i costi senza rinunciare a sicurezza e prestazioni costanti per le loro applicazioni strategiche, SonicWall offre **Secure SD-WAN**. Questa tecnologia – integrata in SonicOS 6.5.3, il sistema operativo dei firewall SonicWall TZ e NSa – consente alle organizzazioni distribuite di creare, utilizzare e gestire reti sicure ad alte prestazioni utilizzando servizi Internet pubblici subito disponibili e a basso costo come DSL, cavo e 3G/4G.

Fungendo da alternativa a tecnologie di connessione WAN più costose quali MPLS, Secure SD-WAN consente praticamente ad ogni organizzazione, tra cui [rivenditori al](#)

Secure SD-WAN: sicura, veloce e affidabile

dettaglio, [banche](#), produttori e altri, di collegare siti geograficamente lontani allo scopo di condividere dati, applicazioni e servizi. Funzionalità come il failover e il bilanciamento del carico intelligenti garantiscono prestazioni e disponibilità costanti delle applicazioni aziendali e SaaS critiche.

Inoltre, a differenza delle soluzioni SD-WAN di fornitori pure-play, Secure SD-WAN di SonicWall non richiede l'acquisto di licenze o hardware aggiuntivi.

Secure SD-WAN: sicura, veloce e affidabile

La riduzione delle spese è sempre una priorità per ogni organizzazione. Ma ecco alcuni altri aspetti che le aziende distribuite possono risolvere con Secure SD-WAN:

- 1. Protezione della rete dai cyber criminali.** Il traffico sia crittografato che non crittografato passa attraverso un **firewall** SonicWall di nuova generazione, dove viene analizzato alla ricerca di minacce quali malware e **ransomware**, garantendo il massimo livello di rilevamento e prevenzione delle minacce. Se si utilizza una singola soluzione SD-WAN dedicata, occorre assicurarsi di avere strumenti adatti per proteggersi dai moderni attacchi informatici come le **minacce crittografate** e il **ransomware**.
- 2. Prestazioni costanti e ottimizzate delle applicazioni.** Le organizzazioni possono ottenere prestazioni più veloci e coerenti per le applicazioni SaaS e business-critical quali VoIP, video e comunicazioni unificate grazie a caratteristiche come le prestazioni deterministiche, che indirizzano le applicazioni verso collegamenti meno congestionati per superare jitter, latenza, perdita di pacchetti e altre condizioni di rete sfavorevoli.
- 3. Maggiore agilità.** SonicWall Zero-Touch Deployment semplifica notevolmente l'implementazione di nuovi siti. Il provisioning dell'hardware da remoto elimina la necessità di far eseguire questo processo da personale IT sul posto. Inoltre, gli amministratori IT possono gestire l'intera rete, inclusi i dispositivi presso filiali/sedi remote dotate di SD-WAN, attraverso un unico pannello di controllo utilizzando **Capture Security Center**, la piattaforma di gestione e analisi basata su cloud di SonicWall.

Scopri maggiori informazioni su come SonicWall può aiutare la tua azienda distribuita a ridurre i costi e la complessità e migliorare al contempo la sicurezza passando da una costosa soluzione MPLS a **Secure SD-WAN**.