Forcepoint

Sintesi della soluzione

Le tre tipologie di sicurezza necessarie per qualsiasi SD-WAN

Introduzione

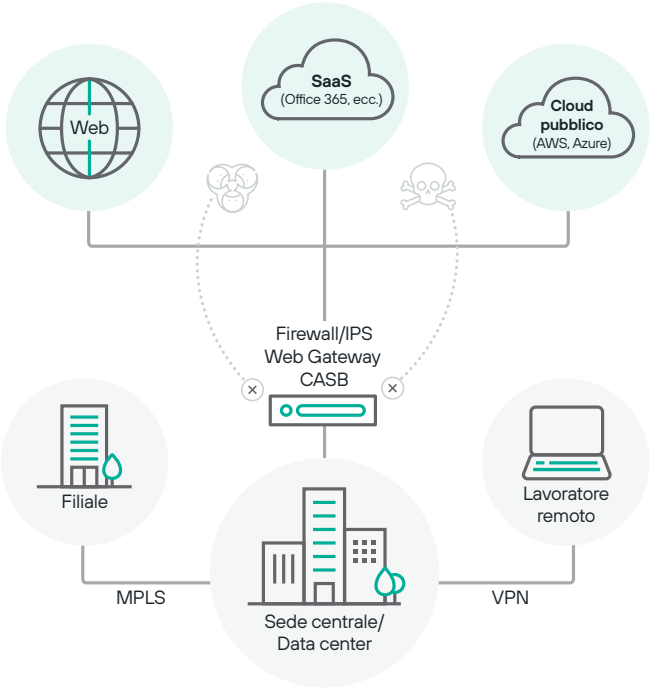
Le aziende sono sempre più distribuite e i metodi tradizionali per collegare filiali e lavoratori remoti alle risorse necessarie non riescono a tenere il passo con la migrazione di applicazioni e dati al cloud. Le reti hub-and-spoke basate su connessioni MPLS interne e le reti VPN esterne non possono fornire in modo economicamente vantaggioso le prestazioni necessarie per app cloud moderne e altamente interattive come Microsoft Office 365 e videoconferenze. Anche se probabilmente le linee MPLS continueranno a essere utilizzate in applicazioni aziendali specializzate, molte aziende stanno migrando verso architetture direct-to-internet. Combinando i collegamenti a banda larga con le tecnologie SD-WAN (Wide Area Networking) definite da software, imprese e agenzie governative forniscono ai loro dipendenti nuovi livelli di connettività per accelerare le iniziative di trasformazione digitale e aziendale quali:

- → Adozione del cloud (app SaaS di terze parti e app interne su piattaforme cloud)
- → Capacità per applicazioni video ad alta intensità
- → Consolidamento delle infrastrutture in occasione di fusioni e acquisizioni
- → Agilità e costi ridotti per aprire filiali in modo più rapido ed efficiente

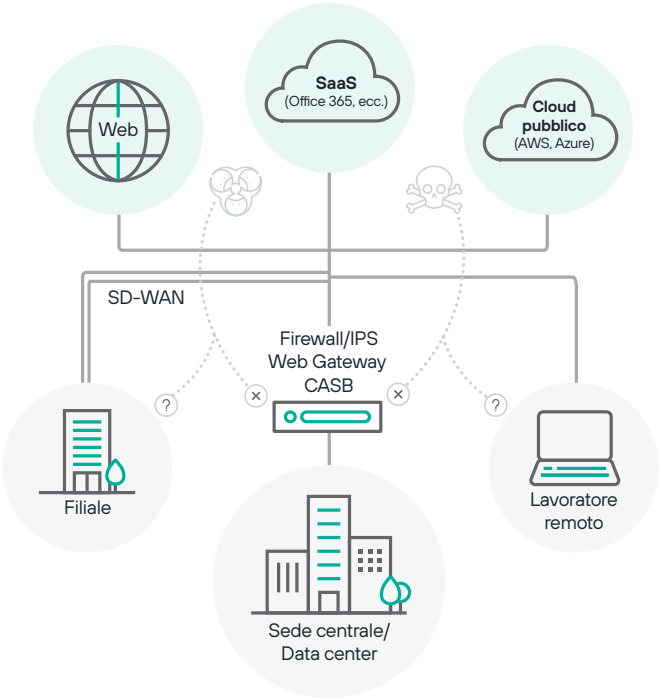
La SD-WAN rende possibili nuove forme di collaborazione e di efficienza aziendale, ma aumenta anche drasticamente il numero di potenziali bersagli per ladri e hacker, ampliando la superficie di attacco delle aziende. Inoltre, le difese IT che erano state adottate per proteggere gli uffici centrali e le postazioni remote con backhauling potrebbero non essere più d'aiuto in un mondo distribuito e incentrato sul cloud. In poche parole, l'implementazione della SD-WAN richiede un nuovo approccio alla sicurezza.

Sfide per la sicurezza derivanti dalla SD-WAN

Originariamente, la sicurezza aziendale aveva la forma di un pacchetto di prodotti hardware forniti in un ufficio centrale, spesso come appliance quali firewall, gateway web e CASB (Cloud Access Security Broker). Questi dispositivi difendevano l'ufficio centrale, le filiali e anche gli utenti remoti che li utilizzavano per connettersi al mondo esterno.



Con la migrazione di applicazioni e dati al cloud, le aziende distribuite hanno cominciato ad abbandonare le tecnologie di rete con backhauling come l'MPLS per passare alla banda larga di Internet e alle SD-WAN per collegare le sedi delle filiali. Gli utenti remoti hanno seguito rapidamente l'esempio, utilizzando le app cloud direttamente, cioè senza prima connettersi alla rete interna tramite VPN. Questa soluzione migliora notevolmente le prestazioni, ma a discapito della protezione fornita dalle tradizionali difese del gateway.



La SD-WAN si basa sulla privacy, non sulla sicurezza

La maggior parte delle soluzioni SD-WAN crittografa il traffico che viaggia tra siti remoti e cloud. In questo modo la privacy è garantita, poiché si evita che il traffico di rete venga spiato, ma non si fornisce protezione contro gli attacchi. Per utilizzare la SD-WAN in modo sicuro, le imprese devono:

- → Tenere gli intrusi di Internet fuori dalle reti delle filiali
- → Impedire ai malware di intrufolarsi attraverso le pagine web o i contenuti scaricati
- → Controllare quali app cloud possono essere utilizzate

Queste tre tipologie di difesa, Network Security, Web Security e Cloud Access Security, sono essenziali per la SD-WAN.

Sicurezza di rete

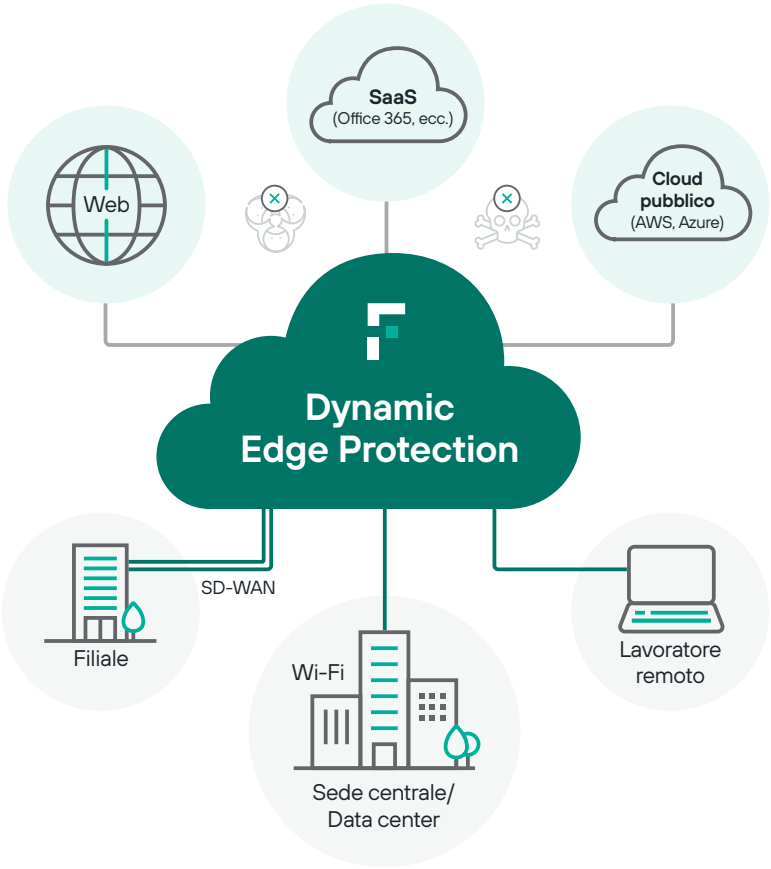
I firewall sono in genere la prima linea di difesa per qualsiasi organizzazione distribuita. Originariamente, controllavano soltanto l'accesso in base alla provenienza e alla destinazione del traffico, ma i moderni firewall di nuova generazione (NGFW) integrano una prevenzione avanzata delle intrusioni e difese contro i malware, attive su tutte le porte e in tutti i protocolli. Molte soluzioni SD-WAN si basano sull'implementazione di un firewall separato in ogni postazione. Approcci più recenti basati su Secure SD-WAN, introdotti da Forcepoint, combinano in un'unica soluzione la rete SD-WAN e la sicurezza NGFW, eliminando la necessità di acquistare, distribuire e gestire due stack tecnologici separati. Le nuove soluzioni di sicurezza, come Forcepoint Dynamic Edge Protection (DEP), portano questo consolidamento a un livello superiore, sostituendo le appliance locali con firewall come servizio nel cloud.

Sicurezza su web

Le due attività tipiche di chi si connette a Internet sono la navigazione sul web e l'uso delle app cloud. All'inizio, i Secure Web Gateway (SWG) venivano utilizzati dalle aziende per impedire ai dipendenti di accedere a siti web inappropriati dal luogo di lavoro e per dimostrare agli auditor che venivano applicate policy di utilizzo accettabile. Nel tempo, mentre si diffondeva l'abitudine di utilizzare contenuti provenienti dai siti web, i gateway cominciarono ad analizzare i file scaricati per rilevare e bloccare i malware. Oggi molti gateway web svolgono anche una funzione di prevenzione della perdita di dati e analizzano anche i file in uscita al fine di prevenire l'upload accidentale o intenzionale di dati sensibili. I gateway web sono nati come appliance, ma si sono rapidamente spostati anche nel cloud e vengono spesso utilizzati in ambienti IT ibridi in cui il controllo viene eseguito in locale in alcune sedi e nel cloud per tutte le altre.

Cloud Access Security

I siti web che consentivano di archiviare e manipolare i dati si sono rapidamente evoluti in vere e proprie applicazioni cloud. Tuttavia, con la dispersione dei dati in Internet, il controllo delle app utilizzabili è diventato un elemento critico della sicurezza aziendale moderna. Inizialmente i CASB (Cloud Access Security Broker) venivano utilizzati come strumenti per monitorare le applicazioni cloud utilizzate dai dipendenti, spesso all'insaputa dell'azienda. L'uso di app cloud non autorizzate è noto come IT Shadow ed è diventato un'arma a doppio taglio: da un lato, accelera la produttività dei dipendenti e dall'altro costituisce un rischio potenziale per i dati sensibili. I CASB di nuova generazione offrono la possibilità di applicare i criteri di protezione dei dati, adottando automaticamente azioni come la crittografia o la messa in quarantena dei dati sensibili all'interno di applicazioni autorizzate come Microsoft Office 365. Sebbene talvolta il CASB sia implementato come appliance, il più delle volte viene erogato come servizio dal cloud.



Il passo successivo: l'unificazione di Network, Web, e Cloud Access Security con SASE

Anche se Network, Web e Cloud Access Security vengono forniti come servizi, la maggior parte delle aziende cerca di ridurre il numero di sistemi e di fornitori che utilizza. L'uso di prodotti diversi per sedi e lavoratori remoti crea delle falle che possono essere sfruttate dagli aggressori, costa troppo e pesa sulle spalle già sovraccariche delle risorse IT. Di conseguenza, le difese che un tempo venivano fornite con un mosaico di prodotti autonomi, stanno convergendo in un nuovo approccio che Gartner chiama Secure Access Service Edge (SASE). Le soluzioni SASE, come Forcepoint Dynamic Edge Protection (DEP), offrono una metodologia all-in-one che fornisce una sicurezza web, di rete e delle applicazioni come servizio dal cloud, sempre aggiornata.

La DEP unisce funzionalità di sicurezza avanzate come firewalling, prevenzione delle intrusioni, ispezione dei contenuti web, scansione dei malware, filtraggio degli URL, accesso alle applicazioni e altro ancora, in un singolo servizio cloud unificato. Questo approccio convergente elimina lacune e ridondanze per impedire sistematicamente agli aggressori di accedere alle aziende da Internet, contenuti web o app cloud, a prescindere da dove lavorino i dipendenti.

Le soluzioni SASE come DEP forniscono una protezione completa e sistematica dell'accesso a web, rete e cloud in tutte le filiali, a prescindere dal prodotto SD-WAN utilizzato. Con questo approccio, le obsolete e lente reti MPLS possono essere sostituite con connessioni a banda larga rapide e poco costose, in modo sicuro, efficiente e senza esporre l'azienda a rischi.

forcepoint.com/contact