BUSINESS PAPER

aruba
a Hewlett Packard Enterprise company

LA RETE SD-WAN E L'ARCHITETTURA SASE MIGLIORI DELLA CATEGORIA SONO IL PROPULSORE DELL'IMPRESA DIGITALE

INDICE

DOCUMENTO DI SINTESI

Le imprese continuano ad avanzare verso la trasformazione digitale allo scopo di diventare più efficienti, migliorare il livello di soddisfazione dei clienti, perseguire nuove opportunità di mercato, incrementare la redditività e conservare un vantaggio competitivo. La migrazione delle applicazioni aziendali nel cloud è essenziale per il successo di qualsiasi iniziativa di trasformazione digitale. Perché? Oggi nel cloud vengono eseguite più applicazioni rispetto ai tradizionali data center aziendali e la maggior parte di queste applicazioni viene utilizzata in modalità software-as-a-service (SaaS). In più, in un mondo cloud-first, le aziende devono assicurarsi che sia possibile accedere alle applicazioni in modo diretto e sicuro in qualsiasi momento, da qualsiasi luogo e con qualsiasi dispositivo. Un'ulteriore esigenza è che la rete offra sempre un'esperienza della massima qualità tanto ai dipendenti quanto ai clienti. Infine, la proliferazione dei dispositivi IoT e mobile in azienda ha esteso drasticamente la superficie di attacco, esponendo le imprese a violazioni della sicurezza che possono compromettere i dati e causare downtime della rete.

In origine, le reti aziendali di oggi non erano state progettate per il mondo cloud-first e quindi non sono in grado di affrontare le problematiche di sicurezza informatica legate alla trasformazione digitale. Per le imprese è essenziale non soltanto mettere in sicurezza le applicazioni nel cloud, ma anche proteggere gli utenti che si collegano a tali applicazioni all'interno della WAN (Wide Area Network). Al tempo stesso, la proliferazione dei dispositivi IoT ha ampliato in modo significativo la superficie di attacco, esponendo le organizzazioni a un numero crescente di minacce alla sicurezza informatica.

L'imperativo strategico consiste quindi nell'adottare una Software-Defined Wide Area Network (SD-WAN) più intelligente e sicura, altamente automatizzata e perfettamente integrabile con i servizi di sicurezza forniti nel cloud, per dare vita all'architettura SASE (Secure Access Service Edge) migliore della categoria. L'architettura SASE deve essere integrata con una sicurezza zero trust basata sull'identità, per applicare una segmentazione che consenta a utenti e dispositivi IoT di accedere soltanto alle destinazioni della rete pertinenti al loro ruolo all'interno dell'azienda.

Poiché la trasformazione della WAN e della sicurezza rappresentano un percorso, l'azienda può iniziare dalla modernizzazione dell'una o dell'altra componente, ma per mettere realizzare pienamente il valore degli investimenti effettuati nel cloud, è necessario modernizzarle entrambe.

Ed è altrettanto importante evitare la dipendenza da un fornitore scegliendo partner di soluzioni tecnologiche che offrano flessibilità e libertà di scelta. Dopo aver trasformato le architetture di rete e di sicurezza, l'azienda può adottare tempestivamente le innovazioni per incrementare la produttività e accelerare la crescita e la redditività, contenendo al tempo stesso i costi.

In origine, le reti aziendali di oggi non erano state progettate per il mondo cloud-first e quindi non sono in grado di affrontare le problematiche di sicurezza informatica legate alla trasformazione digitale. Per le imprese è essenziale non soltanto mettere in sicurezza le applicazioni nel cloud, ma anche proteggere gli utenti che si collegano a tali applicazioni. Al tempo stesso, la proliferazione dei dispositivi IoT ha ampliato in modo significativo la superficie di attacco, esponendo le organizzazioni a un numero crescente di minacce alla sicurezza informatica

LE APPLICAZIONI VENGONO FORNITE NEL CLOUD: ANCHE PER LA SICUREZZA DOVREBBE AVVENIRE LA STESSA COSA

Tradizionalmente, tutto il traffico delle applicazioni proveniente dalle filiali verrebbe trasportato in backhaul tramite servizi MPLS privati al data center aziendale per verifiche e ispezioni di sicurezza (vedere figura Figure 1). Questa architettura era adeguata quando le applicazioni venivano ospitate esclusivamente nel data center aziendale. Ma con la migrazione di applicazioni e servizi nel cloud, questa architettura di rete tradizionale non si rivela all'altezza, soprattutto perché compromette le prestazioni delle applicazioni e offre un'esperienza utente non uniforme, dato che il traffico destinato a Internet passa innanzitutto attraverso il data center e il firewall aziendale prima di arrivare a destinazione.

Inoltre, con l'aumento del numero di dipendenti che lavorano al di fuori della rete aziendale collegandosi direttamente alle applicazioni cloud, la tradizionale sicurezza basata sul perimetro risulta insufficiente. Il cloud e il modello SaaS hanno cambiato per sempre il modo in cui gli utenti si connettono alle applicazioni e interagiscono con esse. Trasformando le architetture WAN e di sicurezza, le aziende possono garantire un accesso diretto e sicuro alle applicazioni e ai servizi in ambienti multi-cloud, indipendentemente dal punto di accesso e dal dispositivo utilizzato.

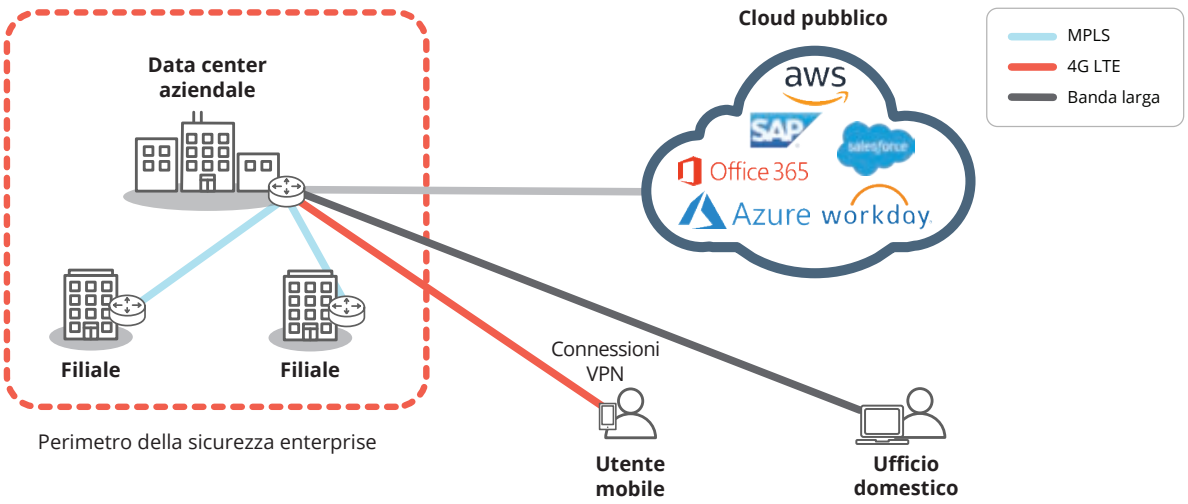

Figura 1: le reti WAN aziendali tradizionali e gli approcci alla sicurezza basati sul perimetro non sono stati progettati per il cloud. Effettuare il backhaul del traffico di tutte le applicazioni dalle filiali al data center riduce le prestazioni e offre un'esperienza utente non coerente.

Nel 2019, Gartner ha coniato il termine SASE, ovvero Secure Access Service Edge, per designare un framework che coniuga SD-WAN a funzioni SSE (Security Service Edge) erogate tramite cloud, tra cui Secure Web Gateway (SWG), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB) e Zero Trust Network Access (ZTNA). In precedenza, queste erano tutte funzionalità separate e dedicate, mentre ora possono essere fornite tramite cloud e in maniera unificata, come mostrato nella Figura 2.

Alcuni tra gli early adopter delle soluzioni SSE non sono riusciti a implementare anche una SD-WAN che permettesse di applicare l'adaptive Internet breakout direttamente dalle filiali. Pertanto, non erano in grado di indirizzare il traffico dalla filiale direttamente al cloud. Senza la componente SD-WAN, era comunque necessario effettuare il backhaul del traffico destinato al cloud tramite il data center, pregiudicando le prestazioni delle applicazioni.

L'adozione di soluzioni SSE e di una SD-WAN elimina i costi e le complessità associate alla gestione di più firewall on-premise, ma rimane comunque necessario un firewall presso le filiali per bloccare le minacce in entrata. Come mostrato in figura 3, utilizzando una soluzione SD-WAN avanzata, le aziende possono connettersi direttamente al cloud attraverso l'adaptive Internet breakout utilizzando connessioni a Internet a banda larga. La tecnologia intelligente, che riconosce le applicazioni inserite nella white list, permette di sfruttare il local breakout tra la filiale e il PoP (Point of Presence) più vicino, eliminando la latenza e fornendo un'esperienza della massima qualità per le applicazioni cloud e SaaS affidabili, come Microsoft Office 365, 8x8 e RingCentral. Il riconoscimento delle applicazioni consente inoltre di inviare i dati di altri tipi di traffico diretti verso il web a un servizio di sicurezza erogato tramite cloud per effettuare un'ispezione avanzata prima di inoltrarli al fornitore SaaS. Le avanzate funzionalità SD-WAN integrate con i moderni servizi di sicurezza basati sul cloud garantiscono un'applicazione coerente delle policy e del controllo degli accessi per utenti, dispositivi, applicazioni e IoT. Questo permette alle aziende di rispettare i criteri di conformità, prevenire i downtime e ridurre i rischi di compromissione dei dati associati alle violazioni della sicurezza.

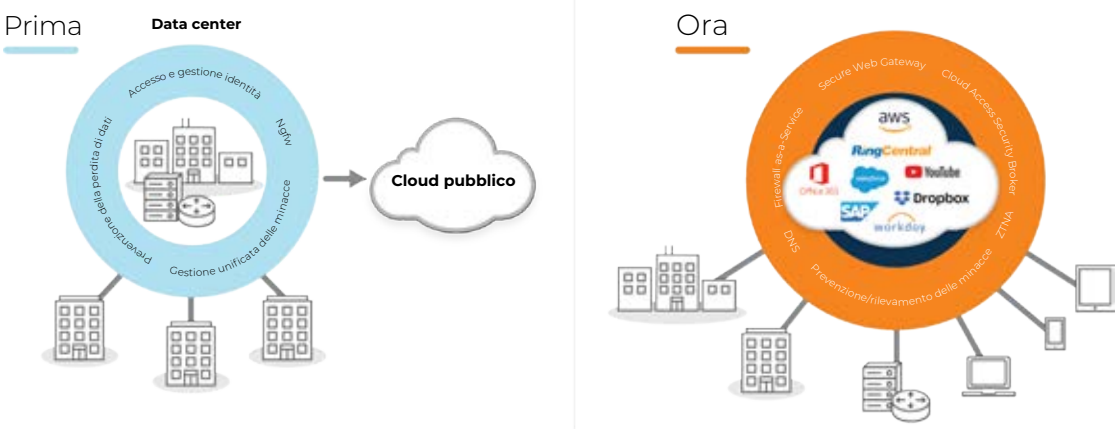

Figura 2: in passato era essenziale mettere in sicurezza il data center aziendale, l'unico luogo in cui erano ospitate le applicazioni. Ora che le applicazioni si sono spostate sul cloud e vengono fornite da lì, la sicurezza aziendale basata sul perimetro si sta rivelando sempre più inefficace. È fondamentale pensare in maniera diversa e spostare sul cloud anche la sicurezza.

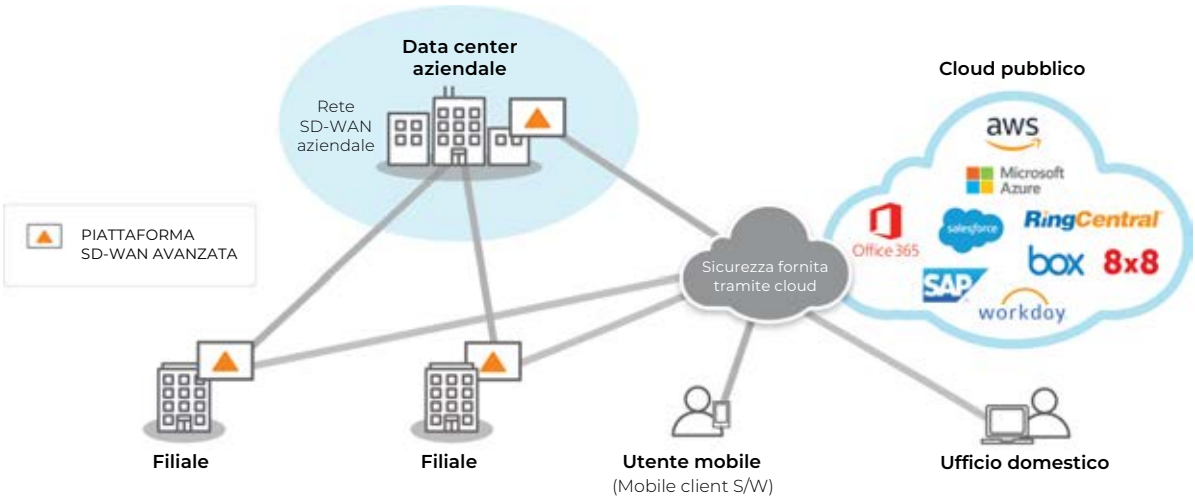

Figura 3: una rete SD-WAN avanzata offre alle aziende un accesso sicuro al cloud. Le filiali possono usare connessioni a banda larga e l'adaptive Internet breakout per connettere direttamente gli utenti alle applicazioni cloud, ottimizzando le prestazioni delle applicazioni e l'esperienza utente. Combinando una SD-WAN avanzata e una soluzione di sicurezza basata sul cloud si crea un'architettura SASE (Secure Access Service Edge) che mette al sicuro utenti, dispositivi e applicazioni.

L'ARCHITETTURA SASE MIGLIORE DELLA CATEGORIA GARANTISCE LA MASSIMA LIBERTÀ DI SCELTA

Con la costante evoluzione degli approcci alla protezione della rete e le difficoltà associate alla creazione di soluzioni di rete complesse, è importante prendere in considerazione le migliori soluzioni di rete e di sicurezza offerte da fornitori di comprovata esperienza e specializzazione nel settore. Sebbene sia improbabile trovare un single vendor in grado di offrire le funzionalità SASE migliori della categoria in entrambi gli ambiti, le aziende non dovrebbero essere costrette ad accontentarsi di soluzioni di base né in uno né nell'altro caso.

Vista la costante evoluzione del panorama delle minacce, la sicurezza rappresenta una delle principali preoccupazioni per le aziende, che devono perciò mantenere l'agilità necessaria per adottare rapidamente e a costi contenuti nuove soluzioni di sicurezza senza restare bloccate dalla dipendenza da un unico fornitore. Potendo disporre di una soluzione di rete indipendente, le imprese sono in grado di scegliere e implementare con la massima fiducia e serenità le soluzioni basate sul cloud che meglio soddisfano le loro specifiche esigenze operative e di sicurezza, anch'esse in costante evoluzione.

Una soluzione SD-WAN avanzata si integra perfettamente con vari fornitori SSE, consentendo di scegliere le soluzioni migliori della categoria che combinano SD-WAN e sicurezza fornita tramite cloud tramite l'orchestrazione automatizzata. Con un'architettura SASE all'avanguardia, le imprese creano un sistema di sicurezza omogeneo che contrasta l'impatto degli attacchi informatici, migliorando al contempo l'agilità del business e riducendo la complessità. In definitiva questo consente alle aziende di ottenere un effetto moltiplicatore sugli investimenti passati e in corso in servizi e applicazioni cloud.

APPROCCIO ZERO TRUST PER LA SICUREZZA DELL'IOT AZIENDALE

La proliferazione dei dispositivi IoT nelle aziende porta introduce nuovi modi di monitorare, segnalare, automatizzare e ottimizzare i processi aziendali, nonché di generare i relativi avvisi, e questo avviene sia per le linee di produzione, sia per l'automazione degli impianti di climatizzazione e illuminazione finalizzata al risparmio energetico. L'IoT rende le aziende più efficienti tramite l'automazione, ma espande la superficie d'attacco aggiungendo una nuova dimensione di complessità. L'IT affronta la crescente problematica della sicurezza dei dispositivi mobile implementando soluzioni di accesso alla rete basate sul modello Zero Trust (ZTNA). Le soluzioni ZTNA prevedono l'installazione di un agente endpoint sul dispositivo dell'utente, ad esempio laptop, tablet o cellulare.

L'agente software fa in modo che il traffico in uscita dal dispositivo venga indirizzato a un servizio di sicurezza basato sul cloud prima di essere inoltrato verso un'applicazione SaaS o un fornitore IaaS. Tuttavia, a differenza dei tablet e degli smartphone, i dispositivi IoT non consentono l'installazione degli agenti software ZTNA, né di altri agenti software di terzi, poiché sono dispositivi agentless. Di conseguenza, per proteggere le proprie reti da potenziali vulnerabilità che potrebbero determinare violazioni in grado di compromettere l'operatività aziendale quotidiana, le imprese hanno bisogno di una soluzione di sicurezza diversa per i dispositivi IoT.

Una SD-WAN avanzata che supporta un'architettura zero trust segmenta la rete in modo dinamico e applica i principi di accesso con minori privilegi, permettendo alle aziende di ridurre i rischi associati alle violazioni al momento della distribuzione dei dispositivi IoT. Così utenti e dispositivi dialogano soltanto con destinazioni pertinenti al loro ruolo in base a identità, diritti di accesso e livello di sicurezza. Le reti SD-WAN avanzate orchestrano la segmentazione end-to-end coprendo i percorsi LAN-WAN-LAN e LAN-WAN-data center/cloud, con la garanzia di un'applicazione automatizzata e coerente delle policy di sicurezza, abbinata a una maggior visibilità. Con la segmentazione end-to-end, le aziende possono implementare segmenti isolati per il traffico dei dispositivi IoT. Per ciascun segmento è possibile definire una policy di sicurezza indipendente da applicare al traffico del dispositivo. Poiché il traffico di un segmento è isolato da quello degli altri segmenti, non è possibile che si verifichino accessi non autorizzati. Anche se dovesse sopraggiungere una minaccia, il suo impatto resterebbe limitato al segmento in cui è emersa.

Facciamo un esempio. In un sito remoto in cui sono installati dispositivi IoT agentless come sistemi PoS e di climatizzazione (figura 4 di seguito), una piattaforma SD-WAN avanzata identifica in modo univoco le applicazioni utilizzate dai dispositivi. Una policy di sistema intercetta il traffico del PoS e lo trasmette al data center aziendale, che ospita l'applicazione di elaborazione delle transazioni con carta di credito. In questo esempio vengono applicati i servizi di sicurezza basati su firewall già esistenti, implementati nel data center. Al contrario, le policy del sistema di climatizzazione segmentano e trasmettono il relativo traffico al servizio di sicurezza basato sul cloud per un'ispezione di sicurezza aggiuntiva, prima di inoltrarlo al centro di comando IoT ospitato nel cloud pubblico. Poiché il traffico IoT è isolato in base alle policy aziendali, un'eventuale violazione del segmento dedicato all'impianto di climatizzazione non potrà compromettere o mettere a rischio i dati personali e delle carte di credito che transitano sul segmento dedicato al sistema PoS. La segmentazione contribuisce al rispetto dei requisiti di conformità PCI (o di altro tipo) da parte delle organizzazioni nello svolgimento della loro attività. Come mostrato nell'esempio, l'implementazione di una soluzione di sicurezza completa con una piattaforma SD-WAN avanzata offre alle aziende più dinamiche una tutela maggiore nel percorso di trasformazione, consentendo loro di sfruttare i benefici dell'IoT.

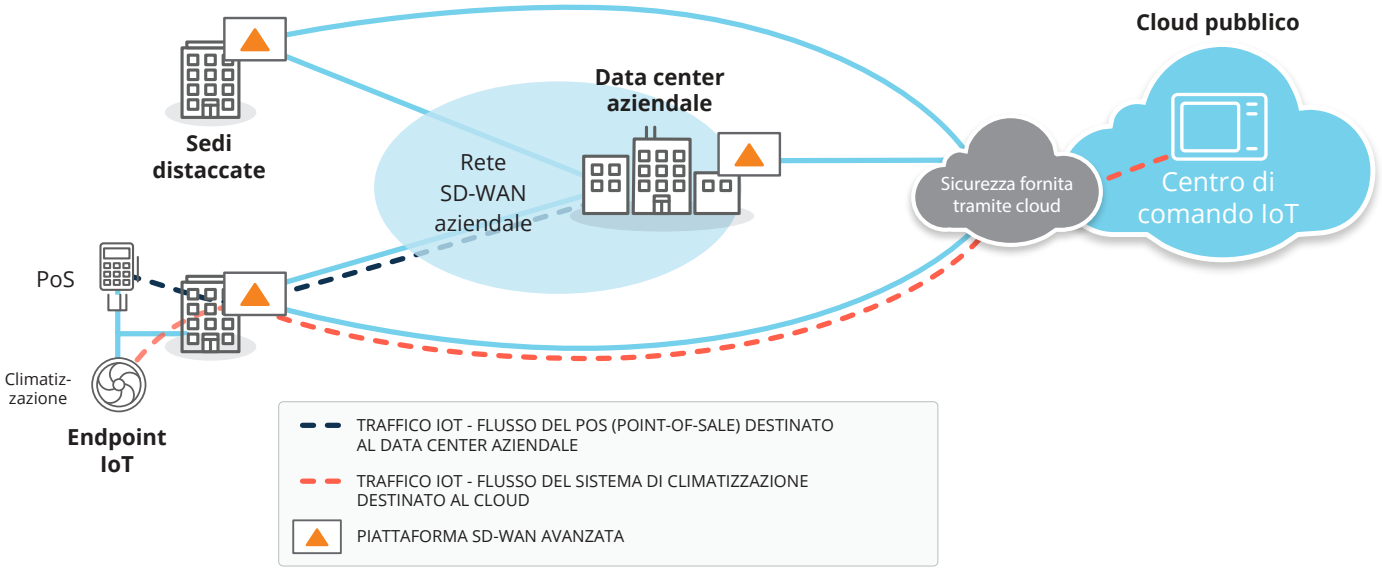

Figura 4: gli endpoint IoT si stanno moltiplicando e creano nuovi rischi di violazioni della sicurezza. Usando una piattaforma SD-WAN avanzata, le aziende possono proteggere i dispositivi IoT tramite l'implementazione di un'architettura zero trust e la segmentazione dinamica della rete. Come mostrato nel diagramma, tutti i dati delle transazioni del sistema PoS provenienti dalla filiale vengono inoltrati al data center aziendale, mentre il traffico del sistema di climatizzazione viene indirizzato al centro di comando IoT nel cloud.

RETE SD-WAN AVANZATA PER PROTEGGERE LE FILIALI DALLE MINACCE ESTERNE

Con la digitalizzazione delle imprese, il rischio di attacchi informatici è cresciuto notevolmente nell'ultimo decennio. Negli ambienti di rete tradizionali basati su router, le filiali hanno accumulato numerose apparecchiature di rete e di sicurezza, che però sono difficili da configurare, gestire e mantenere aggiornate con le più recenti informazioni sulle minacce. Ma non è tutto: le sedi remote non dispongono di personale IT esperto e questa carenza le espone a potenziali violazioni della sicurezza.

Oltre a garantire la sicurezza delle operazioni cloud con l'architettura SASE migliore della categoria, una soluzione SD-WAN avanzata può proteggere le filiali dalle minacce. È realizzata con un firewall di nuova generazione (NGFW) dotato di funzionalità di difesa dalle minacce come il rilevamento e la prevenzione delle intrusioni (IDS/IPS) e degli attacchi DDoS per proteggere le filiali dalle minacce dannose.

In genere un sistema IDS basato sulle firme monitora il traffico di rete per individuare schemi che corrispondono a una determinata firma dell'attacco. Quando viene rilevata un'intrusione, il sensore innesca operazioni quali l'interruzione, l'ispezione e l'autorizzazione del traffico. Gli Intrusion Prevention System possono funzionare in modalità strict o in modalità performant. In modalità strict, il traffico passa attraverso il sensore, in modo da essere immediatamente bloccato quando si verifica un'intrusione. In modalità performant, una copia del traffico viene inviata per l'esecuzione dell'analisi, garantendo una maggiore efficienza senza intaccare le prestazioni della rete. L'eventuale intrusione viene bloccata dopo il suo rilevamento. A seconda dei propri requisiti di sicurezza, le organizzazioni possono scegliere tra le due modalità.

Una rete SD-WAN avanzata è anche in grado di rilevare in modo dinamico gli attacchi DDoS, come attacchi ai protocolli, ICMP flood, SYN flood e IP spoofing. Dopo aver rilevato un comportamento anomalo della rete, la soluzione limita il numero di richieste tramite azioni quali rapid aging, drop excess, e block source. Inoltre, può instradare il traffico su collegamenti di rete non compromessi da un eventuale attacco DDoS, garantendo la continuità operativa.

Integrando funzionalità avanzate di rete e di sicurezza, come routing, ottimizzazione WAN e ngfw, in un'unica soluzione SD-WAN, le organizzazioni possono semplificare notevolmente le operazioni di rete nelle filiali. Inoltre, è possibile distribuire automaticamente le policy di sicurezza alle filiali da una posizione centrale con un provisioning zero touch, per facilitare la configurazione dei criteri di rete e di sicurezza. La creazione di nuove filiali è semplice e veloce e le modifiche alle policy di sicurezza possono essere distribuite automaticamente a centinaia o migliaia di filiali in pochi minuti, riducendo al minimo gli errori.

LA TRASFORMAZIONE DELLA RETE WAN È FONDAMENTALE PER IL SUCCESSO DELLA TRASFORMAZIONE DIGITALE

Oltre a tutti i benefici derivanti dalla migrazione a una moderna architettura di sicurezza basata sul cloud, la trasformazione della WAN costituisce un valore enorme per le odierne aziende cloud-first. Le tradizionali WAN incentrate sui router non erano state progettate per il cloud. Le aziende devono modernizzare la loro architettura WAN e ripensare la progettazione delle reti delle filiali per migliorare le prestazioni e la sicurezza delle applicazioni cloud. Le imprese utilizzano sempre più il cloud e il modello SaaS, con l'obiettivo di offrire un'esperienza utente della massima qualità.

La trasformazione della WAN comprende la creazione di un percorso più efficiente e un'esperienza migliore tra utenti e cloud. Come indicato in precedenza, l'adozione dell'adaptive Internet breakout per le applicazioni ospitate sul cloud o SaaS direttamente dalle filiali non soltanto consente di ottimizzare la larghezza di banda disponibile, ma riduce anche la latenza e il suo impatto negativo sulla produttività degli utenti.

Molte organizzazioni stanno trasformando l'edge delle proprie reti e si affidano all'SD-WAN per collegare le filiali con connessioni a Internet a banda larga. Una piattaforma SD-WAN offre funzionalità di scelta intelligente del percorso incentrate sulle applicazioni tra più collegamenti WAN (MPLS, Internet a banda larga, LTE e così via) in base al policy definite a livello centrale. I vantaggi dell'SD-WAN includono:

- delivery economicamente vantaggiosa delle applicazioni aziendali
- miglioramento in termini di prestazioni delle applicazioni, disponibilità e qualità dell'esperienza dell'utente finale
- rispetto dei requisiti dei moderni siti remoti e delle moderne filiali
- integrazione di applicazioni e servizi SaaS e basati su cloud
- miglioramento dell'efficienza dell'IT nelle filiali tramite il provisioning automatico dei servizi

RISPONDERE AI REQUISITI DEGLI SLA DELLE APPLICAZIONI

Tutto questo si traduce direttamente in una maggior produttività aziendale e agilità del business. Le aziende hanno bisogno di reti ad alte prestazioni, costruite su fondamenta che ne consentano l'elevata disponibilità e in grado di supportare in modo affidabile le applicazioni business-critical. La sicurezza non deve mai passare in secondo piano. La capacità di supportare funzionalità di micro-segmentazione e l'applicazione di policy granulari consente alle imprese di proteggere la WAN, rispettare i requisiti di conformità e difendersi dalle violazioni.

Le aziende devono poter contare sull'agilità necessaria per aprire nuove filiali e adeguare dinamicamente le policy e le norme di sicurezza. La possibilità di propagare il contesto delle policy è un fattore essenziale per l'automazione delle filiali. Tutto ciò rende molto interessante per le imprese la prospettiva di una soluzione SD-WAN avanzata, poiché contribuisce a eliminare la necessità di più appliance che eseguono funzioni di sicurezza dedicate e al tempo stesso consente di semplificare e consolidare (o "snellire") l'architettura edge WAN delle filiali. Le piattaforme edge SD-WAN avanzate permettono alle aziende di trasformare la propria WAN unificando SD-WAN, routing, ottimizzazione delle WAN, segmentazione e sicurezza delle filiali in un'unica piattaforma gestita centralmente.

L'orchestrazione dell'SD-WAN centralizzata e un approccio specifico per applicazione garantiscono che il comportamento della rete rifletta sempre le esigenze prioritarie del business. L'unificazione dell'orchestrazione delle policy di rete e sicurezza fa sì che i parametri di QoS e sicurezza vengano applicati in modo uniforme alle applicazioni, o a classi di applicazioni, indipendentemente da come o dove avviene l'accesso. Le prestazioni e la sicurezza delle applicazioni possono essere definite da policy aziendali dall'alto verso il basso, anziché dai limiti tecnologici dal basso verso l'altro. Una SD-WAN avanzata monitora continuamente lo stato della rete e delle applicazioni, rileva i cambiamenti e innesca in tempo reale reazioni immediate e automatizzate volte a neutralizzare l'impatto di cali di tensione, blackout e minacce alla sicurezza. Inoltre, l'automazione della connettività della piattaforma cloud con l'integrazione tramite API (Application Programmable Interface) semplifica le operazioni IT, fornendo alle imprese un accesso tempestivo a modelli IaaS, SaaS e servizi di sicurezza basati sul cloud. Per garantire dinamicamente le prestazioni, la sicurezza e l'esperienza di altissima qualità richieste dagli ambienti multi-cloud, le reti di oggi devono essere caratterizzate da visibilità end-to-end, programmabilità e automazione. Una rete WAN intelligente progettata con le migliori soluzioni SD-WAN e di sicurezza basata sul cloud può accelerare le iniziative di trasformazione digitale e l'evoluzione delle aziende, consentendo di adottare rapidamente le innovazioni senza conseguenze sulla produttività e sulla crescita, il tutto riducendo al minimo l'esposizione ai rischi per la sicurezza.

CONCLUSIONI

Proseguendo nella migrazione delle proprie applicazioni dai data center al cloud, le moderne aziende cloud-first devono avviare la trasformazione della WAN e della sicurezza, per ottenere il massimo ritorno sugli investimenti nel cloud. L'architettura SASE (Secure Access Service Edge) permette al settore di muoversi in questa nuova direzione. Come mostrato in figura 5, è importante che, nella progettazione di un edge di servizi ad accesso sicuro, le aziende valutino la trasformazione della WAN e della sicurezza, per fornire un'esperienza ottimale.

Una piattaforma SD-WAN avanzata consente di collegarsi senza problemi a numerosi servizi di sicurezza cloud all'avanguardia, per creare l'architettura SASE migliore della categoria. Realisticamente, nessun singolo fornitore SASE potrà offrire le migliori tecnologie di rete e di sicurezza su un'unica piattaforma. Con la continua evoluzione del panorama delle minacce, le imprese devono conservare l'agilità necessaria per adottare in tempi brevi e a costi contenuti nuove soluzioni di sicurezza. È opportuno che le aziende prendano in considerazione piattaforme che supportino l'integrazione delle migliori soluzioni SASE. Così possono evitare di dipendere da soluzioni single vendor proprietarie o di doversi accontentare di funzionalità e caratteristiche di base.

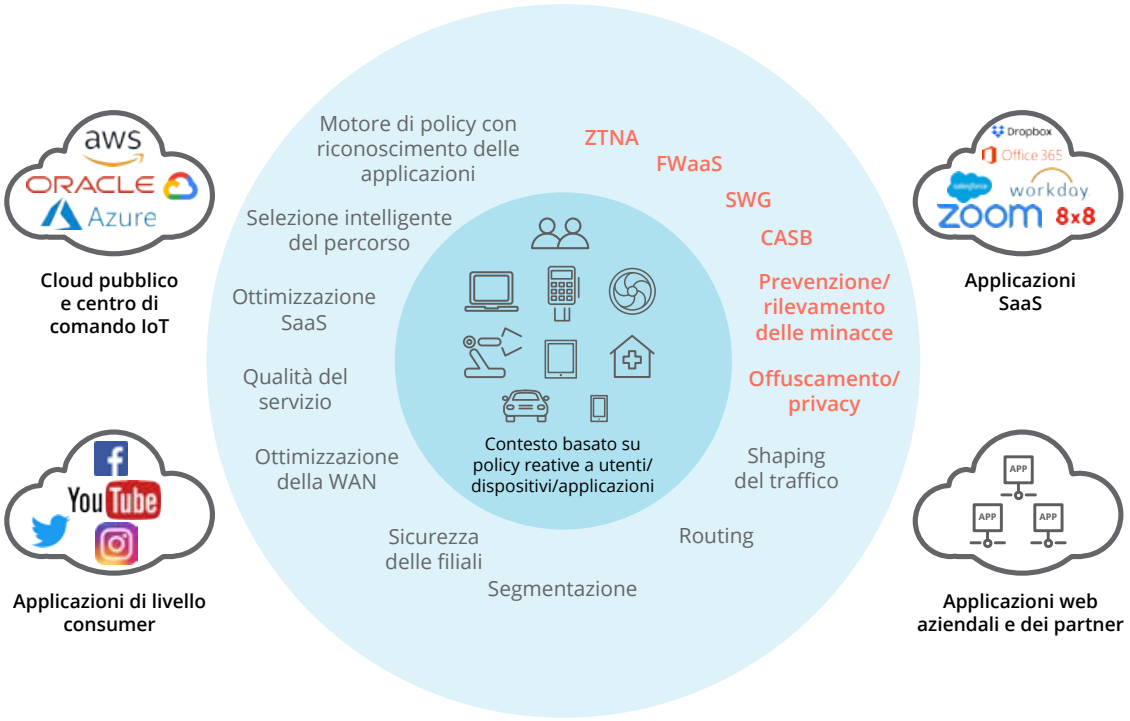

Figura 5: per supportare le iniziative di trasformazione digitale aziendale (ad esempio strategia cloud-first ed esigenze di mobilità della forza lavoro), occorre un edge di servizi con accesso sicuro. In un'architettura SASE affidabile, le avanzate funzionalità WAN devono essere combinate a funzioni di protezione della rete altrettanto complete per soddisfare l'esigenza di un accesso sicuro e dinamico da parte di utenti, dispositivi e applicazioni delle moderne imprese digitali.

In più, con la proliferazione dei dispositivi IoT, l'architettura SASE deve essere integrata con un framework di sicurezza zero trust in grado di segmentare dinamicamente il traffico in base all'identità: in questo modo utenti e dispositivi IoT potranno raggiungere soltanto le destinazioni di rete coerenti rispetto al proprio ruolo in azienda.

Una SD-WAN avanzata supporta le funzioni di sicurezza fondamentali richieste presso le filiali, attraverso la combinazione di un firewall di nuova generazione (ngfw) e funzionalità IDS/IPS e l'integrazione della sicurezza fornita tramite cloud, per garantire un'applicazione continua delle policy di sicurezza end-to-end in tutta l'azienda. Questo permette alle imprese di semplificare l'infrastruttura di rete con la possibilità di passare a una moderna architettura WAN sicura e cloud-first secondo le loro tempistiche e senza compromessi.

Infine, per le aziende non ancora pronte a mettere da parte i firewall delle filiali per affidarsi a un modello di sicurezza completamente basata sul cloud, è importante trovare una piattaforma SD-WAN avanzata che permetta di scegliere liberamente tra le migliori soluzioni software UTM (Unified Threat Management) di terzi da implementare come soluzione integrata presso le filiali. In questo modo si possono eliminare i costi aggiuntivi e le complessità di gestione che normalmente accompagnano i firewall dedicati e separati, mantenendo però la flessibilità necessaria per poter implementare le migliori soluzioni disponibili e, in ultima analisi, supportando una migrazione fluida verso un modello di sicurezza basata sul cloud.

Con il continuo apporto di importanti investimenti nel cloud da parte delle aziende, prendere in considerazione i requisiti per la trasformazione della WAN e della sicurezza le metterà nelle condizioni di offrire la miglior esperienza possibile agli utenti, affrontando nel contempo le odierne problematiche di sicurezza informatica. In definitiva, avviare un percorso di trasformazione della WAN e della sicurezza attento e senza compromessi consentirà alle imprese di proteggere le proprie risorse digitali e conseguire un effetto moltiplicatore sugli investimenti nel cloud, già effettuati e in essere.

aruba
a Hewlett Packard Enterprise company

BP_WAN-and-Security-Transformation_080422 a00110932ite

Contattaci alla pagina www.arubanetworks.com/contact