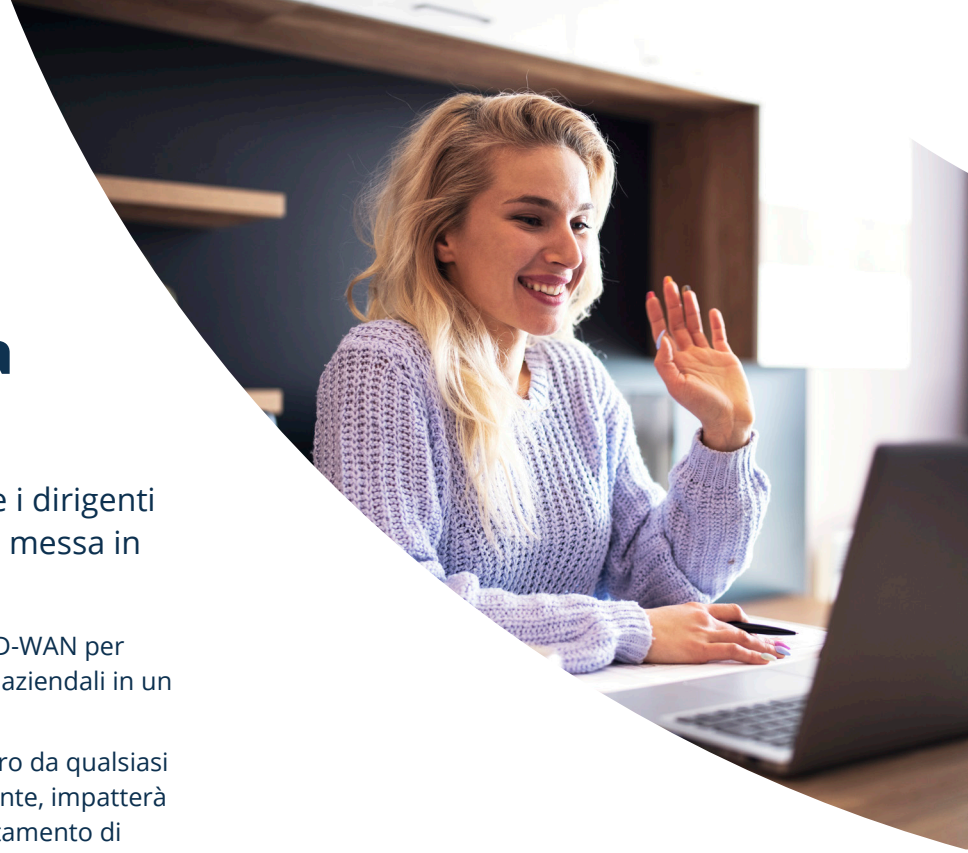
aruba
a Hewlett Packard Enterprise company

EBOOK

Sicurezza edge-to-cloud: un nuovo edge per WAN e sicurezza

Una guida pratica all'adozione di un'architettura SASE (Secure Access Service Edge)

L'impatto della trasformazione digitale e del lavoro da qualsiasi luogo (WFA, work from anywhere) sulle WAN e sulla sicurezza in un mondo basato sul cloud



Con le aziende ancora alle prese con le sfide poste dalla pandemia in corso e dalla nuova normalità del "lavoro da qualsiasi luogo", l'adozione di servizi ospitati nel cloud continua ad accelerare. Questo cambiamento sta rendendo sempre più urgente la necessità di trasformare i convenzionali data center e le normali reti MPLS-centriche e basate su VPN in architetture SASE (Secure Access Service Edge) native del cloud, che da una parte offrono un provisioning più dinamico di servizi di rete sicuri, dall'altra proteggono i dati presenti nella WAN end-to-end.

Le 3 domande più importanti che i dirigenti IT devono porsi con riguardo alla messa in sicurezza delle WAN sono:

- come scegliere la giusta architettura SD-WAN per supportare in sicurezza le applicazioni aziendali in un ambiente basato sul cloud?
- in che modo l'ambiente ibrido del lavoro da qualsiasi luogo, che si prospetta come permanente, impatterà sulle decisioni dell'IT in merito all'adattamento di un'architettura di sicurezza all'interno di una più ampia architettura SASE?
- in che modo l'IT può affrontare le sfide in tema di sicurezza associate alla proliferazione di dispositivi IoT in larga parte senza agenti?

Esaminiamo il modo in cui le esigenze di rete e di sicurezza stanno mutando in un mondo sempre più basato sul cloud.

50%
la percentuale degli intervistati in In process 2021 che stanno implementando o attuando diverse iniziative di trasformazione digitale (nel 2020 era il 38%)[1]

45%
le aziende che adottano una politica cloud-first[2]

1, 2. Sondaggio ESG sulle intenzioni di spesa in tecnologia IT, dicembre 2020

Zero Trust, ZTNA e SASE in un mondo basato sul cloud

Le soluzioni di sicurezza tradizionali non sono state progettate basandosi sul cloud. Il backhauling del traffico verso un data center centralizzato aveva senso quando tutte le applicazioni risiedevano lì. Con l'intensificarsi del traffico generato da utenti nelle filiali e con la migrazione delle applicazioni nel cloud, tuttavia, il backhauling del traffico nelle reti hub-and-spoke comporta un'esperienza utente insoddisfacente, maggiori rischi per la sicurezza e maggiori costi.

Le soluzioni di sicurezza per le reti preesistenti potrebbero non applicare il concetto Zero Trust, un modello di sicurezza IT per la gestione delle identità e degli accessi, basato sul principio per cui nessun utente e nessuna attività in rete possono essere considerati sicuri finché non sono autenticati. In altre parole, prima viene autenticata ogni cosa, poi si limita l'accesso solo alle applicazioni e ai dati coerenti con il ruolo dell'utente o del dispositivo. Il modello Zero Trust richiede che tutte le istanze di utenti, applicazioni e dispositivi devono dimostrare di essere chi affermano di essere e che siano autorizzate ad accedere solo alle risorse di cui hanno bisogno, indipendentemente dal fatto che tali istanze provengano dall'interno o dall'esterno della rete.

Lo Zero Trust Network Access (ZTNA) è un set di tecnologie che opera in un quadro Zero Trust e in cui l'accesso è consentito sulla base di dettagliate politiche "need-to-know" (solo le informazioni necessarie) e "least privilege" (con il più basso livello di privilegi sufficiente). Lo ZTNA fornisce agli utenti una connettività sicura e senza interruzioni ad applicazioni private senza inserirli nella rete e senza esporre le applicazioni su Internet.

E poi c'è il SASE, un neologismo coniato da Gartner. Con "SASE" si definisce un'architettura edge che unisce un vasto corpo di funzionalità WAN a vaste funzionalità di sicurezza di rete fornite tramite cloud quali secure web gateway (SWG), cloud access security broker (CASB), firewall-as-a-service (FWaaS), ZTNA e altre.

Le sfide relative alle WAN e alla sicurezza delle reti

Nel mondo di oggi, basato sul cloud, le esigenze rispetto alle WAN e alla sicurezza delle reti sono più interdipendenti che mai. Per realizzare appieno la promessa della trasformazione digitale, le aziende devono trasformare l'architettura sia della WAN sia della sicurezza: solo così potranno supportare al meglio le applicazioni aziendali che risiedono ovunque e alle quali è possibile accedere dappertutto e con qualsiasi rete di trasmissione.

Prendiamo in esame le più importanti sfide relative alla sicurezza e alle WAN che i team IT e di rete aziendali devono affrontare:

- come posso sfruttare i vantaggi commerciali e operativi del cloud mantenendo elevati livelli di sicurezza e riducendo i rischi complessivi?
- come posso assicurare un'esperienza utente di qualità elevata costante nel tempo per tutte le applicazioni aziendali ospitate nel cloud su tutta la WAN?
- come posso implementare e applicare politiche di accesso alla rete coerenti per i dipendenti che lavorano in un ambiente ibrido (in ufficio o in filiale solo in parte) o da qualsiasi luogo (WFA)?
- come posso mantenere la sicurezza e la connettività WAN dell'enorme numero di dispositivi, utenti e applicazioni?
- scegliere la piattaforma SD-WAN giusta può migliorare l'integrazione delle funzionalità di WAN e sicurezza della rete?
- posso ottenere tutti i servizi di sicurezza di cui ho bisogno da un unico fornitore?

Integrazione tra funzionalità SD-WAN e politiche di sicurezza

Nel frenetico contesto dell'economia globale odierna, le aziende devono poter avviare nuove filiali in tempi rapidi e regolare le politiche e le regole sulla sicurezza dinamicamente. La propagazione del contesto delle politiche è critica anche per l'automazione delle filiali ed è una delle funzionalità più importanti che solo una soluzione SD-WAN avanzata come la piattaforma Aruba EdgeConnect SD-WAN edge è in grado di offrire.

Una soluzione SD-WAN avanzata può anche aiutare le aziende a eliminare la necessità di ricorrere a più appliance unificando le principali funzionalità WAN edge per filiali, quali:

- SD-WAN
- Routing
- Firewall basato sulla zona e segmentazione
- Unified threat Management (UTM)
- Visibilità e controllo della rete e delle applicazioni
- Ottimizzazione WAN

Il consolidamento di queste funzioni semplifica o "snellisce" il WAN edge per le filiali, oltre a generare significative efficienze IT e a permettere una Quality of Service (QoS) e un'applicazione delle politiche di sicurezza più coerenti grazie alla gestione centralizzata.

L'orchestrazione SD-WAN centralizzata di Aruba EdgeConnect unifica la configurazione e la gestione routinaria. Inoltre permette che QoS e politiche di sicurezza vengano implementate in modo coerente tra le applicazioni (o classi di applicazioni) indipendentemente da come e da dove vi si accede. Gli obiettivi delle prestazioni delle applicazioni e della sicurezza sono dettati dall'alto dalle politiche aziendali, non dalle limitazioni tecnologiche provenienti dal basso.

L'SD-WAN consente una sicurezza più coerente

L'implementazione di un'architettura SASE che unisca funzionalità di sicurezza fornite nel cloud e una soluzione SD-WAN avanzata elimina i costi e le complessità associate alla gestione di più firewall di nuova generazione in locale, senza però escludere la necessità delle funzionalità dei firewall con stato basati sulla zona presso le filiali per bloccare le minacce in entrata.

La piattaforma EdgeConnect include:

- intelligenza e application awareness in grado di riconoscere le applicazioni inserite in appositi elenchi e autorizzarne l'accesso diretto alle risorse ospitate nel cloud
- integrazione e orchestrazione automatizzate con i fornitori di soluzioni di sicurezza tramite cloud dalla filiale al più vicino Point of Presence (PoP) per l'applicazione delle politiche di sicurezza

Tra i principali vantaggi:

- latenza ridotta
- prestazioni delle applicazioni ottimizzate
- massima qualità dell'esperienza utente per le applicazioni SaaS fidate

L'integrazione di Aruba Threat Defense con la piattaforma Aruba EdgeConnect SD-WAN edge estende le avanzate funzionalità di rilevamento e prevenzione delle intrusioni (IDS/IPS) della prima all'SD-WAN. Le appliance fisiche e virtuali di EdgeConnect sfruttano l'infrastruttura di Aruba Threat e gli aggiornamenti sulle minacce di Aruba Central, permettendo alle imprese di mettere in sicurezza il traffico est-ovest e i local Internet breakout dalle filiali. Tali appliance possono essere implementate centralmente, in loco o nel cloud. L'attività di logging delle minacce trova sbocco nell'invio dei dati analitici sulla rete e sulla sicurezza ad Aruba Central e in avanzate funzionalità UTM edge-to-cloud.

Zero Trust: mettere l'edge in sicurezza basandosi su ruolo, contesto e applicazione

Con l'incremento dei dispositivi mobile, della forza lavoro da remoto, delle applicazioni ospitate nel cloud e dei dispositivi IoT (Internet of Things), le aziende devono trovare il modo di allineare le politiche di rete basate sulle esigenze aziendali alle politiche di sicurezza.

L'integrazione del controllo degli accessi basato sull'identità di Aruba ClearPass Policy Manager nella piattaforma Aruba EdgeConnect SD-WAN incrementa l'intelligenza delle applicazioni aggiungendo la conoscenza dell'identità di utenti, dispositivi, ruoli e stato di sicurezza per porre le basi per un WAN edge sicuro.

Questo ulteriore livello di contesto permette una dettagliata segmentazione dei tipi di dispositivi basata sul ruolo nell'organizzazione, eliminando le complessità derivanti dalla gestione di migliaia di VLAN. Per esempio è possibile definire una dettagliata politica di segmentazione che impedisca alle videocamere di sorveglianza di accedere all'elaborazione delle transazioni effettuate tramite carta di credito o ai sistemi di gestione della climatizzazione. La politica potrebbe anche impedire alle videocamere di sorveglianza di comunicare tra loro, consentendo di comunicare solo con il terminale di sorveglianza o col dispositivo di registrazione. Così si aiuta l'IT a gestire la conformità della sicurezza delle applicazioni e i controlli in tema di sicurezza. Inoltre vengono generati log delle minacce esportabili in applicazioni SIEM (Security Information and Event Management) di terze parti.

57%

la percentuale di intervistati secondo cui la propria organizzazione ha implementato o intende implementare un modello basato sulla filosofia Zero Trust[3]

49%

la percentuale di intervistati secondo cui la propria organizzazione ha implementato o intende implementare un'architettura SASE[4]

71%

la percentuale di intervistati che selezionerebbe uno dei fornitori leader per l'implementazione di una SD-WAN e di una soluzione di sicurezza basata sul cloud per un'architettura SASE[5]

3, 4, 5. Ponemon Institute, The State of SD-WAN, SASE and Zero Trust Security Architectures (Lo stato delle architetture SD-WAN, SASE e Zero Trust Security), aprile 2021

ClearPass: mettere in sicurezza l'IoT con una SD-WAN avanzata

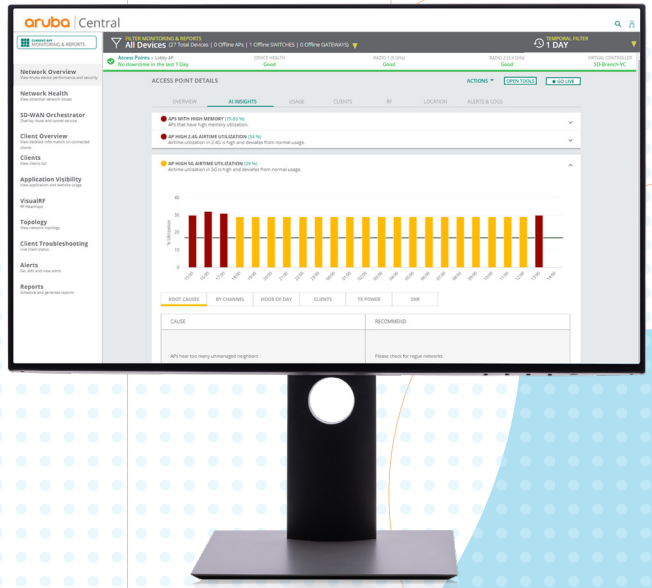
Se smartphone, portatili e tablet possono essere messi in sicurezza con agenti software ZTNA, non è invece possibile installare agenti software di sicurezza sui dispositivi IoT, essendo questi ultimi dispositivi senza agenti. Ciò pone una sfida di sicurezza che l'architettura SASE non è in grado di affrontare direttamente.

I rischi associati all'impiego dei dispositivi IoT possono essere ridotti con l'adozione di una piattaforma SD-WAN Aruba EdgeConnect. La piattaforma EdgeConnect è in grado di identificare e classificare il traffico delle applicazioni al primo pacchetto, intercettarlo all'edge della rete e spostarlo sul segmento appropriato. Questa segmentazione a grana grossa è sufficiente a metterlo in sicurezza dal resto del traffico della rete.

L'integrazione di ClearPass in EdgeConnect incrementa l'intelligenza delle applicazioni con politiche basate sull'identità dell'utente e del dispositivo e sul ruolo, consentendo una segmentazione a grana più fine. L'ulteriore contesto basato sull'identità permette un'applicazione coerente delle politiche di sicurezza su tutta la rete, dall'edge al cloud.

La segmentazione dinamica di Aruba Zero Trust aiuta le aziende a individuare le minacce alla sicurezza sulla base del dispositivo, del ruolo e dell'applicazione, continuando ad aderire agli standard di conformità del settore quali PCI, HIPAA e SOX.

Unendo una SD-WAN avanzata e una soluzione di sicurezza basata sul cloud usando un approccio alla rete Zero Trust (ZTNA) basato sulle politiche si può garantire sempre la sicurezza della WAN aziendale, degli utenti, dei dispositivi e delle applicazioni.



WAN e sicurezza al meglio e senza compromessi!

I migliori servizi di sicurezza ospitati nel cloud e orchestrati centralmente hanno un doppio vantaggio: soddisfano tanto le esigenze di sicurezza quanto quelle di contenimento dei costi. Per questo, dopo la loro emersione, hanno conosciuto una rapida diffusione. I servizi di sicurezza forniti tramite cloud e gestiti centralmente offrono protezione a tutti gli utenti, che vengono supportati dall'applicazione di politiche coerenti in centinaia, se non migliaia, di siti facendo peraltro a meno delle complessità derivanti dall'implementazione e dalla gestione di appliance di sicurezza fisiche.

Le soluzioni SD-WAN avanzate come la piattaforma Aruba EdgeConnect SD-WAN edge consentono alle imprese di immettere localmente e in modo intelligente in Internet il traffico delle filiali diretto verso il cloud. Inoltre, il supporto di funzionalità che consentono la micro-segmentazione e l'applicazione delle politiche a un alto livello di dettaglio offre alle aziende la possibilità di rendere la propria WAN sicura, soddisfare i requisiti di conformità e proteggersi dalle violazioni.

L'orchestrazione automatizzata di un servizio di sicurezza fornito nel cloud della massima qualità integrato nella piattaforma application-aware Aruba EdgeConnect SD-WAN edge offre una potente soluzione SASE che non compromette né la funzionalità della rete né le funzionalità di sicurezza.

L'architettura SASE protegge l'azienda dalle minacce e offre prestazioni delle applicazioni e un'esperienza utente del massimo livello, contenendo nel frattempo i costi.

Tra i vantaggi dell'integrazione tra SD-WAN e sicurezza fornita tramite cloud ci sono:

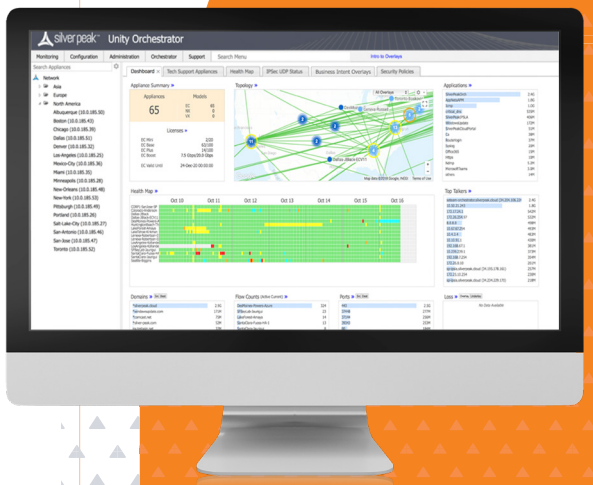
- una maggiore agilità aziendale e politiche IT semplificate grazie a un'architettura SASE che consente di sfruttare al massimo i vantaggi del cloud
- un'integrazione semplificata e snellita di funzionalità di sicurezza native del cloud con funzionalità SD-WAN ottimizzate
- la libertà di scegliere le soluzioni di sicurezza della rete ed SD-WAN migliori
- evitare di vincolarsi a un solo fornitore
- evitare di implementare costosi e complessi firewall di nuova generazione da gestire in ogni filiale
- la flessibilità di poter implementare, in futuro, soluzioni di sicurezza innovative

Automazione della sicurezza basata sul cloud con l'SD-WAN

Le aziende cercano modi sempre più semplici per integrare e gestire le proprie applicazioni sulla propria infrastruttura WAN e di sicurezza. Uno dei modi migliori per semplificare l'orchestrazione dei servizi di sicurezza basati sul cloud nelle filiali è sfruttare l'automazione della piattaforma Aruba EdgeConnect SD-WAN.

EdgeConnect sfrutta API (Application Programmable Interfaces) e l'orchestrazione di servizi di terze parti per integrarsi con i fornitori di sicurezza tramite cloud leader nel settore quali ZScaler, Check Point, NetSkope e Palo Alto Prisma Access. Aruba Orchestrator verifica le credenziali di sicurezza del cloud per connettersi e poi automatizzare o orchestrare il processo di connessione delle filiali nel tessuto dell'SD-WAN tramite i PoP di applicazione della sicurezza del cloud primario e secondario/opzionale più vicini.

Grazie all'intuitiva interfaccia utente di Aruba Orchestrator, la configurazione delle politiche di sicurezza diventa una semplice operazione di drag-and-drop. Le organizzazioni possono così applicare un set di politiche di sicurezza a tutte le filiali con un'unica azione.



Flessibilità e libertà di scelta

Il panorama delle minacce è in costante evoluzione e le aziende devono poter godere della flessibilità necessaria per adottare nuove soluzioni di sicurezza rapidamente e in maniera economicamente conveniente. È opportuno che le aziende prendano in considerazione piattaforme che consentano di integrare le migliori soluzioni di rete e di sicurezza. In questo modo possono evitare di dipendere dalle soluzioni proprietarie di un unico fornitore o di doversi accontentare di funzionalità basiche.

La piattaforma Aruba EdgeConnect SD-WAN, basata sulle esigenze dell'azienda, costituisce un pilastro fondamentale della miglior architettura SASE, poiché offre la possibilità di integrare nella miglior piattaforma SD-WAN i migliori servizi di sicurezza forniti nel cloud. Aruba EdgeConnect supporta inoltre le funzionalità di sicurezza di base necessarie per le filiali a complemento dei servizi di sicurezza forniti via cloud in modo da offrire un'architettura SASE senza interruzioni in tutta l'azienda.

Per maggiori informazioni, vai su www.arubanetworks.com/sdwan

eBook_Aruba-Edge-to-Cloud-Security_DC_062321 a00114994enw

aruba
a Hewlett Packard Enterprise company