Solution Brief

I 3 vantaggi principali del modello SASE e come ottenerli

Perché scegliere il SASE (Secure Access Service Edge)?

I moderni modelli di business digitale consentono nuovi livelli di coinvolgimento dei clienti e dei dipendenti, offrendo un accesso globale uniforme ad applicazioni e servizi, indipendentemente da dove i dipendenti e i clienti si connettano o da quali dispositivi utilizzino.

Con applicazioni e utenti distribuiti, la nozione tradizionale di sicurezza della rete non è più sostenibile in un mondo digitale. Gartner ha sviluppato un nuovo modello di rete e sicurezza compatibile con i requisiti dell'impresa digitale. Questo approccio è chiamato SASE (Secure Access Service Edge).

> L'architettura SASE fa la differenza. Idealmente, la soluzione nasce sul cloud ed è basata su microservizi, con la possibilità di offrire scalabilità in base alle esigenze. Per ridurre al minimo la latenza, i pacchetti devono essere copiati in memoria, elaborati e inoltrati/bloccati, e non vengono passati da macchina virtuale (VM) a VM o da cloud a cloud. Il set di servizi software non deve avere alcuna dipendenza hardware specifica e deve essere istanziato quando e dove necessario, per fornire un'ottimizzazione del rischio e funzionalità basate su policy per l'identità degli endpoint".— **Gartner**[1]

N°1

Riduce i costi e la complessità dell'IT

Con la diffusione dei dati tra applicazioni cloud e servizi SaaS, e con gli utenti che lavorano da qualsiasi luogo, il tradizionale modello di sicurezza basato sulla rete ha raggiunto il suo limite. Per compensare tale limite, le organizzazioni sono state costrette a implementare servizi aggiuntivi volti a colmare le lacune nella sicurezza; di conseguenza, sono aumentati significativamente i costi operativi, di implementazione e di gestione, ma i team non crescono con la stessa rapidità. Nonostante questo aumento dei costi e della complessità, il modello di sicurezza della rete non è comunque scalabile, non è agile e risulta semplicemente inefficace in un mondo digitale.

Invece di cercare di utilizzare un concetto obsoleto per risolvere un problema moderno, Zero Trust SASE rivoluziona l'approccio alla sicurezza. Mentre gli approcci legacy si concentrano sulla creazione di perimetri attorno alle applicazioni, il SASE si concentra sulle entità, come gli utenti che accedono alle applicazioni, portando la sicurezza il più vicino possibile a essi. In quanto servizio cloud, il SASE consente o nega le connessioni al servizio in modo dinamico, in base alle regole definite dall'organizzazione. Tutto questo viene svolto attraverso un singolo servizio che unifica diverse funzioni in precedenza separate, come SWG, ZTNA e così via.

COSA CERCARE

La componente più importante di una soluzione SASE efficiente è l'architettura su cui è costruita. Gartner ha definito dettagliatamente il tipo di architettura necessaria per mantenere la promessa su cui si fonda il modello SASE. È inoltre fondamentale che sia una soluzione costruita da zero per soddisfare la scalabilità richiesta da un servizio di sicurezza completamente fornito sul cloud.

Ciò significa che deve essere distribuita e supportare la multitenancy, per poter adattare le prestazioni a livello globale e in modo dinamico in base alla domanda. Deve allontanarsi dai principi della rete tradizionale e dei livelli di policy e basarsi invece sulle policy aziendali. Infine, questa architettura deve supportare una piattaforma realmente integrata con una gestione unificata distribuita sul cloud.

COSA EVITARE

Gartner mette specificamente in guardia contro gli approcci tradizionali alla sicurezza della rete che utilizzano soluzioni basate su VM nelle infrastrutture dei provider di servizi cloud. Questo tipo di approccio in un ambiente di computing IaaS non consentirà una scalabilità efficiente e fornirà un'esperienza utente incoerente, a causa dell'hairpinning del traffico tra i fornitori di servizi cloud e le applicazioni a cui accedono gli utenti.

Questo modello si fonda su un'architettura single-tenant che tenta di utilizzare policy di accesso basate sulla rete in un modello SASE basato sull'accesso degli utenti, creando distribuzioni molto più complesse che non rispondono ai criteri del SASE. Inoltre, questi approcci molte volte impiegano più prodotti non realmente integrati tra loro e assemblati mediante un'interfaccia utente di servizi indipendenti, spesso inglobati durante le acquisizioni.

> Il SASE è una soluzione emergente che combina in modo completo le funzionalità WAN con quelle di sicurezza della rete (come SWG, CASB, FWaaS e ZTNA), per supportare le esigenze di accesso sicuro e dinamico delle imprese digitali".— **Gartner**[1]

N°2 Offre un'esperienza utente ottimale

C'è una buona ragione per cui il SASE si concentra prevalentemente sull'esperienza utente. Quando gli utenti erano sulla rete, le applicazioni risiedevano nel data center, e i server e l'infrastruttura erano gestiti dall'IT; in questo contesto, era facile controllare e prevedere le prestazioni dell'esperienza utente. Oggi invece le applicazioni sono distribuite su più cloud, e nonostante questo il metodo di accesso è rimasto basato sul vecchio modello in cui la sicurezza era data da una VPN che si connetteva a una rete. Questo approccio porta l'utente alla sicurezza e non la sicurezza all'utente, un aspetto fondamentale per ottenere un'esperienza utente ottimale. Il SASE richiede che la sicurezza venga applicata vicino agli utenti, gestendo in modo intelligente le connessioni di questi ultimi in corrispondenza degli Internet Exchange e ottimizzando le connessioni dirette (peering) alle applicazioni e ai servizi cloud, per garantire una larghezza di banda ottimale e una bassa latenza.

COSA CERCARE

La chiave per offrire un'esperienza utente ottimale consiste nel fornire una larghezza di banda efficiente con la latenza più bassa possibile. L'unico modo per farlo in modo efficace è quello di ridurre i passaggi (i cosiddetti "hop") per accedere alle applicazioni e garantire che venga allocata la larghezza di banda corretta tramite appositi controlli.

Negli Internet Exchange, l'approccio giusto colloca il set di servizi di sicurezza il più vicino possibile all'utente attraverso una vasta distribuzione geografica. L'accesso alle applicazioni da questi punti di scambio richiede la capacità di instradare in modo intelligente il traffico verso la posizione geografica più prossima all'applicazione mediante il peering diretto.

COSA EVITARE

Le soluzioni basate su VM dei provider di servizi cloud o IaaS richiedono l'hairpinning del traffico. È importante notare che, come specificato nelle documentazioni relative ai modelli SASE, queste soluzioni non sono da considerarsi realmente tali, quindi dovrebbero essere evitate.

Ciò avviene principalmente perché le architetture basate su VM non offrono scalabilità e non controllano la connessione dell'utente, bensì operano dall'ambiente di calcolo dell'applicazione e non sono quindi in grado di garantire un'esperienza utente ottimale. Inoltre, queste soluzioni non sono scalabili in modo dinamico e richiedono una pianificazione dell'utilizzo che non offre la possibilità di consentire modifiche future senza periodi di inattività programmati.

> Un modello SASE deve consentire la definizione e l'applicazione delle policy ovunque vi siano identità endpoint [...]. Le soluzioni SASE che utilizzano solo la capacità della dorsale Internet dell'IaaS senza funzionalità locali di POP/edge generano latenza, problemi prestazionali e, di conseguenza, insoddisfazione negli utenti finali". — **Gartner**[1]

N°3

Riduce i rischi

La sicurezza consiste nell'identificazione e nell'eliminazione dei rischi. In quanto servizio cloud, Zero Trust SASE è progettato per affrontare le sfide specifiche della nuova realtà digitale, in cui utenti e applicazioni sono altamente distribuiti. Definendo la sicurezza come una funzione integrata nella struttura intrinseca del modello stesso, e non come una funzione separata dalla connettività dei servizi, questo servizio garantisce che tutte le connessioni siano ispezionate e protette, indipendentemente da dove si connettano gli utenti, da quali app stiano accedendo o dalla crittografia utilizzata.

COSA CERCARE

La chiave per ridurre il rischio risiede nella capacità di abbandonare i concetti della connettività basata sulla rete e connettere invece gli utenti alle applicazioni implementando il vero ZTNA (Zero Trust Network Access). Lo ZTNA garantisce che solo gli utenti autorizzati possano accedere a una data applicazione, e questa autorizzazione è definita attraverso policy aziendali delineate in modo semplice e a più livelli.

Un altro modo attraverso cui una piattaforma SASE riduce il rischio è eliminando la superficie di attacco. Nascondendo la rete aziendale e le identità sorgenti da Internet, il SASE impedisce agli aggressori di sferrare attacchi come il DDoS.

Il modello SASE viene fornito tramite un'architettura basata su proxy, che gestisce tutte le comunicazioni tra utenti e applicazioni. Questa architettura assicura che tutto il traffico possa essere decifrato e ispezionato; fornisce inoltre una visibilità completa. Infine, l'architettura SASE si fonda sul contesto completo dei dati che vengono scambiati tra entità e applicazioni, per garantire che tutte le connessioni soddisfino i requisiti di conformità e governance.

COSA EVITARE

Gli approcci tradizionali fondati sulla sicurezza del perimetro utilizzavano un modello basato su firewall che esaminava i flussi di pacchetti e determinava il rischio attraverso la loro ispezione. Questo modello funzionava bene in passato, ma è inefficiente di fronte alle nuove sfide della distribuzione basata su SASE.

Il problema più grande è che un'architettura firewall come servizio determina le minacce dopo gli eventi; queste sono quindi in grado di raggiungere la destinazione prima che vengano individuate. Il motivo è semplice: queste soluzioni non hanno la capacità di conservare i dati e di determinare i risultati prima dell'invio. Questa limitazione complica significativamente la decifrazione della sessione e la protezione dei dati, perché si tratta di funzioni che richiedono la conservazione e il riassemblaggio del flusso, in modo analogo a un proxy.

Con un servizio firewall, le funzioni di decifrazione, ispezione e riassemblaggio richiedono un processo separato dal servizio; questo complica le policy, introduce latenza e influisce negativamente sulle prestazioni, e spesso, quando implementato, fornisce funzionalità limitate. Il SASE richiede un'architettura single-pass per elaborare tutti i contenuti contemporaneamente. Le offerte firewall basate su stream espongono l'indirizzo IP sorgente della rete host a potenziali aggressori, rendendo a tutti gli effetti pubblica la superficie di attacco, che così può essere presa di mira dagli aggressori.

L'approccio di Zscaler al SASE

La piattaforma di cloud security di Zscaler, basata sull'IA, è un servizio SASE costruito da zero per massimizzare prestazioni e scalabilità. In quanto piattaforma distribuita a livello globale, gli utenti sono sempre vicini alle loro applicazioni e, attraverso il peering con centinaia di partner nei principali Internet Exchange di tutto il mondo, Zscaler garantisce prestazioni e affidabilità ottimali a utenti, workload, partner commerciali e sedi.

Zscaler Zero Trust SASE si basa sulla piattaforma SSE più collaudata del settore e adotta un nuovo approccio alla SD-WAN. Oggi, per una guida nell'era del digitale, più del 30% delle organizzazioni Forbes Global 2000 si affida a Zscaler.

Grazie alla sua consolidata esperienza nel mercato, Zscaler ha dimostrato che la sua architettura è progettata per garantire scalabilità: attualmente, ogni giorno elabora infatti oltre 360 miliardi di transazioni e oltre 500 bilioni di segnali giornalieri sfruttando l'effetto cloud basato sull'IA/ML.

L'architettura Zscaler Zero Trust SASE è distribuita attraverso oltre 150 data center in tutto il mondo, garantendo agli utenti connessioni sicure, veloci e locali, indipendentemente dalla loro posizione.

Per saperne di più sull'approccio di Zscaler al SASE, visita
zscaler.it/capabilities/secure-access-service-edge

[1] Gartner, The Future of Network Security Is in the Cloud; Lawrence Orans, Joe Skorupa, Neil MacDonald

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it