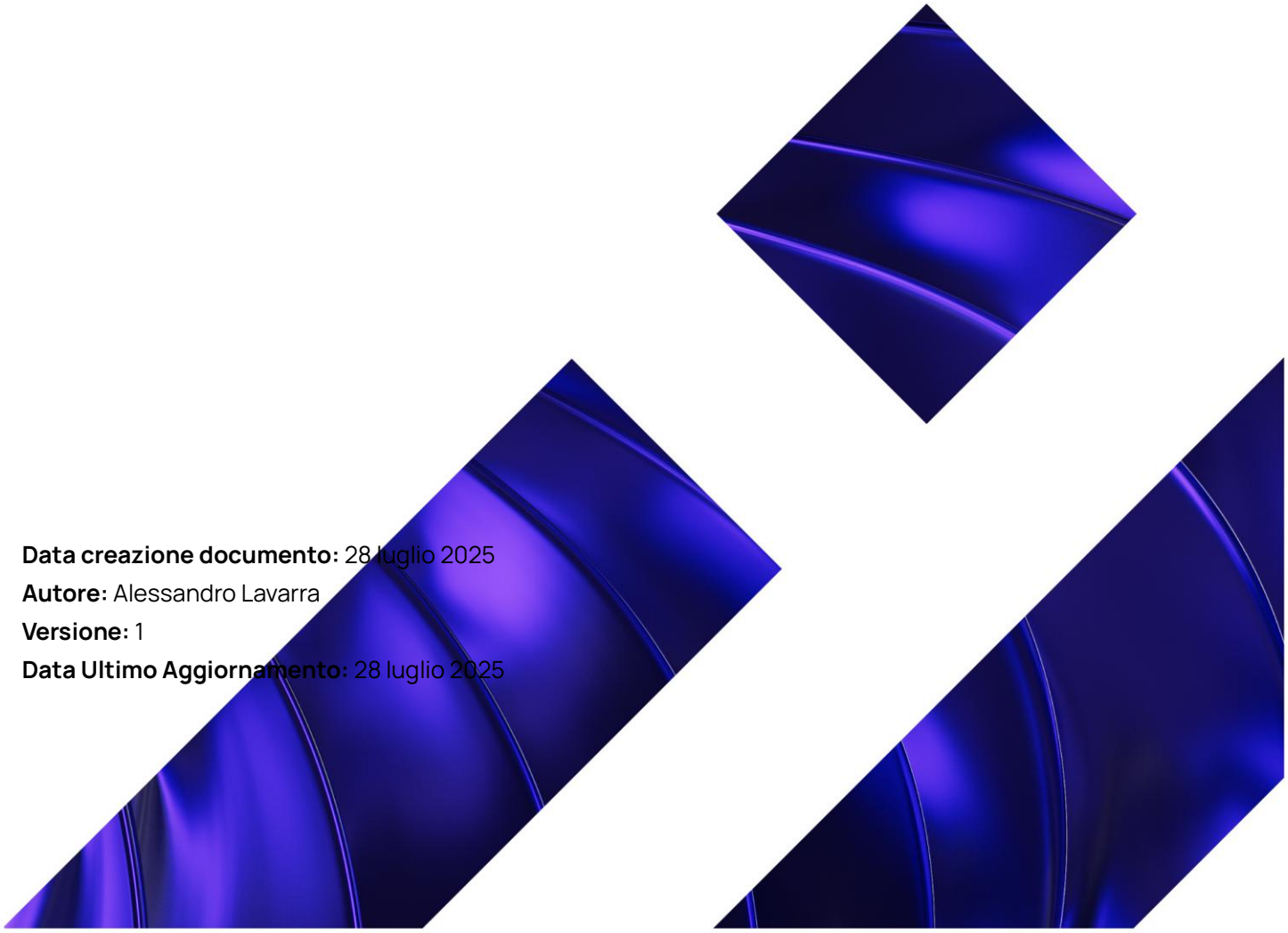
Road to SASE

Le sfide di connettività e sicurezza per le reti geografiche



Data creazione documento: 28 luglio 2025
Autore: Alessandro Lavarra
Versione: 1
Data Ultimo Aggiornamento: 28 luglio 2025

L'industria manifatturiera italiana controlla più di 7.000 aziende estere e impiega quasi un milione di persone in tutto il mondo. I Network Manager di queste imprese si trovano ad affrontare diverse sfide nell'amministrazione delle reti geografiche. Il loro compito è quello di garantire una connessione stabile e a costi contenuti per le filiali e gli utenti mobili, indipendentemente dalla loro posizione nel mondo, e di assicurare una gestione uniforme in tutte le periferie. Questo implica superare i compromessi tra costi, prestazioni e sicurezza.

Spesso con risorse scarse questi professionisti devono preoccuparsi della fornitura, configurazione e manutenzione degli apparati distribuiti nelle filiali con cicli di aggiornamento sempre più serrati e devono essere in grado di rispondere ai cambiamenti imposti dalle dinamiche aziendali a volte anche in ore ma sicuramente non in settimane o mesi.

Il tradizionale scenario, in cui i sistemi gestionali legacy e i sistemi dipartimentali erano centralizzati, poteva essere gestito mediante un'architettura a stella integrata con elementi di sicurezza perimetrale. Oggi, invece, è necessario rivedere l'intero sistema a causa dell'espansione del perimetro della WAN verso i servizi cloud, sia per le infrastrutture (IaaS) sia per le applicazioni (SaaS), e dell'adozione di nuove modalità di lavoro agile.

Nelle architetture tradizionali la connessione delle sedi è realizzata con circuiti MPLS o tunnel IPsec che, nel primo caso, offrono stabilità ma hanno il limite della rigidità e rappresentano un single point of failure e, nel secondo caso, espongono la comunicazione all'instabilità del traffico internet e fanno proliferare gli apparati di sicurezza da distribuire nelle periferie.

In aggiunta con l'aumento del traffico verso il cloud e i servizi SaaS queste reti "chiuse" perdono ancora più efficacia non essendo progettate per comprendere risorse esterne al proprio perimetro.

La situazione in termini di sicurezza è altrettanto eterogenea, e le diverse aziende adottano approcci diversi. Talvolta, all'interno dello stesso gruppo aziendale, si possono riscontrare forti disomogeneità dovute a fusioni o acquisizioni che comportano l'eredità di apparecchiature e architetture diverse da integrare nella propria infrastruttura IT oppure, ancora, per contenere i costi i branch più piccoli vengono trattati con soluzioni più economiche o riciclate da altre sedi in seguito ad aggiornamenti tecnologici.

Difficilmente sono coperte in modo uniforme le differenti categorie di soluzioni di network security, firewall o di accesso al cloud o della gestione degli utenti mobili e si riscontrano ampi margini di miglioramento in direzione della ricerca di uniformità nella strategia di mitigazione dei rischi.

Implementare SASE: l'evoluzione delle reti geografiche

Le architetture SASE (Security Access Service Edge) rappresentano una delle innovazioni più interessanti nel mondo delle reti geografiche degli ultimi vent'anni e offrono soluzioni ai limiti delle architetture tradizionali menzionati in precedenza.

L'acronimo SASE, coniato nel 2019 da Gartner, riassume i quattro punti chiave di questa approccio:

Security e Access indicano che si sta affrontando contemporaneamente la sicurezza e l'accesso alle risorse di rete.

Service fa riferimento alla sua natura completamente orientata al servizio, con funzionalità e prestazioni che operano in modo indipendente dalle infrastrutture fisiche e dall'hardware.

Edge si riferisce a tutte le estremità della rete, sottolineando così l'importanza di trattare in modo uniforme utenti, sedi periferiche, data center, servizi SaaS, terze parti e fornitori.

In sintesi, SASE rappresenta un paradigma che unisce i concetti di sicurezza e networking as a service, garantendo un approccio uniforme a tutti i punti della rete.

Dopo questa introduzione, esploreremo nel corso di questo articolo vari aspetti, tra cui:

- Il corretto posizionamento delle architetture SASE.
- Le premesse e i pre requisiti per la sua adozione
- Le caratteristiche dei fornitori e il processo di implementazione

Il corretto posizionamento delle architetture SASE.

Quando si considera l'adozione di architetture SASE è già implicito che stiamo parlando di reti geografiche e di organizzazione multi sede. Chiaramente più l'azienda è distribuita geograficamente e più alta è la numerosità di siti da gestire maggiori saranno i benefici dell'adozione di SASE grazie ad approccio centralizzato e unificato e alla riduzione di hardware distribuito localmente.

Altri aspetti importanti da valutare sono l'agilità e la capacità di adattamento richieste alla rete per rispondere ad esigenze di business. SASE infatti diventa particolarmente vantaggioso per gestire in modo flessibile cambiamenti nelle architetture come il passaggio a servizi cloud, nuove aperture di filiali o punti vendita, acquisizioni di stabilimenti, alta mobilità degli utenti…).

Le architetture SASE consentono di centralizzare e virtualizzare la gestione della rete, separandola dall'hardware, il che si traduce in notevoli vantaggi per le aziende con una rete distribuita e situazioni eterogenee da standardizzare.

In sintesi, ci sono diverse situazioni in cui un'organizzazione dovrebbe sicuramente valutare l'adozione di SASE:

Migrazioni verso Servizi Cloud - quando sono in programma migrazioni a servizi in cloud per cui la rete MPLS o SD-WAN tradizionale non garantisce accesso o facilità di implementazione,

Aperture e acquisizioni - quando sono in roadmap aperture o acquisizioni di filiali, uffici commerciali, punti vendita, centri logistici per cui garantire il rapido ed economico onboarding nella rete senza compromessi di performance e sicurezza e senza dover affrontare lunghi processi di acquisto, installazione e configurazione di apparati,

Gestione utenti mobili - se l'organizzazione richiede la gestione efficace degli utenti mobili in ottica ZTNA senza generare sovraccarico di traffico nei sistemi di rete e sicurezza,

Risorse IT limitate - Quando il personale IT è sottodimensionato o non esistono referenti IT adeguati nelle sedi periferiche e l'azienda deve gestire reti geografiche estese, SASE offre un vantaggio significativo attraverso la gestione centralizzata anche delle sedi remote e dei diversi fusi orari abilitando anche l'attivazione di servizi per una co-gestione della WAN con il fornitore di servizi.

Questi sono gli scenari in cui l'adozione di questo modello garantisce ritorni dell'investimento quasi immediati ma chiaramente SASE è un modello efficace anche per altri casi d'uso dal punto di vista tecnico, economico e strategico.

Premesse e pre-requisiti per l'adozione di SASE

Il team di lavoro

Trattandosi di una soluzione che garantisce la convergenza tra networking e sicurezza è necessario che "converga" anche la visione delle figure titolari dei diversi dipartimenti coinvolti.

Network manager e CISO dovranno condividere la valutazione delle tecnologie e ridisegnare assieme la strategia di implementazione e gestione delle regole. Nel caso di SASE la convergenza in un unico servizio permette di pensare alla rete e alla sicurezza partendo dal modello ideale progettato from scratch per l'intera organizzazione e man mano estenderlo alle periferie.

Ruolo del CIO

Il ruolo del CIO dovrà rafforzare le motivazioni all'implementazione di SASE di questi dipartimenti spesso legati a prodotti o tecnologie stand- alone per competenze acquisite, per abitudine, per lock-in tecnologico, tutti fattori che condizionano le scelte e che rendono poco intuitivo l'approccio SASE che riduce la complessità infrastrutturale legata all'hardware e ai singoli servizi e che pare semplificare fin troppo l'ecosistema di componenti, servizi, apparati.

Definire la priorità tra sicurezza e gestione rete

Il gruppo di lavoro così composto (CIO, network e security manager) dovrà immaginare il futuro della rete in ottica SASE partendo da una priorità tra sicurezza e gestione della rete condividendo l'architettura di atterraggio in una unica soluzione.

A volte il driver per il cambiamento è la rete (superamento dell'MPLS, costi e performance delle reti internazionali nelle aree più remote, eterogeneità di situazioni da gestire tra i siti..) oppure la sicurezza (bisogno di uniformare la gestione della sicurezza, allargamento del perimetro di sicurezza al cloud con servizi SSE, approcci ZTNA, rinnovo dei servizi di sicurezza perimetrale…)

Stabilita, tra questi due bisogni, la priorità sarà necessario scegliere il fornitore in base alla capacità di rispondere a questa prima esigenza e garantire una roadmap di adozione per la completa integrazione di tutti i componenti SASE consapevoli che SASE ha impatti duraturi e a lunga scadenza.

La scelta del fornitore

Fino a poco più di due anni fa, il panorama di SASE contava solo pochi vendor e soluzioni, e il nostro ruolo di consulenti era principalmente quello di diffondere conoscenza. Tuttavia, in un breve lasso di tempo, la situazione è cambiata radicalmente, e oggi esistono almeno una trentina di soluzioni che si riferiscono a SASE.

Tra queste, alcune rappresentano semplicemente etichette commerciali associate ad architetture tradizionali, che cercano di coprire i diversi casi d'uso di SASE. Altre sono aggregati di tecnologie più o meno integrate, mentre solo alcune sono considerate servizi "full" SASE.

Il mercato presenta tre categorie di fornitori in grado di implementare SASE:

Vendor e produttore che provengono da soluzioni SD-WAN. Questi fornitori hanno esteso i loro servizi, spesso tramite acquisizioni, per includere anche soluzioni di sicurezza integrandole alla gestione del networking per offrire una soluzione completa

Produttori di servizi SSE (Security Service Edge) : Questi fornitori, originariamente focalizzati sulla sicurezza, hanno acquisito o sviluppato soluzioni SD-WAN per gestire il trasporto dei dati dai siti ai punti di accesso ai loro servizi.

Offerte "native" SASE. Vendor che hanno progettato e sviluppato una soluzione SASE ex novo creando un ambiente integrato fin dall'inizio.

E' importante notare che, a differenza dei "nativi" SASE, nei primi due casi i vendor provengono da tecnologie verticali differenti e sarà necessario valutare l'integrazione effettiva e l'armonia della soluzione oltre che quanto effettivamente l'architettura sia *cloud native*.

La copertura dei casi d'uso SASE può essere raggiunta anche con l'aggregazione di differenti tecnologie di differenti vendor ma si perderebbero così tutti i benefici di semplificazione sia gestionale sia amministrativa.

A questo proposito Gartner ha introdotto la definizione di "single vendor SASE" per indicare soluzioni SASE omogenee e complete sviluppate, appunto, da un singolo attore.

Il processo di implementazione

La strategia SASE inizia, come abbiamo detto, definendo un obiettivo di consolidamento da molte soluzioni puntuali a un fornitore singolo con visione a lungo termine.

I punti di ingresso di una strategia SASE sono il bisogno di prestazioni di rete da un lato o la sicurezza dall'altro. La tendenza potrebbe essere quella di considerare soluzioni specifiche o troppo legate all'hardware per questi bisogni rischiando, così, di compromettere la futura adozione di SASE.

Le organizzazioni che attribuiscono importanza alla gestione unificata e agile, alla facilità di approvvigionamento, alla riduzione dell'onere operativo e all'esperienza d'uso degli operatori e non solo alla mera esigenza di rete o di sicurezza del momento dovrebbero iniziare da subito valutando offerte native single vendor SASE.

SASE come tutte le soluzioni a servizio si presta, tra l'altro, ad essere gestita con il contributo in un partner tecnologico, così da diminuire il carico di lavoro del team IT interno e ridurre l'impatto dato dall'improvvisa indisponibilità di personale.

Il mercato offre approcci MSP e MSSP o semplicemente di co-management e in questo caso i driver decisionali comprendono valutazioni con un approccio strategico all'outsourcing.

Esistono anche altri mercati adiacenti, con alcuni fornitori che offrono un sottoinsieme di funzionalità SASE. Ad esempio, molte soluzioni Zero Trust Network Access (ZTNA) stanno evolvendo per fornire sicurezza in linea per le applicazioni web e SaaS, ma non offrono un set completo di capacità.

E' raccomandabile limitare gli investimenti puntuali in subcomponenti di SASE (ad esempio, ZTNA autonomi, SWG o CASB o SD-WAN), oppure se necessario, mantenendo questi investimenti tattici con un impegno a breve scadenza e a costi contenuti per restare aperti all'adozione dei nuovi approcci SASE.

SASE, nei casi d'uso descritti sarà la soluzione su cui puntare nei prossimi anni per la gestione della WAN.

Conclusioni

Affrontare un progetto SASE richiede una visione a lungo termine e un atteggiamento aperto al cambiamento.

Le organizzazioni con reti geografiche consolidate nel tempo e legate da vincoli tecnologici devono adattare la loro gestione quotidiana e l'implementazione alle restrizioni imposte dall'architettura esistente. Al contrario, SASE offre l'opportunità di ripartire da zero e definire liberamente le regole e il comportamento desiderato della rete, estendendo gradualmente tali modifiche a tutte le periferie della rete, siti, utenti, servizi cloud e partner esterni.

Con un servizio SASE nativo, è possibile adottare un approccio top-down, iniziando dal Data Center e dai servizi che devono essere accessibili e procedendo per gruppi omogenei, definire le modalità di comunicazione tra utenti, siti e risorse di rete. Le regole vengono scritte una sola volta e propagate in tutta l'organizzazione, coprendo progressivamente filiali, utenti e servizi.

Il governo e la gestione della rete diventano centralizzati e indipendenti da componenti hardware e software distribuiti nelle periferie.

Un consiglio pratico è iniziare l'implementazione portando a bordo della nuova architettura nuovi siti o quelli che presentano maggiori vulnerabilità dal punto di vista della rete o della sicurezza. Ad esempio, le piccole filiali sprovviste di strumenti di sicurezza perimetrale comparabili a quelli delle altre sedi o le filiali con costi di connettività più elevati o prestazioni di rete inferiori. Le architetture SASE sono ideali per elevare il livello di sicurezza e prestazioni di rete delle periferie più critiche (com'è per il nostro manifatturiero spesso la Cina).

Oppure ancora, per alcune organizzazioni, un punto di partenza efficace potrebbe essere la sicurezza dei soli utenti mobili, poiché solitamente è necessario sovraccaricare la rete per mettere tutto il traffico in sicurezza oppure accettare il compromesso di gestire solo l'accesso ai servizi aziendali. SASE, invece, consente di implementare una strategia Zero Trust per gli utenti mobili, proteggendo contemporaneamente tutto il loro traffico senza backhaul del traffico in data center.

SASE rappresenta un passo avanti significativo nell'evoluzione delle reti aziendali e della sicurezza. La sua adozione richiede pianificazione, un approccio strategico e una volontà di adattarsi ai cambiamenti. Tuttavia, i vantaggi in termini di sicurezza, prestazioni e semplicità gestionale sono significativi e trasformano positivamente l'ambiente IT di un'organizzazione.