WHITE PAPER

Fortinet offre la soluzione SASE più flessibile

Sintesi preliminare

L'innovazione digitale, l'adozione del cloud e la recente e diffusa tendenza al telelavoro hanno trasformato radicalmente la rete. E con l'aumento della dipendenza dalle risorse basate su cloud, come le applicazioni Software-as-a-Service (SaaS) e i dati che passano dal data center ad ambienti multi-cloud, è emersa chiaramente la necessità di un nuovo approccio alla sicurezza dell'accesso alla rete, soprattutto alle sfide dell'attendibilità implicita insite nelle architetture di rete legacy.

Le odierne organizzazioni hanno bisogno di accedere immediatamente e ininterrottamente alle risorse e ai dati in rete e su cloud, tra cui le applicazioni business-critical, da qualsiasi luogo, su qualunque dispositivo, in qualsiasi momento. La sfida è rappresentata dal fatto che molti problemi derivanti dagli sforzi di innovazione digitale, come il cambiamento dinamico delle configurazioni di rete e la rapida espansione della superficie di attacco, fanno sì che molte soluzioni di sicurezza tradizionali non forniscono più il livello di sicurezza e controllo degli accessi che necessitano alle organizzazioni e agli utenti.

"I clienti vogliono semplicità, scalabilità, flessibilità, latenza bassa e sicurezza capillare. È dunque indispensabile che i mercati della sicurezza di rete e del perimetro della WAN convergano."[1]

Il SASE (Secure Access Service Edge) è una strategia aziendale emergente che combina le funzioni di sicurezza della rete con le funzionalità WAN. L'obiettivo del SASE è quello di supportare le esigenze di accesso dinamico e sicuro delle odierne organizzazioni, in linea con la strategia di rete orientata alla sicurezza che Fortinet sviluppa e promuove attivamente da anni. Il SASE svolge un ruolo fondamentale nel garantire che la sicurezza possa essere fornita ovunque, anche lungo il perimetro della WAN, del cloud, del data center (DC), del core e dei dispositivi endpoint utilizzati dai tanti dipendenti mobili che oggi telelavorano.

Iniziamo definendo accuratamente il SASE

Come per ogni tipo di tecnologia emergente, vi è ancora una certa incertezza sulla definizione precisa di una soluzione SASE. Si tratta di un'offerta rigorosamente basata su cloud? Oppure comprende anche soluzioni fisiche? E quali tecnologie sono coinvolte in una soluzione SASE?

Sebbene il SASE sia generalmente classificato come servizio fornito in cloud, vi sono circostanze comuni che possono richiedere una combinazione di soluzioni fisiche e basate su cloud per l'effettiva integrazione del SASE nella rete come, ad esempio, la combinazione della connettività SASE con i controlli di accesso alla rete e i dispositivi di sicurezza perimetrali, il supporto di un dispositivo fisico SD-WAN (specialmente uno che contiene uno stack di sicurezza completo) o anche la necessità di integrarsi con tecnologie come i controller LAN wireless o i punti di accesso Wi-Fi nelle filiali.

Oltre alle protezioni basate su cloud essenziali, una soluzione SASE solida deve anche supportare elementi come la segmentazione della rete e i requisiti di conformità che la sicurezza basata su cloud non può gestire senza spostare il traffico verso il cloud per l'ispezione. Per questo motivo, Fortinet fornisce le soluzioni più complete e flessibili per la distribuzione del SASE, che comprendono sia l'integrazione che la distribuzione di dispositivi fisici e su cloud.

Lo scopo del SASE è l'accesso sicuro

Concettualmente, il SASE è un tentativo di affrontare le sfide per la sicurezza create dai fornitori di SD-WAN che forse hanno messo a disposizione una soluzione di rete innovativa, ma non sono riusciti a includere nella loro offerta una sicurezza completa e integrata. Fortinet ha affrontato questa sfida a testa alta con una soluzione Secure SD-WAN perfettamente integrata che offre una robusta e ineguagliata suite di caratteristiche e funzioni sia di rete integrata che di sicurezza, caratteristiche e funzioni che rientrano nel concetto di rete orientata alla sicurezza e nella strategia della piattaforma Security Fabric che da anni proponiamo ai clienti.

Fortinet supporta una soluzione SASE perfettamente integrata con la più ampia gamma di soluzioni di sicurezza fisica e su cloud del mercato. La soluzione parte da questi elementi di sicurezza essenziali:

- **Una soluzione SD-WAN completamente funzionale.** Cuore della soluzione SASE, la SD-WAN deve includere elementi quali la selezione dinamica dei percorsi, le capacità di autoguarigione della WAN e la coerenza delle applicazioni e dell'esperienza utente per le applicazioni aziendali.
- **Un firewall di nuova generazione (NGFW) (fisico) o Firewall-as-a-Service (FWaaS) (basato su cloud).** Il SASE deve anche includere uno stack di sicurezza completo che copra sia gli scenari fisici che quelli basati su cloud. Ad esempio, le organizzazioni con

strategia di telelavoro avranno bisogno di una combinazione di sicurezza perimetrale e segmentazione interna per evitare che le minacce guest o Internet-of-Things (IoT) raggiungano risorse di rete aziendali limitate, abbinata a una sicurezza basata su cloud per l'accesso alle risorse ubicate online o su cloud. Un hardware fisico potenziato da processori e una sicurezza cloud-native scalabile possono fornire le stesse prestazioni elevate su scala, consentendo la massima flessibilità e sicurezza per l'organizzazione.

- **Lo ZTNA (Zero-Trust Network Access)** consente identificare utenti e dispositivi e autenticarli per le applicazioni. Poiché lo ZTNA è più una strategia che un prodotto, comprende diverse tecnologie che lavorano insieme. L'autenticazione multifattore (MFA) identifica tutti gli utenti. Sul lato fisico, lo ZTNA prevede il controllo della sicurezza dell'accesso alla rete (NAC), l'applicazione delle policy di accesso e l'integrazione con la segmentazione dinamica della rete per limitare l'accesso alle risorse in rete. Sul lato cloud, lo ZTNA supporta funzioni come la microsegmentazione con l'ispezione del traffico per la sicurezza delle comunicazioni est-ovest tra gli utenti e la sicurezza always-on per i dispositivi sia on-network che off-network. Combinando i servizi ZTNA fisici e basati sul cloud, le organizzazioni possono garantire l'accesso sicuro e l'applicazione delle policy, indipendentemente dal fatto che i dispositivi e gli utenti siano on-premises oppure off-premises.
- **Un Secure Web Gateway** serve per proteggere gli utenti e i dispositivi dalle minacce alla sicurezza online facendo rispettare le policy di sicurezza e compliance di Internet e filtrando il traffico Internet dannoso. Può inoltre far rispettare policy di utilizzo accettabile per l'accesso al web, garantire la compliance alle normative e prevenire la fuga di dati.
- **Un servizio basato su cloud CASB** consente alle organizzazioni di assumere il controllo delle loro applicazioni SaaS, tra cui la protezione dell'accesso alle applicazioni e l'eliminazione delle sfide dello shadow IT. Il servizio deve essere associato al DLP on-premises per garantire una prevenzione completa della perdita di dati.

Migliorare il SASE con tecnologie aggiuntive

Il SASE è progettato per migliorare e supportare l'innovazione digitale, ma non considerando un approccio olistico al SASE, le organizzazioni possono anche finire per creare un'altra soluzione di sicurezza isolata che deve essere gestita separatamente dal resto dell'architettura di sicurezza. Ciò può limitare gravemente sia la visibilità che il controllo in tutta la rete. Quindi, oltre a fornire gli elementi fondamentali necessari

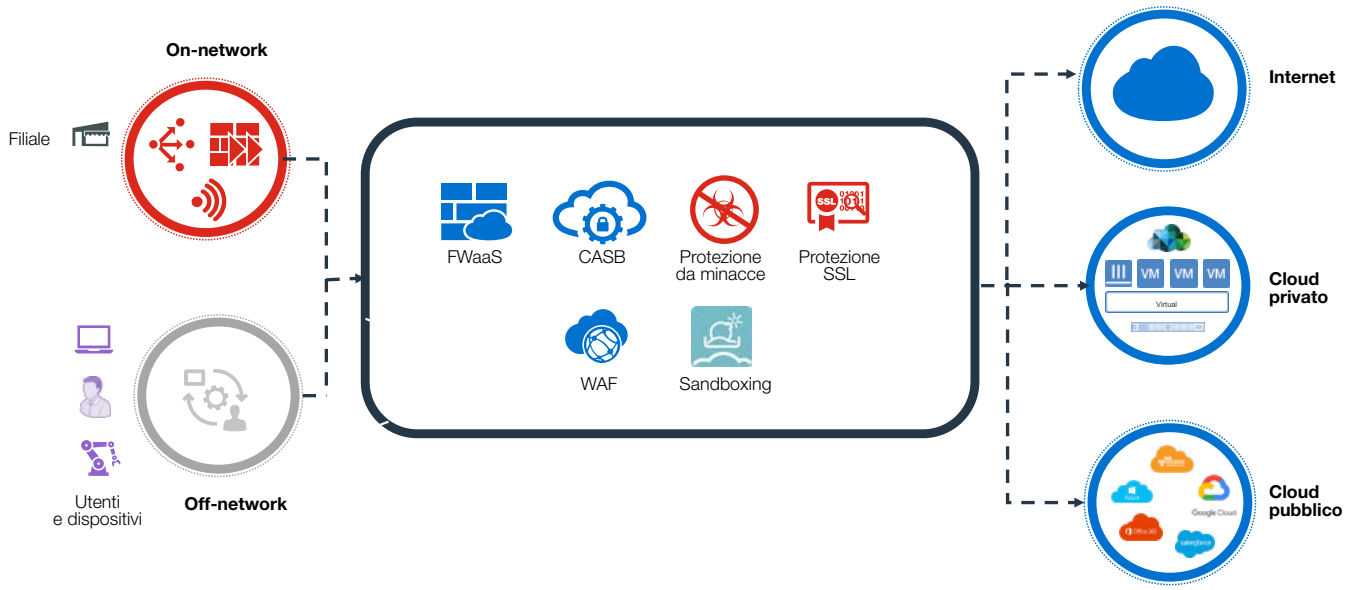

Figura 1: schema del SASE.

per garantire la robustezza di qualsiasi soluzione SASE, Fortinet propone anche strumenti opzionali progettati per estendere e migliorare la sicurezza degli utenti e dei dispositivi che utilizzano tale soluzione, facendo anche in modo che l'intera soluzione possa essere perfettamente integrata nel più ampio Security Fabric.

Ad esempio, la sicurezza degli endpoint, come la protezione degli endpoint (EPP) e le tecnologie di rilevamento e risposta degli endpoint (EDR), garantisce che i dispositivi che sfruttano il SASE siano essi stessi sicuri. Una rete privata virtuale (VPN) avanzata garantisce la sicurezza della trasmissione dati e delle transazioni, gestendo al contempo le complessità che possono sorgere rapidamente quando centinaia o migliaia di uffici e utenti remoti hanno bisogno di collegarsi tra loro. Infine, l'aggiunta di controller Wi-Fi e LAN sicuri assicura che il traffico in uscita o in entrata nella rete sia sottoposto a un ulteriore livello di ispezione.

Ogni organizzazione ha le proprie esigenze, ma è illogico che le organizzazioni adottino solo le tecnologie considerate "core" per il SASE se una soluzione di rete e sicurezza più completa è in grado di fornire all'azienda una gamma più ampia di risultati.

Tante potenzialità e troppo pochi fornitori qualificati

Sebbene il SASE sia stato progettato per affrontare le sfide di controllo dell'accesso e sicurezza della WAN che le odierne organizzazioni si trovano ad affrontare, il problema è che pochissimi fornitori sono qualificati per fornire una soluzione SASE completa. Ad esempio, pochi loro strumenti, se non nessuno, soprattutto i componenti di sicurezza, sono stati testati o certificati. Ciò significa che i consumatori non hanno modo di sapere se i servizi di sicurezza che stanno acquistando li proteggeranno in un ambiente reale.

Questo è già motivo di grave preoccupazione anche nel campo della sicurezza informatica altamente specializzata, dove i fornitori talvolta si sottraggono ai test e alla convalida di terzi quando le loro soluzioni non sono all'altezza delle aspettative del settore. Il problema si amplifica quando i fornitori, pur con un'esperienza di sicurezza minima o limitata, commercializzano soluzioni SASE sottolineando l'accattivante termine "SASE".

Il vantaggio Fortinet

Spesso ci viene chiesto: "Qual è la strategia SASE di Fortinet?" Affinché il SASE funzioni bene, tutti i suoi componenti devono interagire come un unico sistema integrato di connettività, rete e sicurezza, un concetto che ci suona molto familiare anche perchè da anni offriamo i requisiti fondamentali del SASE, e molto di più, nell'ambito della nostra piattaforma di sicurezza integrata e dell'architettura Security Fabric. Ciò crea una vera convergenza tra le funzioni di rete e sicurezza nel quadro di un approccio alla rete orientato alla sicurezza che promuove ulteriormente la rapida accelerazione dell'innovazione digitale, senza mai rinunciare alla protezione. Alcuni nostri clienti intenzionati a introdurre un SASE si sono accorti che, con piccoli adeguamenti, già disponevano di una soluzione SASE grazie alla potenza del Security Fabric.

Il SASE si adopera per risolvere un problema reale, ma è lo stesso tipo di problema che Fortinet ha già affrontato in passato.

- Siamo stati il primo grande fornitore di sicurezza a integrare completamente la sicurezza nella SD-WAN perché siamo riusciti a combinare anni di esperienza nel campo della sicurezza e del networking in un'unica soluzione.
- Abbiamo poi compiuto un passo in più sviluppando il primo processore SD-WAN al mondo progettato per accelerare le funzionalità di rete e sicurezza fornendo il livello di prestazioni richiesto dagli odierni ambienti di rete più esigenti.
- Siamo orgogliosi che oggi gli strumenti di sicurezza Fortinet siano le soluzioni più testate, validate e certificate del settore.

Ciò significa che fornire il tipo di soluzione SASE di cui un'organizzazione ha bisogno fa già parte del nostro approccio alla rete e alla sicurezza. E possiamo personalizzare la soluzione con una gamma di tecnologie avanzate di connettività e sicurezza, assicurando che sia progettata per adattarsi all'evoluzione delle esigenze dell'azienda. Il Security Fabric di Fortinet può anche integrarsi e connettersi con altre soluzioni aziendali, sia on-premises che in cloud. E tutti questi elementi sono coperti dal nostro sistema di gestione basato su un'unica interfaccia per garantire un'ampia visibilità e un controllo capillare di tutta la rete, compreso l'ambiente SASE.

Fortinet è in una posizione unica per offrire una soluzione SASE completa che garantisca una sicurezza costante in tutta la rete, non solo lungo il perimetro della WAN e del cloud, ma anche lungo il perimetro del DC, della rete core e degli endpoint, per una connettività, una visibilità e un controllo senza soluzione di continuità.

Siamo entusiasti del recente slancio del mercato intorno al SASE perché conferma ulteriormente il nostro approccio al Security Fabric e sottolinea ciò che diciamo da anni. Nell'era della connettività nel cloud e dell'innovazione digitale, la rete e la sicurezza devono convergere. Non si può tornare ad architetture antiquate e compartimentate. I prodotti Fortinet è sono pensati per l'era SASE e ben oltre.

[1] Frank Marsala, "The Future of Network Security Is in the Cloud," Gartner, 13 settembre 2019.

FORTINET®

www.fortinet.com

febbraio16,202112:30PM

742476-0-0-IT