Requisiti per una strategia di rete orientata alla sicurezza, da SD-WAN a SASE

L'innovazione digitale costringe tutte le organizzazioni a riprogettare le proprie reti e fornire una migliore esperienza utente a dipendenti e clienti. Il perimetro, un tempo punto di accesso ristretto ai confini della rete, ora si estende a tutta l'infrastruttura IT e introduce nuove esigenze a livello di data center, WAN, LAN e perimetro del cloud. Più recentemente, la pandemia da COVID-19 ha evidenziato la necessità di piani di business continuity che includano un accesso remoto flessibile, ovunque e in qualsiasi momento, sicuro e su larga scala.

Nel contempo, le minacce alla sicurezza non stanno diventando meno sofisticate o frequenti. Oltre un terzo delle violazioni dei dati nel 2020 è stato frutto del social engineering.[1] Questo è solo un esempio del motivo per il quale fornire una sicurezza migliore riprogettando la rete sta diventando fondamentale per tutte le aziende.

Una **strategia di networking orientata alla sicurezza** accelera la convergenza della rete e della sicurezza nell'ambiente connesso (tutti i perimetri e gli utenti) dal centro alle filiali e nel cloud. Questa strategia consente alle organizzazioni di difendere efficacemente gli odierni ambienti estremamente dinamici, preservando al contempo un'eccellente esperienza utente per dipendenti e clienti.

Ponendo al centro la sicurezza, le reti possono evolvere, espandersi e adattarsi alle innovazioni digitali con facilità ai livelli di cui la prossima generazione di calcolo (ad esempio, hyperscale, multicloud, 5G e altre tendenze in rapida ascesa) ha tanto bisogno. La convergenza tra rete e sicurezza significa sicurezza flessibile, sempre e ovunque.

Una strategia di networking orientata alla sicurezza accelera la convergenza della rete e della sicurezza nell'ambiente connesso (tutti i perimetri e gli utenti) dal centro alle filiali e nel cloud.

Elementi fondamentali di una strategia di rete orientata alla sicurezza

Una strategia di rete orientata alla sicurezza deve soddisfare in generale tre esigenze:

- **Capacità di gestire il rischio esterno e interno per gli utenti on-network**
- **Capacità di fornire una sicurezza flessibile cloud-native per gli utenti off-network**
- **Capacità di migliorare l'esperienza utente nel suo complesso riducendo i costi della WAN**

Il primo passo per ottenere una rete orientata alla sicurezza è l'**applicazione di unità di elaborazione della sicurezza personalizzate**, o ASIC, che consentono ai team di gestire la rete e la sicurezza in modo molto veloce, e consentono il **consolidamento di tutte le caratteristiche di sicurezza**, compreso il controllo delle applicazioni, il firewall e i sistemi di prevenzione delle intrusioni (IPS), in soluzioni come i firewall di rete senza compromettere la funzionalità o le prestazioni. Tra i casi d'uso richiesti rientrano SD-WAN, firewall di prossima generazione (NGFW), IPS, ispezione SSL (Secure Sockets Layer), controllo delle applicazioni, web filtering, antivirus e antimalware, sandboxing e segmentazione accelerata. (Quest'ultimo elemento è particolarmente importante per una strategia di rete orientata alla sicurezza, perché molti firewall non sono in grado di gestire l'eccesso di elaborazione necessario per supportare la segmentazione interna dinamica.)

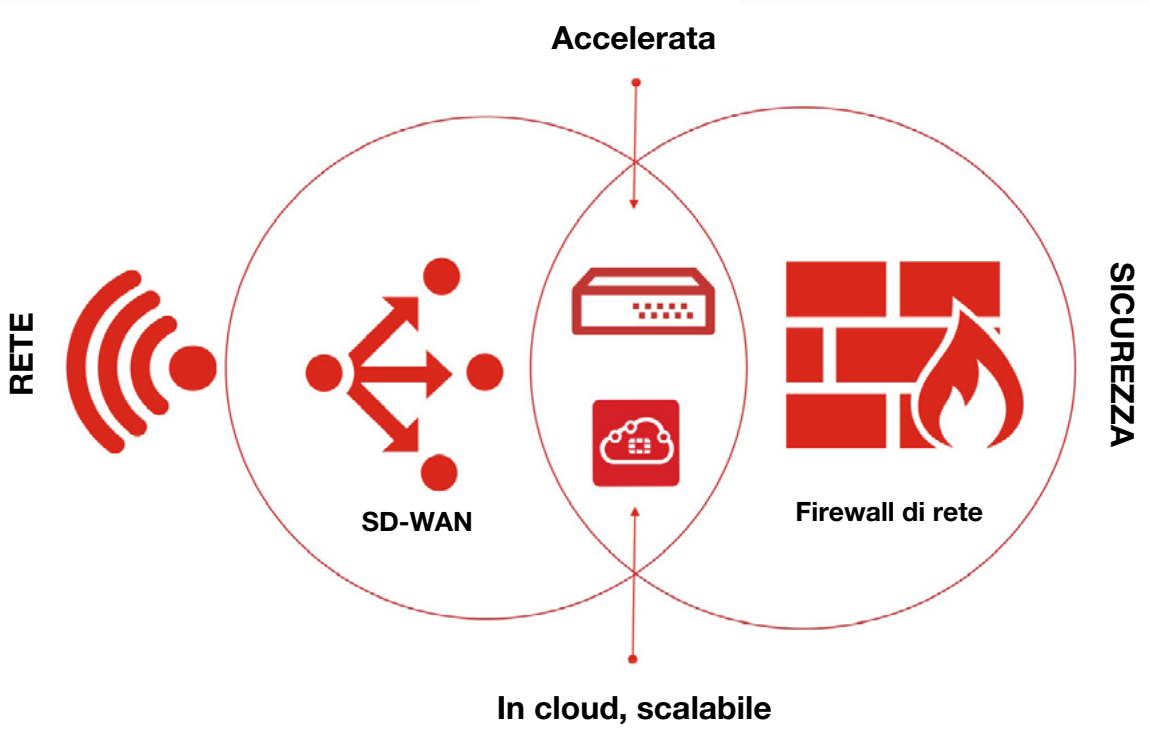
L'**architettura cloud appositamente costruita** permette la convergenza tra rete e sicurezza per le organizzazioni che adottano in via prioritaria il paradigma cloud (cloud first) o sono alla ricerca di flessibilità nella distribuzione di soluzioni.

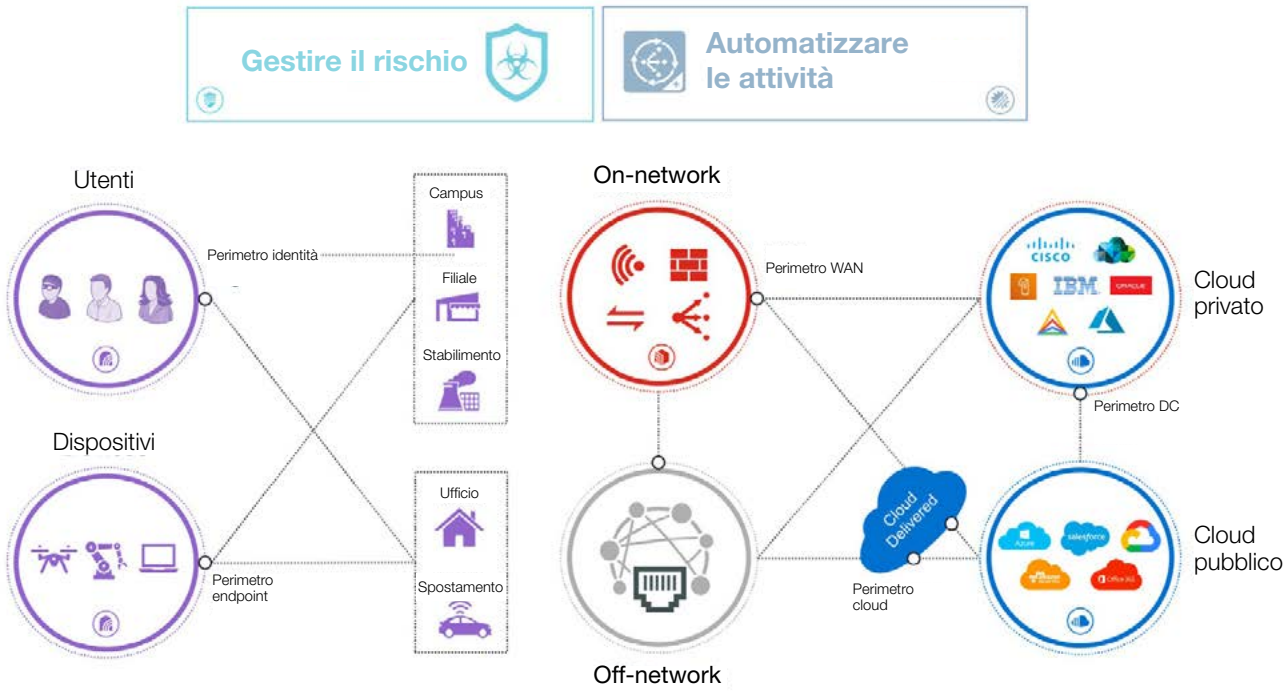
In futuro, le soluzioni firewall di rete dovranno anche **supportare i data center ibridi e hyperscale e le prestazioni 5G**. Le ultime innovazioni ad alte prestazioni (come i flussi di lunga durata, l'edge computing, la protezione dell'HDTV e di altro traffico di rich media, le reti 5G e la segmentazione interna dinamica) richiederanno livelli di prestazioni senza precedenti da un NGFW. Ma alcune soluzioni, non essendo state progettate pensando a queste prestazioni, semplicemente non saranno in grado di soddisfare tali esigenze future senza notevoli investimenti, e in molti casi neanche investendo.

Una strategia di rete orientata alla sicurezza trasforma il perimetro della WAN con una SD-WAN di classe enterprise completamente integrata in un dispositivo NGFW, integrazione che contribuisce a rendere la **SD-WAN** veramente sicura, diversamente dalla tecnologia SD-WAN che ha bisogno della sicurezza come overlay. Un approccio robusto alla SD-WAN include anche l'analisi predittiva basata sull'intelligenza artificiale (AI), l'orchestrazione intuitiva e la capacità di autoguarigione.

Infine, le organizzazioni devono estendere la sicurezza al perimetro delle reti cablate e wireless attraverso una profonda integrazione, consentendo un'applicazione coerente e pervasiva della sicurezza al perimetro della LAN. Queste sono le **condizioni per reti reattive e consapevoli del loro stato di salute** che estendono la sicurezza al perimetro di accesso e della rete.

Tutti questi perimetri richiedono inoltre una **gestione centralizzata** per ridurre la complessità e consentire all'automazione di rendere la rete più agile.





La giusta base per proteggere il perimetro del cloud: SASE

Oggigiorno e in futuro, se parliamo di una rete orientata alla sicurezza non possiamo non parlare di SASE (Secure Access Service Edge). Il SASE è un framework aziendale emergente che combina funzioni di sicurezza della rete a funzionalità WAN per supportare le esigenze di accesso dinamico e sicuro delle odierne organizzazioni, in linea con una strategia di rete orientata alla sicurezza. Il SASE svolge un ruolo fondamentale nel garantire che la sicurezza possa essere garantita ovunque, soprattutto lungo il perimetro del cloud, e nel proteggere gli utenti remoti e mobili.

Il SASE è generalmente classificato in termini di cloud computing, ma 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. Fondamentalmente, il SASE consente alle organizzazioni di **proteggere gli utenti remoti** con una sicurezza sempre attiva (indipendentemente dalla loro posizione), creando una migliore esperienza utente e una maggiore produttività, poiché utilizzano il perimetro del cloud appositamente costruito per percorsi a bassa latenza ottimizzati.

Un'offerta SASE e una strategia di rete orientata alla sicurezza completa non sono la stessa cosa. Oltre alle protezioni basate su cloud essenziali descritte nella definizione nota di SASE,[2] 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.

È allora che il SASE diventa la base per una strategia di rete orientata alla sicurezza completa, in grado di garantire la sicurezza e le prestazioni richieste ovunque dalle organizzazioni.

[1] "2020 Data Breach Investigations Report," Verizon, maggio 2020.

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

FORTINET

www.fortinet.com

febbraio 16, 2021 12:25 PM

745599-0-1-IT