Panoramica su Zero Trust SD-WAN

I vantaggi della soluzione:

Riduzione della complessità
Elimina la complessa rete di VPN site-to-site e il routing di overlay.

Esperienza utente migliore
Elimina l'inutile backhauling del traffico e migliora le prestazioni di app SaaS e cloud senza compromettere la sicurezza; inoltre, applica policy per la sicurezza e la larghezza di banda in oltre 150 data center di Zscaler in tutto il mondo.

Sicurezza migliore
Riduci al minimo la superficie di attacco e il rischio di movimento laterale delle minacce insito nella SD-WAN tradizionale e semplifica la segmentazione da utente ad app e da app ad app utilizzando la piattaforma nativa del cloud Zero Trust Exchange.

Zero Trust SD-WAN connette in modo sicuro filiali, stabilimenti produttivi e data center senza la complessità delle VPN, garantendo un accesso zero trust a utenti, dispositivi IoT/OT e applicazioni in base alle policy dell'organizzazione. Combinando la potenza della piattaforma più avanzata del settore, Zscaler Zero Trust Exchange, con la connettività ottimizzata per sedi, cloud e utenti, le organizzazioni possono adottare un framework SASE (Secure Access Service Edge) e ottenere un'esperienza altamente flessibile e collaborativa.

Perché accontentarsi della SD-WAN tradizionale?

Le SD-WAN tradizionali espandono la superficie di attacco e consentono il movimento laterale delle minacce, che rende le reti vulnerabili. Inoltre, le SD-WAN tradizionali connettono più sedi utilizzando VPN site-to-site; questo introduce complessità nella rete, in quanto le organizzazioni devono comunque continuare a gestire tabelle di routing. Questi overlay instradati attribuiscono l'attendibilità in modo implicito, offrendo alle entità che si connettono alla rete un accesso illimitato alle risorse critiche. Oggi, molte minacce hanno origine proprio dalle filiali, a causa di utenti, dispositivi IoT/OT o server compromessi.

SD-WAN zero trust

- Zero Trust SD-WAN fornisce alle filiali e agli stabilimenti produttivi un accesso rapido e affidabile a Internet, SaaS e applicazioni private attraverso un'architettura direct-to-cloud che offre una sicurezza di livello superiore e un'operatività più semplice.
- Elimina il movimento laterale delle minacce, in quanto utenti e dispositivi IoT/OT vengono collegati direttamente alle applicazioni attraverso Zero Trust Exchange.
- Semplifica drasticamente le comunicazioni delle filiali eliminando il routing complesso, le VPN e i firewall, consentendo al contempo un inoltro flessibile e facilitando la gestione delle policy utilizzando il collaudato framework di ZIA e ZPA

Casi d'uso della soluzione

Sostituisci le VPN site-to-site

Sostituisci la rete di VPN site-to-site che collega filiali, stabilimenti produttivi e data center sostituendola con una semplice connettività plug and play che facilita le operazioni e potenzia la sicurezza.

Accesso sicuro alle risorse IoT/OT

Per massimizzare i tempi di attività della produzione ed evitare le interruzioni dovute ai guasti delle apparecchiature o a problemi nei processi, i dipendenti e i fornitori terzi devono poter accedere regolarmente agli asset IoT/OT. Zero Trust SD-WAN semplifica l'accesso alle risorse IoT/OT senza ricorrere a VPN e senza porte esposte, offrendo a fornitori e collaboratori un accesso desktop remoto completamente isolato e clientless ai sistemi target RDP e SSH interni.

Accelera l'integrazione di fusioni e acquisizioni

Favorisci l'operatività sin dal primo giorno senza la necessità di unire domini di routing o tradurre indirizzi IP sovrapposti. Connetti nuovi utenti a risorse critiche come Active Directory in modo facile, aggiungendo semplicemente dispositivi plug & play nelle nuove sedi.

Rilevamento e classificazione dei dispositivi IoT/OT

I team IT devono fronteggiare la presenza di punti ciechi quando i dispositivi non autorizzati e sconosciuti si collegano alle reti delle filiali; il risultato è l'accrescimento del rischio di subire infezioni di malware in tutta l'organizzazione. Zscaler identifica e classifica i dispositivi per offrire ai team IT una visibilità più granulare sul comportamento e ottimizzare le policy per il controllo degli accessi.

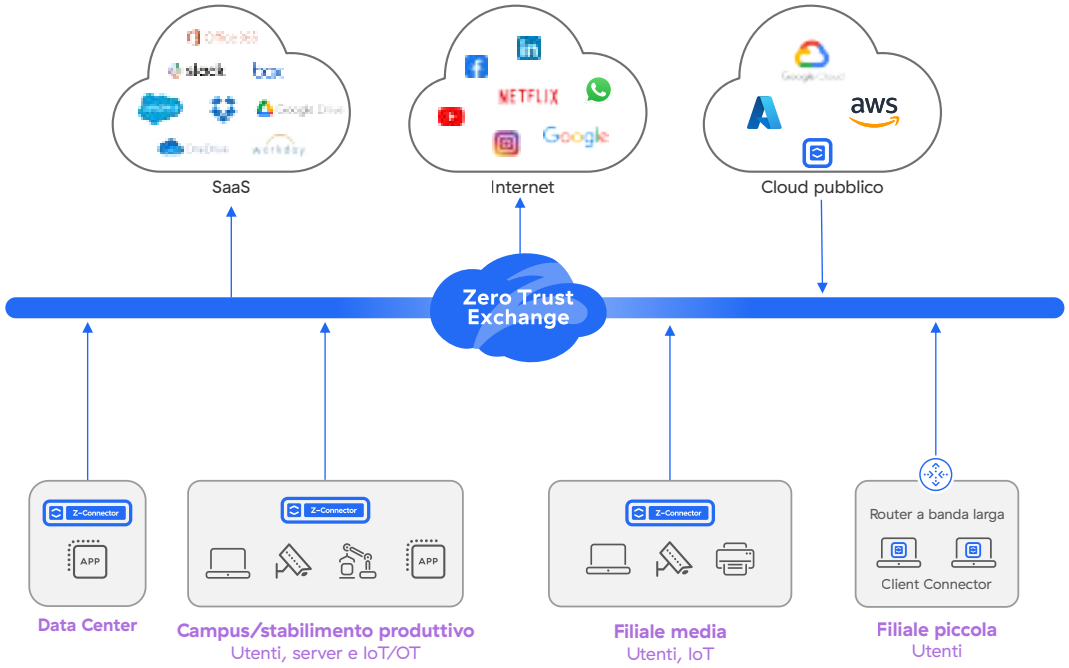

Figura 1: Zero Trust SD-WAN

Zero Trust SD-WAN è un dispositivo plug & play disponibile in formato virtuale o fisico.

Modelli hardware e software di Zero Trust SD-WAN

Funzionalità	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
Tipo	Filiali medio-piccole	Filiale medio-piccola	Filiale medio-grande	Filiale e data center
Throughput/hypervisor	200 Mbps	500 Mbps	1 Gbps	KVM, ESXi
Porte fisiche	4	6	8	N/D
Provisioning zero-touch	✓	✓	✓	✓
Policy di inoltro granulari per Internet, applicazioni private e traffico WAN diretto	✓	✓	✓	✓
Sfrutta il filtraggio degli URL, le policy per il controllo dei tipi di file e per i firewall cloud per il traffico diretto a Internet	✓	✓	✓	✓
Policy zero trust di ZPA per i dispositivi IoT e i server	✓	✓	✓	✓
Visibilità e logging centralizzati	✓	✓	✓	✓

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.it