Scheda tecnica

Zscaler Zero Trust SD-WAN

Connetti in modo sicuro filiali, stabilimenti produttivi e data center ed estendi la sicurezza zero trust a server e dispositivi IoT/OT in qualsiasi luogo.

Con lo spostamento delle applicazioni private sul cloud e l'accesso degli utenti alle applicazioni tramite la rete Internet pubblica, su qualsiasi dispositivo e da qualsiasi luogo, il lavoro flessibile e la trasformazione cloud hanno stravolto i modelli di rete e sicurezza basati sul perimetro.

Nel mondo di oggi, per semplificare le operazioni, numerose imprese usano i dispositivi IoT/OT in molte delle loro sedi, tra cui filiali, stabilimenti produttivi e data center. Inoltre, un numero considerevole di clienti fa affidamento sulla comunicazione dei workload da server a client. I modelli tradizionali, che dipendono da WAN legacy, VPN mesh e firewall per gestire l'accesso alle applicazioni, sono ormai inefficaci in una realtà che dà la priorità alle tecnologie cloud e mobili.

Con l'evoluzione delle esigenze delle organizzazioni, le soluzioni WAN legacy faticano sempre di più a rimanere al passo. La SD-WAN presenta varie sfide, come il limitato livello di sicurezza derivante dall'accesso basato sulla rete, la superficie di attacco estesa, i privilegi eccessivi che favoriscono il movimento laterale e la complessità del routing. L'applicazione dei principi zero trust a questa rete spesso richiede l'aggiunta di ulteriori dispositivi firewall, che incrementano i costi e accrescono la complessità.

Zscaler Zero Trust SD-WAN:

- **Abilita lo zero trust ovunque**, per tutti gli utenti, i dispositivi, i server e gli strumenti IoT/OT, indipendentemente dalla posizione
- **Migliora le prestazioni delle applicazioni**, inviando il traffico delle filiali direttamente a Zero Trust Exchange e il traffico delle applicazioni attendibili direttamente a Internet tramite punti di accesso diretto
- **Previene il movimento laterale delle minacce**, in quanto lo zero trust crea le basi per una connettività sicura che consente la segmentazione est-ovest
- **Elimina la superficie di attacco**, collegando le filiali e i data center tramite Zero Trust Exchange indipendentemente dal vettore di trasporto sottostante
- **Consente il rilevamento e la classificazione dei dispositivi nello shadow IoT** con la classificazione automatica dei dispositivi in base ai profili del traffico
- **Semplifica l'accesso sicuro alle risorse OT**, fornendo un accesso clientless basato su browser alle porte SSH/RDP/VNC sugli asset OT
- **Applica policy di inoltro ottimizzate e granulari** per il traffico Internet e non, utilizzando ZIA o ZPA
- **Introduce l'implementazione plug-and-play:** il provisioning zero touch (ZTP) semplifica la distribuzione e riduce i tempi associati all'integrazione

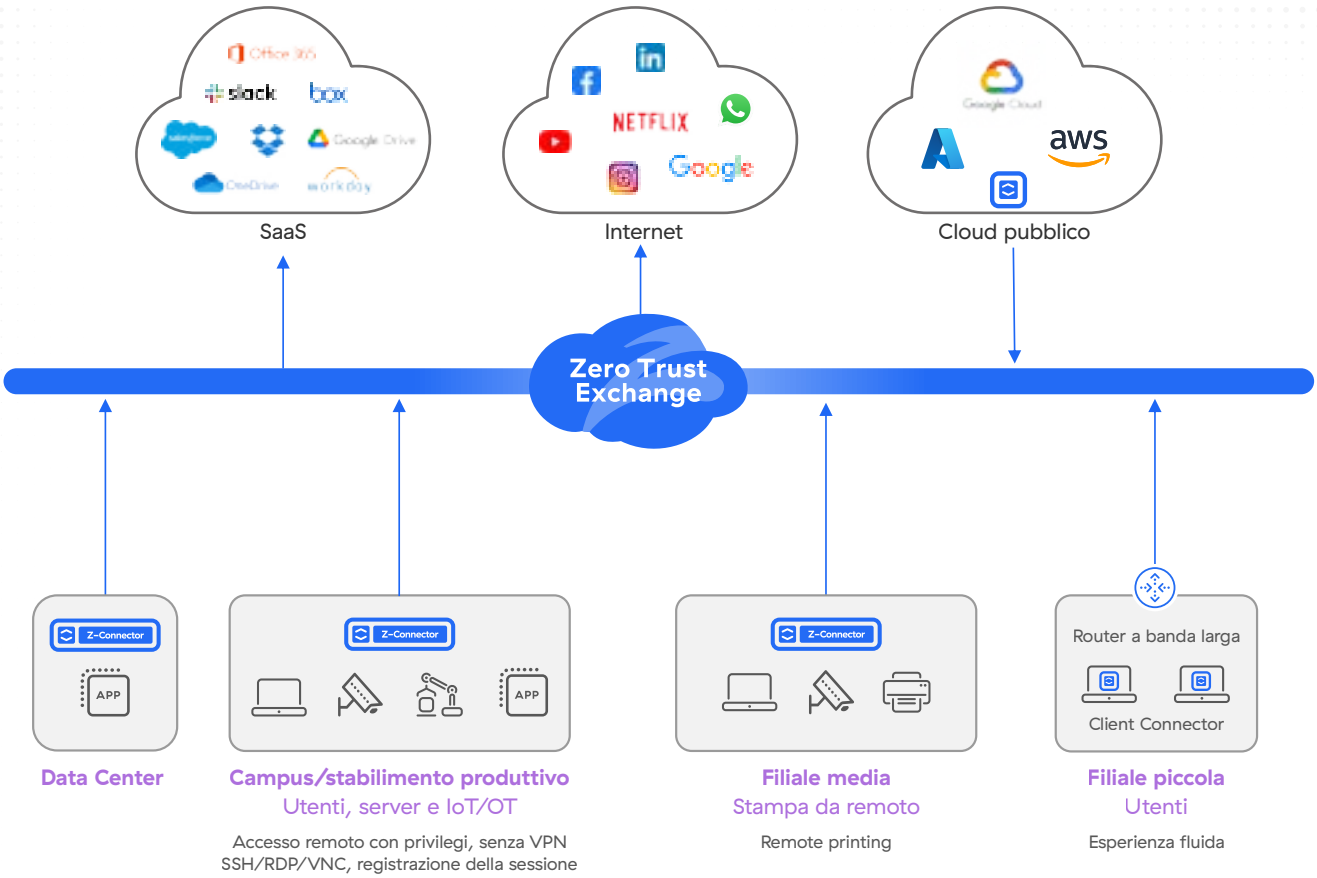

Figura 1: Zero Trust SD-WAN

Zero Trust SD-WAN connette in modo sicuro filiali, stabilimenti produttivi e data center senza la complessità delle VPN, garantendo un accesso zero trust tra utenti, dispositivi IoT/OT e applicazioni basato sulle policy dell'organizzazione.

La SD-WAN tradizionale non è zero trust

Quando si affidano ad architetture di rete e di sicurezza legacy per connettere una filiale a Internet o ad altre applicazioni in un ambiente cloud pubblico o nei data center, le organizzazioni si trovano davanti a non poche sfide, tra cui:

- **Un maggiore rischio di minacce laterali e attacchi Internet** derivante dall'utilizzo di soluzioni di connettività legacy incentrate sulla rete, come VPN site-to-site, firewall o SD-WAN tradizionali. Queste soluzioni estendono in modo eccessivo la rete considerata attendibile su Internet ad altri cloud e ambienti locali, incrementando di conseguenza la superficie di attacco. Un insieme incoerente di dispositivi, strumenti e policy di sicurezza contribuisce inoltre ad accrescere i rischi, in quanto genera lacune note e sconosciuti nella sicurezza.

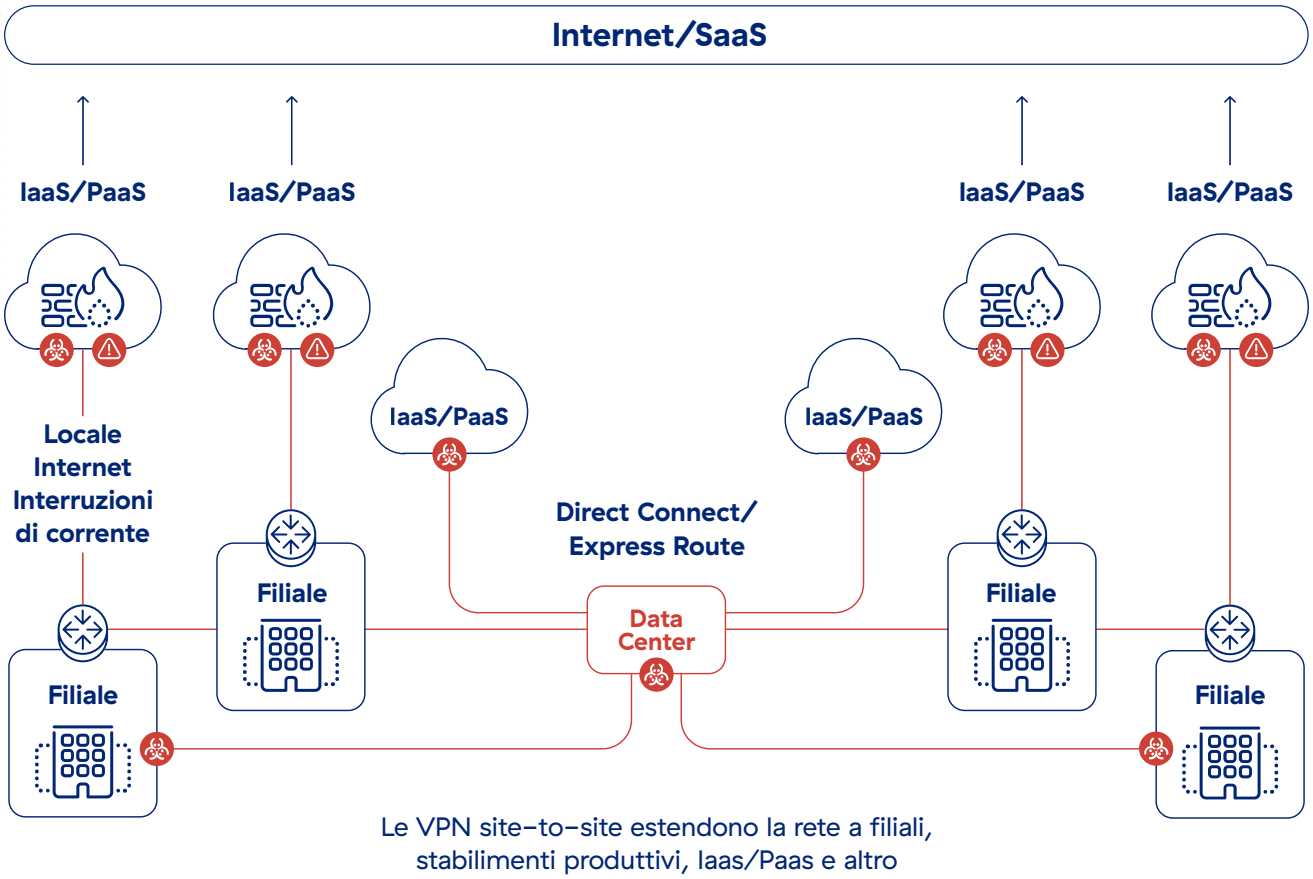

Figura 2: maggiore rischio di minacce laterali e attacchi basati su Internet con le SD-WAN tradizionali

- **Una maggiore complessità**, dovuta al routing complicato, ai troppi hop e dispositivi di rete e alla gestione frammentata delle policy, derivante dall'introduzione di modelli legacy sul cloud. Gestire tale livello di complessità è un compito arduo per i team di networking e sicurezza, che lottano per standardizzare la connettività e applicare policy di sicurezza nelle filiali, nel cloud e nei data center.
- **Mancanza di visibilità** sui percorsi di connettività delle filiali, dei data center e del cloud, che genera punti ciechi nella rete e nella sicurezza.
- **Scarse prestazioni e scalabilità**, a causa del numero crescente di servizi di rete e di sicurezza all'interno delle filiali e negli ambienti dei data center, dell'hairpinning del traffico e dei colli di bottiglia generati dall'ispezione e dal controllo centralizzati per l'applicazione della sicurezza.
- **Costi elevati**, dovuti ai dispositivi di rete e di sicurezza legacy (come firewall, IPS, router e altri prodotti specifici), al provisioning eccessivo dei servizi di rete per compensare la mancanza di scalabilità, e al maggiore utilizzo di servizi nativi del cloud.

Come funziona Zero Trust SD-WAN

Zero Trust SD-WAN consente alle organizzazioni di creare una filiale snella, eliminando l'insieme di prodotti come router, firewall e VPN a favore di un pratico dispositivo plug-and-play che può essere distribuito rapidamente utilizzando semplicemente una connessione Internet. In questo modo, è possibile ridurre la complessità associata alla gestione di più dispositivi e ottimizzare il funzionamento complessivo della filiale. Zero Trust SD-WAN semplifica drasticamente le comunicazioni delle filiali con un overlay di rete zero trust che consente un inoltro flessibile e una gestione semplificata delle policy utilizzando il collaudato framework di policy di ZIA e ZPA.

Tutto il traffico delle filiali viene inoltrato in modo sicuro direttamente a Zero Trust Exchange, dove vengono applicate le policy di ZIA o ZPA per consentire l'ispezione integrale di sicurezza e il controllo degli accessi basato sull'identità per le comunicazioni di filiali e data center. Il traffico delle applicazioni attendibili può essere inviato direttamente tramite Internet sfruttando punti di accesso diretto. Questo approccio esclusivo offre tre principali vantaggi:

- Puoi abbandonare la connettività basata sulla rete e sulle VPN site-to-site a favore della comunicazione basata sull'identità e incentrata sulle applicazioni, in modo da ottenere una vera sicurezza zero trust
- Puoi eliminare l'architettura legacy di tipo castle-and-moat senza compromettere la sicurezza e senza il bisogno di prodotti legacy come proxy Squid, gateway NAT, IPS e così via
- Ottieni una connettività distribuita e scalabile ovunque sia necessaria, con una gestione centralizzata e automatizzata delle policy per semplificare le comunicazioni tra filiali e data center

Casi d'uso della SD-WAN zero trust

Sostituzione della VPN site-to-site

Connetti le filiali direttamente alle applicazioni private senza estendere la tua WAN o fare affidamento sulle VPN, entrambe soluzioni che estendono la superficie di attacco di una rete. Le applicazioni sono nascoste dietro le filiali e l'accesso viene limitato a un dato numero di entità definite attraverso Zero Trust Exchange. L'identità, il contesto e l'aderenza alle policy dei partecipanti specificati vengono tutti verificati prima che sia consentito l'accesso, impedendo così il movimento laterale all'interno della rete.

Fusioni e acquisizioni

L'unione di due reti separate è un processo impegnativo che richiede molto tempo. I problemi vanno dalle sovrapposizioni degli IP e dai problemi di routing all'incremento dei rischi per la sicurezza derivante da una superficie di attacco della rete molto più estesa. Con Zero Trust SD-WAN, le reti possono rimanere separate e le filiali in un ambiente possono connettersi rapidamente alle applicazioni private in un altro, senza interruzioni.

Abilitazione dell'accesso diretto a Internet per le filiali

I modelli di rete e sicurezza on-premise diventano meno efficaci man mano che le organizzazioni spostano le proprie app sul cloud e creano app native del cloud. Zscaler Zero Trust SD-WAN è una soluzione appositamente creata per la trasformazione delle filiali, che inaugura un nuovo modello in grado di consentire alle filiali di comunicare con qualsiasi destinazione in modo sicuro e indipendente dalla rete sottostante.

Lo zero trust per i server e la connettività IoT/OT

Per massimizzare i tempi di attività della produzione ed evitare le interruzioni dovute a guasti delle apparecchiature o problemi nei processi, i dipendenti e i fornitori terzi devono poter accedere regolarmente alle risorse IoT/OT. Zero Trust SD-WAN for IoT/OT fornisce un accesso con desktop remoto completamente isolato e clientless ai sistemi target RDP e SSH, senza dover installare un client sul dispositivo o utilizzare jump host e VPN legacy.

Rilevamento e visibilità sullo shadow IoT/OT

I team IT si trovano a fronteggiare la presenza di punti ciechi quando i dispositivi non autorizzati e non rilevabili si collegano alle reti delle filiali; il risultato è una maggiore vulnerabilità dei dispositivi e una superficie di attacco più estesa. Zscaler identifica e classifica i dispositivi per offrire ai team IT una visibilità più granulare sul comportamento, al fine di migliorare le policy per il controllo degli accessi.

Dispositivi Z-Connector plug & play

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 x GbE	6 x GbE	8 x GbE	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 del tipo 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	✓	✓	✓	✓

LE FUNZIONALITÀ DI ZSCALER ZERO TRUST SD-WAN	
FUNZIONALITÀ	**DETTAGLI**
Funzionalità	
Provisioning zero touch e distribuzione automatizzata	• Provisioning zero touch con modelli predefiniti • Distribuzione completamente automatizzata • Rilevamento dinamico della geolocalizzazione delle filiali
Policy di inoltro granulare per il traffico Internet e quello delle applicazioni private	• Opzioni per inviare il traffico a ZIA, ZPA o direttamente attraverso Internet • Criteri flessibili per la selezione del traffico, con posizione secondaria, gruppo di posizioni, 5 tuple o FQDN
Policy zero trust unificate	• Policy unificata per la comunicazione utente-applicazione, dispositivo IoT-applicazione e server-server attraverso la policy avanzata di ZPA per nuovi tipi di client • Policy basate sulla posizione e sulla geolocalizzazione • Abilitazione delle policy di sicurezza con IPS, proxy SSL, filtraggio URL e protezione dati • Uno stack completo di soluzioni di sicurezza con profilo configurato per l'IoT/OT e i server
Alta disponibilità	• Due istanze di Zero Trust SD-WAN ad alta disponibilità forniscono ulteriore supporto per i picchi di traffico e la ridondanza in caso di guasto hardware • Tolleranza agli errori di tipo attivo-passivo utilizzando un indirizzo IP virtuale (VIP) basato sul protocollo CARP (Common Address Redundancy Protocol) • Circuiti attivo-attivo (singolo apparecchio) • Circuiti attivo-attivo (doppio apparecchio durante il bilanciamento FHRP)
Visibilità centralizzata e logging granulare	• Pannello di controllo centralizzato per il monitoraggio dello stato dei dispositivi e del traffico • Filtraggio disponibile per le distribuzioni su cloud, data center e filiali • Logging dettagliato di ogni sessione e transazione per tutte le porte e i protocolli, comprese tutte le transazioni DNS pubbliche e private • Integrazione completa con l'infrastruttura Nanolog Streaming Service con opzione per la trasmissione dei log al SIEM di proprietà del cliente
Terminazione dell'interfaccia WAN	• Connettività dual ISP (ethernet) • Multihoming con un unico apparecchio
Gestione dell'interfaccia LAN	• Reti LAN L3 multiple • Supporto del tagging VLAN/802.1q • Server DHCP • Gateway del DNS
Policy dei firewall sul dispositivo	• Controllo granulare dell'accesso per il traffico locale da LAN a LAN (est-ovest) • Elenchi di controllo degli accessi L3 (ACL)
Selezione del percorso in base alle applicazioni	• Selezione dinamica del percorso per app private e SaaS critiche • Connettività intelligente ai POP di Zscaler • Monitoraggio SLA e failover integrati
Routing	• Routing statico
Data center/POP di Zscaler	• Zscaler ha costruito la sua piattaforma di cloud security su oltre 150 data center in tutto il mondo posizionati strategicamente dove si trovano i clienti • Disponibilità integrata con failover per il successivo servizio disponibile

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
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 su SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su X (precedentemente Twitter) sull'account **@zscaler.**

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