

ZPA™ Private Service Edge

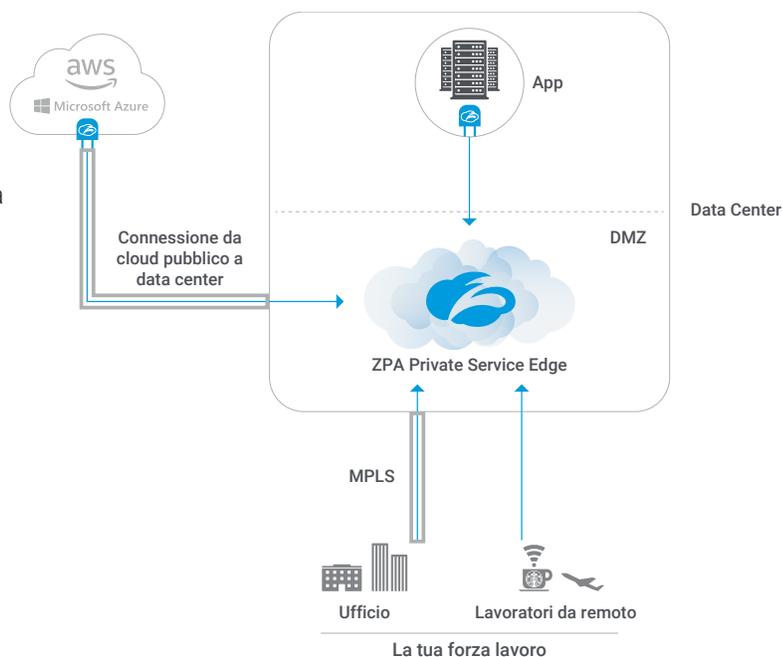
ZTNA (Zero Trust Network Access) fornito in locale e, da oggi, ovunque si trovino gli utenti

Gartner consiglia alle aziende di adottare servizi ZTNA (zero trust network access) per garantire che l'accesso alle applicazioni private sia basato sull'identità, eliminando così la necessità di accedere alla rete e riducendo al minimo la visibilità delle applicazioni su Internet. La spinta per l'adozione dello ZTNA ha portato molte organizzazioni a implementare Zscaler Private Access™ (ZPA), un servizio offerto sul cloud che consente l'accesso alle applicazioni private ovunque gli utenti si connettano, il tutto in modo rapido, sicuro e fluido.

Tuttavia, in alcune situazioni, le aziende potrebbero preferire l'implementazione di servizi di connettività delle applicazioni all'interno dei propri ambienti; ecco perché abbiamo introdotto ZPA Private Service Edge. Ora disponibile come funzionalità aggiunta del servizio ZPA, ZPA Private Service Edge è un broker che rappresenta un'istanza single-tenant (per cliente) completamente funzionale, ospitata dall'organizzazione del cliente e gestita da Zscaler. ZPA Private Service Edge può risiedere all'interno della sede del cliente o in un servizio cloud pubblico. Come il servizio cloud ZPA, il servizio in locale applica le policy e consente la connessione tra un utente autorizzato e un'applicazione privata specifica.

La funzionalità del servizio cloud ZPA, ma più da vicino

Grazie al servizio ZPA fornito sul cloud, quando un utente richiede l'accesso a un'applicazione privata, il traffico dell'utente viene inoltrato a un data center cloud Zscaler™ via Internet. La connessione tra un utente autorizzato e un'app privata viene consentita quindi nel cloud. Ciò rende ZPA ideale per gli utenti in remoto, come ad esempio dipendenti mobili e appaltatori di terze parti, che desiderano accedere alle applicazioni private in esecuzione in locale o in cloud pubblici o privati, poiché ZPA elimina il backhauling. Tuttavia, per gli utenti in locale, che desiderano accedere a un'applicazione anch'essa in esecuzione on-premise, potrebbe non avere senso uscire prima su Internet. È qui che entra in gioco ZPA Private Service Edge.



“ ZPA consente di avere visibilità immediata su ciò che sta accadendo sulla rete, comprese quali sono le applicazioni a cui viene effettuato l'accesso e chi vi accede, con un livello di dettaglio senza precedenti”.

Peter Daly, Direttore dei Servizi di rete -
Infrastruttura globale presso Johnson Controls

Come per il servizio cloud, ZPA Private Service Edge gestisce le connessioni tra Zscaler Client Connector (precedentemente App Zscaler) e App Connector. Quando viene distribuito, si registra sul cloud Zscaler. Ciò consente a ZPA Private Service Edge di scaricare le policy e le configurazioni pertinenti, in modo che possano essere applicate. Inoltre, memorizza nella cache le decisioni di selezione dei percorsi. ZPA Private Service Edge viene distribuito come una macchina virtuale/RPM leggera, installata dai clienti all'interno dei propri ambienti di rete. Una volta configurato, ZPA Private Service Edge funziona esattamente come il servizio cloud ZPA. Per gli utenti locali, o anche gli utenti in remoto in Paesi in cui non esiste un servizio cloud ZPA, l'accesso alle applicazioni private viene negoziato tramite ZPA Private Service Edge ed è sempre veloce, sicuro e senza interruzioni.

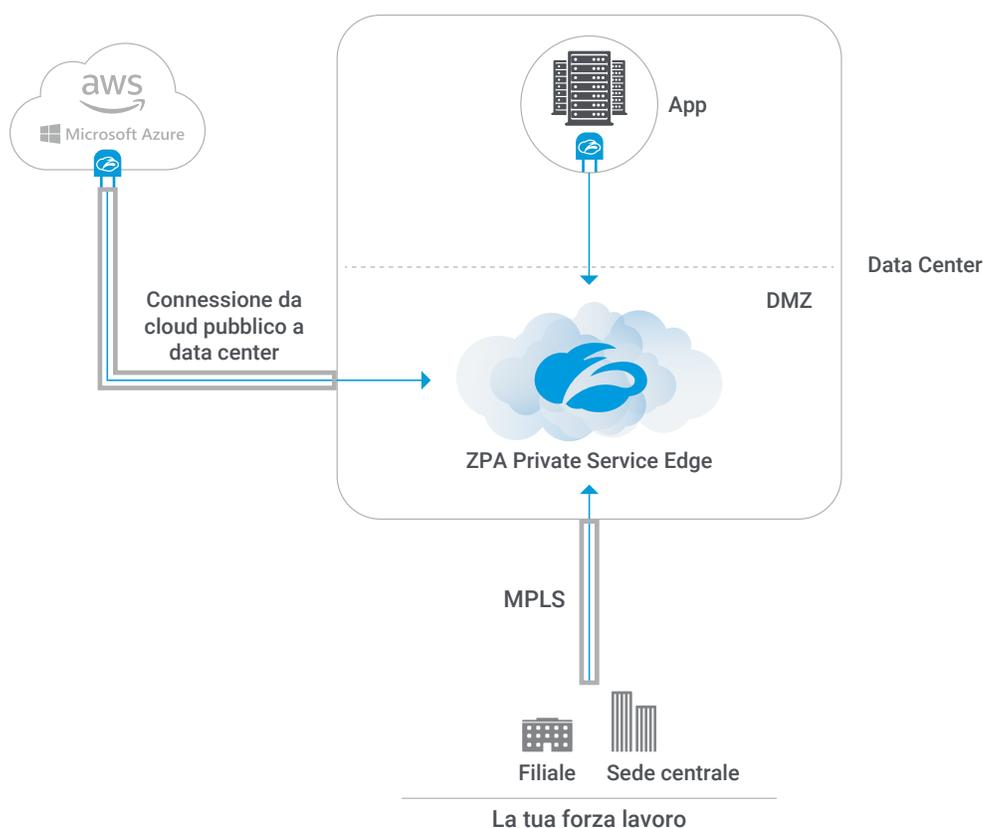
È importante notare che gli amministratori possono sempre configurare ZPA in un modo che entrambi ZPA Private Service Edge e il servizio cloud ZPA possano essere utilizzati per garantire la migliore esperienza per gli utenti che desiderano connettersi alle applicazioni private.

Casi d'uso comuni di ZPA Private Service Edge

L'estensione del servizio ZPA nell'ambiente on-premise aiuta ad avere successo in molteplici di scenari:

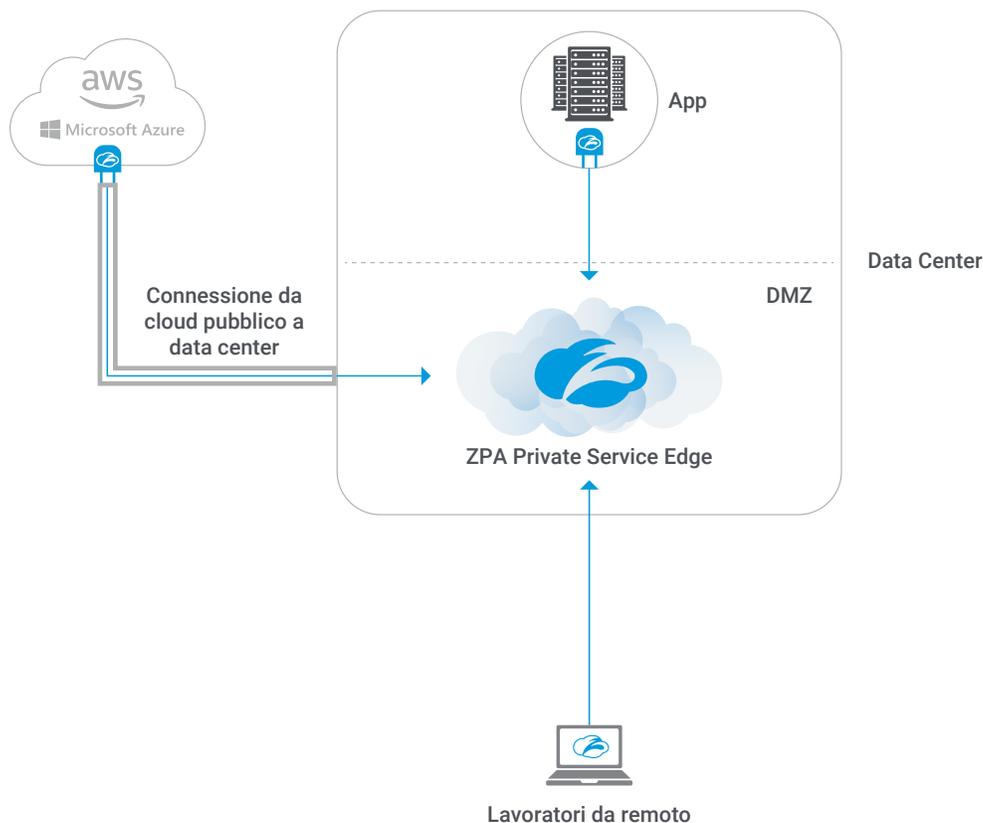
ZTNA per la forza lavoro locale

Per gli utenti che lavorano presso la sede centrale o le filiali, che desiderano accedere alle applicazioni che vengono eseguite on-premise o in cloud pubblici, non ha senso che il traffico venga prima indirizzato a un broker pubblico ZPA e poi di nuovo verso l'applicazione in esecuzione localmente. ZPA Private Service Edge fornisce intermediazione locale tra utenti e applicazioni on-premise, il che crea un'esperienza più rapida per gli utenti, riduce la complessità per gli amministratori di rete, nonché i rischi per i dati aziendali, grazie all'accesso in base al privilegio minimo.



Edge del servizio locale per la forza lavoro in remoto

In Paesi (come l'Algeria) senza ZPA Public Service Edge, gli utenti in remoto dovranno connettersi a un Edge di servizio pubblico ZPA in esecuzione in un Paese straniero (come la Germania) per accedere a un'app in esecuzione on-premise presso la propria sede centrale. Grazie a ZPA Private Service Edge, tali utenti in remoto possono accedere alle applicazioni in esecuzione on-premise e ZPA determina automaticamente il percorso più veloce per ogni utente e seleziona il broker più adatto per il lavoro.



Infrastruttura privata necessaria per la conformità

Alcuni Paesi, in particolare quelli inclini a catastrofi naturali, e settori regolamentati (come quello bancario) richiedono l'esecuzione di servizi di sicurezza on-premise, non ospitati nel cloud, per garantire un'elevata disponibilità. ZPA Private Service Edge consente ai clienti di conformarsi alle normative di settore nazionali, operando localmente e gestendo tutte le operazioni di intermediazione all'interno dell'ambiente del cliente.

“ Lo ZTNA fornisce accesso controllato alle risorse, riducendo la superficie di attacco. L'isolamento offerto dallo ZTNA migliora la connettività, eliminando la necessità di esporre direttamente le applicazioni a Internet. Internet diventa un mezzo di trasporto non attendibile e l'accesso alle applicazioni avviene attraverso un intermediario. Tale intermediario può essere un servizio cloud controllato da un provider di terze parti o un servizio ospitato in autonomia”.

Gartner, Market Guide for Zero Trust Network Access | Steve Riley, Neil MacDonald, Lawrence Orans, aprile 2019

VANTAGGI PRINCIPALI DI ZPA PRIVATE SERVICE EDGE

La possibilità di ospitare servizi di intermediazione ZPA in loco (in base all'identità), senza segmentazione della rete, porta a una serie di vantaggi per i clienti di Zscaler Private Access™ esistenti e per quelli nuovi.

- **Segmentazione semplificata:** è possibile passare da "IP sorgente a IP di destinazione" alle policy "utente a nome host", riducendo quindi la complessità della segmentazione della rete, che include il mantenimento di un elenco di indirizzi IP per firewall e l'impostazione di policy diverse per gli utenti locali o in remoto. Con ZPA Private Service Edge, la struttura delle policy diventa più snella e facile da gestire.
- **Adozione accelerata di strutture cloud ibride e multicloud:** ZPA Private Service Edge può essere eseguito all'interno del data center o di un cloud pubblico. Ciò significa che non vi è alcun cambiamento nella policy di accesso, anche dopo la migrazione di un'app privata su servizi cloud pubblici, come Azure, AWS e Google.
- **Accesso a privilegio minimo per gli utenti locali:** la possibilità di consentire lo ZTNA in locale crea una connessione precisa e intermediata 1:1, tra un utente locale autorizzato e un'app specifica, evitando l'accesso laterale alla rete e riducendo al minimo i rischi.
- **Alta disponibilità:** le zone del mondo con scarsa connettività a Internet possono trarre vantaggio da ZPA Zscaler Private Service Edge, in quanto memorizza nella cache le policy di accesso per settimane, consentendo una connettività sicura anche nel caso si perda la connettività a Internet.
- **Esperienza utente rapida e senza interruzioni:** l'accesso è identico, indipendentemente dal fatto che si lavori in remoto oppure on-premise. La funzionalità di doppio accesso dell'intermediazione in locale e su cloud pubblico ottimizza automaticamente l'esperienza degli utenti locali, quando accedono alle app private eseguite in locale, e degli utenti in remoto all'interno dei Paesi in cui non vi è alcun broker cloud ZPA.
- **Riduzione dei costi:** è possibile ridurre l'uso di firewall interni, e la necessità di nuovi investimenti può essere eliminata completamente. Non è necessario acquistare ulteriori firewall o creare nuovi segmenti di rete solo per consentire agli utenti locali di accedere alle app.
- **Conformità:** per i settori altamente regolamentati, questa infrastruttura privata può aiutare i clienti a ottemperare a tutti gli standard che impediscono l'uso della tecnologia ospitata sul cloud.

Per domande sul servizio ZPA, contattaci o visita zscaler.it/zpa. Per ulteriori informazioni su ZPA Private Service Edge, consulta la [Guida di Zscaler](#).

A proposito di Zscaler

Zscaler è stata fondata nel 2008 su un concetto semplice, ma allo stesso tempo fondamentale: dato che le applicazioni si spostano sul cloud, anche la sicurezza deve spostarsi lì. Oggi, sono migliaia le organizzazioni globali che vengono supportate dall'azienda nel loro percorso di trasformazione per operare sul cloud.

