SOPHOS
Cybersecurity evolved.

I sei principali vantaggi di ZTNA

Rispetto alle VPN di accesso remoto

Whitepaper Sophos. Ottobre 2021

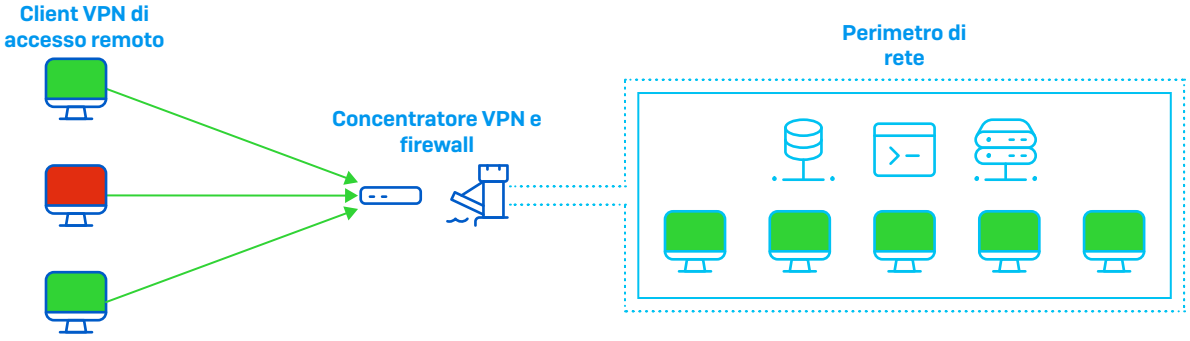
Le VPN di accesso remoto sono state senza dubbio uno strumento molto utile in passato, ma ultimamente la maggiore diffusione dello smart working ha messo in luce i limiti di questa tecnologia, che sta diventando obsoleta. Sebbene alcune organizzazioni abbiano deciso di continuare a sfruttare le VPN per quanto più tempo possibile, molte cercano un'alternativa migliore: una soluzione in grado di risolvere i problemi delle VPN di accesso remoto. Molte organizzazioni hanno già cominciato a utilizzare la prossima generazione di tecnologie di accesso remoto: ZTNA, ovvero Zero Trust Network Access. ZTNA offre una protezione superiore, con controllo più granulare, maggiore visibilità e un'esperienza utente più trasparente rispetto alle tradizionali VPN di accesso remoto.

In questa guida all'acquisto di soluzioni ZTNA valuteremo i limiti e le sfide delle VPN di accesso remoto tradizionali, nonché i vantaggi di Zero Trust Network Access. Concluderemo con un riepilogo delle funzionalità essenziali da includere in una nuova soluzione ZTNA.

Le sfide per le VPN di accesso remoto

Le VPN di accesso remoto sono state per decine di anni uno dei componenti fondamentali della maggior parte delle reti, grazie alla loro capacità di fornire un metodo sicuro per accedere da remoto ai sistemi e alle risorse situati all'interno della rete. Tuttavia, sono state progettate in un'epoca in cui le reti aziendali erano paragonabili a fortezze medievali, fortificate con mura e fossati lungo l'intero perimetro, per proteggere le risorse all'interno della rete. Le VPN offrivano l'equivalente di un corpo di guardia, e permettevano agli utenti autorizzati di accedere all'interno del perimetro protetto. Tuttavia, una volta entrati, questi utenti avevano pieno accesso a tutte le risorse.

VPN di accesso remoto tradizionale



Naturalmente, nel tempo le reti si sono evolute in maniera considerevole e sono oggi estremamente distribuite. Applicazioni e dati si trovano ora nel cloud, gli utenti lavorano da remoto e le reti sono sotto assedio da parte di hacker e cybercriminali che cercano qualsiasi punto debole da sfruttare.

Implementare una soluzione di accesso remoto basata su una VPN tradizionale (IPSec/SSL) in un ambiente moderno può essere un compito estremamente arduo. Implica fattori quali la gestione degli IP, i flussi e il routing del traffico, le regole di accesso del firewall, nonché la distribuzione e la configurazione di client e certificati. Per qualsiasi struttura con più di una quantità minima di nodi e qualche decina di utenti, la gestione diventa un vero e proprio lavoro a tempo pieno, e non dovrebbe essere così. Come se non bastasse, anche attività come monitoraggio e controllo della sicurezza sono un vero e proprio incubo.

In pratica, la tradizionale VPN di accesso remoto presenta un'enorme quantità di limiti e sfide che potrebbero essere evitate:

1. **Attendibilità implicita**: la VPN di accesso remoto è molto utile per accedere al perimetro della rete aziendale come se si dovesse essere fisicamente presenti in ufficio. Tuttavia, una volta entrati, gli utenti vengono considerati implicitamente attendibili e possono accedere a tutte le risorse della rete, il che comporta vari rischi di sicurezza molto gravi ed evitabili.
2. **Potenziale vettore per le minacce**: la VPN di accesso remoto non riconosce lo stato di sicurezza del dispositivo utilizzato per la connessione alla rete aziendale. Di conseguenza, offre alle minacce un potenziale canale di accesso alla rete da dispositivi che potrebbero essere stati compromessi.
3. **Backhaul inefficiente**: la VPN di accesso remoto offre un singolo punto di accesso alla rete, che potrebbe richiedere backhaul del traffico da più posizioni, data center o applicazioni, attraverso il tunnel VPN di accesso remoto.
4. **Mancanza di visibilità**: la VPN di accesso remoto non riconosce il traffico e i pattern di utilizzo. Di conseguenza rende più complicato l'ottenere visibilità sulle attività degli utenti e sul loro utilizzo delle applicazioni.
5. **Esperienza utente**: i client VPN di accesso remoto sono noti per offrire una pessima esperienza utente, in quanto aggiungono latenza o hanno un impatto negativo sulla performance. Inoltre, presentano problemi di connettività e costituiscono generalmente un peso per il reparto tecnico.
6. **Amministrazione, distribuzione e registrazione**: i client VPN di accesso remoto sono difficili da configurare e distribuire e sono caratterizzati da processi molto complicati per la registrazione di nuovi utenti e per la rimozione delle autorizzazioni degli ex dipendenti. La VPN è anche difficile da amministrare su firewall e gateway, specialmente in presenza di una quantità elevata di nodi, regole di accesso per il firewall, opzioni di gestione degli IP e flussi e modalità di routing del traffico. Diventa subito un'attività che richiede lo stesso impegno di un lavoro a tempo pieno.

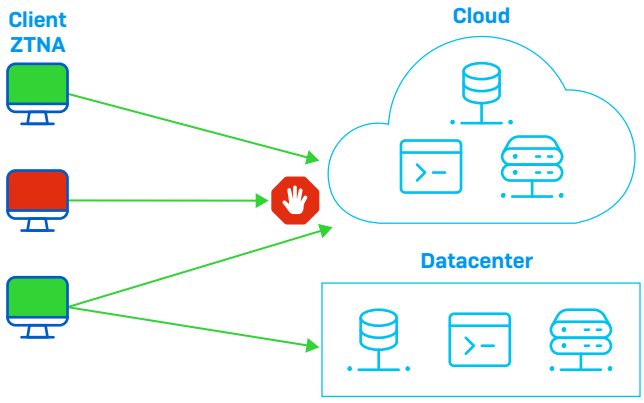
Cos'è ZTNA e come funziona

ZTNA, ovvero Zero Trust Network Access, è un sistema concepito e progettato per risolvere i problemi e superare i limiti delle VPN di accesso remoto, in quanto offre una soluzione superiore per gli utenti, ovunque si trovino. Permette di stabilire connessioni sicure per accedere solo ed esclusivamente alle applicazioni e ai dati necessari per svolgere il proprio lavoro. Ci sono alcune differenze fondamentali che contraddistinguono ZTNA dalle VPN di accesso remoto.

Come suggerisce il nome, ZTNA si basa sui principi dell'approccio zero trust, il cui motto è "mai fidarsi di niente, meglio controllare tutto". Zero trust essenzialmente elimina il concetto ormai obsoleto di un castello con mura e fossati, adottando quello di assegnare un perimetro individuale a ogni utente, dispositivo e applicazione di rete, interconnettendoli solo dopo la convalida di credenziali, stato di integrità dei dispositivi e policy di accesso. Il risultato è un livello nettamente superiore di sicurezza, segmentazione e controllo.

Un'altra differenza fondamentale delle dinamiche di ZTNA è il fatto che gli utenti non vengono semplicemente introdotti nella rete con piena libertà di movimento. Vengono invece stabiliti tunnel individuali tra l'utente e il gateway specifico dell'applicazione a cui è autorizzato ad accedere, niente di più, per un livello di microsegmentazione molto più sicuro. Tutto questo implica vari vantaggi in termini di sicurezza, controllo, visibilità, efficienza e performance. Ad esempio, una VPN di accesso remoto non offre informazioni sulle applicazioni a cui accedono gli utenti, mentre ZTNA può fornire dati in tempo reale sullo stato e sulle attività per tutte le applicazioni. Si dimostra così uno strumento dal valore inestimabile per l'identificazione di potenziali problemi e per l'esecuzione di controlli sulle licenze. Aggiungendo opzioni di micro-segmentazione, ZTNA garantisce che non abbiano luogo movimenti laterali di dispositivi e utenti tra le varie risorse della rete. Ogni utente, dispositivo, applicazione e risorsa ha un perimetro di rete indipendente e protetto, e viene eliminato il concetto di attendibilità implicita.

Zero Trust Network Access



ZTNA è anche più dinamico e trasparente per natura, in quanto opera in background senza richiedere alcuna interazione da parte dell'utente dopo la convalida iniziale dell'identità. L'esperienza può essere talmente trasparente e priva di problemi che gli utenti non si accorgeranno nemmeno di utilizzare tunnel sicuri cifrati per connettersi alle applicazioni.

I vantaggi di ZTNA

Zero Trust Network Access offre enormi vantaggi in molti ambiti, ma viene adottato principalmente per uno o più dei seguenti motivi:

- **Smart Working:** ZTNA è una soluzione molto più semplice per la gestione dell'accesso remoto dei dipendenti che lavorano da casa. Semplifica la distribuzione e la registrazione, trasformando quello che con le VPN era diventato un impegno a tempo pieno in un'attività che richiede un dispendio molto minore di risorse. Inoltre, semplifica e rende più trasparente l'intera esperienza per i dipendenti in smart working.
- **Applicazione della micro-segmentazione:** le soluzioni ZTNA offrono una protezione delle applicazioni superiore, grazie alla micro-segmentazione, all'inclusione dello stato di integrità dei dispositivi nelle policy, alla verifica continua dell'autenticazione, oltre all'eliminazione dell'attendibilità implicita e dei movimenti laterali che erano possibili con le VPN.
- **Blocco del ransomware:** con le soluzioni ZTNA viene eliminato un vettore di attacco frequentemente utilizzato dal ransomware e da altri attacchi di infiltrazione nella rete. Poiché gli utenti ZTNA non si trovano più "all'interno della rete", le minacce che un tempo sfruttavano le VPN per infiltrarsi nella rete ora non possono andare da nessuna parte con ZTNA.
- **Inclusione rapida di nuove applicazioni e nuovi utenti:** ZTNA offre una sicurezza superiore e maggiore agilità in ambienti in costante cambiamento, con utenti che vengono continuamente aggiunti e rimossi. Ora si possono implementare nuove applicazioni in maniera rapida e sicura, e anche il processo di registrazione e rimozione delle autorizzazioni per utenti e dispositivi diventa più facile. È inoltre possibile ottenere approfondimenti sullo stato e sull'utilizzo delle applicazioni.

In sintesi, i vantaggi di ZTNA rispetto alle soluzioni VPN di accesso remoto tradizionali includono:

1. **Zero Trust**: ZTNA si basa sui principi dell'approccio zero trust, il cui motto è "mai fidarsi di niente, meglio controllare tutto". Il risultato sono una sicurezza e una micro-segmentazione nettamente migliorate, grazie al fatto che ogni singolo utente e dispositivo viene considerato come un perimetro a sé stante, con valutazione e verifica continue dell'identità e dello stato di integrità prima di concedere l'accesso ad applicazioni e dati aziendali. Gli utenti possono accedere solamente alle applicazioni e ai dati definiti esplicitamente nelle loro policy, riducendo così i movimenti laterali e i potenziali rischi che tali movimenti implicano.
2. **Stato di integrità del dispositivo**: ZTNA include la conformità e lo stato di integrità dei dispositivi nelle policy di accesso, offrendo l'opzione di escludere i sistemi non conformi, infettati o compromessi e impedendo a questi sistemi di accedere ad applicazioni e dati aziendali. In questo modo si elimina uno dei principali vettori di minacce e si riduce il rischio di furto o perdita dei dati.
3. **Funziona ovunque**: ZTNA è indipendente dalla rete e in grado di funzionare con la stessa efficienza da qualsiasi rete, sia che l'utente si trovi a casa, in un hotel, in un bar o in ufficio. La gestione delle connessioni è sicura e trasparente, ovunque siano gli utenti e i dispositivi, per un'esperienza trasparente da qualsiasi posizione.
4. **Maggiore trasparenza**: ZTNA offre un'esperienza utente trasparente e priva di problemi, in quanto stabilisce automaticamente connessioni sicure in background su richiesta, a seconda delle esigenze. La maggior parte degli utenti non si accorgerà neppure che ZTNA li sta aiutando a mantenere protetti i dati.
5. **Migliore visibilità**: ZTNA fornisce una visibilità superiore sulle attività delle applicazioni, un'opzione che può essere molto utile per monitorare lo stato delle applicazioni, pianificare la capacità, gestire le licenze e svolgere controlli.
6. **Amministrazione semplificata**: le soluzioni ZTNA sono spesso più leggere, nitide e pertanto anche più semplici da distribuire e da gestire. Spesso possono anche essere più agili da usare in ambienti in continua evoluzione, con un flusso costante di utenti aggiunti e rimossi. La gestione quotidiana diventa così un compito rapido e privo di problemi, invece di un lavoro a tempo pieno.

Guida all'acquisto: cosa cercare in una soluzione ZTNA

Quando si compila una checklist di piattaforme supportate per client, gateway e provider di identità, occorre tenere presente le seguenti funzionalità essenziali quando si mettono a confronto le soluzioni ZTNA dei vari vendor:

Distribuzione e gestione dal cloud

La gestione dal cloud offre enormi vantaggi: consente di utilizzare subito la soluzione, presenta un'infrastruttura di gestione dalle dimensioni ridotte, offre opzioni di distribuzione e registrazione e permette di accedere da qualsiasi posizione. Uno dei vantaggi principali della gestione dal cloud è la possibilità di cominciare subito dopo aver effettuato il login, senza bisogno di aggiungere altre infrastrutture o altri server di gestione. La gestione dal cloud offre inoltre accesso sicuro e immediato da qualsiasi luogo e su qualsiasi dispositivo, per una modalità di lavoro più flessibile. In aggiunta, semplifica il processo di registrazione di nuovi utenti, indipendentemente da dove si trovino.

Integrazione con altre soluzioni di cybersecurity

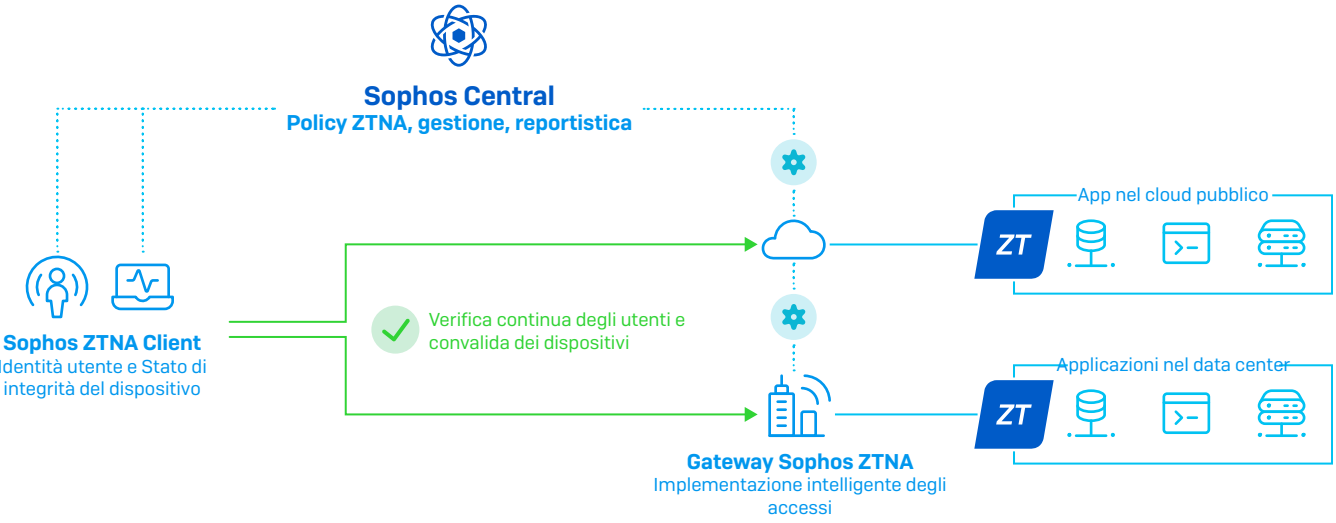
Anche se nella maggior parte dei casi le soluzioni ZTNA possono essere utilizzate in modalità standalone, una loro integrazione con altri prodotti di cybersecurity come quelli per firewall ed endpoint implica notevoli vantaggi. Una singola console di gestione integrata e basata sul cloud permette di estendere il potenziale del team. Utilizzando una finestra unica per gestire dalla stessa schermata l'intero sistema di sicurezza, incluso ZTNA, è possibile ridurre i tempi di formazione e le spese legate alla gestione delle attività quotidiane. Inoltre, questa strategia permette di ottenere funzionalità esclusive di analisi approfondita sui vari prodotti di IT security, specialmente se questi ultimi condividono reciprocamente i dati di telemetria. La protezione ne risulta così potenziata e in grado di rispondere in tempo reale quando un dispositivo compromesso o una minaccia riesce a infiltrarsi nella rete. I prodotti agiscono insieme per offrire una risposta coordinata alla presenza di un attacco o di una minaccia, impedendone qualsiasi movimento laterale e qualsiasi tentativo di diffusione o furto di dati.

Esperienza utente e di gestione

La soluzione che prendete in considerazione deve garantire sia un'ottima esperienza per l'utente finale che la massima semplicità di amministrazione e gestione. Oggi come oggi, dato l'incremento del numero di persone che lavorano in smart working in tutto il mondo, è essenziale che i processi di registrazione e configurazione dei dispositivi siano efficienti, per permettere ai nuovi utenti di essere subito operativi e garantirne la produttività. Valutate la modalità di distribuzione dell'agente ZTNA e la semplicità con cui è possibile aggiungere nuovi utenti alle policy. Inoltre, la soluzione in cui decidete di investire deve offrire un'esperienza trasparente e priva di complicazioni per gli utenti finali. Allo stesso tempo, deve garantire tutta la visibilità necessaria, con approfondimenti in tempo reale sulle attività delle applicazioni, per permettere l'identificazione proattiva di eventuali problemi legati a picchi massimi, capacità, utilizzo delle licenze e applicazioni.

Sophos ZTNA

Sophos ZTNA è stato concepito e progettato per semplificare l'implementazione del sistema Zero Trust Network Access e renderlo integrato e sicuro. Sophos ZTNA viene distribuito e gestito dal cloud, ed è integrato in Sophos Central: la scelta numero uno tra le piattaforme cloud di cybersecurity con funzionalità di gestione e reportistica. Da Sophos Central è possibile non solo gestire ZTNA, ma anche i Sophos Firewall e prodotti di protezione per endpoint, server, dispositivi mobili, cloud, e-mail e molto di più.



Sophos ZTNA offre vantaggi unici anche grazie alla stretta integrazione con i Sophos Firewall e gli endpoint su cui è installata Sophos Intercept X. Questa integrazione permette infatti di usufruire dell'interazione reciproca tra Synchronized Security e Security Heartbeat, che condividono lo stato di integrità con firewall, dispositivi, ZTNA e Central, per abilitare una risposta automatica alle minacce o alla presenza di dispositivi non conformi alle policy. È così possibile limitare automaticamente l'accesso dei sistemi compromessi e isolarli fino alla loro disinfezione.

I clienti Sophos concordano che implementare una soluzione di cybersecurity Sophos completamente integrata comporta notevoli vantaggi in termini di risparmio di tempo. Sostengono che utilizzare e gestire l'intera suite di prodotti Sophos con Sophos Central insieme a Synchronized Security per l'identificazione automatica e la risposta alle minacce equivale a raddoppiare il numero di dipendenti nel proprio reparto IT. Naturalmente Sophos ZTNA è compatibile con i prodotti di sicurezza di qualsiasi vendor, ma offre il massimo della funzionalità se utilizzato insieme agli altri prodotti dell'ecosistema Sophos, in quanto garantisce vantaggi tangibili e concreti in termini di visibilità, protezione e risposta.

Per saperne di più, visitate:

sophos.com/ztna

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

21-10-07 IT (DD)

SOPHOS