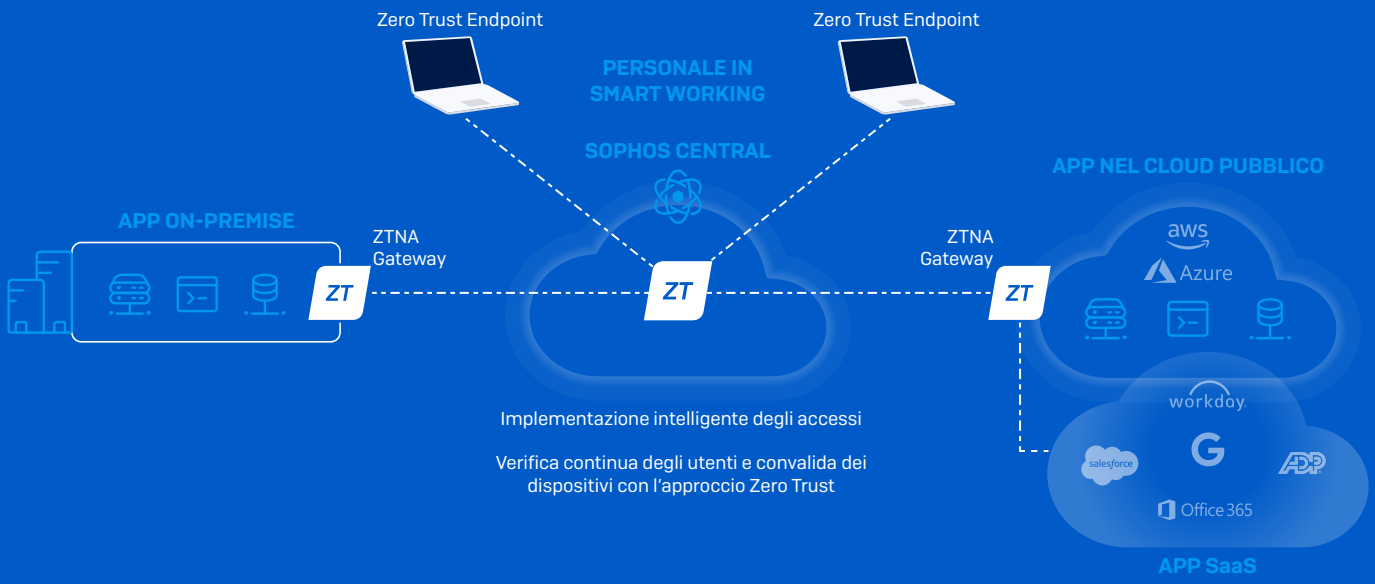
SOPHOS

Checklist per l'implementazione di Sophos ZTNA

Implementare Sophos ZTNA è un processo facile e veloce, in quanto prevede la distribuzione e la gestione dal cloud tramite la console Sophos Central: la scelta migliore per chi cerca una piattaforma di gestione dei prodotti di cybersecurity. Questa checklist può essere utilizzata per verificare di avere tutte le tecnologie necessarie per un'implementazione semplice e priva di problemi.



Checklist per l'avvio rapido dell'implementazione:

- ✔ Volere microsegmentare le applicazioni gestite nella rete e quelle ospitate su AWS, per garantire accesso sicuro per gli utenti remoti.
- ✔ Avere una piattaforma hypervisor o un provider di servizi cloud supportato per il o i gateway ZTNA.
- ✔ Utilizzare un provider di identità moderno: Azure oppure Okta. Azure può supportare gratuitamente diversi provider di identità con funzionalità di base e offre integrazione locale rapida con Active Directory.
- ✔ Avere Windows 10 o macOS per l'accesso alle applicazioni thick client o voler offrire un accesso alle applicazioni web basato su browser e indipendente dal client, su qualsiasi piattaforma.
- ✔ Facoltativamente, il desiderio di integrare la verifica dell'integrità dei dispositivi nei criteri di accesso, utilizzando Sophos Synchronized Security con Intercept X.

Considerazioni dettagliate:

Identifica tutte le applicazioni gestite: identifica le applicazioni da microsegmentare e a cui desideri fornire accesso remoto sicuro. Come requisito di Sophos ZTNA, queste applicazioni devono essere ospitate on-premise, nel datacenter, su un provider di servizi di hosting o nel cloud pubblico di Amazon Web Services (AWS). Sophos ZTNA è anche in grado di controllare l'accesso alle applicazioni SaaS che offrono restrizioni per il controllo dell'indirizzo IP.

Definisci la tua strategia per i gateway: I gateway Sophos ZTNA semplificano le connessioni sicure a livello dell'applicazione. I gateway ZTNA sono un requisito obbligatorio al gateway di rete di ciascuna sede di hosting delle applicazioni. Se ad esempio sono presenti applicazioni ospitate su due data center diversi e su AWS, occorreranno tre gateway ZTNA.

Sono disponibili due tipi di gateway, che possono essere utilizzati contemporaneamente in modalità ibrida:

- Gateway cloud: un gateway a impatto minimo e implementato on-premise, che si connette automaticamente a Sophos Cloud attraverso i Point of Presence Sophos locali. Questa soluzione offre l'implementazione semplificata per eccellenza; non richiede configurazioni extra sul firewall e aiuta a nascondere e rendere più sicure le applicazioni.
- Gateway on-premise: offrono una connessione con piano dati privato tra gli endpoint e le applicazioni. Questa soluzione si adatta particolarmente alle esigenze dei clienti che desiderano evitare il rischio di latenza sui Point of Presence nel cloud.

Indipendentemente dalla modalità che scegli, i gateway Sophos ZTNA possono essere distribuiti gratuitamente e implementati nella quantità richiesta. Il supporto delle piattaforme viene indicato nella tabella riportata di seguito. Verifica che queste piattaforme siano disponibili per la tua implementazione del gateway.

Definisci la tua strategia per l'identità: avrai bisogno di un provider di identità (Identity Provider, IDP) supportato da Sophos ZTNA per autenticare gli utenti. L'elenco dei provider viene indicato nella tabella riportata di seguito. Sophos ZTNA è compatibile con la maggior parte delle soluzioni di autenticazione a fattori multipli (Multi-Factor Authentication, MFA) in grado di integrarsi con i provider di identità supportati. È possibile utilizzare Active Directory localmente e importare un albero delle directory in Sophos Central per la creazione di criteri basati sull'utente; tuttavia, questa opzione non è sufficiente come soluzione di provider di identità per l'accesso remoto.

Stabilisci il numero di utenti: le licenze ZTNA sono molto semplici, poiché si basano sugli utenti; basta quindi sommare il numero di utenti che richiedono accesso sicuro alle applicazioni. Per semplificare l'implementazione del client, il processo di distribuzione di Sophos Client è facile e può essere svolto da Sophos Central insieme al nostro agente endpoint Intercept X. Tuttavia, l'implementazione può anche essere effettuata indipendentemente, insieme a qualsiasi altro prodotto AV per desktop.

Considera la tua strategia di verifica dello stato di integrità del dispositivo (facoltativo): questo è un livello di sicurezza aggiuntivo che aiuta a controllare l'accesso alle applicazioni in base allo stato di integrità o conformità del dispositivo. Inizialmente, Sophos ZTNA supporta Sophos Security Heartbeat per l'integrità e la conformità del dispositivo. È pertanto richiesta Sophos Intercept X, una soluzione gestita anch'essa da Sophos Central, che offre una finestra unica per la gestione di tutte le esigenze di cybersecurity. Intercept X condivide con Sophos ZTNA lo stato di integrità del dispositivo, che può a sua volta essere utilizzato nei criteri di accesso per le applicazioni.

Piattaforme supportate da Sophos ZTNA

Piattaforme supportate	Attualmente	In programma
Provider di identità	Microsoft Azure e Okta	Provider di identità aggiuntivi, a seconda della richiesta
Piattaforme ZTNA Gateway	VMware ESXi 6.5+, Hyper-V e AWS	Azure, Nutanix e GCP
Piattaforme ZTNA Client	Windows 10 1803 o versioni successive, macOS 11 (Big Sur) o versioni successive	iOS e Android
Stato di integrità del dispositivo ZTNA	Sophos Security Heartbeat (Intercept X)	È in programma l'inclusione degli attributi di valutazione dello stato del Centro sicurezza Windows

Point of Presence (PoP) per i Sophos ZTNA Cloud Gateway

Per l'implementazione di Sophos Cloud Gateway, sono disponibili Point of Presence nelle seguenti aree geografiche:

- Europa (Irlanda e Francoforte)
- Nord America (Ohio e Oregon)
- Asia-Pacifico (Mumbai e Sydney)

Licenze Sophos ZTNA

- Le licenze Sophos ZTNA vengono calcolate semplicemente in base al numero di utenti.
- I gateway Sophos ZTNA possono essere distribuiti gratuitamente, per consentirne l'implementazione nella quantità richiesta.
- La gestione con Sophos Central è inclusa senza alcun costo aggiuntivo.
- Sophos ZTNA offre risultati ottimali quando viene utilizzata insieme a Sophos Intercept X e Sophos Firewall, ma è anche perfettamente compatibile con qualsiasi prodotto endpoint o firewall.

Altre risorse

Approfitta di queste risorse per pianificare ulteriormente l'implementazione di ZTNA:

- Documentazione di Sophos ZTNA.
- Risorse della community per Sophos ZTNA.

Prova Sophos ZTNA gratuitamente per 30 giorni:
sophos.it/ztna

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

23-01-10 IT (DD)

SOPHOS