PANORAMICA DELLA SOLUZIONE

Aruba ESP con sicurezza Zero Trust

Sicurezza per l'Edge

Le problematiche di protezione della rete sono cambiate notevolmente nel corso degli anni per la crescente decentralizzazione degli utenti e la trasformazione degli attacchi, divenuti sempre più sofisticati e persistenti. I tradizionali approcci alla sicurezza che si concentravano principalmente sul perimetro della rete non sono più efficaci come strategie autonome. La moderna sicurezza di rete deve gestire un insieme di utenti e dispositivi diversificati e in continua evoluzione, nonché un numero decisamente più alto di minacce prevalenti rivolte a parti dell'infrastruttura un tempo "attendibili".

Il modello Zero Trust è emerso come soluzione efficace per rispondere ai mutevoli requisiti di sicurezza dell'azienda moderna, partendo dall'ipotesi che tutti gli utenti, i dispositivi, i server e i segmenti delle reti sono intrinsecamente non sicuri e potenzialmente ostili. Aruba ESP con sicurezza Zero Trust migliora la protezione complessiva della rete applicando un set più rigoroso di best practice e controlli alla risorse di rete precedentemente attendibili.

ARUBA ESP: FONDAMENTI DEI PRINCIPI ZERO TRUST

Il modello Zero Trust varia notevolmente in base al dominio di sicurezza considerato. Sebbene i controlli a livello di applicazione siano stati un punto essenziale di Zero Trust, una strategia completa deve anche considerare la protezione della rete e il crescente numero di dispositivi connessi, incluso l'ambiente di telelavoro. Aruba ESP con sicurezza Zero Trust offre visibilità complessiva, microsegmentazione Least Access e controllo, nonché monitoraggio e applicazione continui. Anche le tradizionali soluzioni VPN vengono ottimizzate con la verifica che gli stessi controlli applicati alle reti di campus o filiali siano estesi anche a coloro che lavorano da casa o in remoto.

Nell'era dell'IoT, i basilari principi di un'adeguata protezione della rete sono spesso difficili da implementare. Se possibile, tutti i dispositivi e gli utenti dovrebbero essere identificati e correttamente autenticati prima di concedere loro l'accesso alla rete. Oltre all'autenticazione, a utenti e dispositivi dovrebbe essere fornito il livello di accesso minimo necessario per

l'esecuzione delle attività business-critical una volta connessi alla rete. Questo significa stabilire le risorse di rete e le applicazioni a cui determinati utenti o dispositivi possono accedere. Infine, tutte le comunicazioni tra utenti finali e applicazioni dovrebbero essere crittografate.

L'ESIGENZA DI VISIBILITÀ COMPLETA

Con la crescente adozione dell'IoT, la visibilità totale dei dispositivi e degli utenti sulla rete è diventata una problematica sempre più seria. Senza visibilità, è difficile applicare controlli di sicurezza essenziali che supportano il modello Zero Trust. Automazione, machine learning basato sull'IA e capacità di identificare velocemente i tipi di dispositivi sono fattori determinanti.

Aruba ClearPass Device Insight sfrutta una combinazione di tecniche di rilevamento e profilazione attive e passive per individuare tutti i dispositivi connessi o che tentano di connettersi alla rete, tra cui quelli standard basati sugli utenti come portatili e tablet. Si differenzia dagli strumenti tradizionali per la sua capacità di rilevare un insieme di dispositivi IoT sempre più diversificato e diffuso sulle reti di oggi.

ADOZIONE DEL CONCETTO DI "LEAST ACCESS" E DELLA MICROSEGMENTAZIONE

Dopo la visibilità, i passaggi successivi essenziali riguardano l'applicazione delle best practice Zero Trust correlate al concetto di "Least Access" e microsegmentazione. Questo implica l'impiego del miglior metodo di autenticazione possibile per ciascun endpoint sulla rete (ad esempio autenticazione 802.1X e multifattore completa per i dispositivi degli utenti) e l'applicazione di una policy di controllo che autorizzi l'accesso soltanto alle risorse assolutamente necessarie per il dispositivo o l'utente in questione.

Aruba ClearPass Policy Manager consente la creazione di policy di accesso in base al ruolo con cui i team IT e di sicurezza possono rendere operative queste best practice tramite un solo ruolo e i privilegi di accesso associati che vengono applicati su tutta la rete: infrastruttura cablata o wireless, in filiale o nel campus. Dopo la profilazione, ai dispositivi viene automaticamente assegnata la corretta policy di controllo degli accessi e ne viene eseguita la segmentazione da altri dispositivi tramite le funzionalità di segmentazione dinamica di Aruba. L'applicazione è garantita dal PEF (Policy Enforcement Firewall) di Aruba, un firewall applicativo completo incorporato nell'infrastruttura di rete di Aruba. L'infrastruttura Aruba adotta inoltre i più sicuri protocolli di crittografia come lo standard WPA3 sulle connessioni di rete wireless.

ClearPass Policy Manager si integra anche con numerose soluzioni di autenticazione, supportando l'utilizzo di un processo multifattore e la possibilità di forzare la ripetizione dell'autenticazione in punti chiave della rete. Tramite l'ecosistema ClearPass, i clienti possono integrare facilmente altre soluzioni per rispettare i requisiti Zero Trust associati alle informazioni contestuali e altri elementi della telemetria di sicurezza.

Questo significa che ClearPass è compatibile con un'ampia gamma di soluzioni, tra cui gli strumenti di sicurezza degli endpoint, e favorisce decisioni più intelligenti sul controllo degli accessi in base alla situazione di un dispositivo. Le policy di controllo degli accessi possono inoltre essere modificate a seconda del tipo di dispositivo usato, del luogo da cui si collega l'utente e di altri criteri basati sul contesto.

MONITORAGGIO E APPLICAZIONE COSTANTI

Con l'adozione del controllo degli accessi in base al ruolo per applicare la segmentazione granulare, il monitoraggio continuo di utenti e dispositivi sulla rete costituisce un'altra best practice Zero Trust. In questo caso si affrontano i rischi associati a insider threat, malware avanzato o minacce persistenti che hanno aggirato le tradizionali difese perimetrali.

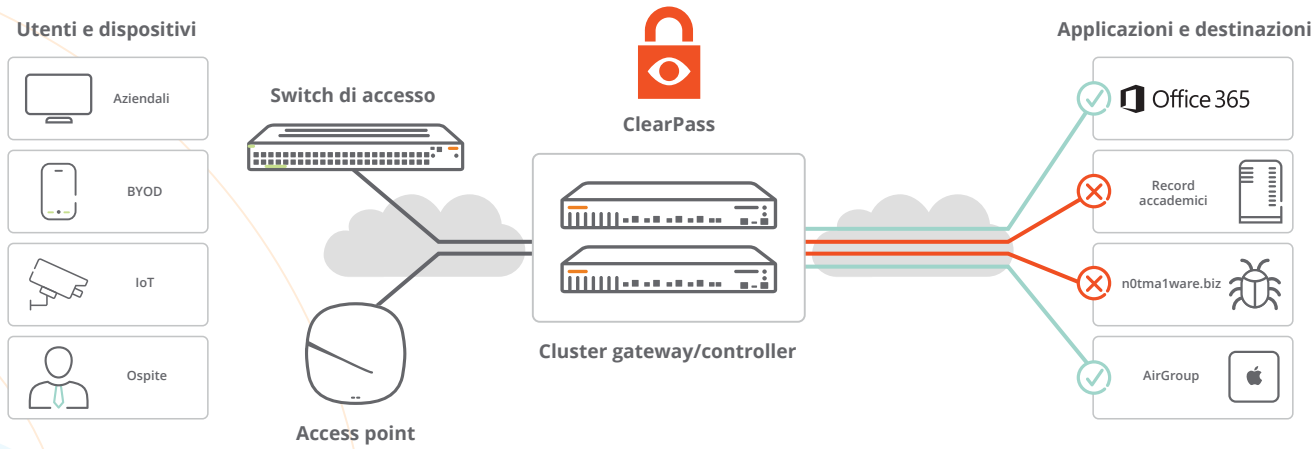

Figura 1: Aruba ClearPass assegna automaticamente policy di controllo degli accessi in base al ruolo applicate tramite segmentazione dinamica

ARUBA ESP (EDGE SERVICES PLATFORM)

La prima piattaforma del settore con 6° senso basato sull'IA per l'automazione e la protezione

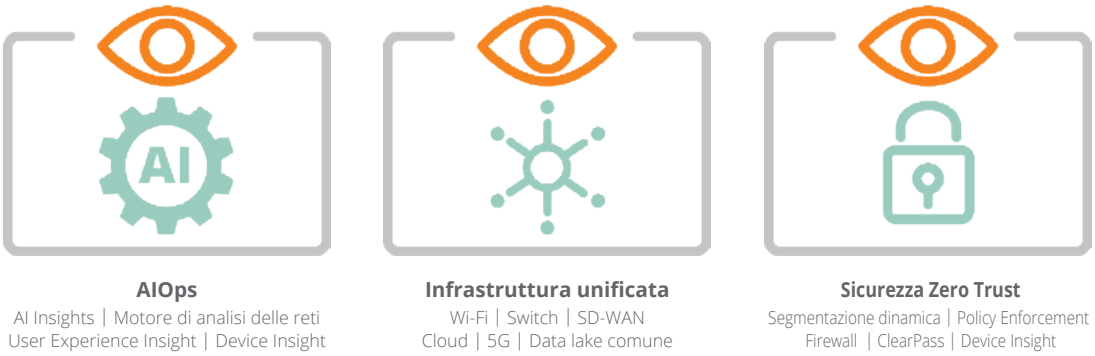

Figura 2: La sicurezza Zero Trust è un elemento chiave di Aruba ESP

Difesa dalle minacce con IDS/IPS

Le funzionalità di difesa dalle minacce di Aruba proteggono contro una miriade di minacce, tra cui phishing, attacchi di tipo DoS (Denial of Service) e attacchi ransomware sempre più diffusi. I gateway SD-WAN Aruba 9000 eseguono processi di rilevamento e prevenzioni delle intrusioni (IDS/IPS) basati su identità, in combinazione con Aruba Central, ClearPass Policy Manager e il PEF (Policy Enforcement Firewall). I processi IDS/IPS basati su identità effettuano l'analisi del traffico, secondo schemi e firme, sia sul traffico della rete LAN delle filiali (est-ovest) sia sul traffico SD-WAN (nord-sud) che attraversa il gateway, offrendo protezione della rete della filiale integrata. Un dashboard di sicurezza avanzato all'interno di Aruba Central fornisce ai team IT visibilità su tutta la rete, metriche multidimensionali per il monitoraggio delle minacce, dati di intelligence per la gestione delle minacce, correlazione e gestione degli incidenti. Le minacce vengono inviate ai sistemi SIEM e ClearPass per la risoluzione.

360 Security Exchange

Con oltre 150 integrazioni costituite dalle migliori soluzioni di sicurezza che comprendono i set di strumenti SOAR (Security Operations and Response), ClearPass Policy Manager è in grado di assegnare dinamicamente gli accessi in base alla telemetria delle minacce in tempo reale proveniente da varie origini. È possibile creare policy per prendere decisioni di controllo degli accessi in tempo reale, sulla base degli avvisi provenienti da NGFW (Next-Gen Firewall), strumenti SIEM (Security Information and Event Management) e molte altre origini. Le azioni di ClearPass sono totalmente configurabili, dalla limitazione degli accessi (ad esempio solo Internet) alla rimozione completa di un dispositivo dalla rete per la risoluzione del problema.

ARUBA ESP (EDGE SERVICES PLATFORM)

Per consentire ai nostri clienti di sfruttare al massimo le opportunità all'Edge, abbiamo sviluppato Aruba ESP, la prima piattaforma basata sull'IA del settore, progettata per unificare, automatizzare e proteggere l'Edge. La sicurezza Zero Trust è un componente chiave di Aruba ESP che, combinato con AIOps e un'infrastruttura unificata, permette alle imprese di ridurre i costi, semplificare le operazioni e garantire la sicurezza.

RIEPILOGO

L'odierno ambiente di rete e il panorama delle minacce richiedono un approccio diverso. La tradizionale protezione della rete incentrata sul perimetro non è stata progettata per la forza lavoro mobile di oggi o per i dispositivi IoT emergenti. Aruba ESP con sicurezza Zero Trust offre un set completo di funzionalità che includono visibilità, controllo e applicazione per rispondere ai requisiti di un'infrastruttura di rete decentralizzata e basata sull'IoT.

SO_ZeroTrustSecurity_051120 a00097694ite