aruba
a Hewlett Packard Enterprise company

PANORAMICA DELLA SOLUZIONE

SEGMENTAZIONE DINAMICA

Accesso semplice e sicuro per unificare reti wireless e cablate

Il numero crescente di dispositivi IoT e l'utilizzo di mobilità business-critical e servizi cloud guidano le innovazioni digitali sul posto di lavoro e questa tendenza porta a porsi questa domanda: network edge smart è sufficiente a collegare in modo sicuro tutti i tipi di dispositivi e di utenti? Le reti Legacy cablate e wireless sono state create senza tenere in considerazione aspetti come la mobilità business-critical, l'accesso IoT access o la sicurezza. L'approccio attuale basato sull'utilizzo di configurazioni manuali e statiche per questi dispositivi mobili e IoT in continua trasformazione e situati in intere reti di campus e di filiali aziendali presenta nuovi rischi per la sicurezza ed è diventato un'attività ingombrante che i team IT devono affrontare ogni giorno.

Per semplificare e proteggere la rete, la segmentazione di Aruba Dynamic unifica l'applicazione delle policy in tutte le reti cablate e wireless: per mantenere il traffico sicuro e separato. Adesso è facile ottenere la coesistenza di operazioni rivolte al business e reti gestite dall'azienda con dispositivi client IoT e gestiti dall'IT, garantendo nel contempo l'ottimizzazione dell'esperienza di rete e delle operazioni IT end-to-end.

La segmentazione dinamica utilizza l'intelligenza raccolta dalle funzionalità fondamentali delle policy basate sul ruolo di Aruba, dai firewall dell'utente, dall'ampia visibilità delle applicazioni di Layer 7 e dalla filtrazione integrata dei contenuti web.

PRINCIPALI DRIVER TECNICI E DI BUSINESS

Amministrazione delle polizze più semplice

Per il processo di onboarding dei dispositivi IoT e client sono di solito necessari touchpoints multipli: spesso è necessaria la configurazione manuale di nuovi VLAN, ACL o subnet in ogni hop della rete. Continui spostamenti, aggiunte e modifiche per reti distribuite e di grandi dimensioni possono anche richiedere tempo ed essere soggetti a errore. Nella progettazione delle reti un elevato livello di sicurezza e un limitato livello di complessità tipicamente si escludono reciprocamente.

VANTAGGI PRINCIPALI

- **esperienza migliore e coerente** – estendere il ruolo dell'utente, l'ispezione dei pacchetti accurata (DPI) delle applicazioni e le funzioni di profilazione dei dispositivi dalle reti wireless alle reti cablate
- **operazioni di rete più semplici** – risparmiare tempo ed eliminare la proliferazione di VLAN attraverso la riduzione della configurazione richiesta per SSID, ACL, subnet e porte cablate
- **maggiore sicurezza e visibilità dei dispositivi** – ClearPass e Policy Enforcement Firewalls (PEF) forniscono maggiore visibilità e applicazione delle policy

Migliorare l'esperienza utente

Quando gli utenti abbandonano lo stato desk-to-desk o site-to-site, si aspettano la stessa esperienza di rete indipendentemente dalla posizione o dalla modalità di collegamento: cablato o wireless. E chiedere loro di utilizzare una rete VPN (Virtual Private Network) rappresenta una problematica. Qualsiasi esperienza di rete che richieda il supporto IT viene infatti considerata negativa. L'esperienza utente, che sia per dipendenti, ospiti, clienti o studenti, influisce sul successo di un'impresa. Il collegamento di nuovi tipi di dispositivi, come smartphone, stampanti o attrezzature per conferenze video avviene spesso senza competenze o supporto IT. L'aspettativa è che l'IT fornisca un'esperienza impeccabile e al tempo stesso mantenga la visibilità e la gestione di qualsiasi aspetto su una rete sicura.

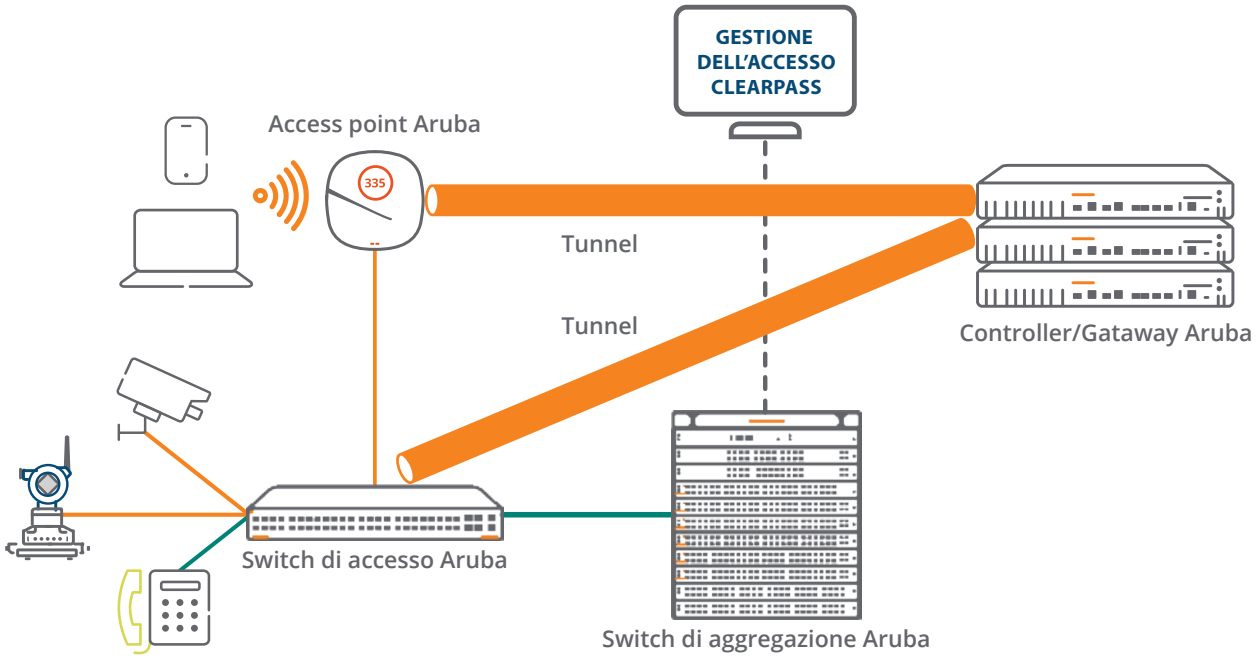
La vulnerabilità della rete viene mostrata con il numero di dispositivi IoT/headless collegati alle rete aziendali, di cui si prevede la crescita fino a oltre 20 miliardi entro il 2020.

Fonte: Gartner (gennaio 2017)

Dall'illuminazione intelligente alle telecamere di sicurezza o ai lettori di badge, i dispositivi IoT si stanno rapidamente sviluppando in tutte le reti di qualsiasi dimensione. Questa nuova connettività di rete apporta molti importanti vantaggi ma espone anche la rete a rischi per la sicurezza, poiché tali dispositivi si collegano sugli stessi percorsi in cui si trovano dati sensibili di natura finanziaria, medica e business critical. I dispositivi infatti integrano raramente funzioni di elevata sicurezza e mancano anche di funzioni di autenticazione robusta. Le password sono conservate in chiaro, non dispongono di supplicant di sicurezza e spesso si trovano fisicamente in aree pubbliche prive di sicurezza: e tutto ciò spiana la strada a violazioni della rete.

ESTENDERE LE INNOVAZIONI WLAN ALLO SWITCHING

La segmentazione dinamica consente l'estensione della gestione della policy sicura di Aruba e delle funzionalità di applicazione delle policy WLAN per rendere l'accesso alle reti cablate semplice e sicuro. Questa capacità significa che ai dispositivi di client cablati possono essere assegnate in modo dinamico le policy basate sulle porte o sul ruolo dell'utente: la



Segmentazione dinamica, parte di Esperienza Edge

soluzione ideale, dato che si prevede che nel 2020 il numero di dispositivi IoT raggiunga la cifra di 20 miliardi. Gli switch di rete Aruba, ora potenziati con ClearPass per la gestione delle policy e migliorati da controller mobilità, svolgono un ruolo fondamentale nel processo di unificazione dell'accesso alla rete.

Policy basate sui ruoli

Grazie all'implementazione della segmentazione dinamica, le decisioni sulle policy basate sui ruoli e i diritti di accesso sono prese sulla base del tipo di dispositivo, dell'applicazione utilizzata e persino della posizione dell'utente o del dispositivo. Utilizzate in origine per affrontare gli aspetti della sicurezza in rete, le policy basate sui ruoli segmentavano il traffico di rete per tipologia di utente, come dipendenti, guest o contractor, semplificando al tempo stesso in modo drastico la gestione delle reti grazie all'eliminazione di configurazioni di rete complesse e statiche. Questa potente funzionalità semplificava i flussi di lavoro IT, come la gestione degli accessi e delle policy BYOD, garantendo migliori prestazioni applicative.

L'estensione della gestione mica delle policy basate sui ruoli attraverso AP wireless e switch cablati fornisce un modo fondamentalmente semplice, sicuro ma anche diverso di gestire e rafforzare le policy per mobilità, IoT e cloud. I gateway/controller mobilità di Aruba che potenziano le definizioni policy di ClearPass sono ora in grado di comprendere e utilizzare i ruoli in modo dinamico. Questa capacità elimina la necessità di ricorrere a una gestione lunga e soggetta a errori di un sistema complesso e statico di VLAN, ACL e subnet, mediante policy di assegnazione dinamica.

Segmentazione di Layer 4-7

La seconda funzionalità fondamentale che gli switch Aruba sfruttano è la segmentazione. L'architettura WLAN Aruba mantiene il traffico sicuro e separato attraverso il tunnelling tra punti di accesso e un controller o gateway. Questa segmentazione basata sul tunnelling fornisce caratteristiche di sicurezza, come l'ispezione del firewall sul traffico ad alto rischio, attraverso l'utilizzo integrato di Policy Enforcement Firewall (PEF) di Aruba. PEF fornisce un contesto granulare (utente, dispositivo, applicazione, posizione), riducendo la necessità di costosi firewall per la prima linea di interrogazione e difesa. Grazie a policy contestualizzate e basate su identità, tipo di dispositivo e luogo, si possono soddisfare le esigenze di gruppi di utenti diversi con una singola configurazione di rete, dato che i flussi di traffico si adattano semplicemente ai ruoli assegnati.

La segmentazione dinamica semplifica e protegge le reti cablate e wireless, utilizzando il controller mobilità come motore di esecuzione di policy unificate. Il traffico attraverso AP o switch viene incapsulato in tunnel GRE per essere ispezionati dal firewall di applicazione dei criteri (Policy Enforcement Firewall, PEF).

Attraverso l'utilizzo di questa architettura di tunnelling WLAN, adesso gli switch Aruba possono fornire un approccio alla segmentazione basata sul ruolo invece di ricorrere al tradizionale e maggiormente manuale utilizzo di VLAN locali. Tale approccio è ideale per i dispositivi IoT non affidabili oppure per fornire visibilità sulle applicazioni, dato che gli switch Aruba adesso possono eseguire il tunnelling dinamico del traffico selezionato verso il controller per l'ispezione approfondita dei pacchetti e l'autenticazione dei dispositivi, esattamente come si comporta un punto di accesso. Ad esempio, è possibile assegnare in modo dinamico a una telecamera di sicurezza un ruolo con diritti che ne limitano il traffico soltanto a server specificati, eliminando la possibilità di accessi malintenzionati ad altre parti della rete.

Questa nuova capacità di segmentazione migliora l'approccio alla sicurezza mediante funzioni tunnelling impostabili come Port-Based Tunnelling (PBT) con tutte le autenticazioni su controller oppure come User-Based-Tunnelling (UBT) con autenticazione eseguita sullo switch. Poiché agisce da overlay, questa segmentazione può coesistere con le implementazioni VLAN attraverso l'utilizzo di tunnel sicuri in aree selezionate, senza la sostituzione integrale dell'intera infrastruttura di switching.

GLI INGREDIENTI DELLA SOLUZIONE

Punti di accesso wireless Aruba

Prestazioni Wi-Fi 802.11ac e 802.11ax Wi-Fi che soddisfano le esigenze di qualsiasi ambiente. Intelligenza IA integrata e servizi sulla posizione forniscono all'IT i processi di automazione e la visibilità necessari per garantire un'esperienza ottimale a utenti e dispositivi IoT.

Switch di rete Aruba

Create una base integrata per reti cablate e wireless, in grado di fornire scalabilità, sicurezza e prestazioni elevate a reti di campus e filiali d'azienda. La segmentazione dinamica è l'unica soluzione che offre ai team IT un modo semplice di applicare policy, utilizzare servizi avanzati e segmentare in modo sicuro il traffico di utenti cablati e IoT in qualunque punto della rete utilizzando tunnel: mediante Port-Based Tunnel (PBT) con autenticazione eseguita su controller oppure mediante User-Based Tunnel (UBT) con autenticazione eseguita su switch Aruba.

Gateway Aruba e controller mobilità

Quale aspetto cruciale di questa soluzione, i controller o i gateway agiscono da applicativi di policy per il traffico sia di reti cablate che di reti wireless. Il controller mobilità Aruba (in funzione su AOS 8.1 o versioni successive) consente all'IT di sfruttare l'applicazione delle policy, i contratti per ampiezza di banda e anche altre restrizioni del traffico. In un ambiente di filiale, il gateway per filiali a gestione centralizzata di Aruba svolge questo ruolo. Il Firewall di applicazione dei criteri serve da tecnologia di rete sottostante a supporto di questi due ambienti.

Aruba ClearPass Policy Manager con creazione di profili

Gestite e applicate in modo centralizzato le policy di accesso alla rete per il controllo degli accessi alle reti wireless e cablate. Le principali funzioni sono la creazione di profili, l'autenticazione e l'autorizzazione dei dispositivi e l'applicazione delle policy. Grazie a ClearPass, una volta definiti ruoli e privilegi seguono l'utente o il dispositivo attraverso gli accessi alle reti wireless e cablate. In tale modo, se l'utente apporta modifiche a un dispositivo sconosciuto oppure si trova in una rete non sicura, la policy cambia automaticamente i privilegi di autorizzazione. ClearPass configura i Downloadable User Roles (DUR), eliminando la necessità di definire i ruoli o le policy su uno switch.

RIEPILOGO

Per gestire meglio la mobilità business critical e i requisiti di connettività IoT emergenti, l'innovativa soluzione Aruba di segmentazione dinamica semplifica le operazioni IT e migliora la sicurezza attraverso l'applicazione dinamica di policy unificate e l'esecuzione di servizi avanzati in qualsiasi posizione della rete. Ciò garantisce che gli accessi adeguati e le policy di sicurezza siano distribuite senza soluzione di continuità, siano applicate in modo automatico e siano eseguite allo stesso modo per tutti gli utenti e i dispositivi su reti wireless e cablate.

SO_DynamicSegmentation_SK_092419 a00058593enw