



HPE Aruba Networking Dynamic Segmentation

Controllo degli accessi basato sull'identità per la sicurezza zero trust e il SASE dall'edge al cloud su scala globale



La proliferazione di dispositivi IoT (Internet of Things) e l'adozione di iniziative di lavoro ibrido hanno prodotto reti complesse, distribuite in diverse aree geografiche e con problematiche specifiche di visibilità e sicurezza. Inoltre, con le organizzazioni che accelerano la trasformazione digitale per promuovere l'efficienza aziendale, i team IT devono affrontare la crescente problematica dell'implementazione dei framework di sicurezza zero trust e SASE dall'edge al cloud.

HPE Aruba Networking Dynamic Segmentation è un elemento fondamentale della sicurezza edge to cloud integrata nella rete basata sull'AI e incentrata sulla sicurezza di HPE Aruba Networking. Si basa sull'impostazione dell'accesso con privilegi minimi alle risorse IT tramite la segmentazione del traffico in base alle identità e alle rispettive autorizzazioni di accesso. Si tratta di un concetto fondamentale dei framework zero trust e SASE, per cui l'attendibilità è basata su ruoli e policy e non dipende da dove o come si connettono i dispositivi degli utenti.

HPE Aruba Networking Dynamic Segmentation unifica l'accesso in base al ruolo e l'applicazione delle policy nelle reti cablate, wireless e WAN con la definizione centralizzata delle policy, consentendo a utenti e dispositivi di comunicare soltanto con le destinazioni previste dal rispettivo ruolo, per garantire un traffico sicuro e differenziato.

Principali vantaggi

- **Operazioni di rete più semplici:** risparmia tempo e contribuisce a eliminare la proliferazione di VLAN tramite la riduzione della configurazione richiesta per SSID, ACL, subnet e porte cablate
- **Sicurezza e visibilità ottimizzate:** garantiscono la comunicazione di utenti e dispositivi esclusivamente con destinazioni coerenti con i loro compiti tramite la definizione centralizzata delle policy e l'accesso basato sui ruoli
- **Gestione e automazione basate su cloud:** sfrutta i flussi di lavoro intuitivi basati sugli obiettivi per la definizione delle policy e la configurazione della rete
- **Scala globale e interoperabilità:** supporta la scala globale, affidandoti all'interoperabilità con l'infrastruttura di terzi
- **Prestazioni ed efficienza:** contribuisce a eliminare il sovraccarico dell'IT con policy aggiornate in automatico e applicate in modo costante

La segmentazione basata sull'identità è la chiave per zero trust e SASE

È stato riconosciuto da tempo che le decisioni sul controllo degli accessi basate sulla modalità e sulla posizione da cui un utente o un dispositivo si connette portano a una configurazione della rete prettamente manuale e soggetta a errori, con notevoli lacune nella sicurezza. Il framework zero trust è stato introdotto un decennio fa per affrontare questa problematica, fornendo un'architettura di sicurezza che consente alle organizzazioni di definire e applicare policy di accesso IT che limitano l'accesso alle risorse a seconda dell'identità e del ruolo di un utente o di un client. Ad esempio, a una stampante non dovrebbe mai essere consentito l'accesso a un server con le informazioni sui salari.

Una rete zero trust segmenta il traffico sulla base delle policy di controllo degli accessi, indipendentemente dal metodo di connessione. Diversi anni fa, l'architettura SASE ha riconosciuto l'importanza dei carichi di lavoro basati su cloud e ha esteso zero trust con l'inclusione di SD-WAN e dei servizi di sicurezza erogati tramite cloud. I framework zero trust e SASE offrono il modello per realizzare un'infrastruttura di rete sicura che utilizza la segmentazione basata sull'identità integrata nella rete per proteggere l'organizzazione.

I principi di HPE Aruba Networking Dynamic Segmentation

Hewlett Packard Enterprise è leader di mercato nella fornitura di reti che supportano i meccanismi di controllo degli accessi definiti da zero trust e SASE. HPE Aruba Networking Dynamic Segmentation utilizza l'identità, le policy e l'infrastruttura di rete per ottimizzare e automatizzare le modalità di protezione degli asset essenziali da parte dell'IT e include le seguenti funzioni:

Individuazione e profilazione dei dispositivi

Con un numero sempre maggiore di dispositivi IoT all'interno della rete, la capacità dell'IT di individuare e tracciare tutto ciò che è connesso è limitata. Di conseguenza, si creano punti ciechi operativi e di sicurezza che rischiano di compromettere l'intera organizzazione. Un elemento chiave di HPE Aruba Networking Dynamic Segmentation è HPE Aruba Networking Client Insights basato sull'AI e parte di HPE Aruba Networking Central. Questa soluzione utilizza la telemetria dell'infrastruttura di rete di HPE Aruba Networking e il machine learning per profilare automaticamente un'ampia gamma di client che si connettono alla rete, compresi i dispositivi IoT.

HPE offre anche un'opzione di profilazione dei client automatizzata basata sull'AI, compatibile con distribuzioni di rete di terzi. Approfondisci la tematica per saperne di più su visibilità e informazioni per le moderne reti basate sull'IoT.

Identità e autenticazione

Una volta identificato un utente o un dispositivo attraverso un processo di autenticazione che utilizza 802.1X o altre tecniche, l'IT può definire il ruolo appropriato e le autorizzazioni di accesso che vengono applicate in modo automatico. Questo lega i privilegi

di accesso all'identità, che è indipendente dalla connessione di rete o dalla posizione dell'utente o del dispositivo.

Policy basate sui ruoli

Il ruolo è un raggruppamento logico di autorizzazioni assegnate una volta stabilita l'identità di un utente o di un client. Le autorizzazioni possono includere un elenco di applicazioni a cui è possibile accedere, i servizi e gli altri client raggiungibili o persino i giorni della settimana in cui uno specifico utente può connettersi alla rete. I ruoli e l'applicazione sono determinati dall'approccio complessivo dell'organizzazione ai framework zero trust e SASE, oltre ai requisiti di compliance applicabili come il GDPR.

Applicazione automatizzata

Una volta definiti i ruoli, l'applicazione viene eseguita dall'infrastruttura di rete mediante l'utilizzo dei diritti di accesso per indirizzare e segmentare correttamente il traffico. HPE Aruba Networking Dynamic Segmentation offre una scelta di modelli di applicazione che possono essere impiegati singolarmente o in combinazione.

Modelli di HPE Aruba Networking Dynamic Segmentation

HPE Aruba Networking supporta due modalità di esecuzione della soluzione Dynamic Segmentation sulla base dell'architettura di rete complessiva dell'organizzazione.

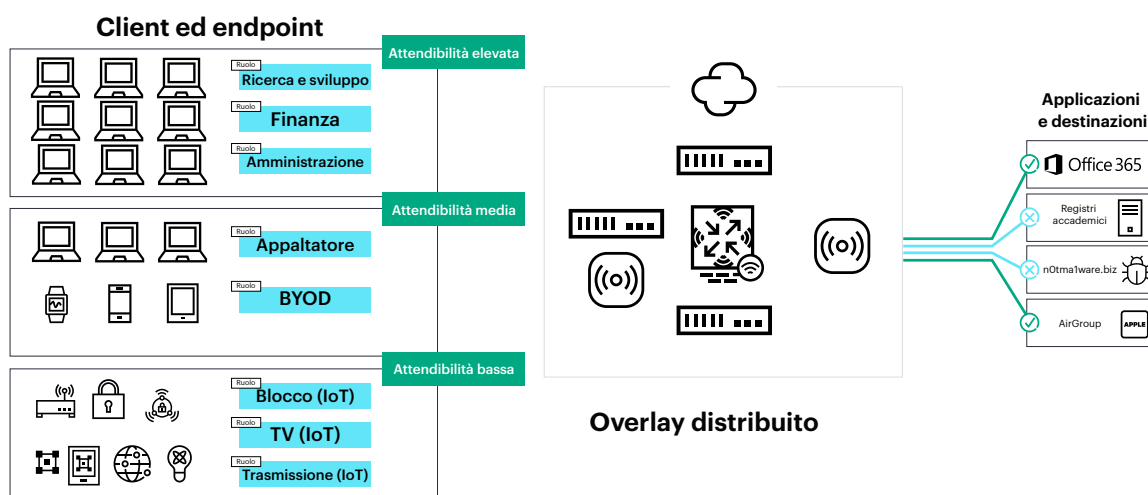


Figura 1. HPE Aruba Networking Dynamic Segmentation con un fabric di overlay distribuito

Dynamic Segmentation distribuita

Con le organizzazioni che modernizzano le reti adottando overlay e protocolli diffusi come EVPN/VXLAN, è possibile sfruttare tali overlay per una maggior protezione e scalabilità con HPE Aruba Networking Dynamic Segmentation. Con l'introduzione di HPE Aruba Networking Central NetConductor, Dynamic Segmentation può essere gestita tramite il cloud, con la possibilità di definire e propagare centralmente le policy di accesso, applicandole in modo distribuito in linea tramite switch e gateway HPE Aruba Networking (Figura 1).

Flussi di lavoro basati sugli obiettivi aziendali

Con HPE Aruba Networking Central NetConductor, l'IT può utilizzare una procedura guidata del fabric per astrarre la complessità della rete sottostante e semplificare la determinazione delle policy, automatizzando al contempo la definizione e la configurazione della rete. Gli intuitivi flussi di lavoro grafici, abbinati alla rapida automazione, eliminano la necessità della programmazione basata su CLI, dei fogli di calcolo con tabelle di routing o della configurazione manuale degli ACL.

GPID (Group Policy Identifier) per l'applicazione di policy in linea

HPE Aruba Networking Central NetConductor Policy Manager definisce i ruoli e le relative policy di accesso. Queste ultime sono espresse in GPID (Group Policy Identifier) e consentono alla rete di trasportare le informazioni sul controllo degli accessi tramite il traffico stesso, riflettendo il ruolo e le autorizzazioni di accesso dell'utente o del client. Gli identificatori sono incorporati nell'intestazione del pacchetto e interpretati in linea dagli switch e dai gateway HPE Aruba Networking CX (Figura 2). Se lo stato di sicurezza di un client cambia, il suo ruolo viene automaticamente modificato in modo da limitare l'accesso, e la modifica al ruolo viene propagata a tutta la rete.

Con i GPID, la modalità di Dynamic Segmentation distribuita migliora significativamente la scala di applicazione delle policy, riducendo al contempo la latenza e l'overhead del traffico. Gli identificatori si basano su standard di settore e supportano l'integrazione bidirezionale con le reti di terzi.

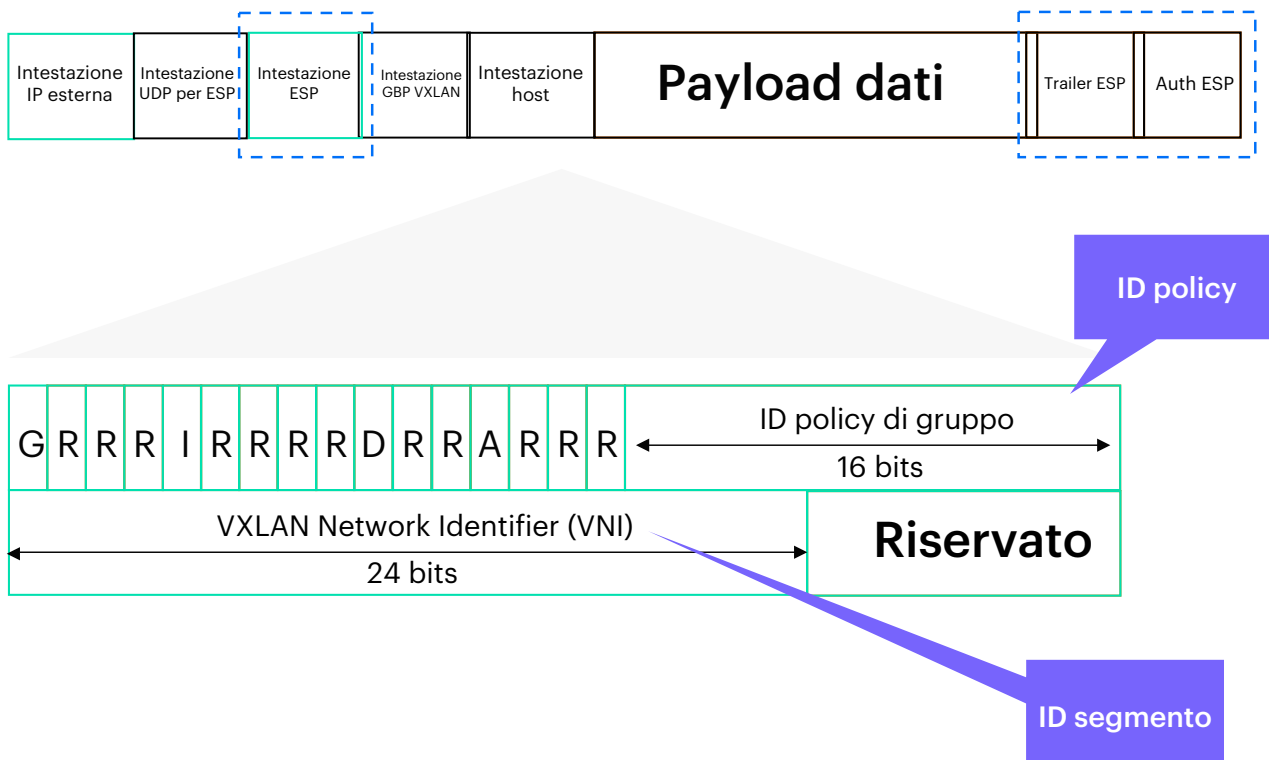


Figura 2. I GPID trasportano le informazioni sul controllo degli accessi tramite il traffico di rete per l'applicazione di policy in linea

HPE Aruba Networking Client Insights

Visibilità e profilazione basate sull'AI

GPID

Applicazione dell'accesso in linea tramite switch e gateway HPE Aruba Networking compatibili con il fabric



Policy Manager

Sviluppo delle policy

Cloud Auth (o) HPE Aruba Networking ClearPass

Autenticazione, assegnazione del ruolo

Figura 3. Componenti della soluzione per la modalità di Dynamic Segmentation distribuita con HPE Aruba Networking Central NetConductor

HPE Aruba Networking Central NetConductor - componenti della soluzione

I componenti di HPE Aruba Networking Central NetConductor supportano la modalità di Dynamic Segmentation distribuita per la scalabilità e le prestazioni, come illustrato nella Figura 3.

- **HPE Aruba Networking Client Insights:** la prima e unica funzionalità di visibilità e fingerprinting di client agentless integrata in una piattaforma di gestione cloud-native per contribuire all'eliminazione dei punti ciechi della rete. HPE Aruba Networking Client Insights, uno strumento basato sull'AI, sfrutta la telemetria dell'infrastruttura e i modelli di classificazione incentrati sul machine learning per il fingerprinting, l'identificazione e la profilazione precisa di un'ampia gamma di client, compresi i dispositivi IoT, nell'intera infrastruttura cablata e wireless
- **Cloud Auth:** consente l'onboarding senza problemi di utenti finali e dispositivi client tramite l'autenticazione basata su indirizzo MAC o tramite integrazioni con archivi di identità cloud comuni quali Google Workspace™ o Azure Active Directory, per assegnare automaticamente il giusto livello di accesso alla rete
- **Policy Manager:** consente di definire gruppi di utenti e dispositivi, per poi creare le relative regole di applicazione degli accessi alla rete fisica (Figura 4)

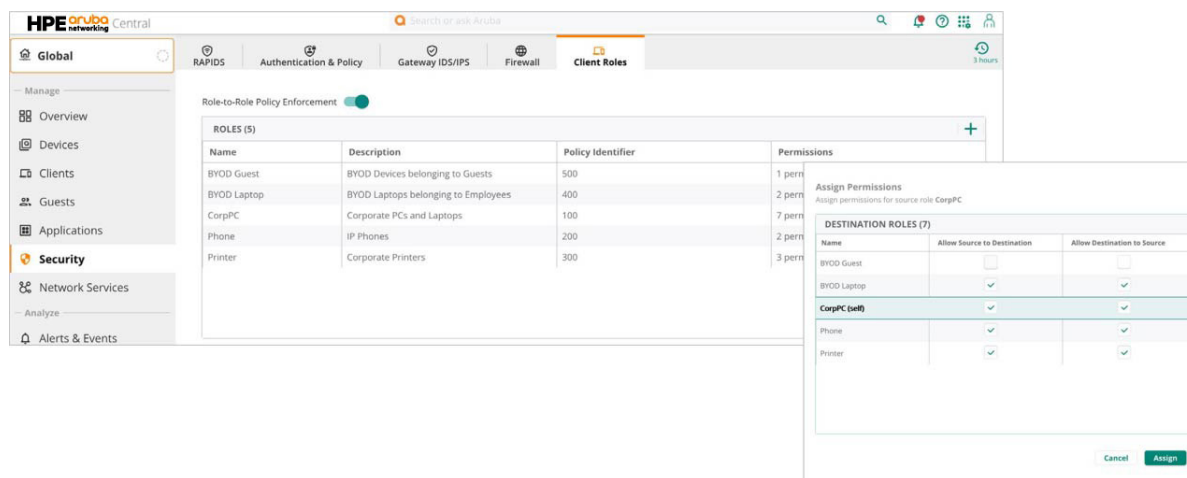


Figura 4. Interfaccia grafica intuitiva per la definizione globale delle policy

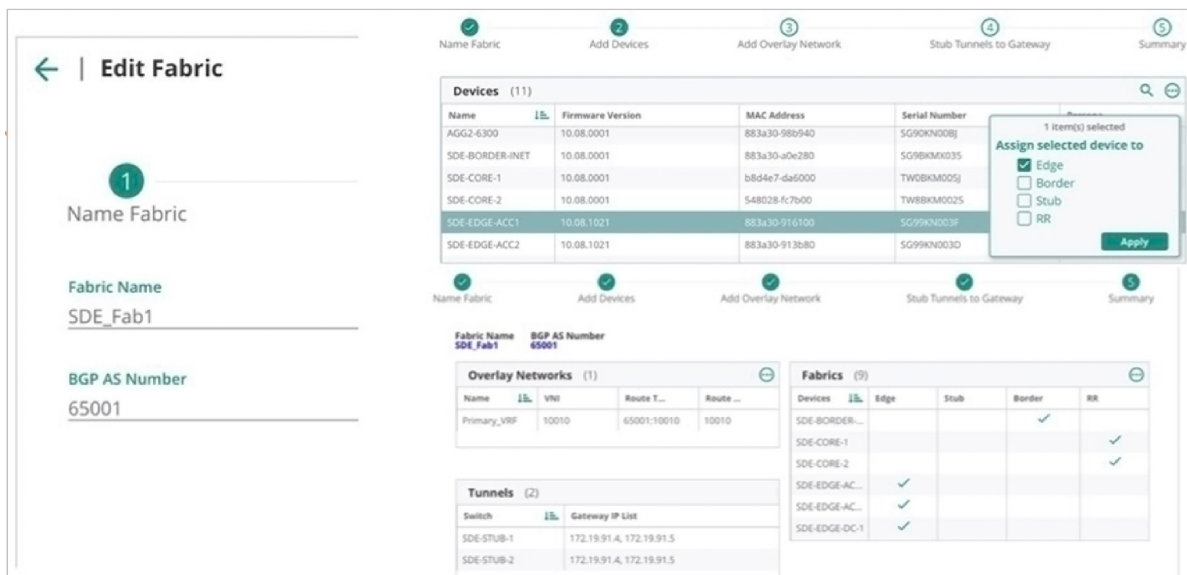


Figura 5. Flusso di lavoro grafico di facile utilizzo per la configurazione semplificata e la distribuzione automatizzata dell'overlay di fabric

- **Procedura guidata del fabric:** semplifica la creazione di overlay mediante un'interfaccia utente grafica intuitiva, che facilita notevolmente le modalità di definizione dei componenti virtuali e la generazione di istruzioni di configurazione da inviare a switch e gateway (Figura 5)
- **GPID:** trasporta le informazioni delle policy dei client nel traffico per l'applicazione in linea delle policy, riducendo in tal modo i costi di configurazione e sicurezza e favorendo la mobilità e la scalabilità
- **Switch e gateway HPE Aruba Networking con supporto per il fabric:** supportano la configurazione e l'applicazione basate sulle istruzioni di routing e sui privilegi di accesso definiti nel GPID

Nota: le reti che utilizzano HPE Aruba Networking Central NetConductor Policy Manager per l'orchestrazione delle policy possono usare il

cloud HPE Aruba Networking Central oppure HPE Aruba Networking ClearPass per l'autenticazione e l'assegnazione dei ruoli.

Dynamic Segmentation centralizzata

Da diverse generazioni di tecnologia di rete, la modalità di Dynamic Segmentation centralizzata è l'approccio tradizionale per il controllo degli accessi IT. Con questo modello, il traffico rimane sicuro e separato con l'uso di un overlay centralizzato che include i tunnel GRE tra gli access point e i gateway HPE Aruba Networking (o i controller mobilità HPE Aruba Networking in ambienti basati su controller). I gateway fungono da punti di applicazione delle policy in entrata che conoscono i ruoli dei client o delle applicazioni di origine e destinazione (Figura 6).

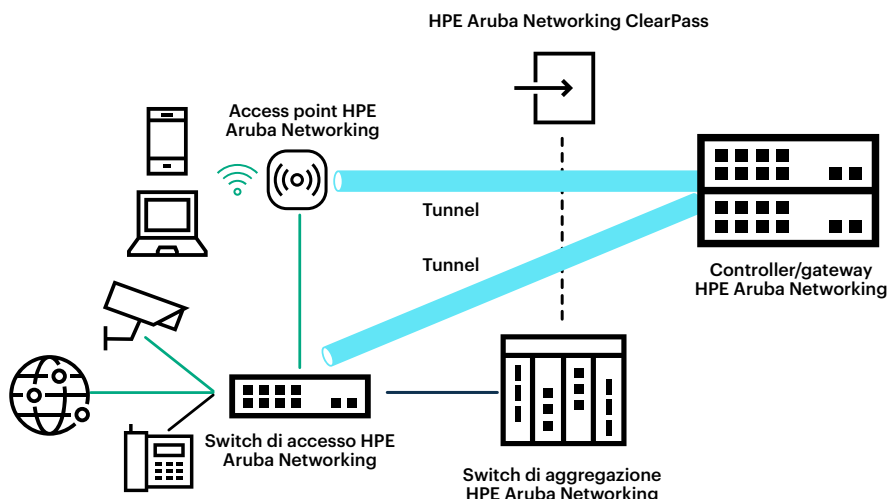


Figura 6. HPE Aruba Networking Dynamic Segmentation centralizzata

Definizione delle policy

È possibile centralizzare la definizione delle policy tramite HPE Aruba Networking ClearPass o HPE Aruba Networking Central NetConductor Policy Manager per il modello di applicazione centralizzata.

HPE Aruba Networking ClearPass prevede definizioni di policy di autenticazione, autorizzazione e centralizzate che seguono l'utente nell'intera rete e vengono applicate in modo uniforme a connessioni wireless, cablate, WAN e VPN. Se l'utente passa a un dispositivo sconosciuto o accede a una rete non protetta, la policy cambierà automaticamente i privilegi di autorizzazione.

HPE Aruba Networking ClearPass supporta l'applicazione basata su standard 802.1X e altre tecniche per l'autenticazione sicura. Si integra con un'ampia varietà di soluzioni di autenticazione, supportando l'uso dell'autenticazione a più fattori e la possibilità di forzare la ripetizione dell'autenticazione in punti chiave della rete.

HPE Aruba Networking ClearPass supporta anche il programma HPE Aruba Networking 360 Security Exchange con oltre 150 integrazioni di partner per una copertura e una risposta di sicurezza integrate e complete.

Ulteriori informazioni su HPE Aruba Networking ClearPass Policy Manager.

Policy Enforcement Firewall

I firewall tradizionali che sfruttano VLAN basate su IP per il controllo si attivano solo dopo che un utente o un dispositivo è stato ammesso alla rete, aprendo

potenzialmente le porte agli attacchi avanzati. Il PEF (Policy Enforcement Firewall), un firewall stateful di livello 7 di HPE Aruba Networking, utilizza l'identità, gli attributi del traffico e altre informazioni di contesto per applicare centralmente i privilegi di accesso al momento della connessione iniziale. L'ispezione del traffico tramite PEF fornisce un contesto granulare su utenti, dispositivi, applicazioni e posizioni. Il PEF funge da tecnologia di rete sottostante che supporta l'applicazione delle policy sui gateway HPE Aruba Networking (o sui controller mobilità in ambienti basati su controller).

Possibilità di scelta dei modelli di HPE Aruba Networking Dynamic Segmentation

L'estensione di architetture basate su VLAN con un fabric di overlay intelligente che utilizza EVPN/VXLAN risolve le problematiche di sicurezza e configurazione in silo, semplificando l'applicazione delle policy in reti complesse distribuite a livello globale (Figura 7). L'utilizzo di protocolli ampiamente adottati consente l'interoperabilità tra più fornitori per l'integrazione con reti di terzi, senza la necessità di una sostituzione integrale dell'infrastruttura esistente.

I clienti possono utilizzare un fabric di overlay centralizzato o distribuito oppure entrambi, poiché i due modelli di applicazione possono coesistere nello stesso ambiente. Le organizzazioni che attualmente si affidano a una strategia centralizzata possono adottare in modo flessibile un approccio distribuito in cui l'applicazione viene eseguita dai dispositivi di accesso, al proprio ritmo.

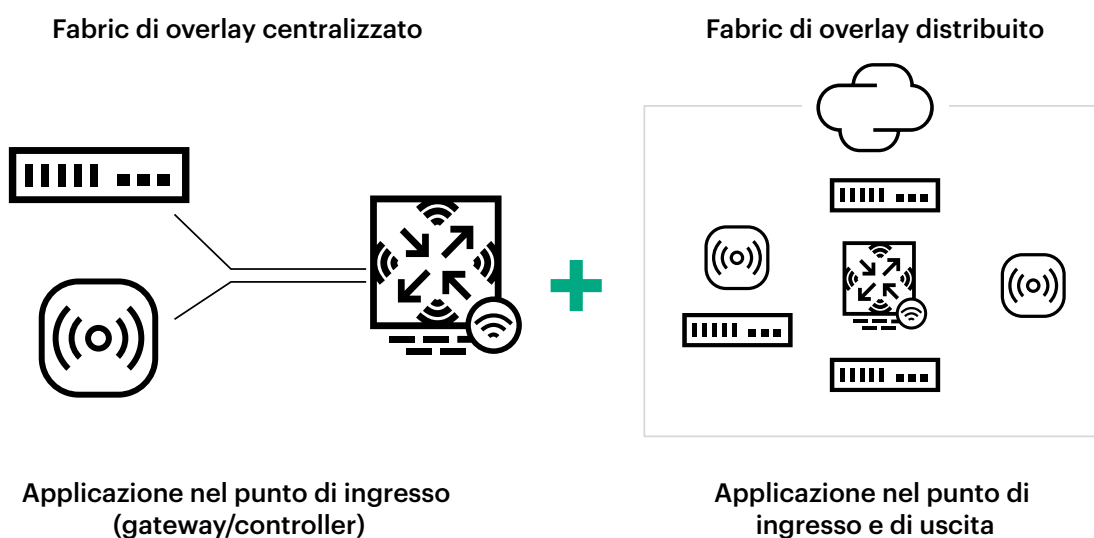


Figura 7. La modalità di Dynamic Segmentation distribuita supporta livelli superiori di scalabilità e prestazioni, sfruttando un fabric di overlay distribuito per l'applicazione delle policy nei punti di ingresso e uscita

Riepilogo

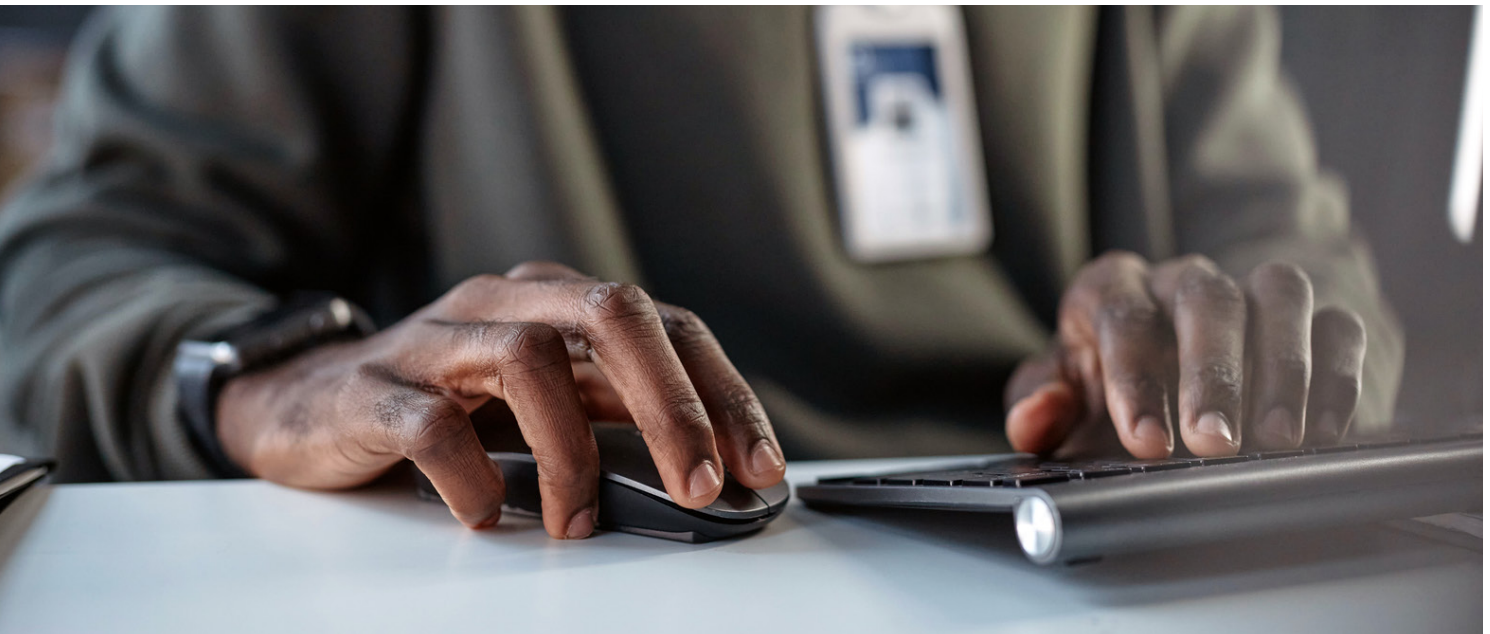
Per le organizzazioni che desiderano proteggere meglio le proprie reti, la segmentazione del traffico IoT, dei client BYOD e degli utenti assume la massima importanza. L'innovativo approccio di HPE Aruba Networking Dynamic Segmentation consente all'IT di scegliere il modello più adatto all'ambiente per ottimizzare la sicurezza, implementando in modo dinamico le policy unificate e le funzionalità di applicazione dall'edge al cloud. Con le autorizzazioni di accesso granulari basate sui ruoli applicate da HPE Aruba Networking Dynamic Segmentation, è possibile impedire facilmente la partecipazione a un attacco di utenti e client compromessi, bloccando o mettendo in quarantena automaticamente il client endpoint quando viene rilevato un attacco.

Visita [HPE.com](https://www.hpe.com)

Ulteriori informazioni alla pagina

[HPE.com/ww/
network-security](https://www.hpe.com/network-security)

Una scelta di modelli centralizzati o distribuiti che possono essere implementati on-premise o tramite il cloud garantisce alle organizzazioni la capacità di controllare gli accessi appropriati e supporta l'aggiornamento automatico e l'applicazione continua delle policy di sicurezza in qualsiasi topologia di rete. HPE Aruba Networking Dynamic Segmentation semplifica l'adozione dei framework di sicurezza zero trust e SASE, indipendentemente dalla dimensione e dalla complessità della rete su scala globale.



[Avvia chat](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. Le informazioni contenute nel presente documento sono soggette a modifica senza preavviso. Le uniche garanzie per i prodotti e i servizi Hewlett Packard Enterprise sono quelle espressamente indicate nelle dichiarazioni di garanzia esplicite che accompagnano tali prodotti e servizi. Nulla di quanto contenuto nel presente documento potrà essere interpretato come garanzia supplementare. Hewlett Packard Enterprise declina ogni responsabilità per eventuali omissioni o errori tecnici o editoriali contenuti nel presente documento.

Google Workspace è un marchio di Google Inc. Active Directory e Azure sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Tutti i marchi di terzi appartengono ai rispettivi titolari.

a00058593ITE, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

