AKAMAI SOLUTION BRIEF

Akamai and Aruba EdgeConnect

The Akamai and Aruba solution is a combination of Akamai Secure Internet Access Enterprise and Aruba's EdgeConnect Enterprise SD-WAN. This joint solution enables businesses to quickly deploy a SASE solution that provides cost-effective, fast, and secure direct internet access for branch and remote office locations.

Wide area networks (WANs) are now widely deployed and enable organizations to have a unified network across multiple locations. However, with the increasing adoption of SaaS, IaaS, and public cloud applications, and the increase in remote working, the legacy approach of backhauling traffic to a central location is no longer efficient or economical, causing enterprises to reevaluate the design of their WAN infrastructure.

WANs based on Multiprotocol Label Switching (MPLS) are expensive compared with broadband connections, and backhauling internet application traffic wastes bandwidth and leads to congestion, which can cause performance degradation.

In response to these financial and performance challenges, companies are adopting software-defined WANs (SD-WANs) to connect branch locations directly to the internet and eliminate the unnecessary backhauling of traffic over costly MPLS links. This reduces cost, improves performance, and increases agility.

However, the elimination of backhauling also removes the ability to inspect and secure traffic at a central location. One approach is to add hardware-based security appliances at each branch, but this adds cost and complexity. The Akamai and Aruba solution addresses these challenges by enabling companies to route all internet-bound traffic from branch locations to Akamai Secure Internet Access.

Secure Internet Access Enterprise is a cloud-based secure web gateway (SWG) that ensures devices can connect to the internet wherever they happen to be, without the complexity and management overhead associated with other legacy security solutions.

It is deployed on the global Akamai Intelligent Edge Platform, which ensures that wherever your users are located, they are close to a Secure Internet Access point of presence. This global footprint confirms that your users are secured without any impact to performance.

Aruba EdgeConnect and Akamai Secure Internet Access

Aruba EdgeConnect integrates directly with Akamai Secure Internet Access to provide companies with a secure, high-performance SD-WAN solution for branch locations that use standard broadband internet transport.

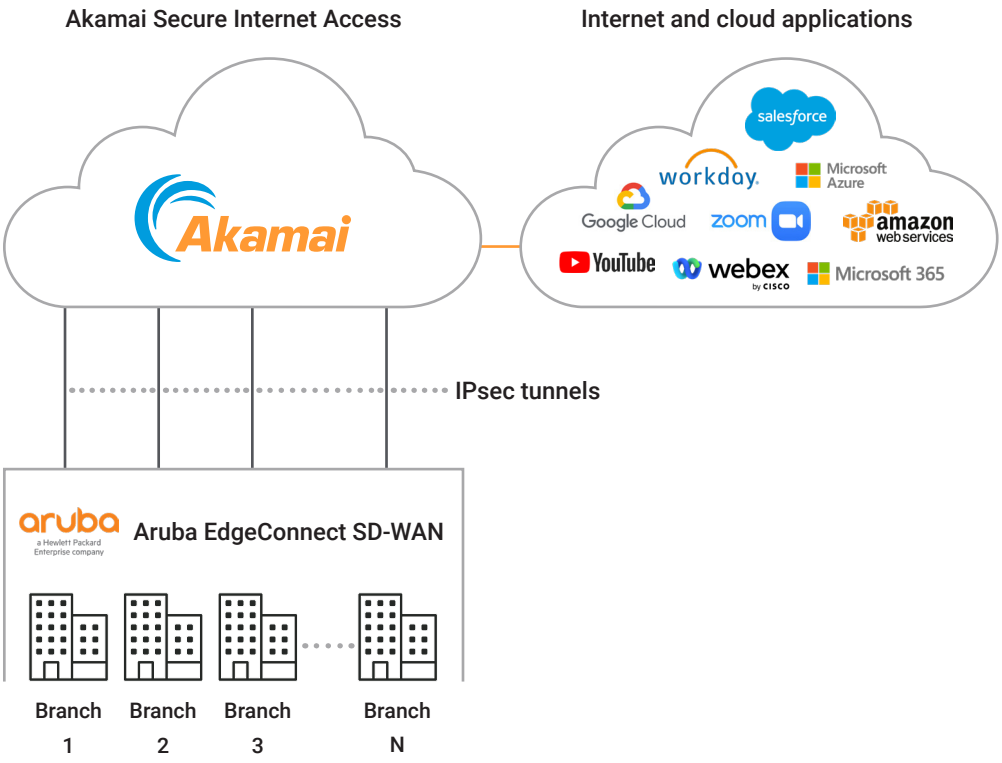
Using the Business Intent Overlay policy framework within Aruba Orchestrator, network administrators can define which traffic should be steered to the Akamai Secure Internet Access cloud service. Typically, the default policy will forward all internet traffic to and from branch offices and mobile devices to Secure Internet Access.

Key features

- **Secure direct-to-internet traffic:** Apply comprehensive security controls to protect direct-to-internet traffic irrespective of where the user is located. Akamai's SWG delivers multiple layers of protection to proactively block malware, ransomware, and phishing, ensuring users and devices can connect safely to the internet.
- **Optimize WAN connections:** Provide direct internet access for web traffic from branches, eliminating costly and inefficient backhauling to data centers.
- **Minimize appliance sprawl, reducing cost and complexity:** EdgeConnect eliminates the needs for additional hardware appliances, such as firewalls, and performs all the WAN functions. Akamai Secure Internet Access is cloud-based, eliminating the need for on-premises security appliances.
- **Rapid deployment with security:** Installation and commissioning of new branch locations is as simple as adding an EdgeConnect Enterprise appliance and using the automation capabilities of Aruba Orchestrator to automatically provision a pair of IPsec tunnels, primary and backup, to the Akamai cloud.

Akamai

EdgeConnect nodes in branch offices connect to the Akamai Secure Internet Access cloud service using standards-based IPsec tunnels.



Rapid integration

When integrating with cloud security services, Aruba Orchestrator works with each EdgeConnect branch node to determine the closest Secure Internet Access point of presence. Aruba and Akamai have developed a quick and easy approach to integration that combines EdgeConnect's ability to do local DNS resolution with Akamai's global geolocation-based DNS infrastructure. This enables Aruba Orchestrator and EdgeConnect to use Akamai DNS as the underlying geolocation mechanism, ensuring that EdgeConnect automatically builds IPsec tunnels to the closest Akamai Secure Internet Access point of presence from each branch location. This automatic configuration and creation of IPsec tunnels, enables a secure SD-WAN deployment to be delivered quickly, without the overhead and complexity associated with manual configuration.

To learn more, visit akamai.com or contact your Akamai sales team.

 | Support | Published 09/22