# The Cloud Application Gateway: Solving Connectivity Challenges for IGA

## Making the Right Connectivity Choice for your IGA Deployment

As enterprises scale cloud adoption, many still rely on legacy or on-premises systems across data centers and operational networks. These systems are often excluded from modern identity governance and administration (IGA) programs due to factors such as a lack of standard connectors or restrictive network boundaries, creating blind spots that auditors flag, including unmanaged admin accounts, incomplete records, and inconsistent policy enforcement.

These gaps are more than technical oversights. Any unmanaged system outside the reach of IGA, cloud or not, weakens your security posture. For security leaders pursuing Zero Trust, such inconsistencies challenge continuous identity verification and may erode credibility with regulators and the board.

To address this, organizations typically choose between two integration models:

- **Site-to-site VPNs** extend private network perimeters to the cloud using encrypted tunnels. This is often preferred where firewall infrastructure, centralized network management, or compliance frameworks are already in place.

- **Cloud Application Gateways**, powered by software-defined agents, provide a more modern option. Acting as a secure runtime environment for Omada Identity Cloud connectors, the Cloud Application Gateway initiates secure outbound sessions only when needed, enabling application and identity-level access without major network changes. Cloud Application Gateways align well with Zero Trust and scale efficiently across environments.

When choosing between a Cloud Application Gateway or a VPN connection, it is important to note that the functional capabilities of Omada Identity Cloud connectors remain the same in both deployment models. The difference lies in the connectivity approach, not in connector features.

Both models are valid. Omada supports each, helping organizations govern IGA systems securely and strategically, wherever they reside.

## Solving Integration Barriers with The Cloud Application Gateway

Many organizations seeking speed and flexibility choose software-defined agents. The Omada Cloud Application Gateway is one such solution, designed to extend identity governance across cloud environments, data centers, and distributed infrastructures: all without the burden of complex networking.

Enterprises often face integration challenges when connecting cloud IGA platforms to systems outside the cloud. Long deployment cycles, rigid network setups, and outdated trust models, combined with process-heavy network change procedures, can slow adoption and increase risk. The Omada Cloud Application Gateway directly addresses these issues. It is lightweight, initiates only outbound HTTPS connections (eliminating the need for inbound firewall changes), and requires no network reconfiguration or persistent tunnels.

The solution reduces onboarding time, lowers exposure, and reinforces Zero Trust principles by supporting BYOK (Bring Your Own Keys) with customer-controlled private keys stored in Windows or PAM vaults such as HashiCorp or Azure Key Vault. Whether managing multiple domains or scaling cloud adoption, the Cloud Application Gateway enables secure IGA integration without unnecessary complexity.

The following table highlights how it addresses common IGA deployment challenges:

| Connectivity Challenges | Cloud Application Gateway |
|---|---|
| **Complex setup and configuration** | • Secure, lightweight, outbound-only gateway for Omada identity Cloud connectors<br>• Avoids network infrastructure reconfigurations |
| **Increased attack surface** | • Designed with Zero Trust in mind, no blanket network access<br>• Enforces identity and application-level trust<br>• Enables organizations to keep workloads isolated in separate VLANs |
| **Key management and ownership** | • BYOK with customer-controlled private keys<br>• Zero Knowledge Posture: Omada never holds private keys<br>• Key retrieval from Windows store or PAM vaults |
| **Limited access visibility** | • Context-aware RBAC access policies<br>• Auditing and enforcement at the application and identity level |
| **Difficult to scale across sites** | • Software defined cloud-native scalability<br>• Rapid deployment across multiple environments<br>• No complex routing or manual IP handling |
| **Infrastructure lock-in** | • Hardware and Operating System Agnostic<br>• Runs on any hypervisor, bare metal, or cloud environment including support for Docker<br>• Deployable in containers or servers without vendor lock-in |
| **Slow onboarding timelines** | • Fast time-to-value for application onboarding<br>• Quick IGA adoption: being software defined, systems can be connected in hours |
| **Operational Efficiency** | • Over-the-air updates. No need for software patching |

## When VPN Solutions are the Right Fit

As mentioned earlier, extending IGA across cloud and on-premises systems is essential for a complete security posture. While many organizations adopt software-defined approaches, there are cases where a **site-to-site VPN** is the better option.

This may apply when:

- **A mature VPN stack is in place.** Your organization has invested in centralized infrastructure and dedicated network teams.
- **Perimeter controls are required.** You operate in a tightly regulated industry where encrypted tunnels are compliance essentials.
- **Existing infrastructure is already deployed.** Significant investments have been made in firewalls, VPN licensing, and related tooling.
- **Network segmentation is a priority.** Your architecture depends on routing isolation and strict traffic separation.

In these cases, Omada's IGA platform integrates seamlessly with Microsoft Azure VPN services, Omada's providing strong encryption, audit ready IPsec logging, and smooth integration with existing environments while supporting secure, policy-based identity governance across both legacy and cloud systems.

## Conclusion

Extending identity governance across hybrid environments requires a deliberate integration strategy. Both **Cloud Application Gateways** and **VPN based solutions** offer proven models, each suited to different regulatory, architectural, and operational needs.

Cloud Application Gateways offer agility and Zero Trust alignment, ideal for modern, distributed IGA deployments. Site-to-site VPNs remain a strong fit in environments with strict perimeter requirements or embedded infrastructure.

Omada Identity Cloud supports both models, enabling organizations to adopt the right approach for their needs. Regardless of the path, the goal is the same: secure, scalable, and governance-ready access across your entire application and system environment.

Omada

Omada Identity simplifies Identity Governance by providing a full-featured, cloud-native IGA solution that streamlines the complex processes of managing user identities, access, and entitlements. With a focus on automation and user-centric design, Omada reduces manual tasks and enhances operational efficiency, ensuring that organizations can easily enforce security policies, comply with regulations, and manage user access at scale. By leveraging advanced technologies such as AI-driven decision-making and role-based access control (RBAC), Omada enables businesses to achieve stronger security, better compliance, and improved user experiences - without the complexities traditionally associated with identity governance.

**www.omadaidentity.com**