Omada

WHITEPAPER

# Why Virtual Private Networks (VPN) is the best option for connecting an IGA SaaS solution for customer on-prem connectivity

## A comparison between VPN and cloud application gateway(CAG) technologies

# Why Virtual Private Networks (VPN) is the best option for connecting an IGA SaaS solution for customer on-prem connectivity

Many customer networks are hybrid in nature having business applications and systems both on-premises as well as in the cloud. To meet the needs of these customer environments, the right identity governance and administration (IGA) solution first and foremost needs to be secure, available, reliable, and performant. For these reasons, Omada recommends a site-to-site VPN between Omada Identity Cloud and a customer organization network over the use of a cloud application gateway approach.

Omada Identity Cloud is a modern, cloud native IGA platform that helps customers govern their digital identities providing complete lifecycle management. By using Omada, customers can quickly get identity governance under control and enable them to stay in control assuring compliance across all business applications and IT systems.

VPN technology is superior over cloud application gateways in all aspects of security, performance, compatibility, and ease of management for our customers. These aspects are summarized below:

- **Security:** VPN (using IPsec) offers encryption, authentication, integrity protection, replay detection, and session management. CAG, based on a proprietary software agent, may introduce vulnerabilities and access issues.
- **Performance:** VPN provides high performance and low latency due to its lightweight protocol (IPsec). CAG, operating at the application level, may degrade performance and increase latency.
- **Compatibility:** VPN is widely compatible with different network devices and supports various protocols and applications. CAG may not interoperate with different vendors and platforms.
- **Ease of Management:** VPN is easy to deploy, maintain, and monitor, with zero application footprint and no frequent updates. CAG requires more management effort due to its significant footprint and regular maintenance needs.
- **Cost of ownership:** VPN has a lower cost of ownership over time compared to CAG, which incurs increased costs due to frequent configuration changes, patches, upgrades, and additional software layers.

## Security

### *VPN*

A virtual private network, or VPN, is an encrypted connection over a less secure network, such as the Internet. VPN technology is widely used in corporate environments, it is stable, performant, and secure. There are different types of VPN, the specific type of VPN in focus for our purposes is the Site-to-Site which is often referred to as 'S2S' VPN.

VPN security is provided using the IPsec technology. IPSec provides the protocols for network security handling encryption and authentication, protecting data packets exchanged between the customer on-prem network and the IGA SaaS solution using the internet. VPN provides the required high security and protects the data packets from interception, modification, and replay attacks. VPN also supports multiple encryption algorithms and authentication methods, allowing the customer to choose the best level of security for their needs.

IKEv2, as part of the IPSec framework, is responsible for setting up the security associations (SAs) that IPSec needs to secure the traffic. It negotiates the cryptographic parameters, such as keys and algorithms, and manages the dynamic aspects of these associations, ensuring that they are established, maintained, and terminated securely and efficiently.

Therefore VPNs provide secure and stable connections with the following security measures:

- **Integrity Protection:** IKEv2 ensures the integrity and authenticity of the messages exchanged using cryptographic checksums.
- **Replay Detection:** This prevents attackers from sending a repeated or delayed copy of a valid data transmission, which can be used to perform unauthorized actions.
- **Session Management:** IKEv2 efficiently manages VPN sessions, allowing for the rekeying and renegotiation of connections to maintain security over long sessions.

### *Cloud Application Gateway*

Cloud application gateways (CAG) are network application services that function as a proxy between the customer (on-prem) network and the cloud IGA SaaS solution. Application gateways work at the application level and are installed on the customers' network. Note that this network could be a traditional on-premises network, or a network segment operating in a public cloud. Application gateways use HTTP with TLS to secure traffic between the application gateway network and the cloud service.

## Performance

### *VPN*

VPN offers high performance and low latency for connecting IGA SaaS solutions to customer on-prem infrastructure. VPN uses IPsec, which is a lightweight and efficient protocol that operates at the network layer. IPsec has limited overhead to data packet processing, and it can leverage the existing network infrastructure and routing protocols.

### *CAG*

CAG, operating at the user application level rather than the service level (VPN), may potentially degrade performance and increase latency. CAG is essentially a remote software agent, which adds extra layers of processing and routing to data packets. The use of CAGs may also introduce bottlenecks, delays, or failures, depending on the network conditions and the service availability. CAGs by their very nature, will introduce additional processing needs, and as such throughput of network traffic will be reduced as compared to a VPN.

## Compatibility

VPN is widely adopted in corporate enterprises and is compatible with a wide variety of network devices and firewalls. VPN can interoperate with different vendors and platforms, and it can support various network architectures and topologies. VPN also supports multiple protocols and applications, such as TCP, UDP, ICMP, HTTPS, SFTP, SSH, LDAPS, and more. VPNs provide seamless and secure access to the IGA SaaS solution without the additional processing overhead of a CAG.

## Ease and cost of management

### *Deployment*

VPN is easy to manage and maintain as it has a zero application footprint on the customers' network. VPN does not require any software installation or configuration on the customer network, as it uses the existing network infrastructure and devices. VPN can be deployed and activated quickly and easily and is monitored and controlled centrally. VPN also does not need frequent updates or patches, as it uses a stable and mature protocol.

CAG, on the other hand, is complex and cumbersome to manage and maintain, as it has a significant footprint on the customer's network and operations. As with any software, there will be application updates to address functional and non-functional needs relating to the CAG. Examples include security patching needs as well as scheduled functional upgrades. Without regular maintenance, the CAG may introduce compatibility issues or security flaws if left unpatched. Organizations are recommended to confirm these schedules and understand the obligations around patching, upgrades, and service availability during maintenance times.

### *Key configuration/lifecycle*

Omada recommends organizations fully appreciate the needs of key and certificate lifecycle maintenance operations. If key parameter configuration can be performed (at all) on the CAG and how/where keys are stored, retrieved, and used.

### *Availability*

For organizations looking at deploying a critical component like the CAG, it's strongly advised to consider redundancy and availability as critical. This creates more work in the form of configuration, testing, backup, and recovery tasks.

### *Log Retrieval/Consolidation*

Since the CAG is a separate software application component, organizations are recommended to ensure their log consolidation strategy takes this into account.

## Conclusion

**Leveraging an IPSec VPN is the best choice for connecting a cloud-native IGA SaaS solution to a customer's on-prem infrastructure, as it provides :**

- Highest Security
- Highest performance
- Highest compatibility
- Ease of management (Zero on-prem footprint)
- Lower cost of ownership

VPN security is based on IPsec, which is a secure, efficient, standardized, and versatile protocol that can support multiple encryption algorithms, authentication methods, transport modes, protocols, and applications. VPN/IPsec provides end-to-end encryption and authentication between the customer network and the IGA SaaS solution, and it can use the existing network infrastructure and devices. VPN can also provide seamless and secure access to the IGA SaaS solution from any device or location and can be deployed and activated quickly and easily. VPN has zero footprint on customer infrastructure.

CAG, on the other hand, is not a good choice for connecting IGA SaaS solutions to customer on-prem infrastructure, as it has drawbacks in terms of security, performance, compatibility, and ease of management. CAG is based on a proprietary software agent and a proxy service, which may introduce vulnerabilities, maintenance burdens, performance issues, compatibility issues, and access issues.

Over time maintaining a CAG will increase in costs as more frequent configuration changes, unscheduled patches, scheduled upgrades, monitoring, and host software layers (virtualization, containerization, operating system maintenance) all increase the ownership cost significantly with a remote cloud application gateway.

For these reasons, Omada Identity recommends VPN as the most secure and performant choice, coupled with a low cost of ownership.

Omada

Omada, a global market leader in Identity Governance and Administration (IGA), offers a full-featured, enterprise-grade, cloud native IGA solution that enables organizations to achieve compliance, reduce risk, and maximize efficiency. Founded in 2000, Omada delivers innovative identity management to complex hybrid environments based on our proven best practice process framework and deployment approach.