idaptive

SOLUTION BRIEF

Idaptive App Gateway

Secure, behind-the-firewall access to your on-premises applications without a VPN

As organizations migrate their workloads to the cloud, some of the key applications remain hosted in local, on-premises data centers. Concerns over security, application availability, and compliance are some of the main reasons why CIOs choose to keep applications in-house. Employees need to access these on-premises applications in the same way they access cloud-based apps – seamlessly, from any device, and at any time – to stay productive. Therefore, IT must expand its security perimeter in both directions — out to the cloud, and back into their data centers. Traditionally, IT leveraged Virtual Private Networks (VPNs) to provide employees the remote access to resources hosted on-premises.

VPNs: Time-consuming and not always secure

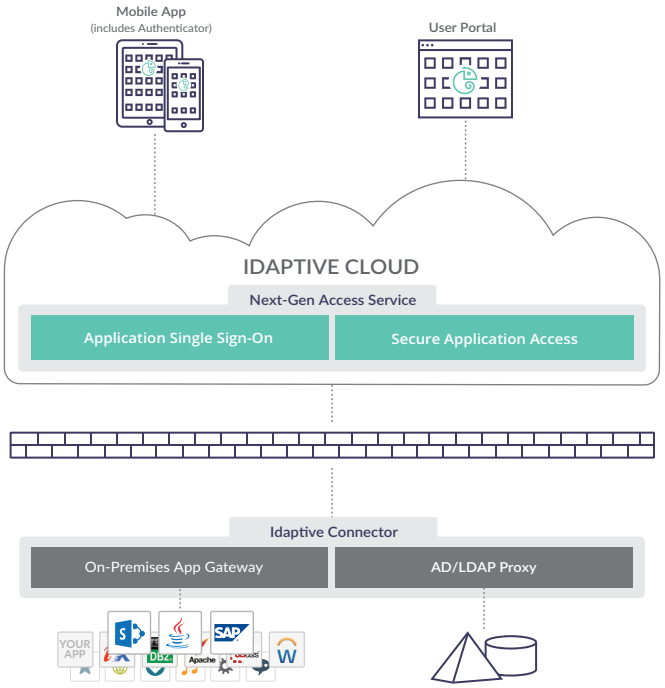
Organizations typically set up VPN infrastructure to allow trusted users to get fully encrypted, secure access to apps residing behind the firewall. The two types of VPN services prevalent in enterprises are IPsec VPNs and SSL VPNs. The major difference between an IPsec VPN and an SSL VPN is the network layers at which encryption and authentication are performed. Both types of VPNs require the installation of hardware, client software, and modification of firewall rules. SSL VPNs also require certificates and endpoint clients. However, unlike IPsec VPNs, they also offer more granular, browser-based login access to apps on the internal network.

Both types of VPNs operate invisibly to the end-users and introduce no dependencies on applications. Once users are authenticated and connected to a VPN, they can theoretically access any server on the entire network, limited only by policies already in place at the authentication and authorization step.

Installing and maintaining VPN solutions, however, requires time and effort. And, VPNs are not without security risk. One cannot assume that all traffic entering into the network over an encrypted tunnel is harmless. Any VPN solution requiring only username and password and not leveraging Multi-Factor Authentication (MFA) and user access policies puts the network at risk.

Remote access and SSO without VPNs

Idaptive provides adaptive Single Sign-On (SSO) for cloud and mobile applications to improve user experience and simplify identity and access management for IT. With the Idaptive



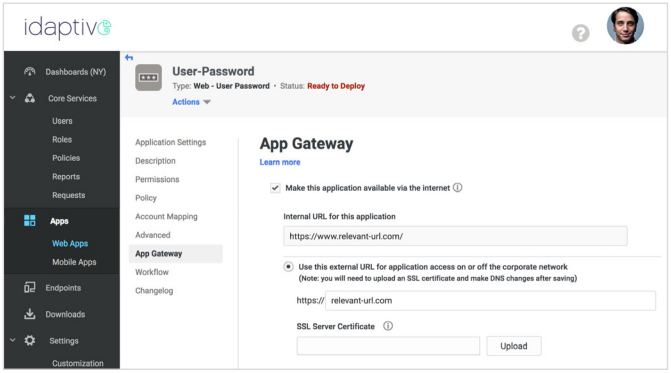
App Gateway service, you can enable secure remote access and expand SSO benefits to on-premises web apps — like SharePoint and SAP — without the complexity of installing and maintaining VPNs.

The App Gateway service is easy to install. All you need is a single agent installed on any Windows or domain-joined server behind your firewall. The agent makes a secure, SSL-encrypted outbound connection to the Idaptive platform and verifies each user's identity against your existing identity repositories such as Active Directory, LDAP, or Cloud Directory. Once authenticated, a user can connect to your on-premises apps with a single click.

For an additional layer of security, you can also implement an adaptive Multi-Factor Authentication (MFA) service. Leveraging device, network, and user behavior context, Idaptive intelligently assigns risk to each access event and allows you to create dynamic access policies for on-prem apps that are triggered when anomalous access requests are detected.

Simplify access to legacy apps

With App Gateway, you can set up one-click access to internally hosted apps such as SAP, Microsoft SharePoint, and Oracle. Users simply authenticate to Idaptive Portal with their Single Sign-On credentials and access all of their assigned cloud and on-prem apps.



Integrate faster

Setting up remote access to any on-premises application with App Gateway requires no on-prem code changes or additional infrastructure. You can leverage Kerberos, IWA, and header-based authentication to integrate on-premise apps and retire your existing WAM solution.

Implement stronger controls

You can secure access to legacy apps with adaptive MFA and configure per-app access based on user roles. App Gateway enables you to prevent both inadvertent and intentional identity–related security breaches and manage access policies for all apps in one management interface.

Conclusion

Idaptive App Gateway is available as an add-on to the Idaptive Single Sign-On service. It provides an easy and secure way to access on-premises apps without requiring configuration of VPN clients, modification of firewall policies, or changing of on-prem code. With Idaptive, IT can provide users SSO access only to the apps they need and manage user identities across all applications and endpoints from a single console.

For more information on the Idaptive App Gateway, visit here.

Idaptive provides a SaaS-delivered platform to securely manage identity and access for employees, partners, and customers. The Idaptive platform seamlessly combines the fundamental pillars of identity and access management (IAM) – single sign-on (SSO), multi-factor authentication (MFA) and user behavior analytics (UBA). Idaptive enables organizations to improve employee productivity, enhance customer and partner experiences, and reduce the risk of weak or default passwords – the primary cause of security breaches.

Ready to learn more?

Please contact us at hello@idaptive.com