Okta and F5 Networks® for Complete Access Management for Hybrid IT

okta

IDC predicts that worldwide spending on public cloud services will grow at a 19.4% compound annual growth rate (CAGR) from nearly $70B in 2015, to more than $141B in 2019.

With this rapid uptake of SaaS, PaaS and IaaS, it has been commonly understood that most enterprises will need to maintain a hybrid IT environment with a significant number of legacy applications remaining on-prem.

The first phase of cloud app adoption saw enterprises attempt to use on-prem IAM tools to integrate to the cloud. Identity-as-a-Service (IDaaS) provided an alternate approach, with a cloud-based bridge to the cloud and lightweight AD integration. Enterprises are now beginning to centralize their IAM programs around IDaaS, moving the center of gravity of identity management to the cloud. With this transition, comes the need to modernize on-prem applications, or implement solutions that enable more direct integration to IDaaS.

Okta and F5 Networks provide a joint solution that enables enterprises to seamlessly manage access to all applications, on-prem and in the cloud. With Okta and F5 Networks, customers are able to leverage best of breed products for IDaaS and network gateways. Once the F5® BIG-IP® platform and, more specifically, F5 BIG-IP Access Policy Manager® (BIG-IP APM®) is deployed and configured to Okta, IT admins can manage access through a single pane of glass in the Okta admin console. Network admins are able to maintain the security of on-prem access through F5 BIG-IP APM.

Secure Access to On-Prem Apps from Outside the Firewall

Enterprises typically use Okta for the 5000+ integrations pre-built into the Okta Application Network. Okta also has full support for federation protocols for additional applications that support federation standards. Applications in the cloud with any kind of login form can, additionally, be easily added to Okta.

When applications are behind the firewall, authentication is not enough. Users must gain network access to the application. This can be cumbersome with the standard VPN approach, requiring multiple steps for the end user.

With F5 BIG-IP APM integrated with Okta, end users can authenticate once into Okta and seamlessly access on-prem applications. In addition, F5 BIG-IP APM extends Okta's authentication capability to applications that do not have native authentication mechanisms or support header-based authentication. Finally, F5 BIG-IP APM provides an additional layer of security for on-prem applications by securing all HTTP traffic to and from an application.

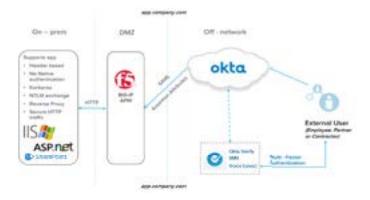| Application Authentication Mechanism	Integration
Pre-built integration in Okta Application Network (5000+ integrations)	Okta
Federation protocols SAML, WS-Fed, OpenID Connect	Okta
Any application with a login form	Okta
No native authentication	Okta + F5 BIG-IP APM
Kerberos/NTLM Exchange Authentication	Okta + F5 BIG-IP APM
Header-based authentication	Okta + F5 BIG-IP APM
Reverse proxy—access on-prem app from outside firewall	Okta + F5 BIG-IP APM
Secure HTTP traffic to/from on-prem app	Okta + F5 BIG-IP APM

Contractor and Partner Access to On-Prem SharePoint Portals

It can be a challenge to expose SharePoint Server (on-prem) to external users such as contractors or partners. Okta can integrate to SharePoint for SSO via federation. However, in order to use certain SharePoint modules, such as SharePoint business intelligence features, users must have a Kerberos token.

F5 BIG-IP APM supports the key requirement of exchanging SAML assertions for Kerberos tokens, enabling use of the full set of functionality in SharePoint. Okta, paired with F5 BIG-IP APM, can manage contractor or partner identities and enforce multi-factor authentication.

**External User Access to
Published Internal Applications**

Multi-Factor Authentication for Legacy Applications on IaaS
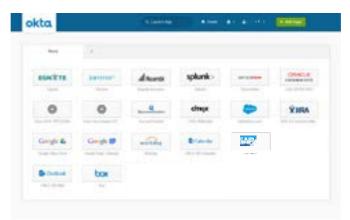
Enterprises that are moving on-prem servers to IaaS need to have a strategy for protecting access to those resources. One of the benefits of moving to IaaS may be that the service can be more easily reached from any network. F5 BIG-IP APM plays a key role in exposing these on-prem servers to the internet. Given the greater exposure, a good practice is to require

multi-factor authentication to access these services. Okta can easily add multi-factor authentication with a soft token (iOS, Android or Windows Phone), SMS or voice as factors.

One End User Portal for All Applications, On-Prem and Cloud

The Okta end user portal is built to make it easy for end users to access all their applications from one place. The portal is customizable by end users, which drives a high level of user adoption. Typically, organizations using the Okta portal want all the end users' applications exposed and accessible through the portal. Integrating Okta with F5 BIG-IP APM enables the user to log in once to Okta, and access all applications, cloud and on-prem, in one place.

One End User Portal for all your Applications

"F5 and Okta are leaders in providing secure authentication and access to an enterprise's IT infrastructure. With this integration, customers will have the best possible solution to access both on-prem and cloud applications," said F5's Ron Carovano, Director, Business Development. "F5 and Okta working together will help ensure end users' secure and seamless access to an application, no matter the type of application or where it sits."