SOLUTION OVERVIEW

Identity Aware Proxy: The Gateway to a Zero Trust Architecture

Securing Virtual Private Networks

As home or remote working becomes the norm, organizations must provide secure, authorized access to applications and resources, regardless of where the application or user is located. Many organizations rely on virtual private networks (VPNs) to secure remote user access to applications and resources. But while VPNs enable secure user access, they can also be unwieldly.

If a user accesses an application on your network via VPN, then accesses a public cloud or Software-as-a-Service (SaaS) application, the data and code for the native cloud or SaaS app passes through your network, then to the user. This can create a bottleneck within the VPN. And that can increase latency, negatively affecting user experience and productivity. Plus, VPNs can be hacked. There have been many cases where a VPN has fallen victim to an insidious man-in-the-middle (MitM) attack, particularly if the user is accessing resources and applications in a remote location over public Wi-Fi. It can even happen to home workers, as their home router can be infected, enabling MitM attacks and data theft.

THERE HAVE BEEN MANY CASES WHERE A VPN HAS FALLEN VICTIM TO AN INSIDIOUS MAN-IN-THE-MIDDLE (MITM) ATTACK, PARTICULARLY IF THE USER IS ACCESSING RESOURCES AND APPLICATIONS IN A REMOTE LOCATION OVER PUBLIC WI-FI.

VPN access also uses the now outdated “castle and moat” approach to security: If the user has the correct credentials, they are able to access any application and resource to which they are authorized within your network. While convenient, this sort of access can be disastrous for your organization. Even a trusted, known user can unknowingly and inadvertently become an insider threat.

Attackers can initiate credential stuffing attacks on your organization’s VPN login to gain access to your network, applications, and data. They can steal data, drop additional malware on your network, and take over a user’s account and launch business email compromise (BEC) attacks. They can even move horizontally within your network to infect other users or pilfer more data. Even worse, they can move upstream or downstream within your network and attack your supply chain. It can be damaging for your organization, users, and even your partners and suppliers.

The Advance of a Zero Trust Architecture

Many organizations like yours are adopting a Zero Trust architecture. Zero Trust encourages approaching security as if attackers have already infiltrated your network and are lurking, waiting for the opportunity to launch their attack. A Zero Trust approach to security eliminates the idea of a trusted insider within a defined network perimeter. It assumes that there is a limited, or even no, secure network perimeter, unlike the “castle and moat” security approach that has been employed for decades. And with many applications migrating to public clouds or being replaced by SaaS applications, and network resources being usurped by those in the clouds, a Zero Trust approach is more relevant and applicable than ever.

The Zero Trust axiom is, “Never trust, always verify.” Never trust users, even if they’ve already been authenticated, authorized, and granted access to applications and resources. Always verify and scrutinize user identity, device type and integrity, location, the applications and resources to which access is being requested, and more. And verify not just at the time a user requests access, but throughout the entire time they have access to the application or resource, and upon every subsequent access request and attempt. A Zero Trust approach means applying least privilege rights to user access; that is, allowing users access only to the applications and resources to which they are authorized, and restricting their access to a single application or resource at a time.

The core tenets of a Zero Trust architecture are identity and context. Always ensure that a user is who they claim to be by leveraging a trusted, verifiable source of identity. And ensure that only the right user securely accesses the right app, at the right time, with the right device, with the right configuration, from the right place.

Identity Aware Proxy: The Gateway to Zero Trust

Identity- and context-awareness are also what Identity Aware Proxy (IAP) enables and delivers. Identity Aware Proxy provides secure access to specific applications leveraging a fine-grained approach to user authentication and authorization. IAP enables only per request application access, which is very different than the broad access approach of VPNs, which apply session-based access. The difference is between limiting user access to a specific application or resource to which they are authorized access, versus enabling them to access every application or resource that they are authorized to access. Centralizing authorization enables application-level access controls to be created.

Context is vital within IAP. It enables the creation and enforcement of granular application access policies based on contextual attributes, such as user identity, device integrity, and user location, to name only a few. IAP relies on application-level access controls, not network-layer imposed rules. Configured policies reflect user and application intent and context, not ports and IP addresses. Finally, IAP requires a strong root of trusted identity to verify users and their devices, and to stringently enforce what they are authorized to access.

What Is Identity Aware Proxy

Identity Aware Proxy is principal in F5 BIG-IP Access Policy Manager (APM). BIG-IP APM and F5 Access Guard deliver Identity Aware Proxy, using a Zero Trust model validation for every access request. Providing authenticated and authorized secure access to specific applications, it leverages F5's best-in-class access proxy. BIG-IP APM centralizes user identity and authorization. Authorization is based on the principles of least privileged access. With its IAP approach, BIG-IP APM is able to examine, terminate, and authorize application access requests.

The context-awareness required for Zero Trust compels the development and enforcement of extremely granular authorization policies. BIG-IP APM, through its IAP support, delivers just that. Policies within BIG-IP APM may be created to verify user identity, check device appropriateness and posture, and validate user authorization.

You can also create policies to:

- Confirm application integrity and sensitivity
- Confirm time and date accessibility
- Limit or halt access if the user's location is deemed incorrect, inappropriate, or insecure
- Request additional forms of authentication—including multi-factor authentication (MFA)—if the user's location or the sensitive nature of the device or the application or files to which access is being requested warrant it
- Integrate data from user and entity behavior analytics (UEBA) and other API-driven risk sources

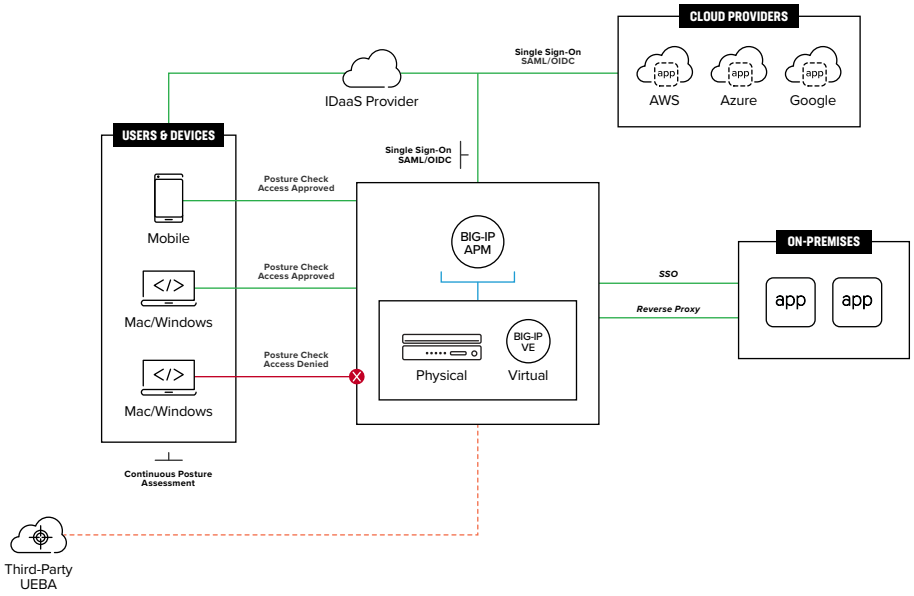

Figure 1: Identity and context validations are vital to granting the most secure remote access.

To ensure a device is appropriate and secure, and before the user can be authenticated and their application access authorized, BIG-IP APM checks their device security posture via F5 Access Guard, which is included with BIG-IP APM. However, BIG-IP APM and F5 Access Guard go beyond simply checking device integrity at authentication. Instead, they deliver continuous, ongoing device posture checks, ensuring that user devices not only meet but continuously adhere to endpoint security policies throughout the user's application access. And if BIG-IP APM senses any change in the device integrity, it may either limit or stop the user's application access, thereby limiting or eliminating potential attacks before they can be launched.

Identity Aware Proxy also simplifies application access for remote or home-based workers and better enables and secures application accessibility for your organization. Since VPN access allows users to access any application or resource to which they're authorized, it does not adhere to a Zero Trust model. However, Identity Aware Proxy empowers users to request access to a specific application directly and to have encryption protection. This significantly reduces your need for VPNs, saving your organization time and cost, while delivering a safer alternative.

An Identity Bridge for Zero Trust

A true Zero Trust security approach, though, requires that access to all applications to which a user may be authorized be secured, including applications that are not native to the public cloud or offered as Software-as-a-Service (SaaS). This must include even classic or custom applications that may not or cannot work with cloud-based identity, such as Identity-as-a-Service (IDaaS). Many of these applications remain on-premises, in a data center, or in a private cloud. Most of these applications also support classic authentication methods, like Kerberos, header-based, or others. They are unable to support modern authentication and authorization protocols like Secure Assertion Markup Language (SAML), or OpenID Connect (OIDC) and OAuth. They can't support identity federation, single sign-on (SSO), or even MFA.

BIG-IP APM solves this issue. BIG-IP APM, working closely with IDaaS providers including Microsoft (Azure Active Directory), Okta, and others, bridges the identity gap between modern and classic authentication. BIG-IP APM is able to ensure that classic and custom applications can support identity federation and SSO. This not only enhances your user experience, simplifying application access by centralizing access control, but also ensures that a secure, trusted source of identity is in place. By enabling MFA for all applications, BIG-IP APM protects all applications against inappropriate access and enables another layer of security to ensure appropriate application access. BIG-IP APM is a single, centralized control point for managing and securing user access to applications, wherever they may be hosted.

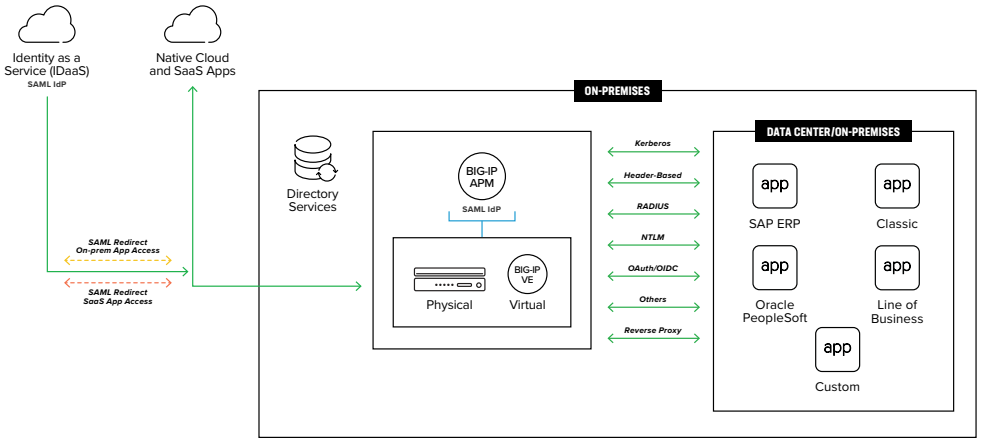

Figure 2: BIG-IP APM is a single, centralized control point for securing and managing user access to applications, wherever they may be hosted.

Conclusion

F5 BIG-IP APM, through its support for Identity Aware Proxy, enables deployment of Zero Trust application access. BIG-IP APM delivers per-request application access, while securing and managing access to all applications, regardless of their location, and authentication and authorization methods. It offers the scalability and reliability synonymous with F5, and leverages F5's industry-leading full-proxy architecture.

BIG-IP APM with Identity Aware Proxy reduces infrastructure costs, increases application security, and enhances your user and administrative experiences.