AKAMAI WHITE PAPER

Enterprise Application Access Architecture Overview

Akamai
FASTER FORWARD

Providing secure remote access is a core requirement for all businesses. Though VPNs have been around for 20+ years, traditional remote access has limitations and risks (see Figure 1), when you consider that enterprises now need to:

- Serve mobile users on mobile devices
- Deliver applications from a variety of global data centers and hybrid cloud environments
- Open up applications and data to an entire digital ecosystem of customers, partners, suppliers, contractors, etc.

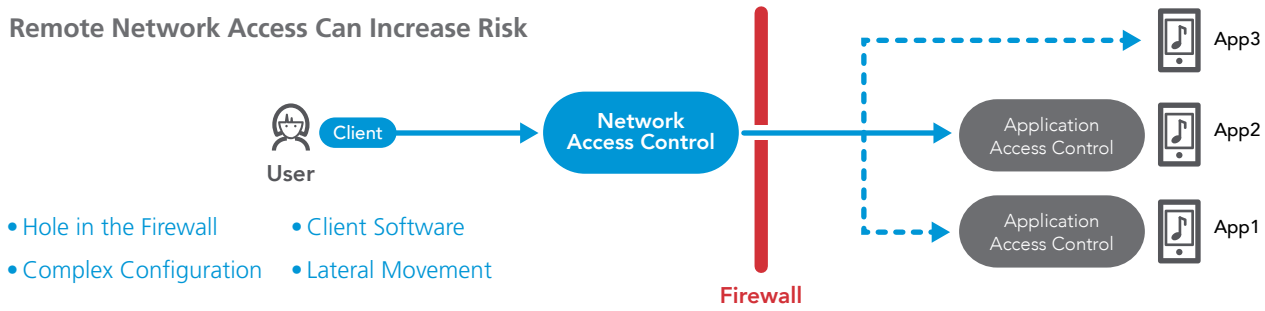

Figure 1 – Traditional Remote Access

Akamai has turned traditional remote access on its head, using a secure cloud to provide a new and better way to solve the pain for applications hosted in data centers and hybrid cloud environments.

Approaching the problem in a fundamentally different way, Enterprise Application Access (EAA) (Figure 2) is a cloud service that delivers access to applications without providing remote users access to your entire network. With EAA, you get a centralized, managed solution that does not require external hardware or software. Managing and controlling remote access becomes simple and uncluttered, and with the elimination of complexity comes fundamentally better security.

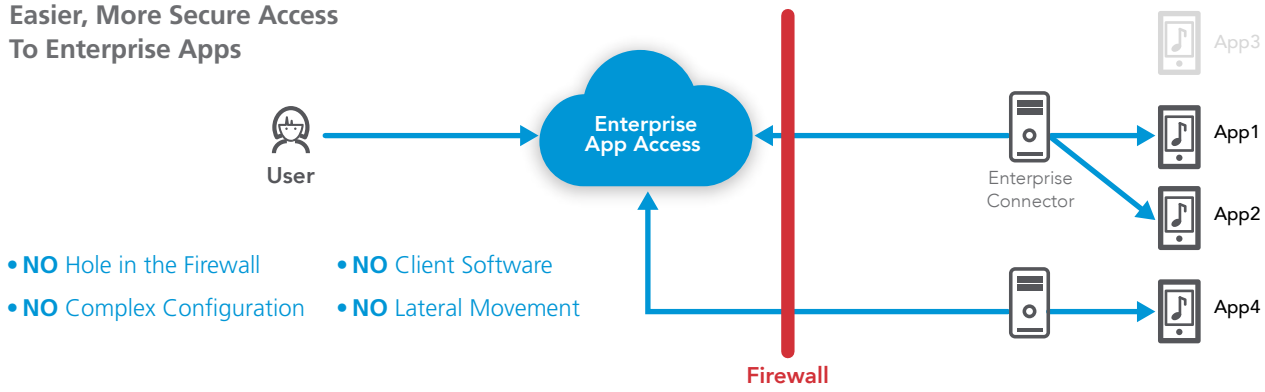

Figure 2 – Enterprise Application Access

With EAA, a Cloud DMZ service, no one can get to applications directly because they are hidden from the Internet and public exposure. A unique dual-cloud architecture closes all inbound firewall ports while providing authenticated end users access to only their specific applications. EAA integrates data-path protection, identity access, multi-factor authentication, application security, and management visibility and control into a single service.

EAA is an integrated, globally distributed service that eliminates the time and complexity of building an access solution out of component parts — and EAA can be deployed in every kind of data center or hybrid cloud infrastructure in minutes to create a central point of access and control.

The EAA Architecture

There are three major components of the EAA architecture: EAA Edge, EAA Management Cloud, and Connectors.

The EAA Edge provides the data path between the user and application as well as the data security, application performance, and optimization components. The EAA Management Cloud provides management, logging, reporting, and configuration.

The EAA Edge and Management Cloud are based on a secure, multi-tenant architecture and are hosted in multiple regions. They utilize modern cloud-scale approaches with rigorous built-in security and DDoS protection. Both are redundant with automatic fail over and can expand elastically to adapt to traffic loads. The Management Cloud is common to all customers.

Connectors are "headless" virtual appliances deployed behind the firewall in customer data centers or hybrid cloud environments. Connectors can also optionally be deployed as Dockers. Each Connector creates secure TLS sessions to EAA, enabling connectivity between users and applications. Each Connector is fully managed and configured via the EAA Management Cloud and is cryptographically unique. Multiple Connectors can be deployed for redundancy and scaling.

Connectors are packaged for deployment in the following environments:

- VMware VSphere
- Amazon AWS (VPC or classic EC2)
- Microsoft Azure
- Microsoft Hyper-V
- IBM Softlayer
- Google Compute Engine
- Openstack
- Docker

Connectors have a number of functional capabilities:

- Proxy access to web applications.
- Convert RDP and SSH sessions to HTML5 for presentation in the user's browser.
- Load balance (SLB) to multiple application servers with session or cookie stickiness.
- Communicate to local directory servers and integrate with enterprise Single Sign-on (SSO) mechanisms (e.g. Kerberos, NTLM, and ADFS).
- Collect statistics for management and performance reporting.
- Provide integration with local security functions (e.g., DLP) via ICAP.

Connectors accept no inbound connections. They only initiate outbound TLS sessions to EAA and to the applications they are configured to communicate with. Because Connectors are proxy connections, they never directly connect users and the network. From a networking perspective, Connectors require:

- A firewall rule to allow outbound connectivity over port 443 (TLS/SSL)
- Reachability to enterprise application(s) being secured by EAA
- Reachability to enterprise directory services for user authentication

How EAA Works

When initially deployed, Connectors "phone home" by establishing an outbound, mutually authenticated TLS session to the EAA Management Cloud. The Connector then pulls its configuration and updates from the Management Cloud.

Connectors establish outbound TLS sessions with EAA and are utilized as needed per policy to provide a Layer-7 path for users trying to access their applications. To prevent attacks or session hijacking, Connectors restart outbound sessions periodically.

When a user attempts to access an application, the user's browser initiates a TLS session to the EAA Edge. The EAA Edge terminates this TLS session, authenticates the user to the directory associated with the application (optionally adding 2-factor or multi-factor authentication), and matches the user against their access policy. The EAA Edge can authenticate users to the following Directories and Identity Services:

- Active Directory (LDAP), including support for Kerberos.
- SAML Identity Providers (Okta, Ping, OneLogin, etc.).
- Open ID Connect implementations (e.g., Google Directory).
- EAA Internal IDP (Identity Provider) - Customers have the option to leverage EAA as their directory source as needed.

After the user is authenticated, the outbound session from the Connector and the inbound session from the user's device are "stitched" together in the EAA. The Connector further proxies this user-to-Connector session to the application (i.e., creates a 3rd session), thereby provisioning a dynamic, end-to-end path for the user to interact with the application.

EAA's deep integration with on-premise directories, data security, and SIEM tools can be extended into cloud environments. For example, access to applications running in Azure can be authenticated to an on-premise Active Directory server in the data center, and access logs can be streamed to an on-premise Splunk appliance.

Centralized Security and Access Control

EAA applies centralized security and access-control policies for both data center and hybrid cloud environments. Key to the architecture is that EAA lies directly in the user's data path and is the only entry point for users gaining access to critical enterprise resources. EAA determines access rights for users as well as the specific applications they are authenticated to use.

EAA is a highly secure approach for application access because it moves the attack surface away from the application. Because the Connector only dials out from the customer's infrastructure, inbound access to the customer's infrastructure environment is removed, and the customer's infrastructure is no longer directly accessible or visible from the Internet.

Unauthorized access is further minimized by authenticating users outside your infrastructure. Two-factor and multi-factor authentication are available for fortified access control.

EAA also shields your infrastructure and protect applications from Internet attacks, including DDoS and botnets. To ensure optimal performance, EAA uses LZ-based payload compression, TCP optimization, and load balancing to ensure end users experience LAN-like response times. Furthermore, EAA leverages channelization strategies to reduce TCP connection setup latencies that can impact the end-user experience.

An end-user's experience while accessing applications through the EAA is fast and seamless. Instead of using a cumbersome VPN client, end users gain access to applications through any browser or mobile app; they simply enter their credentials — username, password, and optional multi-factor authentication — to identify themselves and are dynamically provisioned access to private enterprise applications.

Enterprise Application Access: Putting You Back in Control

EAA removes the chronic pain suffered by IT teams associated with managing third-party access. It is easy to deploy, provision, change, and monitor. EAA removes all the complexity: no device software, no software upgrades or updates, and no additional hardware. User management difficulties — from on boarding to off boarding — is a breeze. As a central point of entry and control, EAA provides a single management pane for detailed audit, visibility, control, and compliance reporting. The result is painless, secure remote application access.

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.