SOLUTION BRIEF

APPLICATION ACCESS MANAGEMENT (AAM)

AUGMENT, OFFLOAD AND CONSOLIDATE ACCESS CONTROL

Authentication and authorization are critical requirements for online communications. It is imperative that both clients and their target recipients verify their respective identities and access is authorized. With more and more remote transactions from e-commerce based electronic funds transfers to remote healthcare diagnostics to inter-governmental diplomatic communiques taking place over the public Internet, the parties involved must be validated. In turn, the deluge of so many sessions can overwhelm network and security infrastructures. Systems must be established that guarantee authenticity, ensure an excellent end user experience and scale to meet the accelerating demands of heightened data center security.

AUTHENTICATION AND ACCESS MANAGEMENT CHALLENGES

Organizations need to overcome the complexities of ensuring data center resources protection while eliminating data leakage. The ongoing shift towards cloud services, BYOD devices and social networks from internal and external web-based access have substantially increased the difficulties in how administrators oversee their IT security. Yet employees, partners, customers and vendors alike now demand secure access to a growing range of applications – from anywhere and on any device. Oftentimes these are mission critical business applications such as Oracle, SAP, SharePoint and Exchange. Rigorous network design and enhanced security policies are needed to provide secure remote access to these assets.

To protect application servers and other resources from unauthorized access, organizations turn to strong authentication and authorization. This requires the implementation of identity-based access controls. Identity and Access

CHALLENGE

Organizations must allow external clients access to web portals, sensitive internal resources and mobile/BYOD applications. At the same time, security must be maintained with authentication and be transparent to the user.

SOLUTION

A10 Networks AAM module enables IT administrators to deploy an authentication offload solution that is fully integrated within Thunder ADC appliances for centralized policy access management and ease of installation.

BENEFITS

- Offloads authentication processing from web and application servers
- Consolidates multiple authentication points to simplify access management
- Supports extensive authentication services and enables Single Sign-On for multiple applications
- Maximizes uptime and scale by server load balancing
- Safeguards server infrastructure with multiple layers of protection
- Provides granular access control
- Enhances security by validating client certificates with OCSP

Management (IAM) solutions help ensure this necessary asset protection while certifying regulatory compliance. This key technique is used to determine whether access should be granted to each individual client. These solutions must also support custom and standardized internal applications as well as Software-as-a-Service (SaaS) applications. Implementing such solutions is not straightforward and requires multiple elements to interoperate.

Implementing IAM tools is just a portion of the authentication puzzle solution. Such solutions can determine if end users are consuming too many network resources, misusing the network by running restricted protocols or accessing inappropriate websites. But such complex processing tasks can be overwhelming and do not scale in an elegant fashion. Setting up and configuring authentication for potentially thousands of applications such as internal and edge-based applications can be an intimidating undertaking. IAM tools can themselves be a target of malicious hacker attacks and need protection. Constant uptime must be ensured and IAM resources must be easily scaled to meet future needs. It is imperative that Single Sign-On (SSO) is supported to provide a superior user experience.

THE A10 NETWORKS AAM SOLUTION: CENTRALIZE AND SECURE AUTHENTICATION AND AUTHORIZATION

A10 Networks® Thunder® ADC line of Application Delivery Controllers with their Application Access Management (AAM) modules provides an easy to implement solution for optimizing and enforcing authentication and authorization for client-server traffic. The AAM feature seamlessly integrates with authentication servers, identity data stores and applications to authenticate users and enforce access privileges. With AAM, the Thunder ADC appliance acts as an edge authentication point for web services. By offloading IAM of many computationally intensive responsibilities, such tools are dramatically scaled. AAM supports all major authentication schemes such as SAML-based SSO and certificate validation methods including Online Certificate Status Protocol (OCSP) for seamless sign-on for mobile devices and computers using certificate-based authentication. There is no need to change multiple configurations in the existing infrastructure.

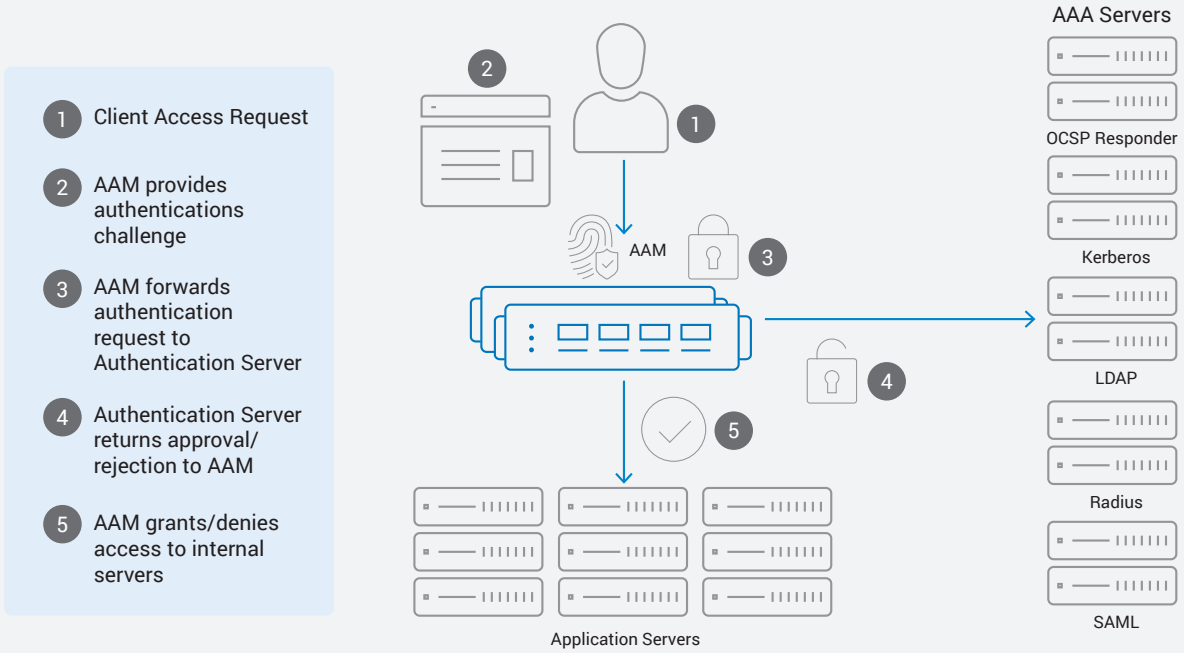

Figure 1: Optimized transparent client authentication with A10

SEAMLESS INTEGRATION OF AAM WITH ACCESS CONTROL INFRASTRUCTURE

A10 Thunder ADC with integrated AAM support is deployed in a straightforward manner and in the same data center location as per the other rich features of these appliances. Thunder ADC provides a multitude of capabilities for application availability, security and acceleration, and these appliances are placed deep within the network near the web, application and database servers. AAM is an additional critical technique to optimize the application infrastructure. Figure 1 shows how A10's AAM solution can be easily incorporated into an existing environment. Whether the scenario involves a web portal, sensitive applications such as online financial transactions or external access to internal assets where authentication may not be needed for internal users, the five step authentication process is straightforward.

FEATURES AND BENEFITS

A10's AAM solution, included in Thunder Series devices powered by A10 Networks Advanced Core Operating System (ACOS®), employs a diverse set of features to optimize authentication and authorization systems. AAM solves the challenges of these security headaches by streamlining the installation and configuration process, reducing CAPEX and OPEX, maximizing server uptime, providing granular policy configurations, supporting all mainstream authentication schemes, adding an extra layer of security and ensuring a simple login process.

NETWORK SIMPLIFICATION WITH REDUCED EXPENSES

- **Simplify and consolidate authentication** – AAM technology provides centralized management of authentication, eliminating the need to maintain separate authentication points on each web server. Consolidation of multiple authentication points reduces interoperability and integration issues and provides an enterprise-wide view of authentication policies and events. This consolidation not only streamlines management, it also lowers operations costs and reduces the number of SSL certificates that must be purchased, enhancing Thunder ADC's Return on Investment (ROI). Plus, if IT administrators wish to replace authentication servers in the future, they can simply update authentication settings in Thunder ADC rather than recoding all of their applications.

OPTIMIZE SERVER AVAILABILITY

- **Maximize uptime and scale by load balancing authentication servers** – Thunder ADC can load balance requests to authentication servers for high availability. Server health checks make sure that authentication servers are up and responsive. In the event of a server failure, Thunder ADC will forward authentication requests to the available server.
- **Offload web and authentication servers for expanded availability** – Authentication processing intensifies overhead and when multiple servers are present, management complexity increases. AAM reduces the burden on web servers thereby increasing efficiency. The Thunder ADC appliance takes on the efforts of sending authentication challenges to the end user, forwarding credentials to the AAA server and, if approved, granting access to the requested application.

ADVANCED ACCESS MANAGEMENT

- **Granular access control for expanded flexibility** – Various segments of a website and the applications present can involve different access policies; such policies demand specific methods for authentication and authorization. AAM's AAA policy ensures granular access control over these applications. IT administrators can apply custom combinations of authentication and authorization criteria based on user or group, VIP, ACL or requested URL to allow or deny access.

EXTENSIVE AUTHENTICATION STANDARDS SUPPORT

- **Easily provision a broad array of authentication schemes** – AAM supports common authentication server protocols including LDAP, RADIUS, RSA SecurID, TDS SQL, Kerberos, NTLM and client certificate authentication. AAM can interface to OCSP responders to validate client certificate status as well as Microsoft Active Directory (AD) servers to authenticate SharePoint and Outlook Web Access users. AAM offers flexible rollout of authentication across an organization.

AUTHENTICATION INFRASTRUCTURE SECURITY

- **Protect server infrastructure** – AAM provides an additional layer of defense for web and authentication servers. AAM proxies all authentication requests, preventing attackers from directly targeting authentication servers. AAM also reduces the attack surface for web attacks by restricting access to authorized users; attackers cannot execute web attacks or steal data because they cannot reach password-protected applications. Support for pre-authentication enables secure access to internal systems without the need to change multiple configurations.

ENHANCED USER EXPERIENCE

- **Single Sign-On with SAML** – AAM supports Security Assertion Markup Language (SAML) for SSO to authenticate users only one time and allows them to access multiple applications and services with no additional required authentication. The Thunder ADC appliance acts as the service provider and enforced authorization while delegating authentication to the IdP servers. AAM is interoperable with multiple SAML 2.0-based compliant Identity Providers.
- **Authentication relay for SSO** – When required by the backend server, AAM can provide relay services by acting on behalf of the client. AAM supports a variety of relays and other authentication requirements when needed. With form-based relay, AAM supports the ability to fill out a login form that is then presented to the AAA servers using information in the user credential cache on the A10 appliance. This capability provides a Single Sign-On experience to the client.

PROVEN INTEROPERABILITY IN MULTIPLE AUTHENTICATION METHODOLOGIES

AUTHENTICATION LOGON

HTML form-based authentication uses a simple HTTP/HTTPS request to challenge clients for their access credentials (typically, username and password). The authentication involves the following process:

- The end user sends an HTTP access request to the server.
- For form-based logon, the end user's browser displays a login screen, requesting username and password.
- Once complete, a request containing the user credentials is sent to the Thunder ADC appliance.
- The A10 appliance forwards the credentials to the authentication server for verification in a way that is transparent to the end user.
- If authentication is successful, the authentication server sends a success message to Thunder ADC.
- Thunder ADC grants the end user access to the requested application

SAML 2.0-BASED AUTHENTICATION

SAML 2.0 has emerged as a dominant standard and enables the secure exchange of authentication and authorization information between security domains. This protocol is an XML-based open standard for exchanging authentication and authorization data between an IdP and a service provider. It ensures Single Sign-On by leveraging SAML assertions for previously authenticated clients, even from a different site. A10 Thunder ADC supports either service provider or IdP initiated authentication. The AAM module verifies authenticity, decrypts content and shares information with the requested application. The application uses this data to sign on subsequent users enabling SSO. The process below in Figure 2 applies to service provider initiation and involves several steps:

- Client sends a request via their browser to the A10 appliance
- AAM redirects this request from the IdP provider
- Client receives an authentication challenge and returns login credentials
- IdP generates an encoded SAML response and sends to client's browser
- The AAM module on the A10 appliance provides access based on predefined policies

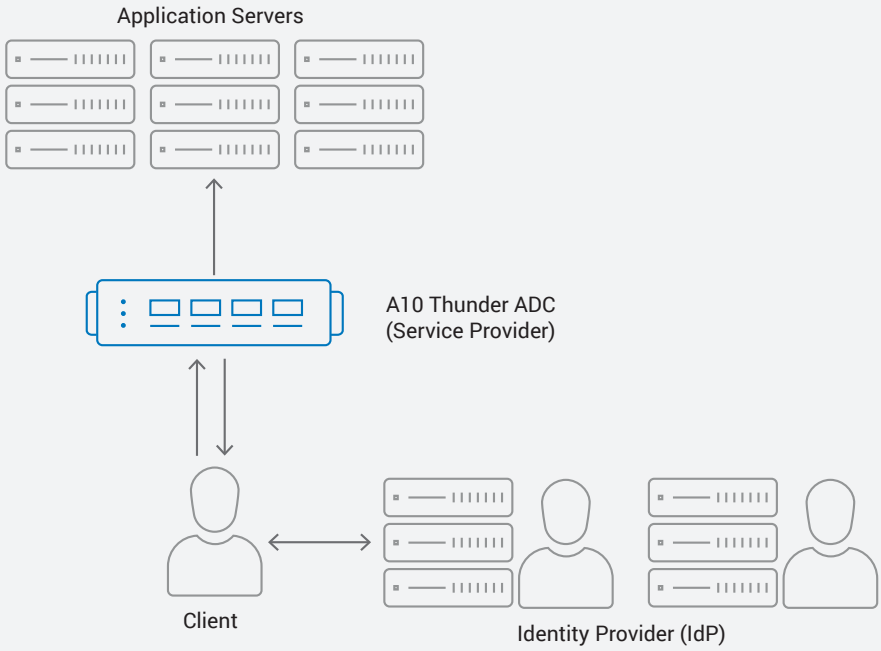

Figure 2: A10 Thunder ADC AAM supports SAML 2.0 for Single Sign-On

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

OCSP is a service that maintains published lists of Certificate Authority's (CA) Certificate Revocation Lists (CRL) and responds to revocation status requests for single certificates. This method is used to check on the status of the received client certificate and further ensure its authenticity. AAM supports OCSP and offloads application servers from this task. For SSL client authentication, OCSP authentication servers enable the A10 Thunder ADC appliance to determine the revocation state of a submitted client certificate. If the status is "good," the client is permitted to access the resources configured on the server. The authentication process involved is straightforward and involves the following steps:

- The client sends a certificate to the AAM module.
- The OCSP responder returns the certificate status (good, revoked or unknown).
- AAM checks the certificate's validity.

RICH SET OF MANAGEMENT TOOLS FURTHER EXPAND SECURITY

- The authentication logging feature enables the ability to track every access by providing an audit trail for user authentication and authorization. Events such as client request and response, session creation and termination are recorded and alerts can be set up. Access logs may be used for tracking incidents, forensics, or to demonstrate compliance.

AAM PROVIDES A VARIETY OF TECHNIQUES TO EASE CONFIGURATION.

- Through a "default portal," an included login form is provided for the authentication portal that can be used as-is or can be customized.
- A10 ACOS with its aFleX® integration provides support for custom authentication and authorization requirements. With this tool, IT can easily modify or transform user names, add domains, handle complex authorization condition statements and send user attributes such as group membership and roles to backend servers. aFleX provides integration flexibility to accommodate complex, non-standard requirements.
- AAM can also be installed in a multi-tenant environment; Thunder ADC supports up to 1,023 independent application delivery partitions (ADPs) and each of these can support a unique AAM policy configuration for increased deployment flexibility.

APPLICATION AAM FEATURES

AUTHENTICATION METHODS

- HTTP authentication (basic, negotiate NTLM/Kerberos)
- Built-in and custom web form
- Certificate authentication with optional OCSP responder
- SAML 2.0 service provider
- Third-party Identity Provider (IdP) support
- Binding support: Redirect, post, artifact, SOAP

AUTHENTICATION SERVER SUPPORT

- Windows Integrated Authentication (WIA)
- LDAP v2/v3
- RADIUS
- Token
  - RSA SecurID
  - Entrust IdentityGuard
  - Passcode authentication
  - Next token and new pin mode
- Kerberos V5
- NTLM v2 or v1
- Online Certificate Status Protocol (OCSP)
  - Client certificate validation
  - OCSP stapling support
- Health monitoring
- Load balancing of AAA servers

AUTHENTICATION RELAY

- HTTP Basic
- Kerberos authentication
  - Kerberos Constrained Delegation/Protocol Transition) (CDPT)
- NTLM
- WS-Federation
- Web Form

HEALTH MONITORING

- LDAP
- RADIUS
- Kerberos

AUTHORIZATION POLICIES

- Flexible authorization policy using LDAP, RADIUS and SAML
- Custom authorization policy using aFleX

AUTHENTICATION LOGS

- Partition-level authentication log
- Configurable authentication log levels
- External Syslog Server

AUGMENT, STREAMLINE AND CONSOLIDATE AUTHENTICATION MANAGEMENT

Organizations of all types, including enterprise, web hosting, cloud services and government use authentication to secure network resources from unauthorized access. To ensure this protection, they require an edge authentication solution that is used to determine whether access should be granted to each individual end user. The support of these web-based solutions allows end users to easily switch between applications, as well as to send and receive information as required to maximize productivity in today's fast faced environment.

AAM consolidates and streamlines authentication, offers seamless integration with a variety of authentication schemes, offloads authentication processes from servers and enhances security. By merging multiple authentication points, AAM eliminates interoperability and integration issues. Only valid clients secure access services and enjoy the benefits of a Single Sign-On experience. End users do not need to log in again for subsequent requests until the session expires.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19139-EN-05 JAN 2018