LEVERAGING RSA SECURID AND A10 FOR OPTIMIZED AUTHENTICATION

Protect, Offload and Scale AAA Servers While Ensuring Availability

Challenge:

In the age of complex Web-based applications, unmanaged mobile devices and an expanded worldwide user base, it is increasingly difficult to ensure data center and resource security. Organizations must implement strong authentication systems that properly validate client access in real time while providing an enhanced user experience.

Solution:

Combine RSA's Authentication Manager and its array of SecurID authenticators with A10 Thunder ADC and AAM module to secure enterprise and cloud-based operations. This interoperable joint solution is fully tested and certified to provide a rapid and transparent integration of authentication services.

Benefits:

- Automatically identify and block unauthorized access using client behavioral analysis
- Expand security though multi-factor authentication while simplifying login
- Scale network security by offloading computational tasks from the authentication server
- Ensure server availability through advanced load balancing and health monitoring
- Offer seamless sign-on and validity checks for BYOD via OCSP
- Eliminate multiple authentication points from diverse application servers

The accelerated use of cloud computing, mobile devices and social networks have radically changed the way organizations administer their IT operations. Employees, partners, customers and vendors alike now demand secure access to a growing range of applications—from anywhere and on any device. The support of secure, 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.

Whether from on premise or web-based client access, organizations need to validate user identities and ensure protection of sensitive information while eliminating data loss. Resources must be accessible yet remain secure and in regulatory compliance. At the same time the end user experience must be enhanced with automatic resetting of passwords and with quick access to content.

Authentication Challenges

As networks, data centers and application resources become more complex, it is increasingly difficult to ensure the necessary security. This is compounded by an ever increasing user base accessing network resources from unmanaged mobile devices via uncontrolled access points such as web portals. With innumerable BYOD clients accessing confidential and sensitive information, it is a constant challenge for IT administrators to identify attempts to compromise passwords, determine suspicious behavior based on login monitoring, and distinguish end users and machines that deviate from network policies.

At the same time, organizations of all types, from enterprise to government to cloud services, run many mission-critical web and business applications – often including Oracle, SAP and Exchange. In most cases, these operations must provide end users and employees with access to these applications over the Internet, and this brings up a potential security concern for IT teams. Organizations need stringent network design and enhanced security policies to provide secure remote access to these high value assets.

To protect application servers and other resources from unauthorized access, organizations turn to strong authentication. This key technique is used to determine whether access should be granted to each individual client. Such tools can determine if end users are consuming too many network resources, misusing the network by running restricted protocols or accessing inappropriate websites. Client admission can be evaluated regardless of location, time or type of requested resources. Access to public websites, sensitive applications such as online banking or shopping portals, and external access to internal assets where internal users do not otherwise need authentication are all fully protected.

The A10 Networks and RSA Joint Solution

RSA® and A10 Networks® have partnered to offer an optimized, proven and interoperable strong authentication solution for organizations of all sizes and types. The RSA Authentication Manager combines the strength of RSA SecurID with the convenience and flexibility of risk-based authentication. This tool authenticates requests and centrally administers user authentication policies for access to enterprise networks.

The A10 Thunder® line of Application Delivery Controllers (ADC) provides a multitude of features for intelligent traffic management, application security, content delivery optimization and SSL offload. With the A10 Thunder ADC Application Access Management (AAM) module, authentication servers are divested of excess processing and an extra layer of security is provided. For this solution, RSA Authentication Manager and Thunder ADC's AAM have been jointly tested and validated to ensure compatibility and ease of deployment.

The RSA Authentication Manager Solution

RSA Authentication Manager provides two-factor authentication to secure access to virtual private networks (VPNs), wireless networks, web applications, business applications and all kinds of operating environments. This tool leverages the largest set of RSA SecurID authenticators in the industry with support for numerous soft and physical tokens. Available as a physical or virtual appliance, this server provides the flexibility to support a wide range of authentication methods, an advanced risk engine, ease of manageability, and interoperability with industry-leading products and vendors, including A10 Networks.

Risk-based Authentication

Risk-based authentication (RBA) is designed to protect access to the most common web-based applications, including SSL VPNs, web portals, Outlook Web Access (OWA) and Microsoft SharePoint environments. With the addition of RBA into the RSA Authentication Manager portfolio, organizations can now cost-effectively secure access to a wider range of applications than ever before.

The RSA Risk Engine is a proven technology that powers the most convenient method of strong authentication. Not a static, rules-based system, the risk engine employs a combination of real-time device and behavioral analytics and dynamically adapts its risk model as new information is collected. Low-risk users are authenticated transparently, while high-risk users are prompted to provide an additional proof of identity. RBA offers strong authentication that is cost-effective and convenient for both end users and IT administrators.

Manageability

RSA Authentication Manager includes a suite of built-in features that address the most time-consuming and costly tasks associated with managing an enterprise authentication suite. The user dashboard is a convenient single-pane view designed to enable Help Desk administrators to quickly address the most common user inquiries without needing to run multiple reports or searches. The customizable Self-Service Console is another feature that saves IT staff time by empowering users to manage their authentication methods. Deployed in the DMZ area of the network, the self-service portal allows users to change their own PIN, request a replacement token, request emergency access and access other troubleshooting services.

Flexibility

RSA Authentication Manager is designed to deliver choice and flexibility, including a range of authenticators such as hardware tokens, software tokens, on-demand authentication and risk-based authentication. An organization can mix and match the preferred type of authenticator and easily provision and manage users on a single console.

Choice and flexibility extend to deployment options. RSA Authentication Manager is offered on a hardware appliance and a virtual appliance. The virtual appliance allows organizations to take full advantage of VMware ESX or ESXi virtualization, which dramatically simplifies deployment. RSA Authentication Manager is designed to support a wide range of options, even including a combination of virtual and physical appliances.

Interoperability

RSA Authentication Manager is interoperable with many of the major network infrastructure and operating system products on the market. The Secured by RSA program, one of the largest alliance programs of its type, brings together hundreds of complementary solutions. Including more than 400 products from over 200 vendors, Secured by RSA helps assure that organizations have maximum flexibility and investment protection. Leading vendors of remote access products, VPNs, firewalls, wireless network devices, web servers and business applications have built-in support for RSA Authentication Manager. And RSA has worked with A10 Networks to ensure full system level compatibility of A10 Thunder ADC.

A10 Thunder ADC with Application Access Management

Authentication Offload

A10's Application Access Management (AAM) solution, included with all A10 Thunder ADC appliances, is a set of services for optimizing and enforcing authentication and authorization for client-server traffic. This module functions transparently, and it is interoperable with RSA Authentication Manager to offload computational tasks from both application and RSA's authentication servers. Authentication processing adds overhead, and when multiple servers are involved, management complexity increases. Authentication servers can also be vulnerable to attacks.

With AAM, the A10 Thunder ADC appliance acts as an edge authentication point for web services. Administrators can offload the drain of authentication processing to the A10 Thunder ADC, thereby increasing server efficiency and adding an extra layer of protection for web servers. AAM also offers Online Certificate Status Protocol (OCSP), which enables seamless sign-on and validity checks for BYOD and similar devices using certificate-based authentication.

The AAM solution provides centralized management of authentication for web servers. For example, an IT team can use AAM to require authentication to a previously internal-only wiki or website when

accessed by external users. AAM serves as the central authentication point for external users. AAM can also eliminate the need to maintain separate authentication points on each web server.

Optimization and Enhanced Security

Managing multiple authentication points for various application servers can be a daunting task and increases network complexity. Setting up a client authentication scheme for each application may require costly and time-consuming custom development work. AAM provides centralized access policy management, while consolidation of multiple authentication points reduces interoperability and integration issues.

A10 Thunder ADC adds an extra layer of security by providing pre-authentication functionality for business-critical web server applications (such as Oracle Financials). Pre-authentication enables secure access to internal systems without the need to change multiple configurations in the existing infrastructure. AAM also offers a Kerberos Single Sign-On (SSO) security solution that allows non-Kerberos end users to access services protected by your Kerberos realm with a single login. End users do not need to log in again for subsequent requests until the session expires.

The A10 Thunder ADC AAM feature supports the identity federation standard – Security Assertion Markup Language (SAML). This protocol is an XML-based process for exchanging authentication and authorization between Identity Providers (IdPs) and service providers. The AAM feature has demonstrated SAML interoperability with RSA and other authentication service offerings.

Deploying RSA Authentication Manager and A10 AAM

The AAM solution from A10 can also be quickly and seamlessly integrated into an existing application infrastructure. AAM provides enhanced protection and server efficiency by offloading authentication processing from AAA servers such as RSA Authentication Manager.

HTML Form-based Authentication

RSA and A10 solutions may be combined to enhance the authentication process (see Figure 1). Basic HTTP or HTTPS authentication uses a simple request to challenge clients for their access credentials. Here's the way this process works:

- The end user sends an HTTP/HTTPS access request to the application server.
- The A10 Thunder ADC AAM module intercepts this request and sends an authentication challenge (WWW authentication header) directly to the end user for authentication.
- The end user's browser launches a login screen requesting the required credentials and then sends this to the A10 Thunder ADC appliance.
- The A10 Thunder ADC appliance transparently forwards the credentials to the RSA Authentication Manager for verification.
- If the authentication is successful, the RSA Authentication Manager sends a success message to the A10 Thunder ADC appliance.
- The A10 Thunder ADC appliance grants the end user access to the requested application.

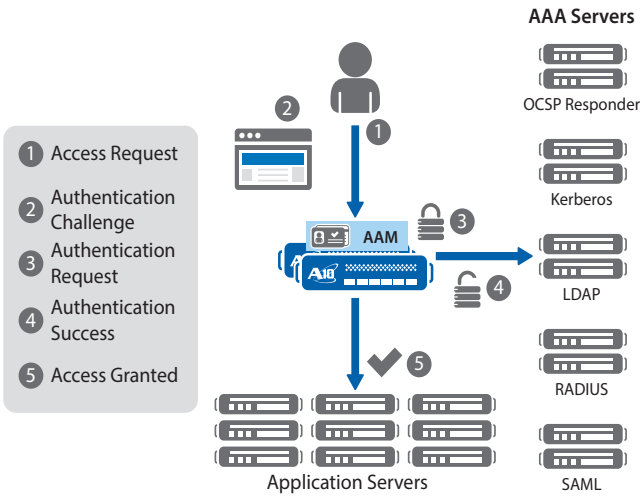

Figure 1: Optimized transparent client authentication with RSA and A10

Features and Benefits

The RSA and A10 joint authentication solution provides users with new capabilities and important business benefits. These include:

- Augmenting any application with a strong, multi-factor authentication layer provided by SecurID
- Offloading authentication servers from excessive processing for better performance, greater scalability and faster response times
- Advanced authentication server load balancing and health checks for ensured availability
- Seamless integration of authentication services for rapid installation and configuration
- Validated interoperable support for a broad base of authentication schemes
- Elimination of complex multiple authentication points from every application server

With RSA and A10 working together, organizations can ensure that their data center applications and networks remain highly available, accelerated and secure.

Summary – Synergistic RSA Authentication Manager and Thunder ADC Solution

Combining the sophistication of superior authentication from RSA with the power of an A10 Thunder ADC appliance and AAM module helps organizations protect, offload and scale AAA servers while ensuring availability.

The security of enterprise, government, cloud services and other industries is greatly improved with strong multi-factor authentication beyond simple username and password. At the same time, the end user experience is enhanced as genuine users are not hampered with unnecessary challenges and authentication delays. Only suspicious activities will involve further proof of legitimacy with this industry-leading solution.

About RSA Security

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats. RSA delivers agile controls for identity assurance, fraud detection, and data protection; robust Security Analytics and industry-leading GRC capabilities; and expert consulting and advisory services.

About A10 Networks

A10 Networks is a leader in application networking, 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, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19138-EN-01
Mar 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.