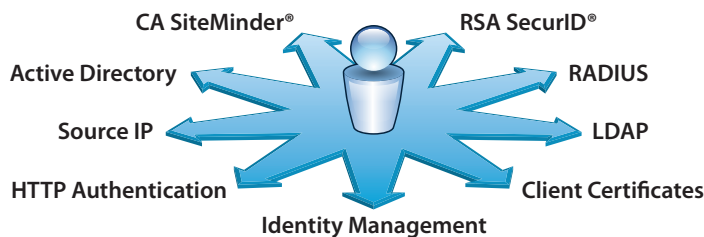


The Barracuda Web Application Firewall: Simple and Versatile Solution for Patient Privacy

Introduction

Healthcare providers must comply with Patient Privacy Rules that ensure an individual's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care. With the increasing adoption of Electronic Medical Records (EMR) and other forms health information systems, access to health information is increasingly available through Web interfaces. As a result, healthcare providers that manage electronic Protected Health Information (ePHI) must implement strong security safeguards to ensure confidentiality and limit access to sensitive data.

Barracuda Networks provides a complete and comprehensive application control platform to reduce the risk of patient privacy breaches. Barracuda Web Application Firewalls extend traditional application firewall delivery capabilities to support comprehensive Identity and Access Management (IAM), ranging from simple application authentication and authorization up to more granular, full-featured Single Sign-On (SSO). This integrated capability is simple, versatile, easy to deploy and available on all Barracuda Web Application Firewall models.



Concepts and Benefits

Traditional Access Management systems support authentication, authorization and accounting (AAA). In the context of Web applications, auditing is used in place of accounting.

1. **Authentication** is the process of verifying the digital identity of a client using the credentials provided by the client. This is normally accomplished by matching the client credentials, such as user ID and password, against an authentication service (AS), which maintains credentials in an Authentication database (AD). Normally, such services also provide for hierarchical grouping of users for ease of management.
2. **Authorization** is the process of verifying that the client, once authenticated, has access rights to a Web resource. For example, an authorization rule may be created to allow clients access to the organization's partner portal only when they belong to the "partners" group in the AD.
3. **Auditing** is the process of tracking the user activities and resource usage through audit log trails, alerts and reporting. This is especially important for meeting HIPAA compliance regulations.

The Problems with Traditional Access Management Implementations

As in any deployment, multiple heterogeneous applications and Web servers act as clients to an authentication service. The success of the implementation depends heavily on the interoperability of all the components from different vendors with the authentication service. This scenario presents a number of issues, as discussed below.

1. **Single Sign On:** Performing single sign on can be a significant challenge when multiple applications are deployed across multiple heterogeneous servers.
2. **Lack of Centralized Auditing:** Administrators need to ensure that user audit trails are properly configured across all the applications. There is no consolidation of such disparate audit trails, which is often necessary for meaningful analysis or forensics.
3. **Application Re-engineering:** Building authentication and authorization into the applications requires significant changes to each copy of each application within the DMZ. This entails API implementations, platform specific support procurement, and ongoing maintenance issues.

RELEASE 1

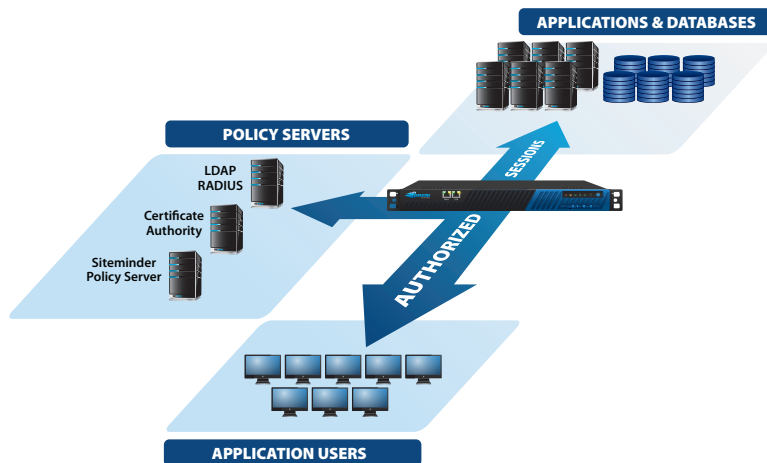
DECEMBER 2010

- 4. Change Management Issues:** Changes must be standardized across all the applications or servers. Third party add-ins may require frequent updates to keep up with the evolving platform and some often reach end-of-life. Interoperability issues may require upgrade or downgrade of the Web server, which may conflict with change management processes.
- 5. Limited Web Authorization Support:** Often, AAA systems do not offer flexible authorization policy specifications for Web resources, as they do not have adequate visibility into the application constructs being used for resource specifications (such as URL query and FORM parameter values).
- 6. Network Management Issues:** Web servers typically reside in the DMZ, whereas the authentication servers are a part of the enterprise server farm. The entire intermediate network infrastructure must be configured to allow the individual Web servers to access the authentication servers.

The inability to provide centralized Identity and Access Management makes it difficult to secure ePHI and monitor access, thereby increasing an organization's risk to data breach.

A simple solution for Application Identity and Access Management

The Barracuda Web Application Firewall assists organizations with the complex task of implementing authentication, authorization and auditing functions across heterogeneous Web applications. It intercepts user requests and enforces external authentication on behalf of the protected applications, acting as a centralized authentication, authorization and auditing management endpoint in the network.



Benefits and Features

- **Simple.** The appliance solves the authentication and authorization problem for an entire Datacenter.
- **Versatile.** The appliance scales to provide multiple methods of authentication and authorization integration.
- **Fast and efficient SSL deployments** are easily achieved by using the extensive SSL capabilities of the Barracuda Web Application Firewall. It supports both certificates for encryption and client certificates for authentication.
- **InstantSSL** is an innovative Barracuda Web Application Firewall capability that takes a non-encrypted HTTP site and transforms it into a secure HTTPS site without any application code modification required.
- **Data Theft Protection** scans all outbound traffic for sensitive information. Patient information such as Social Security Numbers, Patient IDs, or Record Numbers are monitored by the Barracuda Web Application Firewall and can be blocked or masked.
- **Two factor authentication** is provided by built-in integration with RSA SecurID®. The Barracuda Web Application Firewall integrates with RSA SecurID® to support One Time Password (OTP) token generated by hardware tokens.

Barracuda Networks Simple and Versatile Solution for Patient Privacy

- **Extensive logging** capabilities on the Barracuda Web Application Firewall provide visibility and enable administrators to build comprehensive access control policies.
- **Centralized user audit trail and reports** help in meeting compliance and forensic requirements.
- **Standards based support.** Traditional methods using LDAP, RADIUS and Active Directory are easily supported and augmented.
- **Single Sign On (SSO)** capabilities of the Barracuda Web Application Firewall enable architects to easily integrate multiple applications into a single portal. Full scale advanced authentication and authorization, along with identity management is available with the integration of the CA SiteMinder® Policy Server.
- **Internal authentication database** is included in the system for small user groups that do not have directory services deployed in their network.

A Complete, Simple and Versatile solution for Application Identity and Access Management

The Barracuda Web Application Firewall delivers a wide range of Identity and Access Management capability services to secure sensitive ePHI and significantly reduce risk of a data breach. Whether it is full-scale identity access management, data theft protection, single sign on (SSO), two-factor authentication, or comprehensive logging for auditing purposes, the Barracuda Web Application Firewall provides a simple, versatile and high-performance solution for Patient Privacy.

For questions about the Barracuda Web Application Firewall, please visit <http://www.barracuda.com/waf> or call Barracuda Networks for a free 30-day evaluation at 1-888-ANTI-SPAM or +1 408-342-5400. For more information on our other security and productivity solutions, please visit <http://www.barracuda.com/products>.

About Barracuda Networks Inc.

Barracuda Networks Inc. combines premises-based gateways and software, cloud services, and sophisticated remote support to deliver comprehensive security, networking and storage solutions. The company's expansive product portfolio includes offerings for protection against email, Web and IM threats as well as products that improve application delivery and network access, message archiving, backup and data protection.

Coca-Cola, Kaiser Foundation Hospitals, IBM, L'Oreal, BlueCross, BlueShield, Harvard University, Novartis, and Europcar are among the more than 100,000 organizations protecting their IT infrastructures with Barracuda Networks' range of affordable, easy-to-deploy and manage solutions. Barracuda Networks is privately held with its International headquarters in Campbell, Calif. For more information, please visit www.barracudanetworks.com.



Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
+1 408.342.5400
www.barracuda.com
info@barracuda.com