ORACLE Gold Partner

F5 White Paper

Streamlining Oracle Web Application Access Control

Web application security is critical—the data that web servers and their back-end databases house is invaluable to an enterprise. An organization must be able to control who can access their resources and when, as well as audit that information. F5® BIG-IP® Access Policy Manager™ (APM), in conjunction with Oracle Access Management (OAM), helps centralize web application authentication and authorization services, streamline access management, and reduce infrastructure costs.

by
Peter Silva
Technical Marketing Manager—Security, F5

Rey Ong
Sr. Product Manager, Oracle

ORACLE WEBLOGIC READY

Contents

Introduction

Many would say their lives have been transformed by the Internet; but most don't realize that most of the data we interact with daily is actually on the World Wide Web portion of the Internet. Ninety percent of the time when you open your browser, you are going to the Web. Web access management has never been more important to users, corporations, and web applications.

Users have been confirming their digital identities against a user database for over a decade, particularly in work domain environments and financial web applications. Nearly all public portal sites that offer any sort of customization require users to enter a user name and password to access information. Controlling web application access, web application security, and web application authentication is critical to IT infrastructures. Web application security is paramount to protecting the invaluable data that resides on web servers and their back-end databases. This can include an enterprise's financial data, personal data, human resources information, intellectual property, competitive information, customer data, and more. Organizations must secure web applications by carefully controlling and monitoring who accesses what types of information and when, to protect sensitive data and adhere to regulatory compliance mandates.

Oracle Access Manager (OAM) provides an identity management and access control system that can be shared by all your applications. The result is a centralized and automated single sign-on (SSO) solution for managing who has access to what information across your entire IT infrastructure.

Business Requirement: Identity and Access Management

Identity and Access Management (IAM) is a user-provisioning system that manages data access. It seeks to authenticate users and approve system resources for use. The goal of IAM is to provide contextual access to the right users at the right time, but also to protect corporate resources. IAM comprises authentication, authorization, user management, and a central user database.

Authentication confirms that a user is who they say they are; it validates their authenticity. A user name and password is the most common way to authenticate a user. Authorization determines whether the user has permission to access a

particular internal asset by checking the user's request against a specific policy. For instance, organizations can use role- or group-based attributes to determine whether to grant access. User management is essentially the overall process of managing user identities, from adding and deleting users to users' profiles and passwords. It also determines what permissions are available to the user. The central user database is the single authoritative repository that stores and delivers identity information. It contains the current user identities and their affiliation with the different systems. Identity management technology is essential for maintaining regulatory compliance pertaining to data access and management.

In today's rapidly evolving business environment, organizations need to implement IAM solutions that are scalable, highly secure, and cost-effective. One way to achieve this is to remove access management decisions from within an application and instead apply IAM to simplify user authentication, consolidate infrastructure, and reduce costs.

Oracle Access Manager (OAM), part of Oracle's identity and access management platform, provides identity and access control for Oracle and non-Oracle applications. OAM includes these components:

- Directory Server: an LDAP database that contains all the required user information.
- OAM Policy Manager: the policy administration interface that determines who will have access to what resources and how they will be authenticated.
- OAM Access Server: the policy decision point.
- OAM WebGate: the software agent running on the actual web servers or web access proxies that inspects each user request and enforces the policy.

Web Application Access Today

OAM Access Server, OAM Policy Manager, and Directory Server provide the back-end policy infrastructure to classify users and resources and set policies for access permissions. Together, these components make up Oracle Access Manager. A typical OAM enterprise deployment consists of (1), the LDAP-based Oracle Internet Directory, which contains the users; (2), OAM Access Server and OAM Policy Manager, which set the policy and grant organized access to the web resources that reside on the Oracle web servers; and (3), WebGate, the piece of software that runs on and controls access to the web servers.

Users who want to access a web resource have to be authenticated and validated through the WebGate first. The WebGate agent, which is running on a web server, intercepts each client request and compares it to a policy to determine whether the user has permission to access the requested URL. The WebGate agent is the Oracle software component that runs on F5 BIG-IP Access Policy Manager (APM) and provides the same functionality of WebGate.

Traditionally, organizations have had three options to provide access control to web applications. In the first option, the access control decisions are written into the web application code by the developers. This is both costly and difficult to maintain. It is not easily repeatable, the access decisions are decentralized, and it is typically much less secure than other options. In this situation, the access control decisions are enforced by the web application developers and might not take into account various potential context scenarios, such as the user's device, where the user is located, the network type, and whether the device adheres to the corporate security policy. Organizations should consider all of these context scenarios when determining access rights.

The second option involves deploying a software agent on each web server. Using agents can be difficult and costly to administer and maintain. They don't always work with every application or operating system, and they can decrease web application performance. Loading a WebGate on every web server can be a challenge since there are number of different applications, server types, and operating systems. It would be prohibitively time-consuming to update each agent on each server. Similar to option one, the access decisions are decentralized and less secure.

The third option involves deploying a tier of specialized access proxy servers, or a web application management proxy, in front of each web server. The proxy tier can be difficult to manage and expensive to maintain, especially for high availability. You would need a pair of servers for every Oracle application to maintain high availability. As new proxy servers are required for new web servers, this option does not scale well. It adds a whole layer of infrastructure, including the basic data center costs of power, cooling, and maintenance when many companies are looking to consolidate and control costs.

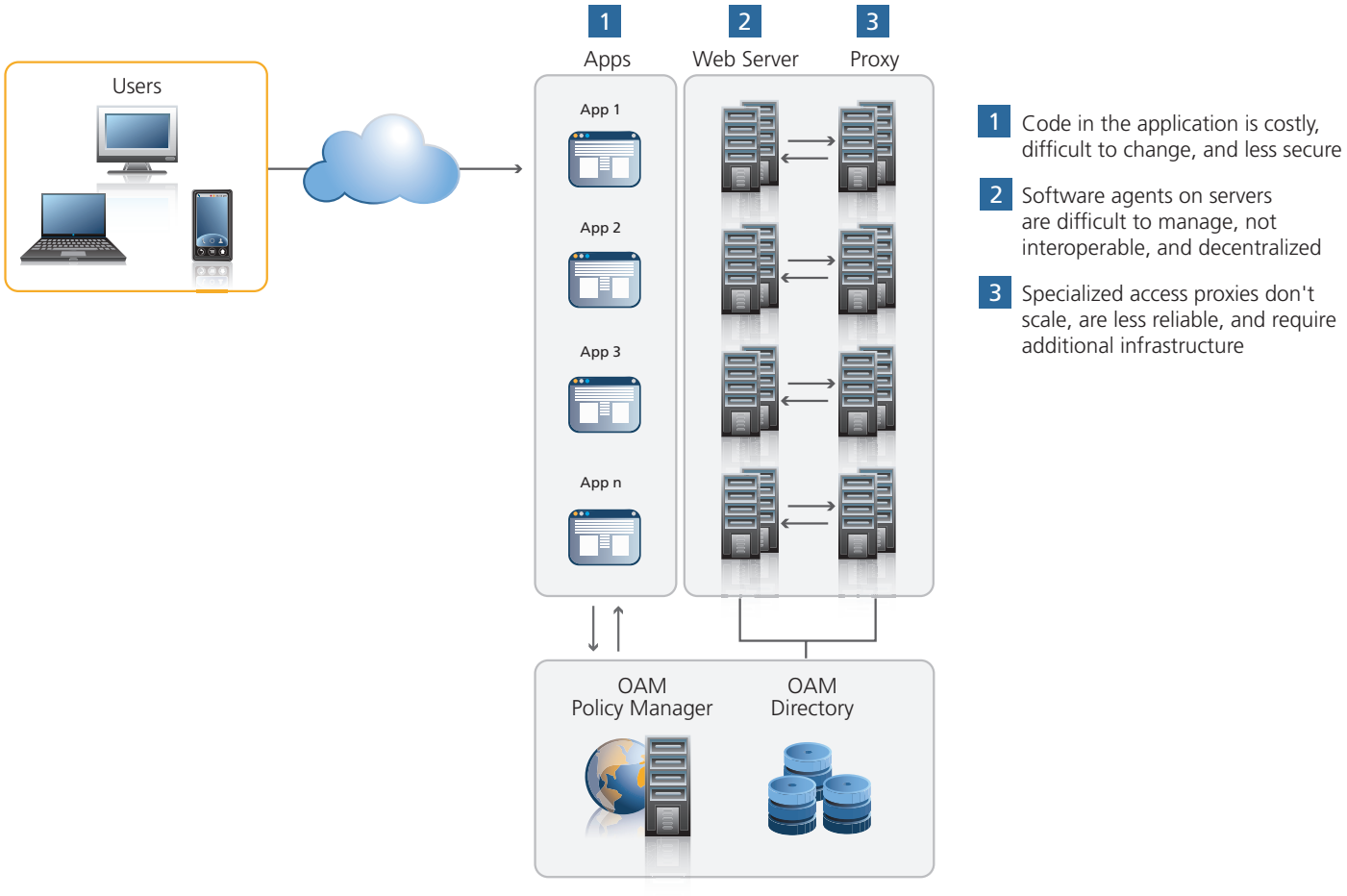

Figure 1: Three traditional approaches to web application access control

There is now a new, superior solution: Integrate BIG-IP APM with Oracle Access Manager (OAM) to avoid having to build or maintain a proxy tier, dramatically reducing capital and operating expenses. BIG-IP APM runs as a module on BIG-IP Local Traffic Manager™ (LTM). In all, this solution provides superior performance, security, and reliability.

Unified Access Integration

BIG-IP APM works in concert with your existing identity management systems to control access to web applications. BIG-IP APM can provide network-based identity management and control client web access by performing client inspections, so your organization can ensure that only users with appropriate security profiles on approved devices are allowed access to your business-critical resources. To improve response time and scale performance, BIG-IP APM can cache credentials and provide SSO capability. These policies are created using the Visual Policy Editor,

F5's easy-to-use graphical interface. BIG-IP APM also includes software components and features from the OAM platform to make integration with Oracle applications easy and hassle-free.

F5 and Oracle's partnership includes the WebGate software functionality with BIG-IP APM. The BIG-IP device is connected to the OAM server. When a user tries to access a website, BIG-IP can now facilitate/function as the WebGate proxy tier, and it queries OAM and Oracle Internet Directory (OID) to authenticate and validate the user, then sets the session cookie for the user. If the user is valid, BIG-IP forwards the request to the actual web server. This functionality can eliminate an entire tier of infrastructure, which saves on hardware, software, maintenance, and operation costs, along with any electrical, rack space, and basic data center costs.

You can obtain a license for the BIG-IP APM module, which runs on BIG-IP LTM, and then enable a host of additional functionality to enhance your Oracle deployment. For example, you could enable BIG-IP Application Security Manager™ (ASM) to provide web application firewall services. Or, to enhance user experience over the WAN, you could enable web acceleration software.

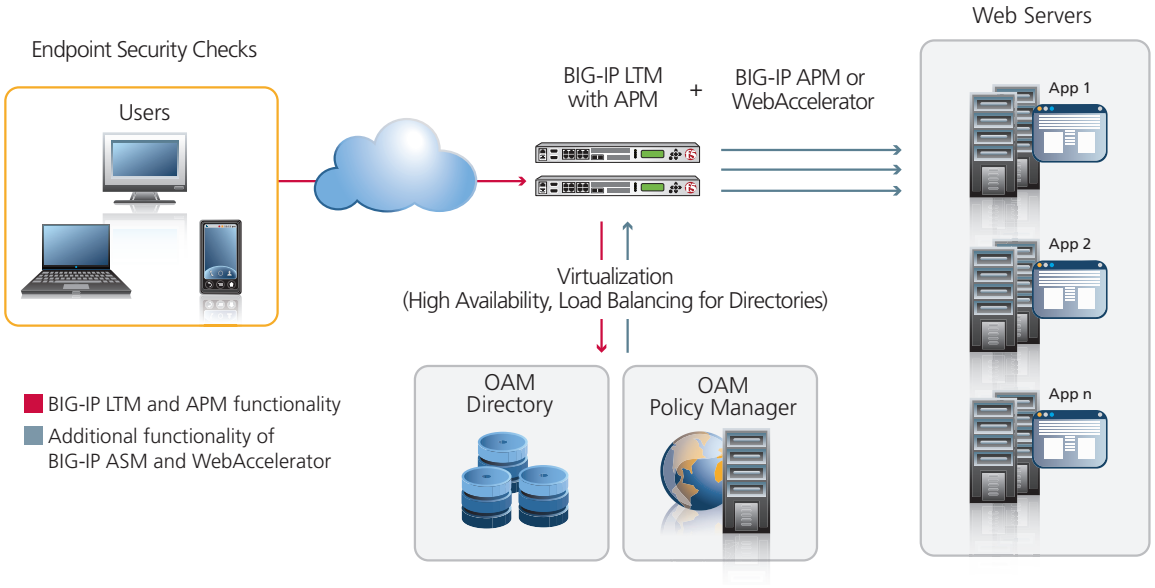

Figure 2: Richer application delivery with BIG-IP LTM and BIG-IP APM

The F5 and Oracle integration offers a unified access and authorization solution that simplifies access to Oracle applications. By consolidating authentication,

authorization, and accounting and policy control onto BIG-IP devices, organizations can reduce their deployment complexity, increase business agility, and satisfy regulatory compliance requirements such as Sarbanes-Oxley and HIPAA.

A BIG-IP APM and OAM integration is a preferable alternative to the three traditional options. By using this integration, organizations can replace their entire proxy tier and WebGate with BIG-IP APM, which includes the WebGate functionality and runs on high-performance software on BIG-IP LTM. This results in numerous benefits for enterprises.

First, organizations will realize a significant savings in both capital and operational expenditures when they eliminate the entire proxy tier, which requires dedicated hardware and software in addition to IT administrator resources. One F5 customer estimated their organization could save $2 million with this solution. The BIG-IP platform can handle a large number of users and high traffic volumes for better performance, and it provides superior scalability and high availability for/to web applications. This solution simplifies the infrastructure as BIG-IP products may already be in the organization's network performing load balancing. An organization simply needs to add the BIG-IP APM module license to BIG-IP LTM and perform a few minutes of configuration to meet their application access control requirements.

There are several additional benefits that an organization can take advantage of when using the BIG-IP platform. BIG-IP APM can perform pre-logon endpoint host inspections such as verifying the client's anti-virus or firewall software. The BIG-IP platform provides load balancing for web applications, and an organization can use it to provide both high availability and load balancing for all of OAM's services. Adding BIG-IP ASM, a web application firewall, as part of your BIG-IP security profile can help protect web applications against layer 7 malicious attacks.

Finally, BIG-IP WebAccelerator™ provides intelligent caching and compression to give users the feeling of instant response and LAN-like performance, and it helps deliver those web applications as fast as possible. This is especially beneficial for remote users, branch offices, or clients that are connected to slow or high latency links. Most important, in conjunction with Oracle, all of this can be achieved with one investment in F5, on one platform.

Conclusion

Web applications deliver critical data to users every day. F5 BIG-IP APM, running on BIG-IP LTM, in conjunction with Oracle Access Manager helps centralize web application authentication and authorization services, streamline access management, and reduce infrastructure costs. BIG-IP APM can reduce TCO, lower deployment risk, and streamline operational efficiencies for customers along with providing a single point of enforcement to simplify auditing and control changes in configuring application access settings. The F5 and Oracle integration is a unified access and authorization solution that simplifies access to Oracle applications on a single platform to ensure they are fast, available, and secure.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com