BROCADE

SOLUTION BRIEF

Securing Web Applications with Attribute-based Authentication

HIGHLIGHTS

- Provides IAAA security with in-depth access control over sensitive and classified information
- Enables an active security layer to supplement PKI infrastructures
- Provides attribute-based authentication for enhanced visibility and control of individual data and content requests
- Scans all in-bound HTTP requests automatically to block harmful traffic from reaching Web application servers
- Filters outbound traffic to mask sensitive or personally identifiable data
- Limits the scope of potential breaches by restricting access to specific users and data sets

A Modern Layered Security Approach for Modern Applications

Organizations must evolve their defense strategies and security architectures to address the changing threat landscape. Public-facing organizations are especially open to the risk of reputation damage and decreased brand loyalty if they are unable to respond to this new type of threat.

Modern Web applications built with HTML and JavaScript provide attackers with a wide range of opportunities for infiltrating an organization's application servers and databases. For example, the Payment Card Industry Data Security Standard (PCI DSS)—the mandatory industry standard for organizations handling branded credit cards—requires that Web applications be protected against known attacks through automated technical solutions, such as Web application firewalls, that detect and prevent Web-based attacks.

One solution for this challenge is the Brocade® Virtual Application Delivery Controller (vADC). This layered security solution provides an affordable, rapid-response approach that helps organizations stay ahead of fast-evolving threats. Adding an attribute-based authentication and application-specific security layer to a security architecture helps to provide proactive enforcement of access controls in an era of increasing Web application complexity. Brocade vADC augments existing infrastructures to extend robust security to the application layer across the network.

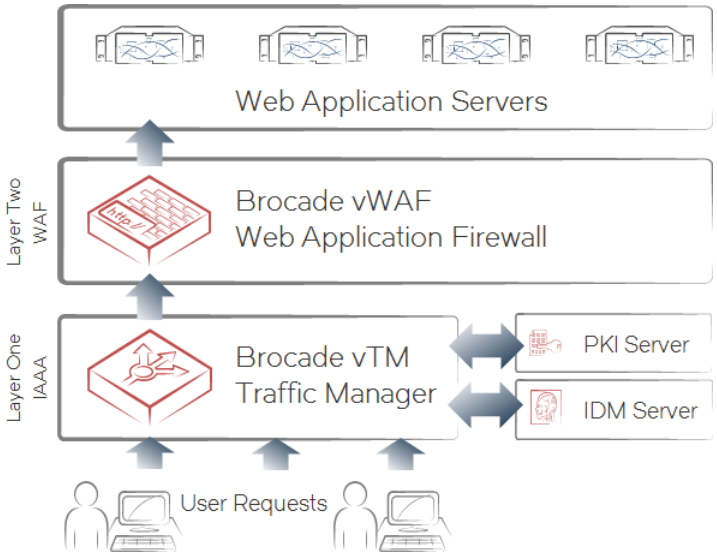

Figure 1: Layered Security with Brocade vADC.

Even with PKI, Data Is Not Always Secure

When it comes to protecting an organization's most sensitive and secure information, Public Key Infrastructure (PKI) is the default approach across the industry. Although PKI is good at providing baseline security for networks, it has been proven that it isn't enough to handle all threats.

For example, security incidents continue to grow significantly year over year, with more than 77,000 reported to the United States Computer Emergency Readiness Team (US-CERT) last year. As seen in numerous high-profile data breaches, PKI-protected networks remain vulnerable to attacks and headline-generating data breaches. That is because PKI is not designed for securing access and data at the more granular application layer. Some of the shortfalls include the following:

- Users with validated credentials-based PKI digital keys gain access to almost everything within that network, leading to unnecessary and inappropriate information access.
- PKI-protected systems are not immune to users with falsified credentials, nor to insider threats—those who have legitimate credentials and access.
- PKI protections cannot safeguard data from the most common attacks that occur at the Web application level, such as those identified on the Open Web Application Security Project (OWASP) Top 10 list that highlight the most critical Web application security flaws.

Furthermore, organizations are pushing more and more of their applications out to the edge of the Internet, making less use of VPN security layers. And more of those applications invite public feedback, collaboration, and participation. This interactive capability encourages users to contribute their own content directly into the application, opening up a new threat vector for attacks on Web applications that PKI cannot protect against.

A Layered Security Approach with Brocade vADC

Whether a cyber threat comes in the form of a Web application attack, a hacker using falsified credentials, or an insider threat, organizations need better security—particularly at the individual application layer—to adequately safeguard their most sensitive information.

To address that challenge, organizations should supplement the baseline security they get from their PKI investments with additional security layers provided by solutions such as the Brocade Virtual Traffic Manager (vTM) and Brocade Virtual Web Application Firewall (vWAF), which together comprise the Brocade vADC.

The Brocade vADC is a software-defined Layer 7 ADC with integrated Web Content Optimization (WCO) and Web Application Firewall (WAF) that is natively designed for virtualization and cloud portability. The Brocade vADC performs traditional ADC functions, such as global load balancing, bandwidth management, traffic shaping, and monitoring service levels. But unlike other ADCs, it also provides robust additional security layers at the application level that enable proactive control and mitigation of security risks, both internal and external.

Brocade Virtual Traffic Manager

One additional security layer that today's threat environment demands is attribute-based authentication, delivered by Brocade vTM. This Brocade vTM-based Identity, Authentication, Authorization, and Access (IAAA) solution does this by creating a new security checkpoint between the end user and the Web application server.

Brocade vTM conducts a deeper level of identity verification for users seeking access to specific stores of protected information and executes policies tailored to specific user attributes. It does this by introducing additional attribute checks derived from third-party sources, such as organizational databases containing a client's employment status, security permissions, and job function. For example, when a PKI-confirmed user logs in to a network and accesses a particular application, Brocade vTM can query an external database to verify that the user is allowed access to that application and its associated data sets.

As a result, access to data becomes more segmented and subject to parameters, enabling IT teams to have better visibility and a deeper level of control over who is accessing what data and how. For example, an attribute check may find that a user is not allowed access to an application or a particular set of data, or that the user is allowed access but only for certain dates and times—or only for certain subsets of data.

The Brocade vTM-based IAAA solution provides the power of in-depth access control over sensitive and classified information. And because Brocade vTM limits the scope of information that a particular individual can access, it helps ensure that no one has access to more information than they need to do their job, thus limiting the scope of any potential breach.

Brocade Virtual Web Application Firewall

Brocade vWAF provides an additional layer of robust security around the Web application itself. It scans all in-bound HTTP requests from the Internet—before they reach the Web application server—to determine whether they represent a known type of attack, such as SQL injection or Cross-Site Scripting (XSS) attacks, and, if so, blocking that traffic to prevent harm.

Brocade vWAF is a massively scalable security solution for off-the-shelf or custom applications that applies business rules to HTTP(s) traffic. It inspects encrypted and unencrypted in-bound Web traffic and blocks attacks, filters outbound traffic to mask personally identifiable information, and supports compliance with industry requirements such as PCI DSS for credit card payments. It also can be deployed across the full range of hosting environments: physical, virtual, and cloud.

Trusted Middleware

Because Brocade vADC resides between the client and the server, it can also perform secure "man-in-the-middle" functions. For example, this could include sending a suspicious user to a contained "sandbox" server to safely observe Web activity and determine whether it represents a potential insider threat. Alternatively, it could prioritize bandwidth to accommodate certain user activities over other types of traffic. It can even be used to "watermark" a PDF document to indicate the user name, time, and date that the document was downloaded.

Conclusion

Networks, applications, and data comprise some of the most valuable organizational assets. As a result, they are increasingly a potential target for malicious attacks. The threat landscape is intensifying—both in scale and complexity—and organizations must respond by continually evolving their own defense strategies and architectures.

One of the most effective approaches is to supplement PKI defenses with added security layers between end users on the Internet and their Web application servers. By focusing more checks and protections around sensitive applications and data, organizations can dramatically improve their security postures and lessen the likelihood and impact of future data breaches.

Learn More

Brocade partners with companies of all sizes to deliver innovative solutions that help organizations maximize the value of their most critical information. To learn more, visit www.brocade.com.

About Brocade

Brocade networking solutions help organizations transition smoothly to a world where applications and information reside anywhere. Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility. Learn more at www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE