Pulse Secure®

WHITE PAPER

Securing Cloud Applications with a Distributed Web Application Firewall

OVERVIEW

Responsibility over IT security is moving away from the network and IT infrastructure and to the application and software architecture itself. In addition to addressing today's advancing security threats, IT organizations also need to adapt to new challenges as a result of this shift, such as:

- Security of distributed applications
- Integration with cloud technologies
- Massive scale and dynamic growth
- Multiple applications and risk profiles
- Rapidly changing threats and L7 attacks
- Interworking with existing security process and workflows

Pulse Secure Virtual Web Application Firewall is designed to help you address all of these challenges.

Introduction

With the massive growth and scale in online business, there is continued pressure to roll out new products and services. That means frequent code updates and changes that add to the complexity of software development. Modern applications are created from building blocks such as off-the-shelf packages, in-house services and third-party components and frameworks, and every one of these has individual loopholes and vulnerabilities.

Complex applications are easier targets, especially when your developers are under pressure to meet deadlines and secure customer data. Your application and security teams can find it difficult to resolve application vulnerabilities in today's dynamic IT environment, and sometimes application vendors are unable to provide patches quick enough to meet your campaign deadlines and product release cycles.

The Never-ending Story of Application Security

Every year, thousands of new vulnerabilities are reported in web applications. With so many new vulnerabilities, it is no wonder that many enterprises find it difficult to secure, maintain, and enhance applications due to the complexities of security analysis and testing.

Applications vendors have a similar problem: not only do they need to remain alert to identify new vulnerabilities supported in their own applications, but they need to determine whether custom integration projects might also compromise security of their own or other applications. For them to identify and solve a security loophole can take significant time and resources in order to bring a patch or solution to market.

While some application vulnerabilities can be solved quickly with a patch in a third-party component or OS module, it is not unusual for logic flaws or data leaks to take months to solve in production systems. Some off-the-shelf applications can go unpatched for a year or more, depending on the priorities of the application vendors and the perceived risk.

Pulse Secure Virtual Web Application Firewall (Pulse Secure vWAF) is a scalable solution for application-level security, both for off-the-shelf solutions, and complex custom applications including third-party frameworks. It can be used to apply business rules to your online traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting (XSS), while filtering outgoing traffic to mask credit card data, and help compliance with PCI-DSS and HIPAA by filtering of outgoing data.

Cloud Applications are Exposed to a Wider Range of Threats

Security budgets have previously focused on network firewalls and antivirus solutions. However, more recently the primary target for attacks has shifted from the network layer to the application layer, because the operating systems and service interfaces available to cloud applications have been hardened to expose a reduced profile. As a result, it is now much easier to target the application logic or application framework than the actual server behind the hardened network perimeter. Although many applications are created in-house, security is rarely a core developer skill, which potentially leads to security problems throughout the application lifecycle.

Furthermore, wider adoption of cloud computing means that attack vectors are increasing as applications leverage external hosting providers for infrastructure, platform, and software. Establishing a comprehensive patch management system is important, but in practice this approach can prove very difficult and costly. Typical web applications are built on open source components by third-party developers who rely on open web frameworks. While you get interoperability and a shorter development time, it comes at the expense of complex patch management to solve security vulnerabilities. A flaw in one component of open source code must be patched for each instance it is used throughout each application in which it is used. In a public cloud environment, with dynamic infrastructure and application frameworks, this can become very difficult to manage.

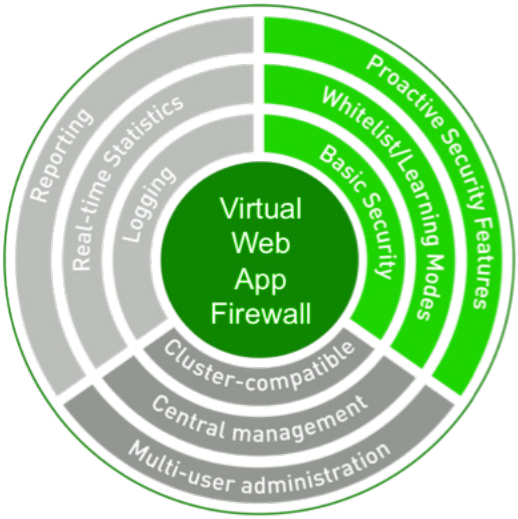


Figure 1: Defense in Depth: Pulse Secure Virtual Web Application Firewall provides multiple layers of protection

Complexity in the Cloud

Large-scale applications developed specifically for a cloud are often very complex, with a design focus on access speed and scalability. Many cloud applications also provide flexibility for third-party development through an open API. For example, Salesforce.com, Google Docs, Facebook, and Twitter, are all good examples of APIs exposed to allow access from custom applications. These 'as a Service' applications are developed in two ways today: (1) by moving on-premise applications to the cloud, and (2) by developing and operating applications directly in the cloud.

Applications that migrate out of your internal company network and into a public cloud infrastructure carry the risks of exposing protected software to external threats that they were not designed to handle. Common security threats include injection attacks, and cross-site scripting or cross-site request forgery.

There are many security challenges involved in developing web applications in a cloud, such as parameter validation, session management and access control, which are key "hotspots" for attackers. If your developers have limited experience designing for application security, they are more likely to create applications that have security problems.

OWASP Top 10—Managing Risks in Web Applications

OWASP, the Open Web Application Security Project, is the leading open source community group in web application security, and regularly publishes an annual "Top Ten" report showing the most common security challenges to online applications, ranging from business policy to application vulnerabilities.

For example, in their most recent "Top Ten" report, published in July 2013, OWASP noted that injection flaws had risen as the highest risk. Because of the risk of high-value data leakage, this kind of vulnerability can give rapid unauthorized access to customer and enterprise information.

This security challenge underscores the need for a solution that is able to validate inputs against business policies and screen outgoing data for suspected data leakage in a way that is independent of the underlying application architecture.

And it doesn't help that each year would-be attackers use new tools and techniques to identify new gaps and loopholes that could be exploited. Therefore, a solution needs to be agile enough to adapt to changing risk priorities and robust enough to handle large-scale attacks on high-throughput web applications processing millions of customers and transactions.

Why a Traditional Web Application Firewall is not Enough

Web application firewalls (WAF) and other security solutions are typically limited to hardware appliances, which can create a serious bottleneck in your cloud infrastructure because dedicated hardware boxes do not allow for multiple levels of delegated administration within a single security policy mechanism. As a result, in addition to traditional network hardware, you may need to have a rack full of dedicated WAF appliances—one per client application—that takes up unnecessary space and resources. In turn, security becomes a barrier to efficiency in your virtualized environment, and this cost is passed on to your customers, making it harder to move more applications to the cloud.

In the cloud, the infrastructure and services are shared between your customers, meaning many of your client applications and business units may be sharing one set of hardware appliances. Each of your applications needs a unique layer of policy settings, use-cases and administrative enforcement requirements, so maintaining security quickly becomes very complex. For example, a major enterprise or cloud provider may have thousands of client applications, each with variable policy settings. In such cases you'd need to manage application policy and filter settings for each of them.

In an ideal world, your applications would be designed from the ground up to meet challenges of virtual and cloud architectures, integrating security

Caption: OWASP.org "Top Ten" Report 2013 shows how attack vectors change over time

Figure 2: OWASP.org "Top Ten" Report 2013 shows how attack vectors change over time.

measures directly within, hence solving a core problem with current cloud application architectures. Until then, you need an alternative to traditional web application firewall appliances in order to reach the full potential and economic model of public cloud computing.

Cloud Security with a Distributed Web Application Firewall

Web application security in a cloud needs to be scalable, flexible, virtual and easy to manage. Below are the key capabilities that you should look for in a solution.

Massive Scalability

A distributed WAF must be able to scale dynamically across CPU, computer, server rack and data center boundaries, and customizable to meet the demands of your individual applications without being limited to discrete hardware form factors. Resource consumption must be minimal and scale in line with the throughput of detection and enforcement. Clouds come in all sizes and shapes, and your application security platform needs to be flexible with changing demands.

Cross Platform Portability

As you evolve and transform your data center, you will use a variety of traditional and virtual technologies, so your security strategy must accommodate a mixed environment. Consider a virtual software appliance, a plug-in, SaaS or a solution that can integrate with existing systems with minimal disruption to the existing network.

Distributed and Delegated Management

A web-based user interface must give you and your customers delegated access to manage security policies. Configuration should be tailored to each of the applications under protection, giving you more granular settings for each application, and not defined by a single, central host. Ruleset configuration must be simple and supported by setup wizards. Statistics, logging, and reporting should be intuitive and should also integrate seamlessly into other systems. Multi-administrator privileges must be made available and flexible enough to manage effectively a wide variety of policy enforcement schemes. You should look for a set of core protection with the ability to delegate policy for individual clients and applications.

Detection and Protection

You need a strong foundation for security, using black, white, and grey listings for application requests and responses. It is also important to be able to test and refine new rulesets in a detection-only mode to ensure new policies are not activated without approval from your security administrator. Only when a detection-only ruleset is stable should it be possible to commit it to selected applications in your cloud or data center. This allows complete transparency for your security administrators to predict outcomes of policy changes, even while allowing new layered rulesets to be tested without compromising existing policy enforcement. It is essential to avoid false positives or weakened defenses, particularly in large-scale cloud applications.

Automated learning and ruleset recommendations can make it easier for your security team to manage policies, while retaining full control over the activation and deactivation of each ruleset. Without this level of control, legitimate traffic may become blocked and policy settings could become compromised.

Application Shielding

Proactive security functions are essential to reinforce your applications in a dynamic cloud infrastructure. Detection is simply not enough for today's web application security: features like transparent secure session management, URL encryption, and form-field virtualization will provide strong deterrence to attack while saving application development and deployment time. These features are effective because session management, URL encryption, and form-field virtualization are done at the web application firewall, and not in the application itself.

An authentication framework that helps you consolidate your applications under one management schema is also desirable. This lets you handle the authentication in front of your applications, adding another security layer. By consolidating all of your applications with a dedicated rights-management capability you can make it easier to administer policies.

Integration with Existing Technology

Avoid vendor-lock-in for both networking and application security. Any solution that extends your infrastructure or applications must connect seamlessly with your existing technology and business processes. Security technologies must be layered to create the best possible protection, so a distributed web application firewall must communicate freely with your security incident and event management systems (SIEMs).

Pulse Secure Virtual Web Application Firewall

Pulse Secure Virtual Web Application Firewall (Pulse Secure vWAF) is a pure software web application firewall designed to support these best practices. Due to its modular construction, you can deploy it very easily in a cloud-computing environment, making it a scalable solution for application-level security. It can apply business rules to online traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting, while filtering outgoing traffic to mask credit card data. The software consists of three scalable components:

1. Enforcer
2. Decider
3. Administration Interface

These can be configured either as a pre-packaged WAF solution, such as an add-on module for Pulse Secure Virtual Traffic Manager to manage a cluster of applications, or as a fully distributed solution across hundreds of web servers and multiple data centers for maximum scalability and performance. The same distributed management interface can be used to protect both types of deployment, or even in a shared services environment.

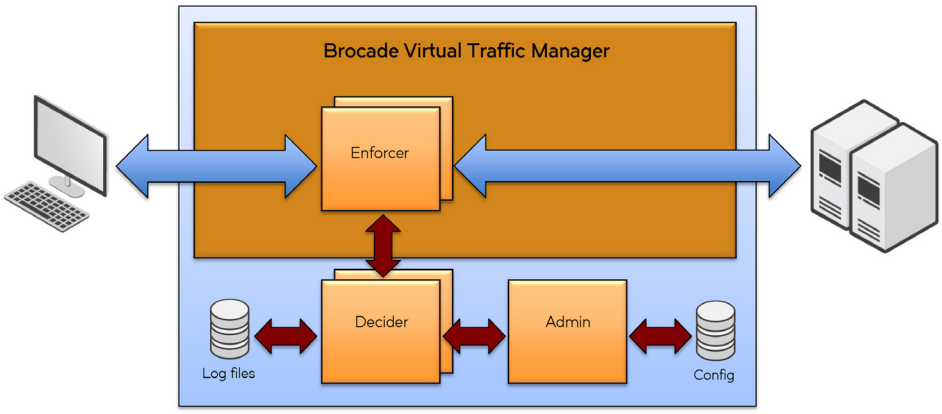


Figure 3: Pulse Secure vWAF as an add-on to Pulse Secure Virtual Traffic Manager.

Enforcer

The Enforcer is a small component or plug-in, which can be installed into any kind of device. A device can be a web server or proxy (such as Apache or Microsoft IIS), or integrated into a network firewall or a software load balancer or application delivery controller (ADC) such as Pulse Secure Virtual Traffic Manager. The Enforcer sends request and response data to a component called the Decider, and modifies requests and responses as needed. The Enforcer is an adapter for the web application firewall to analyze the data to enforce the policy.

Decider

The policy engine checks the data from the Enforcer module and decides how to manage each request/response. The unique architecture allows scaling from one to many CPU cores, and is also capable of scaling horizontally. The decider is the compute-intensive part of the solution, and the workload on the Decider depends on the load of the web infrastructure behind it. As your users and applications generate more traffic, the Decider demands greater CPU resources.

Administration Interface

You can choose to deploy the administration system either as a single server, or fully decentralized. In a cluster installation, every cluster node can be used to administrate applications and their policies. This decentralized architecture is resilient against node failures, and allows groups of security administrators to work on individual application policies, while providing detailed central monitoring and alerting functions.

Integrated ADC Implementation

In integrated ADC deployments, Pulse Secure vWAF is licensed as an add-on for Pulse Secure Virtual Web Traffic Manager, and can be deployed either on a server appliance, or on a VM in virtual or cloud infrastructure. Enforcers and Deciders are co-resident inside the Traffic Manager package, administered as a single platform. The Admin GU is accessed via the standard Traffic Manager console.

PaaS and SaaS Implementation

Software as a service (SaaS) offers user access to virtualized applications through a thin client, usually any standard web browser. The benefit for users is access to software without any of the headaches of owning the programs—scaling and resources, and patching and upgrades are all taken care of. SaaS applications are usually billed on a per-user/per-use basis.

Platform as a service (PaaS) provides customers with virtual databases, storage, and programming models to build custom applications. This service provides scalable resources behind the platform and allows customers to grow throughout the lifetime of the application. It is an effective solution for companies of all sizes, and is often billed on a usage model.

In a shared cloud (PaaS and SaaS) environment, many Enforcer plug-ins from load balancers and web servers could communicate with a Decider service deployed across separate VMs. If the first VM of this Decider service reaches 80% of the available CPU resources, a new VM on a different instance of a cloud will automatically be provisioned, started, and added to the Decider cluster. If the cluster-wide CPU usage of the Decider service drops below 40%, the Decider instances will automatically be removed from the cluster to release resources back to the cloud.

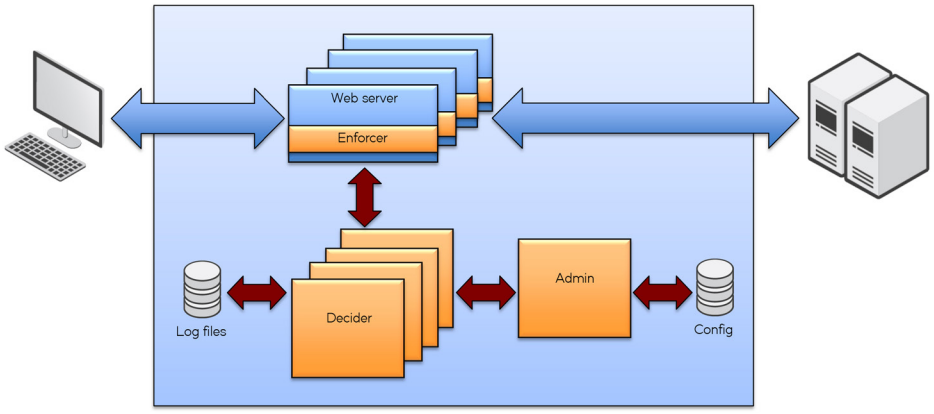
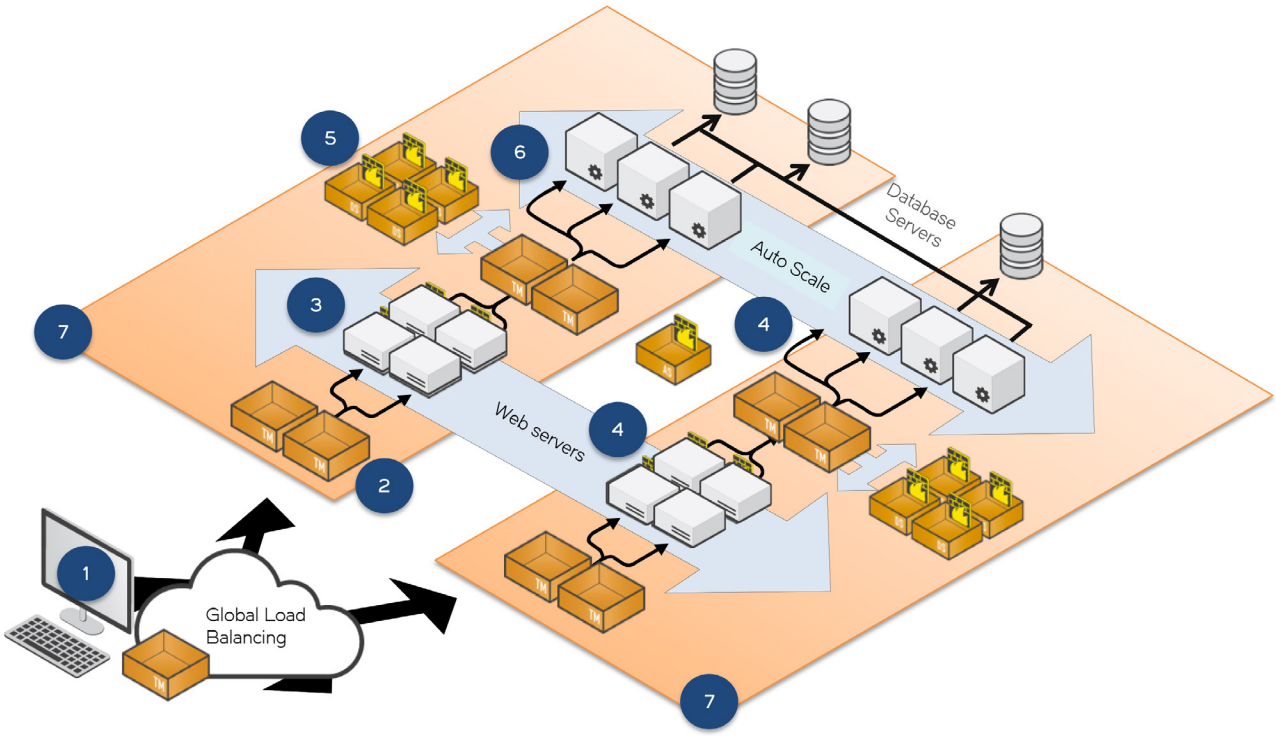


Figure 4: Pulse Secure vWAF in a distributed deployment for a single application.

IaaS Implementation

Infrastructure as a service (IaaS) allows access to large-scale resources to build and manage a complete virtual network. Customers can commission and decommission virtual resources depending on their needs as application workloads change over time. Customers select from a range of infrastructure components and service level agreements to define their application requirements, matching their infrastructure usage costs to their service requirements.

Pulse Secure Virtual Web Application Firewall can be deployed similarly on an IaaS cloud. Each customer can have a private instance of all three modules, which are not shared between customers. As before, many instances can be clustered together to scale up to meet larger traffic demands.
Cloud providers can also provide automatic scaling within the cloud infrastructure to follow the lifecycle of individual applications.



Very Large Scale Applications

For the very largest applications deployed in public clouds, a distributed application firewall needs to scale dynamically to the very highest traffic levels, and adapt to meet the changing transaction demands of public-facing applications. For example, Virtual Web Application Firewall can be deployed in a distributed cloud architecture such as that hosted in Amazon Web Services or Microsoft Azure global data centers:

The components of a highly scalable web application firewall

1. **Global Load Balancing:** In this example, Traffic Manager software serves incoming DNS requests using Global Load Balancing, and routes network traffic to the closest cloud data center.
2. **HTTP Distribution:** Traffic Manager handles incoming HTTP requests, which are distributed across multiple web servers in different availability zones. In addition to fine-grained health checks in the application layer, Pulse Secure software can provide SSL Offload, Compression, Caching, and Layer 7 based request routing.
3. **Application Firewall—Enforcer:** In this example, the Pulse Secure vWAF Enforcers are installed as a plug-in on the web servers. The Enforcer traps HTTP requests and response data and sends it to the cluster of Pulse Secure vWAF Deciders for security processing.
4. **Auto-scaling of Web Servers:** Traffic Manager manages the automatic spin up and spin down of web servers as required to service your application effectively using Traffic Manager's Auto-scaling capability.
5. **Application Firewall—Decider:** A scalable group of Pulse Secure vWAF Deciders processes the HTTP requests and responses to ensure compliance with security policy. Pulse Secure vWAF provides a hybrid security policy model combining traffic signatures and positive security postures to prevent HTTP based security attacks.
6. **Load-Balancing and Health-Checks:** Traffic Manager provides granular application health checking and layer 7 load balancing into the application tier.
7. **Cross-Zone Availability:** Traffic Manager works seamlessly across multiple Availability Zones, multiple regions or across multiple clouds, for the ultimate in cloud high availability.

Discover Pulse Secure vADC with a Free Trial

It's easy to test all of the capabilities available in the Pulse Secure vADC product family. Download the Pulse Secure Virtual Traffic Manager Developer Edition today to find out how to realize greater ROI from data center consolidation and transformation programs.

The Pulse Secure vADC Developer Edition, available either as pure software, or as a virtual appliance, makes the complete ADC technology platform available to every application developer in your organization, enabling them to develop applications faster, test them in a production-identical environment, and bring them to market more quickly.

Find out More

To find out more about Pulse Secure Virtual Web Application Firewall, or to arrange a demonstration or product evaluation, please visit www.pulsesecure.net/vadc/vwaf.

Corporate and Sales Headquarters
Pulse Secure LLC
2700 Zanker Rd. Suite 200
San Jose, CA 95134
www.pulsesecure.net

Pulse Secure®