DATA SHEET

Pulse Secure Virtual Web Application Firewall

HIGHLIGHTS

- **Maximizes deployment flexibility** with a software-based Web Application Firewall (WAF), ideal for Network Functions Virtualization (NFV)
- **Provides massive scalability** so organizations can secure the largest online applications, clustering both within data centers and across global cloud platforms
- **Helps meet compliance requirements** such as PCI DSS

The Ongoing Story of Application Security

Every year, thousands of new vulnerabilities are reported in Web applications. With so many new vulnerabilities, many enterprises find it difficult to secure, maintain, and enhance applications due to the complexities of security analysis and testing.

The 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 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 achieve compliance with PCI-DSS requirements by filtering outgoing data.

Defense in Depth

Enterprise security has traditionally been focused on network firewalls and content filtering 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 of modern IT infrastructure have been hardened to expose a reduced risk profile. As a result, it is now much easier to target the application logic or application framework than the actual server or network behind the hardened network perimeter. Although many applications are created in-house, security is not always fully developed, which potentially leads to security problems throughout the application lifecycle.

KEY FEATURES

- Massive scale for global applications
- Delegated security model for security professionals
- Wide range of proactive security measures
- Protection against key vulnerabilities such as SQL injection and Cross-Site Scripting
- Integration with external security scanners and and workflow tools such as Denim Group's Threadfix
- Dual-mode "detect and protect" operation
- Security automation using REST API
- Available as an NFV-ready virtual appliance

RELIABLE SUPPORT OPTIONS

- Pulse Secure Essential Support
- Provides 24×7 access to Pulse Secure Technical Support expertise, reducing time to resolution
- Provides unmatched expertise in data center networking to optimize network performance
- Simplifies management through online technical support tools

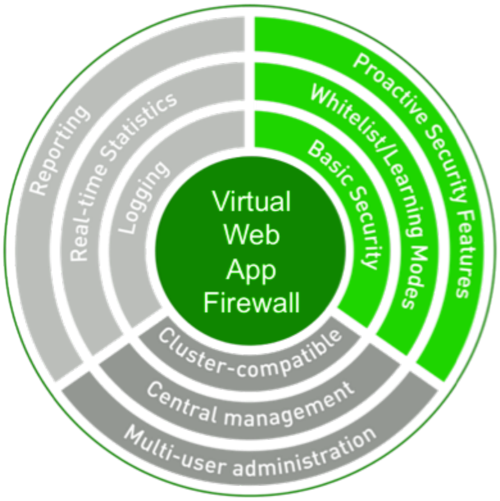

Figure 1. Pulse Secure Virtual Web Application Firewall provides multiple layers of protection.

As a result, network and servers may be secure, but not applications. They must be protected with proactive Layer 7 security. Pulse Secure vWAF brings defense in depth to applications with real-time policy enforcement, including transparent secure session management and form-field virtualisation, in a scalable Web Application Firewall (WAF) solution.

Application Security for the New IP

As enterprise networks evolve, their business requires more flexible and open architectures to support the demand for richer services and customer-focused applications, and to meet the challenges of cloud, mobile, social, and big data. The New IP is based on open standards, with automated provisioning and customer-self service management, to reduce costs and improve the speed of innovation.

Dynamic network and applications need a new approach to manage the security of applications that are developed and launched for the New IP. Rapid application development methodologies mean that a strong security layer essential for any complex Web application that handles sensitive data. No matter how carefully developed and audited application code may be, it is not possible to verify that no vulnerabilities exist in the application and the underlying developer frameworks. The Pulse Secure vWAF provides an additional barrier of protection, and can be compatible with existing security processes and network architectures.

Figure 2. Pulse Secure and the New IP.

Massive Scalability

Organizations must scale dynamically to meet the needs of the largest global applications. Pulse Secure vWAF can extend seamlessly across CPU, computer, server rack, and data center boundaries. Organizations can use a combination of public and private cloud technologies, and be assured of a common application security platform and centralized policies, even when clustering between data centers or across different cloud providers.

Cross Platform Portability

As IT architectures deploy more applications, they must also ensure that they are secure. The Pulse Secure vWAF can extend security policies to all corners of the data center, and as the network transforms to enable the New IP. It can deploy common security policies across a mixture of cloud, software, virtual appliance, Web server plug-in, or even as a bare-metal server, integrating with existing systems with minimal disruption to the existing network.

Rapid Response

Pulse Secure vWAF can close application vulnerabilities faster, by importing ruleset recommendations from third-party vulnerability scanners and workflow tools such as Denim Group's ThreadFix. Automated learning is available help security teams to manage policies. With full control over the activation of individual policies, organizations can maximize application security, while reducing the number of false positives.

Dual-Mode Detection and Protection

Organizations can refine security policies with the dual-mode "detect and protect" operation. Pulse Secure vWAF allows layered rulesets, maintaining a live ruleset to enforce policies which have been approved for production, and simultaneously operating a detection-only ruleset which can include watch lists and trial policies. This enables new rulesets to be tested in a detection-only mode, ensuring that new policies are not activated without approval from security administrators. With this feature, new layered rulesets can be tested without compromising existing policy enforcement, which helps to avoid false positives or weakened defenses, particularly in large-scale cloud applications.

Automated Learning

The Pulse Secure vWAF's security is adaptive through automated learning and can make policy recommendations by learning about application behavior, which can make it easier for security teams to manage policies. Administrators retain full control over the activation and deactivation of each ruleset, with the opportunity to screen for false positive before committing to production.

Integration with Existing Technology

Organizations can avoid vendor-lock-in for both networking and application security. The Pulse Secure vWAF connects with organizations' existing technology and business processes, and can integrate with Security Incident and Event Management systems (SIEMs).

Distributed and Delegated Management

The Pulse Secure vWAF includes a Web-based user interface to give security professionals full distributed access to centralized policy management and reporting. Organizations can now manage policies centrally and also delegate access to business partners to manage the security configurations of specific applications or domains, tailoring access rights granular settings for individual client applications.

Comprehensive Reporting and Logging

Pulse Secure vWAF includes a range of reporting options for threat analysis and data retention. This not only helps security professionals to see potential attacks developing, but also where policies are too restrictive. In addition, data retention can help with local compliance requirements for record-keeping, and also for auditing policy changes.

PCI DSS Compliance

Pulse Secure vWAF helps compliance with PCI DSS, which is a key standard with for organizations which manage credit card payments. Failure to meet the requirements of PCI DSS exposes a merchant to higher risk of fraud, potential liability for costs resulting from leakage of cardholder data, and incurs higher processing fees from credit providers. The PCI DSS standard defines a pragmatic set of security procedure: Section 6.6 of the standard mandates that a merchant must either perform regular security reviews of the source of all public-facing applications or deploy and configure an appropriate Web application firewall.

Pulse Secure vWAF not only helps meet the requirements of PCI DSS 6.6, but it also helps to observe other parts of the PCI DSS standard. Pulse Secure vWAF can easily be configured with additional security policies to detect and prevent attacks specific to all applications.

How the Pulse Secure Virtual Web Application Firewall Works

The Pulse Secure vWAF is a pure software Web application firewall designed to support best practices for application security. Due to its modular construction, organizations can deploy applications very easily in a cloud-computing environment, making it a scalable solution for application-level security. Pulse Secure vWAF 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.

Request Analysis

When activated, the Pulse Secure vWAF receives and analyzes each request against the ruleset assigned to the application, and determines which of the following actions to take:

- Permitted requests are passed to the application
- Requests which are identified as known attacks are rejected, and logged with information to help trace the attacker
- Requests which cannot immediately be categorized can be rejected locally or passed on to the application, and depending on the security policy in force, they are logged and used to help classify future requests of this type

Response Analysis

The Pulse Secure vWAF also monitors outgoing responses as they are returned to the client. Security-sensitive information can be filtered out from responses to ensure that data leakage is captured, even if the initial malformed request is successful. As a result, customer information such as credit card data, social security numbers, or healthcare-related content can be screened out by using comprehensive security policies.

The Pulse Secure vWAF can monitor the behavior of the application and traffic patterns to help optimize protection and recommend additional policies.

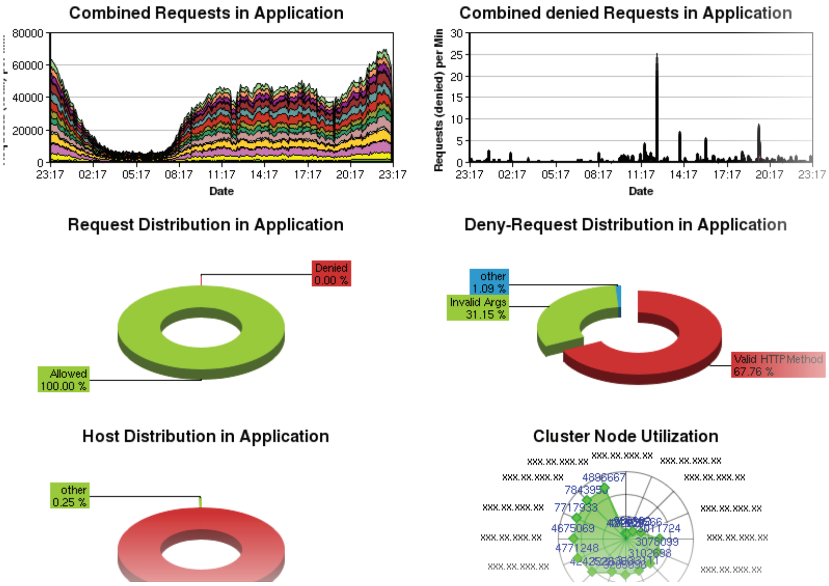

Figure 3. Pulse Secure vWAF provides comprehensive reporting and logging.

Unique Scalable Architecture

The software consists of three scalable components:

- The Enforcer
- The Decider
- The Administration Interface

These can be configured either as a pre-packaged WAF solution with the Pulse Secure Virtual Traffic Manager (Pulse Secure vTM) 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.

Enforcer

The Enforcer is an adapter for the Web application firewall to analyze the data to enforce the policy. The Enforcer sends request and response data to a component called the Decider, and modifies requests and responses as needed.

Decider

The policy engine checks the data from the Enforcer module and decides how to manage each request/response. The unique architecture allows scaling across multiple 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 users and applications generate more traffic, the Decider will utilize greater CPU resources.

Administration Interface

Organizations can choose to deploy the administration system either as a single server, or fully decentralized. 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

The Pulse Secure vWAF is included in the Enterprise Edition of the Pulse Secure vTM as an integrated solution 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 Pulse Secure vTM package and are administered as a single platform. The Admin GU is accessed through the standard Pulse Secure vTM console.

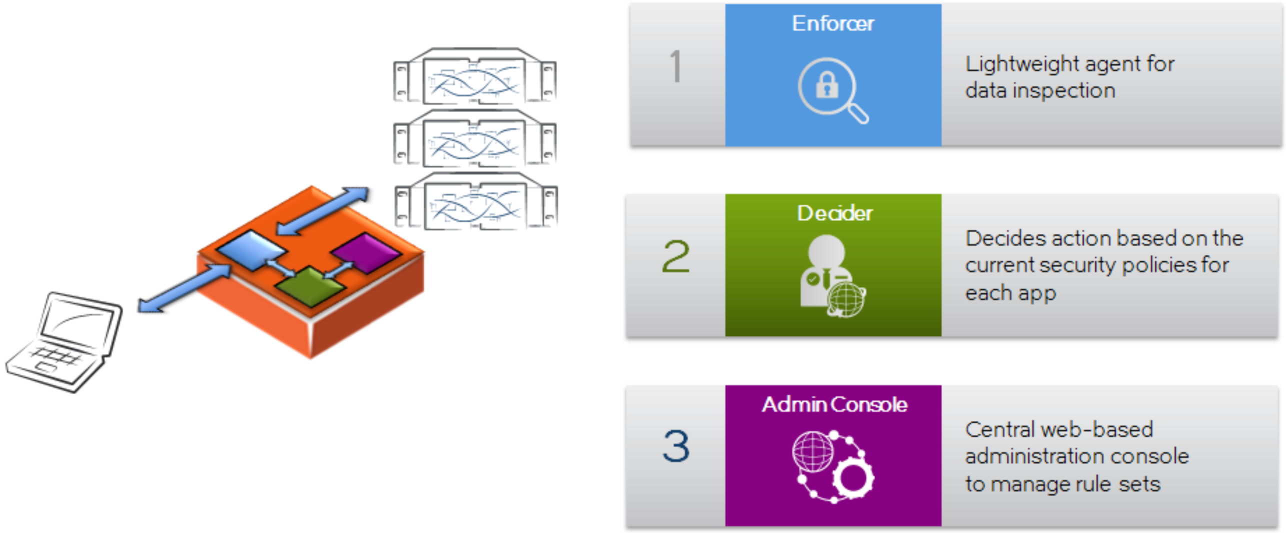
1
Enforcer
Lightweight agent for data inspection
2
Decider
Decides action based on the current security policies for each app
3
Admin Console
Central web-based administration console to manage rule sets

Figure 4. The Pulse Secure vWAF is included in the Enterprise Edition of the Pulse Secure vTM and Pulse Secure Services Director.

Feature Summary

Baseline Protection

The Pulse Secure vWAF includes a Baseline Protection Wizard, which makes it easy to update policies. The baseline policies are a blacklist and regex-pattern match of known vulnerabilities and attacks: when Pulse Secure vWAF detects a suspicious pattern which matches the baseline policies, then the request is rejected without exposing the application.

Pulse Secure publishes regular baseline updates, and the Pulse Secure vWAF dashboard highlights the recommended updates. Note that the new baseline policies are NOT applied automatically - the new rules should be reviewed by the security team and activated through the management console.

Injection Flaws

Injection is a common way for attackers to compromise an application, which attempts to force an application to execute malicious code in a database or script, when the application was only expecting to find user data such as login credentials or an online form. For example, SQL Injection can be used to attack databases, but other forms include LDAP injection or Shell injection, which can be equally damaging.

The Pulse Secure vWAF Baseline Protection Wizard automatically configures standard rules to perform additional validation of user input, in order to detect and drop traffic that contains suspected injection flaw payloads. Alternatively, custom rules can be set to look for application-specific patterns.

Secure Session Management

While many applications use secure passwords and authentication, it is possible for user and session data to be exposed through weak links such as session cookies and tokens. Attackers can use these weak links to create or midify sessions and access live data.

The Pulse Secure vWAF Secure Session Wizard can help to secure vulnerable sessions, using two important tools: the Session Handler can impose additional controls on user session timeouts and session limits, while the Cookie Jar Handler can be used to preserve vulnerable information by exchanging weak session cookies for a more secure session management. With Pulse Secure vWAF, organizations can add an additional authentication layer in front of their applications.

Secure Entry Points

Similarly, many applications enforce authentication when a session is opened, but do not perform access control verification at each step or intermediate function. Attackers can manipulate workflow flaws to access data or bypass session authentication.

The Pulse Secure vWAF offers an Entry Point Handler that can provide additional security by ensuring that new user sessions always start at a pre-determined entry point. This prevents attackers from deep linking into applications, bypassing entry points and authentication steps.

Cross Site Scripting (XSS)

Applications which accept user-generated input, including simple online forms or social media sites, need to ensure that the content has been validated and is safe to be re-posted and viewed by a client Web browser. A Cross-Site Scripting attack (XSS) attempts to insert scripts into the user data, which are executed by the client Web browser when the content is viewed by another user—which can result in hijacked user sessions, defaced Web sites, or uploaded malware.

The Pulse Secure vWAF Baseline Protection Wizard includes policies that validate all user input and exclude traffic that contains suspected XSS payloads. Alternatively, custom rules can be set to trigger on specific XSS patterns.

Cross Site Request Forgery (CSRF)

When a CSRF attack sends a request to the target Web application, and relies on the user being already being logged into the target application—for example, when a user remains logged in to an application using a cookie or other session token, to avoid having to re-authenticate each time. The CSRF attack hijacks the client browser to send a request to the target application, which is pre-authenticated by the existing session token. Because the target application recognises the request as authenticated, the CSRF attack can send commands or queries to any form in the target application, potentially leaking or corrupting data.

Pulse Secure vWAF provides additional protection against CSRF attacks using the Form Protection Handler, which authenticate online forms with a session-based key to ensure that they are only accessed directly, and not through a cross-site linkage.

Masking Sensitive Data

Attackers may attempt a variety of exploits to extract sensitive data, including payment card information, social security information, and security credentials. This kind of sensitive data requires additional layers of protection beyond the encryption of stored data: for example, data in transit should be encrypted using secure transport, and active response filtering can mask out sensitive data which leaks through other defenses.

Redirection and Forwarding Attacks

Many Web applications use redirections and forwarding to transfer control within online services, and may be vulnerable when they use untrusted data or URL parameters to select the target Web page. Attackers may use weak validation of redirection criteria to trigger malware or phishing attacks by forwarding to unauthorised targets.

The Pulse Secure vWAF Baseline Protection Wizard includes policies that check for fully-qualified URL references to protect against unwanted redirection. Security professionals can also define preferred redirection targets for when an invalid redirection target is detected.

Resolving Third-Party Vulnerabilities

Modern online applications often include third-party libraries and tools, which may vulnerable to zero-day attacks. Third-party software providers may be unable to resolve flaws quickly, so attackers may be able to exploit these vulnerabilities before they are corrected.

Known vulnerabilities within application components can be mitigated with the Pulse Secure vWAF. Standard application attacks like SQL Injection or XSS can be mitigated using using the Baseline Protection or the Whitelist Learning Capability. Similarly, the pro-active features of the Pulse Secure vWAF can be used to identify and protect against vulnerabilities in the application logic of applications.

Flexible Deployment Options

The Pulse Secure vWAF supports a full range of deployment options, enabling organizations to choose the best fit for their architecture and application risk profile. The Pulse Secure vWAF can be deployed as a plug-in on the Web server, installed as software on bare-metal servers, or as a virtual appliance in a customer data center or cloud provider—or even installed as an integrated package with the Pulse Secure vTM for enhanced security and control of complex applications.

In addition, the Pulse Secure vWAF is also available as a stand-alone proxy, designed to be used with existing load-balancers and ADCs, and is particularly suitable for cloud deployment to add application-level security to a cloud application without changing the application architecture.

Summary of Deployment Options

Pulse Secure vWAF for the Pulse Secure Virtual Traffic Manager	The Pulse Secure vWAF is included in the Enterprise Edition of the Pulse Secure vTM and the Pulse Secure Services Director, and allows the traffic manager to enforce application-level security to HTTP traffic as part of an integrated ADC solution.
Pulse Secure vWAF Proxy	This WAF proxy solution is available as either a software or virtual appliance, and is typically deployed alongside an existing ADC or load balancer device. The existing ADC routes traffic through the proxy so that the Web Application Firewall can apply deep application-level security.
Pulse Secure vWAF Bare-Metal Appliance Image	For networks that need to deploy a WAF as a hardware appliance, Pulse Secure vWAF can be installed on standard Intel x86 servers, and managed as a stand-alone device.
Pulse Secure vWAF Web-Server Plug-in	For maximum scalability in custom applications, Pulse Secure vWAF can be implemented as Web-server plug-ins to provide a fully distributed application security with optimum flexibility.

Pulse Secure Virtual Web Application Firewall System Requirements —Standard Deployment

Pulse Secure Virtual Web Application Firewall Software and Virtual Appliances (when deployed with the Pulse Secure Virtual Traffic Manager or as a proxy)

Supported OS: Traffic Manager	Linux x86_64: Kernel 2.6.8 – 3.13 (2.6.22+ for IPv6), glibc 2.5+; Solaris 10 (x86_64)
Virtual Environment: Virtual Appliance	VMware vSphere 5.0, 5.1, 5.5, 6.0; XenServer 6.1, 6.2, 6.5; Oracle VM for x86 3.2, 3.3; Microsoft Hyper-V Server 2012 & 2012 R2; Microsoft Hyper-V under Windows Server 2012 and 2012 R2; QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 12.04, 14.04)
Recommended CPU	Intel Xeon/AMD Opteron
Recommended Minimum Memory	2 GB
Recommended Minimum Disk Space	10 GB (Software), 16 GB (Virtual Appliance)

Pulse Secure Virtual Web Application Firewall System Requirements —Distributed Deployment

Pulse Secure Virtual Web Application Firewall Software's three independently scalable components (when deployed as a distributed service)

Decider modules	Decider modules apply security policy to traffic bidirectionally. They are deployed on a cluster of one or more multicore servers. Linux 2.6+ (x86_32 and x86_64), Solaris 10 (x86_64), Microsoft Windows 2012 Server R2 1 GB RAM per core
Enforcer plug-ins	Enforcer plug-ins are deployed on origin Web servers or proxies. They forward selected traffic to the Decider cluster and enforce the decision returned. Apache 2.0, 2.2 or 2.4 on Linux 2.6+ (x86_32 and x86_46), Solaris 10 (x86_64); J2EE servers running Java 1.2 and later and Servlet API 2.3 and later (e.g. Apache Tomcat); Nginx (1.9.7+ LUA module required); IIS 8; CPU utilization of Web server should not exceed 60% before deployment of Enforcer plug-in
Administration Server	The Administration Server manages and deploys security policies to the Decider cluster and reports on security status. Linux 2.6+ (x86_32 and x86_46), Solaris 10 (x86_64), or Microsoft Windows 2012 Server R2 2 GB RAM for Admin Server

Maximizing Investments

To help optimize technology investments, Pulse Secure and its partners offer complete solutions that include professional services, technical support, and education. For more information, contact a Pulse Secure sales partner or visit www.pulsesecure.net.

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