DATA SHEET

Pulse Secure Virtual Traffic Manager

HIGHLIGHTS

- Provides an Application Delivery and Load Balancing solution purpose-built for high-performance Network Functions Virtualization (NFV)
- Uniquely customizable, with comprehensive RESTful APIs for service management, and TrafficScript, a powerful data plane scripting technology
- Unmatched scale and performance, able to scale-up with the latest generation of multi-core CPUs, and scale out with N+M clustering for reliability and throughput
- High-performance Layer 4 load balancing, supporting up to 140 Gbps in a virtual instance and more than one million Layer 4 connection requests per second

Take Control of Your Applications

As application environments become more complex, more distributed, and more virtualized, enterprises need a broader set of tools to solve performance problems for their web-based services.

Pulse Secure Virtual Traffic Manager is a software-based application delivery controller (ADC) designed to deliver faster, high performance user experience, with more reliable access to public websites and enterprise applications, whether they run in a public cloud, private cloud or virtualized environment, while maximizing the efficiency and capacity of web and application servers.

Deliver Fast, Secure, and Available Applications

Web traffic is rarely constant: it has peaks and valleys that can make it difficult to plan for future business growth. The Pulse Secure Virtual Traffic Manager is a unique, high-performance software solution that's mobile, flexible, and scalable. It allows cost-effective scale capacity and move between hardware and deployment platforms as required, and it reduces the strain placed on application infrastructure with network-level buffering, protocol optimizations, and application-specific measures such as dynamic compression and caching. The result is reduced latency, increased capacity, improved availability, and optimized service levels for each end user.

Accelerate, Optimize, and Secure Your Applications

- Accelerate and enhance applications, leading to improved customer satisfaction and higher productivity,
- Reduce costs with flexible capacity management, and scale applications up or down to meet changing traffic demands.
- Take advantage of cost benefits of using cloud technologies, while retaining the performance and security.
- Protect applications against external threats and network attacks, and resolve application problems and vulnerabilities.
- Roll out new applications and services up to 10x faster than traditional ADC solutions.

KEY FEATURES

- *Intelligent load-balancing*
- *Application acceleration*
- *Dynamic content caching*
- *SSL and compression offload*
- *Service-level monitoring*
- *Global load-balancing*
- *Bandwidth management*
- *Cloud bursting and balancing*
- *Service automation using REST API*
- *NFV Appliance for Application Delivery*
- *Data Plane Acceleration mode for high-performance Layer 4 services*

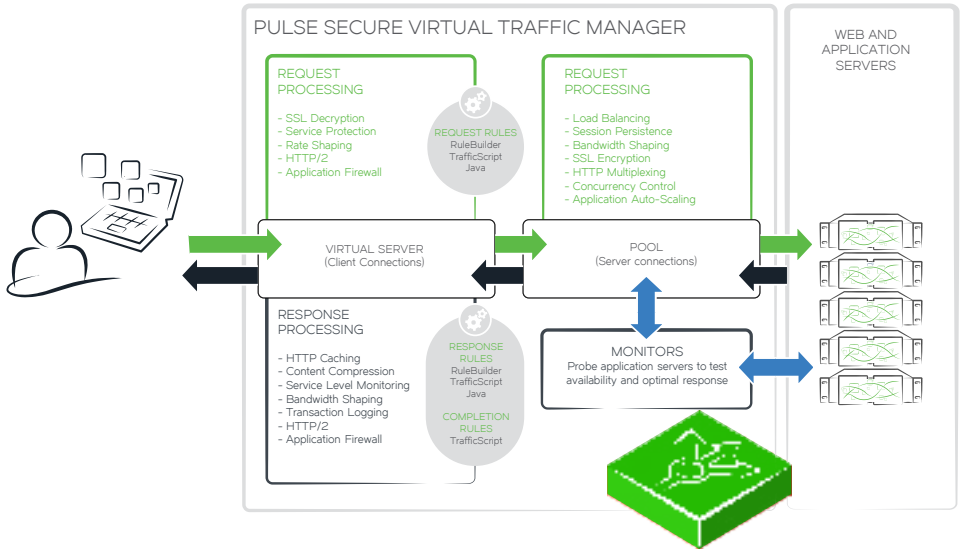

Figure 1. The advanced capabilities in the Pulse Secure Virtual Traffic Manager can be enhanced using TrafficScript or Java extensions.

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*

How Pulse Secure Virtual Traffic Manager Works

The Pulse Secure Virtual Traffic Manager inspects and processes application traffic with full payload inspection and streaming. As requests are received, a range of optimization techniques ensures that requests are presented in the most appropriate manner to the web and application servers. Responses from the application can be compressed, cached, and returned to the client at optimum speed, while freeing up resources on the server. Built-in TrafficScript software controls how individual requests are optimized, routed, and transformed. Traffic management rules may also be created using Java extensions.

The Pulse Secure Virtual Traffic Manager includes a web-based administration interface that provides powerful real-time and analysis and history for traffic across Pulse Secure Virtual Traffic Manager clusters. Alternatively, REST, SOAP and SNMP interfaces can be used to integrate the solution into remote management and event monitoring frameworks for automation of ADC deployment, configuration and integration with customer self-service portals.

Bring New Services to Market More Quickly

ADCs are an important part of the modern application platform. They provide key functionality such as security, centralized authentication, rate shaping and queuing, and content modification to support applications. They also support operations such as the gradual introduction of new servers, session upgrades between application generations, and A/B testing. Their monitoring and debugging capabilities also help deliver reliable applications with predictable performance.

The Pulse Secure Virtual Traffic Manager includes TrafficScript scripting software which provides fine-grained control over how traffic is managed. TrafficScript is designed with application developers in mind, making it far more efficient and easy to use than traditional network or event-based solutions. The Pulse Secure Virtual Traffic Manager also provides graphical analysis and management tools to give control over the complete ADC infrastructure.

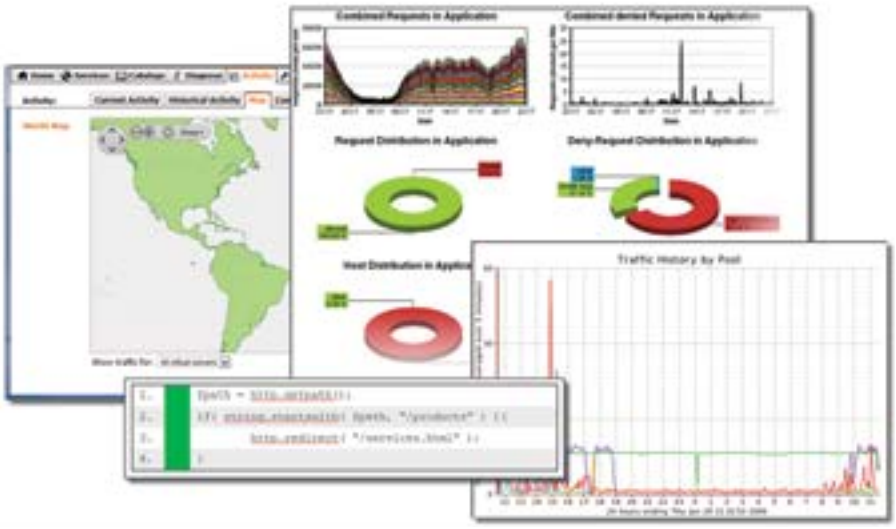

Figure 2. Powerful application management and visibility tools give users full control over the ADC environment.

Feature Summary

Pulse Secure vADC is available in two key feature tiers, the Advanced Edition and Enterprise Edition:

Advanced Edition: Includes the most common load balancing capabilities, including SSL/TLS offload, session persistence, service level monitoring, simple TrafficScript Rule Builder, and support for IPv6 and HTTP/2; and also includes capabilities such as Global Load Balancing, Route Health Injection, and customisation using Pulse Secure's powerful TrafficScript scripting language and Java Extensions;

Enterprise Edition: Adds premium Layer 7 services such as Web Content Optimization (WCO), Web Application Firewall (WAF) and FIPS compliance.

Advanced Edition Features

Load Balancing

The Pulse Secure Virtual Traffic Manager can use a wide variety of algorithms and techniques and balance load based on different criteria (e.g. can send more requests to higher spec machines). Servers can be drained for easy maintenance and uninterrupted service. The client never has to see a server fail.

HTTP/2 Support

Faster web pages with support for HTTP/2 connections. HTTP/2 is a significant enhancement to the HTTP/1.1 standard: Traffic Manager can automatically negotiate an HTTP/2 connection with the client web browser, which may improve web page load time with techniques such as connection sharing, page request multiplexing and header compression. For even more advanced HTML and web content optimization, the optional Pulse Secure Web Accelerator add-on module is available to create custom optimization profiles for individual applications.

Content Routing

Use the Pulse Secure Virtual Traffic Manager to apply business policies to each request for custom routing decisions, applying HTTP pool selection routing based on L7 attributes such as URL and hostname. Content inspection allows rapid web changes such as the insertion of marketing tags, branding changes, and dynamic watermarking, procedures that may be difficult to achieve by modifying the application itself.

Session Persistence

Ensures all requests from a client go to the same server, enabling application data to persist throughout a session without using cookies (e.g. an e-commerce shopping basket).

Health Monitoring

Monitor the health and correct operation of servers with built-In and custom checks. Detect failures of servers and errors in applications, and route traffic away from these servers so that the performance of the application is not compromised and the user experience is maintained.

Simple TrafficScript RuleBuilder

Define rules to control applications with the TrafficScript Rule Builder, using an easy-to-use graphical user interface to create traffic rules and policies. Click and choose from drop-down menus to create simple conditions and actions.

SSL/TLS Offload

Off-loading SSL/TLS key exchanges and decryption to the Traffic Manager frees up the back-end servers use their full resources for generating content and responding to user requests. Decryption on the Pulse Secure Virtual Traffic Manager allows for deep packet inspection. Content can be re-encrypted for secure forwarding of requests to the back-end infrastructure.

HTTP Compression

The Pulse Secure Virtual Traffic Manager can compress content returned to the client rather than have that workload undertaken by the back- end servers. Compression of content can result in bandwidth being used more efficiently. Offloading this workload from the back-end servers can enable it to serve requests faster.

Event Handling and Action System

Configure appropriate responses for key infrastructure events, including email and SNMP alerts, syslog logging and custom user-supplied scripts.

Service Protection

The Pulse Secure Virtual Traffic Manager can enforce an IP black/white list and limit the number of connections to a service. It can also enforce rules on HTTP content (e.g. enforce RFC compliance) and help protect against malicious attacks such as Denial of Service.

Real-Time Analytics

The Pulse Secure Virtual Traffic Manager measures performance and load and gives a graphical representation of the results which can identify bottlenecks and identify where and when high loading occurs which can be useful for identifying future upgrade needs.

HTTP Caching

The Pulse Secure Virtual Traffic Manager can store copies of frequently-requested data on the Traffic Manager rather than the back end servers, freeing them up to deliver newly requested content. This can reduce the need for additional servers as traffic grows and speed up the response to end user requests.

Autoscaling

Ensure reliable application service delivery by automatically managing traffic changes in real time, distributing traffic among a pool of virtual servers. It can orchestrate the provisioning and rightsizing of applications, helping to migrate traffic across multiple virtual and cloud platforms.

Bandwidth Management

You can limit the total bandwidth (kbits/sec) a set of connections can use which can be used to stop a popular site or application taking up so much bandwidth other sites or applications become unavailable. This can enable service providers to enforce access limits based on criteria such as account type or location.

Rate Shaping

The Pulse Secure Virtual Traffic Manager can restrict the number of requests (per min or sec) to a service, from either all or a set of clients. This can stop a small group of intensive users (including spiders) hogging a service, leading to a poor user experience for all users.

Service Level Monitoring

The Pulse Secure Virtual Traffic Manager nonitors the performance of a service or application and can issue an alert if it falls below a pre-determined level such as going out of scope of an SLA.

TrafficScript

TrafficScript is a sophisticated programming language integrated within the core of Traffic Manager that enables high performance, highly-configurable control of traffic management policies. TrafficScript rules can control all aspects of how traffic is managed and can choose when and where to apply request rate shaping, bandwidth shaping, routing, compression, and caching to prioritize the most valuable users and deliver the best possible levels of service.

XML Parsing

It can also help parse complex XML data using XPath in order to make informed routing decisions based on embedded content. Also includes supports for the offload and acceleration of the translation between XML variants via XSL Transformations (XSLT).

Java Extensions

Java Extensions can be used to re-use existing code libraries to implement business policies. You can write rules in any language that can target the JVM, including Java, Python, Ruby, and many others. You can use third party libraries, and invoke business rules against specific transactions.

Multi-Site Capable

Deploy services across multiple sites with location-specific configuration and simplify and the management of services from multiple datacenter locations.

Advanced Session Persistence

Ensures all requests from a client go to the same server, enabling application data to persist throughout a session without using cookies (e.g. an e-commerce shopping basket). In addition to session persistence based on IP addressing, Advanced Persistence mechanisms can be leveraged via TrafficScript, including Named Node and Universal Persistence techniques.

Global Load Balancing

Improve service availability by automatically failing over to an alternative datacenter or cloud deployment in the event of a catastrophic failure. Improve service performance by performance- sensitive load balancing and location- based traffic routing.

Route Health Injection

Route Health Injection (RHI) helps to maintain service availability and low-latency networking, by providing rapid service redirection to alternate service hosts.

Enterprise Edition Features

Web Accelerator Express
Simple content optimization to accelerate the delivery of most web pages, requiring no configuration or tuning.

Web Accelerator
Advanced Web Content Optimization (WCO) technologies, to accelerate page load times up to 4x for HTML applications, including Microsoft SharePoint, content management systems and cloud applications. WCO profiles can be customized for each application.

Web Application Firewall
A scalable Layer-7 Web Application Firewall (WAF) to apply business rules to your online traffic, inspect and block attacks such as SQL injection and cross-site scripting (XSS), and help achieve compliance with PCI-DSS and HIPAA and other regulatory demands.

Kerberos Constrained Delegation
Support for Common Access Cards (CAC) to provide seamless access to services that use Kerberos for authentication.

FIPS
Embedded FIPS 140-2 level 1 cryptographic module per FIPS 140-2 implementation guidance section g.5 guidelines, to support deployments that require FIPS 140-2 level 1 compliance.

Architectural Features
In addition, all Pulse Secure vADC models have the following common architectural benefits:

Data Plane Acceleration
Data Plane Acceleration mode for high-performance L4 services, supporting linear scaling of CPS and throughput with additional CPU cores, unlike traditional kernel network stacks. More than one million L4 connection requests per second and up to 140 Gbps are achievable on supported platforms.

Scalability
The Pulse Secure Virtual Traffic Manager can scale horizontally and vertically very easily, across IT environments and different forms of infrastructure ensuring that it can always scale up to match and support demand for an application or a service.

Clustering
The Pulse Secure Virtual Traffic Manager has unmatched scale and performance, and is able to scale-up with the latest generation of multi-core CPUs, and scale out with N+M clustering for reliability and throughput.

RESTful Control API
Allows the Pulse Secure Virtual Traffic Manager to be configured and controlled by a third-party application and simplifies administration of large/complex configurations. The Control API enables configuration changes to be automated (e.g. In response to an event).

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.

Pulse Secure Virtual Traffic Manager Specifications

Model	Pulse Secure vTM Bandwidth Options								
Throughput	50 Mbps	400 Mbps	1 Gbps	3 Gbps	5 Gbps	10 Gbps	20 Gbps	40 Gbps	80 Gbps
SSL/TLS TPS	Uncapped								
Functionality	Advanced or Enterprise								
Deployment model	Software, Virtual Appliance, Bare Metal image or BYOL on cloud platforms								
License Style	Perpetual or Subscription								

Pulse Secure Virtual Traffic Manager Functionality Matrix

Functionality	Advanced Edition	Enterprise Edition	Developer Edition 1 Mbps limit
Pulse Secure vTM	●	●	●
Pulse Secure Services Director	●	●	-
Load Balancing	●	●	●
HTTP/2 Support	●	●	●
Content Routing	●	●	●
Health Monitoring	●	●	●
Simple TrafficScript Rule Builder	●	●	●
SSL/TLS Offload	●	●	●
HTTP Compression	●	●	●
Event and Action System	●	●	●
Service Protection	●	●	●
Analytics	●	●	●
HTTP Caching	●	●	●
Autoscale	●	●	●
XML Parsing	●	●	●
Bandwidth Management	●	●	●
Rate Shaping	●	●	●
Service Level Monitoring	●	●	●
Traffic Script	●	●	●
Java Extensions	●	●	●
Multi-Site Manager	●	●	●
Global Load Balancing	●	●	●
Route Health Injection	●	●	●
Web Accelerator	-	●	●
Web Accelerator Express	-	●	●
Web Applicaton Firewall	-	●	●
Kerberos Constrained Delegation	-	●	●
FIPS	-	●	●

Pulse Secure Virtual Traffic Manager Licenses

License type	Purpose	Performance	Support	Duration	Cost
Evaluation license	Evaluation, Pre-production	80 Gbps for evaluation	Eval Assistance and updates	15-30 days	No cost
Production license	Production	As licensed	Support and updates	Perpetual or subscription	Per device

Evaluation Licenses

Licensing Feature	Description
Functional capabilities	Pulse Secure Virtual Traffic Manager, full functionality, all options
Licensed performance	80 Gbps for evaluation
Deployment	On multiple servers for pre-production evaluation
Validity	30 days
Support	Software updates and Evaluation assistance available
Evaluation licenses may be used to process production traffic during the limited evaluation period.	

Production Licenses

Licensing Feature	Description
Functional capabilities	As licensed
Licensed performance	From 50 Mbps throughput to 80Gbps for perpetual licenses, more possible using Pulse Secure Services Director
Deployment	On single system, bound to IP or MAC address
Validity	Perpetual or subscription
Support	Software updates and technical support
Production licenses may be used for any purposes, but only on a single system. All licenses are subject to the Pulse Secure End-User License Agreement available at https://www.pulsesecure.net/support/eula.	

Additional Notes

Licensing Feature	Description
Production license keys	Production license keys may be used for any purposes, but only on a single system. Production license keys may be obtained from your Pulse Secure partner. All types of license keys are subject to the Pulse Secure End User License Agreement for Pulse Secure Virtual Traffic Manager, which can be found at https://www.pulsesecure.net/support/eula.
Evaluation license keys	Evaluation license keys may be used to process production traffic during the limited evaluation period. 30-day evaluation licenses Developer Edition software and Evaluation software may be requested at https://www.pulsesecure.net/vadc.
Developer Mode	If the software does not have a valid license key, the software will run in "developer mode." Developer mode enables all of the functionality of Pulse Secure Traffic Manager and imposes a performance limit of 1 Mbps throughput. Users are allowed to distribute the Pulse Secure vADC software and virtual appliances without a license key ('Developer Edition'), so that they can be used in test and development environments to facilitate the creation and testing of production services. There is no charge for the Developer Edition, and Pulse Secure does not provide technical support.
Perpetual Licenses	Perpetual licenses provide a perpetual (non-expiring) license key that may be used on one server. Support and software upgrades are not included with a perpetual license, and require payment of an annual support fee.
Subscription Licenses	Subscription licenses allow you to use the software for a period of time (the "term") and oblige you to pay a periodic subscription fee (monthly) for that term. Subscription licenses include support and maintenance.
Performance Bands	Production licenses include a performance rating which specifies the maximum capacity of the software. The performance rating applies to outgoing bandwidth. Bandwidth capacity is applied to outgoing traffic only, after content compression, and is applied per instance of Pulse Secure Virtual Traffic Manager. It limits the speed at which the Pulse Secure Virtual Traffic Manager reads data from the backend server nodes. If the capacity limit is reached, then outgoing traffic may be delayed momentarily. Connections are serviced in a fair manner. Connections will not be dropped unless outbound traffic greatly exceeds the bandwidth capacity for a sustained period of time, when no data can be transmitted before the client or server timeouts expire. The host hardware must be adequately specified in order to deliver the desired performance.
When are requests discarded or timed out?	Client software (web browsers) and server software (e.g. web or application servers) both impose timeouts for connections. If a connection is idle for longer than the timeout period, it is closed. Under heavy, sustained load, responses are processed in a fair manner and partial responses are delivered to ensure that all connections are serviced equally. This means that connections are rarely idle for long periods of time when there is data waiting to be written, so connections are very unlikely to be closed down prematurely due to the bandwidth shaping.
Which performance band should I choose?	Evaluation licenses do not restrict performance, and may be used for short periods on production sites to gauge performance requirements. You can determine how much traffic an existing service is processing using the historical activity graphs, current data from the activity charts, and data available via SNMP and SOAP. The historical activity charts record bandwidth smoothed over 5-minute periods; you should add a margin of 50 to 100 percent for traffic spikes. When you run with a performance-based license, the Pulse Secure Virtual Traffic Manager software will log a warning and raise an alert to inform any time that it is necessary to limit the performance. Traffic is queued, so your end users will experience a momentary slowdown in your service. You can then upgrade to a higher-capacity license if necessary.
What is "non-production" use?	In "developer mode," software may only be used for non-production use: • "Non-production" use includes development, temporary testing, internal training, and proof-of-concept purposes. • "Production" use includes any purposes which could be regarded as "business-critical;" public Internet and internal intranet services, services that take live traffic, permanent replicas of production sites, permanent benchmarking and load testing environments, and any other services that are run on a commercial basis or for commercial gain.

Additional Notes (Continued)

Licensing Feature	Description
What happens when a license expires?	Perpetual licenses do not expire. Other licenses issued by Pulse Secure will have an expiration date. Once the expiration date has passed, the software reverts to developer mode, with bandwidth and performance restrictions. Pulse Secure Virtual Traffic Manager software raises warnings and alerts well in advance of expiration, and if a license with an expiration date is used in production, customers should configure the Pulse Secure software to email these warnings to an appropriate account. The zero-cost licenses that Pulse Secure issues for non-production use can continue to be used at no cost unless Pulse Secure has terminated the relevant license or developer program.
What does "bound to IP address/MAC address" mean?	Production licenses may be deployed on a single nominated host system only. To this end, they contain either an IP address or a MAC address that identifies the host system, and will only operate on a host with a matching address. Technical workarounds to deploy the license simultaneously on two or more host systems are in breach of the End-User License Agreement.
Upgrading and transferring licenses	Production licenses may be transferred between host machines, operating systems and platorms at no charge. Please request an "IP Address Change" form from your Pulse Secure support contact. Production licenses may be upgraded to increase performance capacity or unlock additional features – license upgrades are seamless and do not require a software restart.

System Requirements: Pulse Secure Virtual Traffic Manager Software and Virtual Appliances

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)
Supported OS: Web Accelerator Add-On Option	Linux 2.6.22 or later (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 & 2012 R2; QEMU/KVM (RHEL/CentOS 6.x, 7.x; Ubuntu 12.04, 14.04)
Recommended Hardware: CPU	Intel Xeon / AMD Opteron
Recommended Hardware: Minimum Memory	2 GB
Recommended Hardware: Minimum Disk Space	10 GB (Software), 16 GB (Virtual Appliance)

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

Pulse Secure®