DATA SHEET

Pulse Secure Services Director CSP

HIGHLIGHTS

- **Scalability:** Create elastic ADC services on demand, which can cluster to massive scale
- **Agility:** Bring new services to market more quickly, adapting capacity to meet demand
- **Management and Control:** Orchestrate Layer 7 services within a virtualized architecture
- **Dramatic Cost Savings:** Optimize resources with enterprise-capacity management and usage model

A New Approach to Application Delivery with the Pulse Secure Services Director

Service providers are increasingly looking for ways to launch new services with innovative business models in order to provide a responsive and adaptive service to client applications. At the same time, they are under pressure to reduce the costs of infrastructure provision and ensure a rapid return on investment. An Application Delivery Controller (ADC) is key for delivering fast, reliable applications and maximizing availability, maintaining security policies, and providing a point of control for monitoring and managing application traffic.

However, most ADCs on the market today are not designed for large-scale virtual or cloud deployments. Their static architectures make them cumbersome and time-consuming to deploy and manage in virtualized and cloud environments.

Pulse Secure delivers new dynamic architectures that remove bottlenecks and deliver improved agility, high automation levels, and faster time to service. These new architectures are called ADC as-a-Service (ADCaaS) and they enable customers to:

- Cut down provisioning time for ADC services from weeks to minutes
- Provide better user experience with per-application tuning and multi-tenancy
- Deliver better security and performance through isolation and scale
- Right-size their ADC commitments to match costs with revenue

This new approach to application delivery provides a complete set of tools to deploy services rapidly, wherever and whenever they are needed. ADC instances can be deployed rapidly, and can be adjusted quickly to meet changing workloads and application updates and developments.

Pulse Secure Services Director: How It Works

The Pulse Secure Services Director enables organizations to provision, license, and meter their inventory of thousands of ADCs in an “as-a-service” model, using the Pulse Secure Virtual Traffic Manager (Pulse Secure vTM) as the core application delivery platform.

The solution also enables a new consumption model to be offered to ADC users.

ADC services can be rapidly scaled and be right-sized on demand to suit each application within their infrastructure, scaling horizontally and vertically as each application deployment is adjusted to meet user demand.

Provisioning: Pulse Secure Services Director can be integrated with pre-existing orchestration tools to enable organizations to provision individual instances of Pulse Secure vTM within a hosted virtual environment for use by each of customer. Alternatively, the Pulse Secure Services Director can register externally deployed instances within the data center or hybrid cloud environment.

Licensing: Each instance is licensed automatically, to define the capacity and capability of each instance based on the configuration requested by each customer from the range of feature packs available to them, including the various add-on options like Pulse Secure Virtual Web Application Firewall (vWAF) or FIPS. There is no limit to the number of Pulse Secure vTMs or vWAFs that can be licensed in this way. The only license that needs to be renewed is the Pulse Secure Services Director itself, once every 12 months.

Metering: The Pulse Secure Services Director tracks each instance and creates usage reports on a range of metrics for monitoring and billing purposes (see Figure 1). These usage reports, or Log Files, are passed to Pulse Secure on a monthly basis for billing.

Feature Summary

Flexible and on-demand licensing:

The Pulse Secure Services Director handles the provision of application delivery services to customers, so there is no need to pre-purchase ADC capacity in advance. Customers can start small and add new licensed capacity only when they need it. With this new usage-based business model, organizations are in control of their costs. They can choose the feature packs to make available as well as the price of each ADC instance for a true ADC-as-a-Service.

Cloud scalability:

The Pulse Secure Services Director can manage the lifecycle of thousands of ADC instances under the same shared resourcing pool. With a high-level view of ADC deployment and utilization across an organization's cloud environment, the Pulse Secure Services Director helps manage application delivery services across customers' infrastructure and helps customers deploy new services quickly.

Agile ADC provisioning:

With agile ADC provisioning, customers can deploy application delivery services in minutes and exactly where needed to reduce time to market for new applications and services. They can create new ADC instances on a per-application or per-tenant basis instantly, start and stop instances for service migration, and even pre-provision ADC instances for even faster "instant-on" services.

High-density multi-tenancy and isolation:

With the Pulse Secure Services Director, ADCs can be right-sized and scaled to meet demand, while maintaining isolation on a per-application or per-tenant basis. This reduces "noisy neighbor" performance concerns, while maximizing ADC utilization and investment. In addition, this service isolation makes it easy to perform upgrades without impacting adjacent applications. Customers can create custom traffic policies for each application—their ADC deployments are now as flexible as their compute deployments.

Automated service metering:

The Pulse Secure Services Director maintains a database of all ADC instances, and the license allocated to each ADC. The Pulse Secure Services Director also maintains an audit trail of which ADC services have been deployed, and records the throughput and peak data rate of each ADC

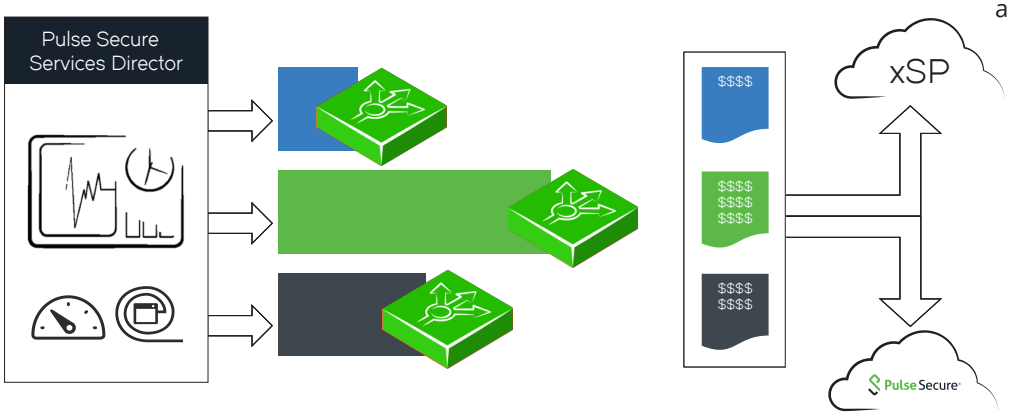

Figure 1. Revenue sharing with the Pulse Secure Services Director.

instance. Log Files containing this data can be fed into an organizations' billing system/finance system for customer billing purposes and are passed to Pulse Secure too.

Create ADC resources to match demand:

Because the Pulse Secure Services Director puts no limit on the number of instances organizations and their customers can license, it is easy to create the resources needed to meet changes in workload with as little friction as their orchestration tools will allow. As the traffic management needs of their applications change through seasonal or periodic cycles, they can add or delete ADC resources as required; they do not need to purchase extra capacity ahead of time or forecast CapEx requirements.

Open APIs:

The Pulse Secure Services Director integrates directly into service provisioning and orchestration systems with a powerful REST-based API. The Pulse Secure Services Director registers each instance that is deployed, capturing all the relevant information for licensing and metering purposes.

Reporting:

The Pulse Secure Services Director provides a Log File of raw data that can be processed to feed into billing/finance systems (See Figure 2).

Pulse Secure vTM status monitoring:

A summary of the deployed Pulse Secure vTM instances ranked by status is delivered using a traffic light system of red, amber and green to indicate instance health, as well as blue for pending and black for stopped or deleted.

CPU Utilization Screen:

For Pulse Secure Services Director-deployed ADC instances, organizations can review CPU utilization and aggregated throughput data on per host basis.

Bandwidth Allocation Report:

This report provides a snapshot of current bandwidth allocation, grouped both by type of instance, and by type of license. As with the other reports, the chart is interactive, so organizations can drill down on the chart to analyze the capacity available per-license.

XSP Licensing

The Pulse Secure Services Director introduces a different approach for the provision of application delivery services. Once integrated with orchestration tools, the Pulse Secure Services Director helps manage the complete lifecycle of Pulse Secure vTM instances, including:

- Deployment
- Licensing
- Metering
- Inventory management
- Performance monitoring

This new innovation in the ADC market allows for on-demand deployment of Pulse Secure vTMs that results in OpEx savings through automated licensing by the Pulse Secure Services Director and offers a much more flexible licensing model. To achieve this, the Pulse Secure Services Director is required to maintain licensing information about each product under its control, in addition to its own license.

Feature Packs

The Pulse Secure Services Director enables organizations to offer their own Pulse Secure vTM "Feature Packs" to their customers. Pulse Secure provides five different base SKUs:

- Basic Load Balancing
- Advanced Load Balancing
- Standard ADC
- Enterprise ADC
- Web Application Firewall

Organizations can now customise each SKU by deciding what features to offer their customers. By creating their own "Feature Packs," ADC solutions can be tailored to address a particular competitive requirement or implement a sell-up path to higher-end products that matches a particular market or vertical focus. Each Feature Pack instance must be associated with a specific Pulse Secure Services Director license and can be used in a cluster of Pulse Secure Services Directors. If the Pulse Secure Services Director fails, the Feature Pack instance associated with the Pulse Secure Services Director remains valid as long as the cluster is still available. Any combination of Pulse

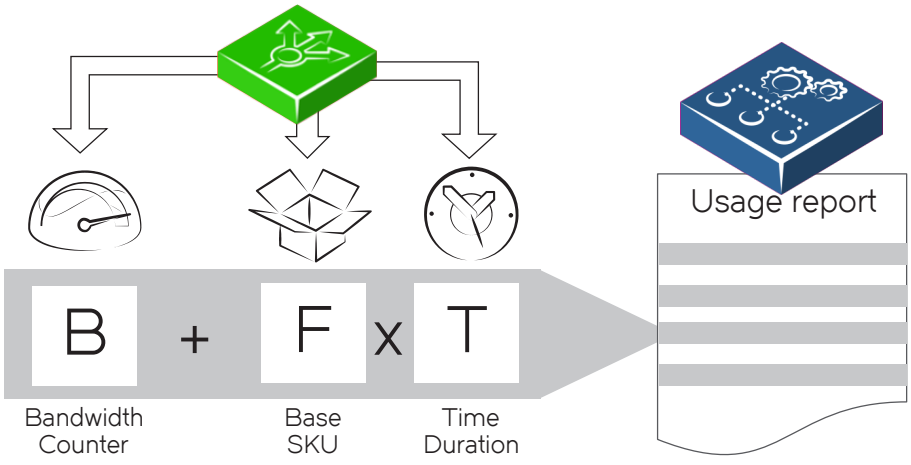

Figure 2. Usage metering with the Pulse Secure Services Director.

Secure vTM and vWAF sizes may be deployed by customers.

Add-On SKUs

Organizations also have the option of providing additional functionality via Add-on SKUs:

- FIPS
- Virtual Web Application Firewall: (vWAF)
- Web Acceleration

These Add-on SKUs can be added to any of the load balancing or ADC SKUs or custom Feature Packs they have created to add FIPS, Application Firewall, and Web Acceleration functionality to each instance. Priced separately, these Add-on SKUs offer another incremental revenue stream and enable organizations to offer a broader Application Delivery proposition to their customers with no OpEx commitment.

The Pulse Secure Services Director keeps track of the total number of instances deployed by customers across Feature Packs and the data throughput of those instances. There is no limit to the number of instances that can be deployed and they are only charged for deployment and usage.

The cost of each instance is a combination of the amount of bandwidth that has passed through the instance plus the number of hours the instance has been deployed times the hourly cost of that base SKU. If a customer wants to deploy a high-capacity version to make sure they can cope with unexpected peaks of traffic, they can do so while only paying for the throughput that actually passes through that instance (see Figure 2).

Pulse Secure Virtual Traffic Manager SKU Function Matrix

Feature Pulse Secure Services Director vTM Edition	STM-B-100	STM-B-200	STM-B-300 Standard	STM-B-400 Enterprise
Load Balancing	Round Robin Least Connections	•	•	•
Content Routing	•	•	•	•
Health Monitoring	•	•	•	•
Session Persistence	IP Address SSL ID	•	•	•
Rule Builder	•	•	•	•
SSL/TLS Offload		•	•	•
HTTP Compression		•	•	•
Event and Action System		•	•	•
Service Protection		•	•	•
Analytics			•	•
Traffic Script			•	•
HTTP Caching			•	•
Autoscale			•	•
Java Extensions			•	•
XML Parsing			•	•
Bandwidth Management			•	•
Rate Shaping			•	•
Service Level Monitoring			•	•
Multi Site Manager			•	•
Global Load Balancing				•

Pulse Secure Virtual Traffic Manager SKU Function Matrix *(continued)*

Kerberos Constrained Delegation				•

Feature Pulse Secure Services Director vTM Edition	STM-B-100	STM-B-200	STM-B-300 Standard	STM-B-400 Enterprise
Route Health Injection				•
Attach LBaaS	OPT	OPT	OPT	•
Attach FIPS	OPT	OPT	OPT	OPT
Attach vWAF			OPT	OPT
Attach Web Acceleration			OPT	OPT

Additional Licensing Notes for the Pulse Secure Services Director for CSP

Production License Keys	vADC services may not be directly resold to any third party without the appropriate cloud service provider license. Contact Pulse Secure for more information. All licenses are subject to the Pulse Secure End User License Agreement.
High Availablity	The Pulse Secure Services Director can be deployed in Active/Standby pairs (Virtual Appliance form factor) or in multi-node cluster (software form factor) to provide high availability. Pulse Secure Services Directors deployed for HA monitor each other and alert the user in case of a failure, allowing a failover to be triggered
Latency Requirements	When all features are required (deployment, metering, monitoring), the Pulse Secure Services Director needs network links with a link latency of 10 ms or less and bandwidth of 100 Mbps or greater to support scales up to 5000 instances. When used purely for instance licensing (i.e. licensing externally deployed instances), the Pulse Secure Services Director needs network links with latency of 400 ms or less to support scales up to 5000 instances.
Grace Period	The Pulse Secure Virtual Traffic Manager supports a licensing “Grace Period” to avoid outages for licensed Traffic Managers if the Pulse Secure Services Director becomes temporarily unreachable. While in Grace Period, a Pulse Secure Virtual Traffic Manager will continue to support the features and bandwidth it was most recently licensed with by the Pulse Secure Services Director. Pulse Secure Virtual Traffic Managers in the Grace Period may be restarted without losing these licensed features and bandwidth. A Pulse Secure Virtual Traffic Manager will remain in Grace Period until either it re-establishes contact with the Pulse Secure Services Director, or the Grace Period expires (after six weeks). In the event of Grace Period expiry, the Pulse Secure Virtual Traffic Manager will continue to run, but fall back to Developer Mode (See “Developer Mode” below for more information). The Pulse Secure Services Director will indicate instances in Grace Period in the GUI when it has not received licensing requests from them for more than a licensing cycle. The Pulse Secure Services Director runs a on a three-minute polling cycle.
Performance Limits	The maximum capacity of each Pulse Secure vTM is set at deployment time, and the Pulse Secure Services Director can be used to modify the performance of each Pulse Secure Virtual Traffic Manager at any time. The performance rating applies to outgoing traffic after content compression (egress from the Pulse Secure vTM sent from the server to the client). Pulse Secure vTM instances managed by the Pulse Secure Services Director are unrestricted in SSL performance, up to the deployed bandwidth. The host hardware/virtual server must be adequately specified in order to deliver the desired performance.
Developer Mode	Developer Mode refers to an instance state where all features are enabled but throughput is limited to 1 MB. When using the Pulse Secure Services Director for CSPs, Developer Mode should only arise in the case of misconfiguration (such as when the Pulse Secure Services Director cannot install a FLA licence on the Pulse Secure Virtual Traffic Manager, or a FLA licence cannot reach the Pulse Secure Services Director to get an initial licence response) or grace period expiry. If Developer Mode instances are required for development and testing, they can be downloaded from www.pulsesecure.net.

Pulse Secure Services Director for CSP Specifications

Pulse Secure Services Director Virtual Appliance	
Hypervisor	VMware vSphere ESXi 5.0+, KVM Virtual Appliance
Recommended CPU	4 vCPUs
Recommended memory	8 GB
Recommended disk space	46 GB (plus additional disk space for metering logs, depending on number of instances metered)
Pulse Secure Services Director Software	
Operating system	Ubuntu 12.04 (x86_64), or Ubuntu 14.04 (x86_64), or CentOS 6.5 (x86_64)
Database	MySQL 5.5 (5.5.32 recommended)
Other services	SMTP
Recommended CPU	Intel Xeon / AMD Opteron
Recommended memory	2 GB
Recommended disk space	10 GB (plus additional disk space for metering logs depending on the number of instances metered)

Additional Note: Software-only installation is recommended for fully automated environments, which do not require a GUI or console

Virtual Environment: Instance Host VA	Small	Large
Hypervisor	VMware vSphere ESXi 5.0+	
Recommended CPU	2 vCPUs	8 vCPUs
Recommended memory	4 GB	16 GB
Recommended disk space	70 GB	70 GB
Software/Virtual Environment: Pulse Secure Virtual Traffic Manager managed by the Pulse Secure Services Director		
OS supported for managed Pulse Secure vTM instances	Ubuntu 12.04 (x86_64), or Ubuntu 14.04 (x86_64), or CentOS 6.5 (x86_64)	
OS supported for externally managed Pulse Secure vTM instances	Same as the Pulse Secure Virtual Traffic Manager (requires Pulse Secure vTM v9.5 or above)	

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

Pulse Secure®