Pulse Secure

WHITE PAPER

Pulse Secure Virtual Web Application Firewall

Network Deployment Options

TABLE OF CONTENTS

Introduction

Pulse Secure Virtual Web Application Firewall (vWAF) supports a full range of deployment options enabling you to choose the best fit for your architecture and application risk profile. Pulse Secure vWAF can be deployed as a virtual appliance, on a web server, or as a physical appliance in a customer data center or cloud provider—or even as an integrated package with Pulse Secure Virtual Traffic Manager (vTM) for enhanced security and control of complex applications.

In addition, 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.

Pulse Secure Virtual Web Application Firewall Deployment Options

A range of deployment options is available to suit any kind of IT environment:

- **Pulse Secure vWAF add-on for Pulse Secure vTM:** This module may be licensed for Pulse Secure vTM (software or virtual appliance), and allows the Pulse Secure vTM to enforce application-level security to traffic.
- **Pulse Secure vWAF Web server plug-in:** For maximum scalability in global applications, the Pulse Secure vWAF can be implemented as Web server plug-ins providing a fully distributed architecture with complete flexibility.
- **Pulse Secure vWAF proxy solution:** This stand-alone Pulse Secure vWAF 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 Pulse Secure vWAF can apply deep application-level security.

Deploying Pulse Secure vWAF Add-on for Pulse Secure vTM

Pulse Secure vWAF for Pulse Secure vTM is enabled via license key as a capability of the Pulse Secure vTM. The network deployment options are same as Pulse Secure vTM network configurations as described in Chapter 2 of the user guide located at www.pulsesecure.net/vadc (See Figure 1).

Deploying Pulse Secure vWAF Web-Server Plug-In

The fully distributed version of Pulse Secure vWAF is installed as a Web server plug-in and is therefore very simple to deploy from a network perspective. For more details on installation and deployment, please refer to the support and documentation pages at www.pulsesecure.net/vadc (See Figure 2.)

Deploying Pulse Secure vWAF Proxy Solutions

Pulse Secure vWAF proxy solution is deployed as a stand-alone proxy device either sandwiched within an existing ADC deployment (much like a firewall or other proxy device) or in front of a single Web server. The remainder of this document discusses deployment scenarios for Pulse Secure vWAF.

Pulse Secure vWAF for Load-Balanced Environments

Pulse Secure vWAF can be deployed in an existing load-balanced scenario without having to change or rewire the existing network topology. Logically, Pulse Secure vWAF devices are sandwiched between two layers of ADCs so that they can be scaled, and the ADCs perform the health-checks and load balancing against the back-end servers.

Deployment alongside an Existing ADC or Load Balancer

Although the logical design of the software calls for a network "sandwich" between two ADC layers, in practice the deployment is generally performed with a single layer of ADCs. This ADC layer runs two load-balancing services; one to forward traffic out to the Pulse Secure vWAF devices, and one to load-balance traffic from the devices across the backend servers. This configuration, which loops traffic out to the Pulse Secure vWAFl devices, is sometimes referred to as a network "trombone" (See Figure 3 on the following page).

Pulse Secure vWAF can be deployed in one of the following ways:

1. One-armed deployment (single network segment)
2. Two-armed deployment (public and private network segments)

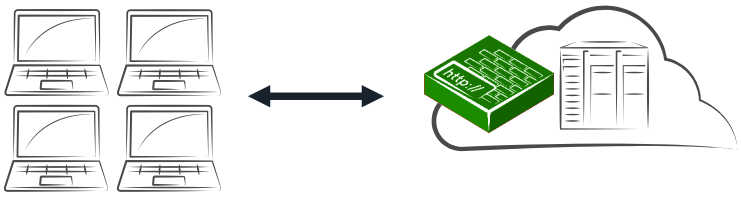

Figure 1: Pulse Secure vWAF deployed as an add-on module for the Pulse Secure vTM.

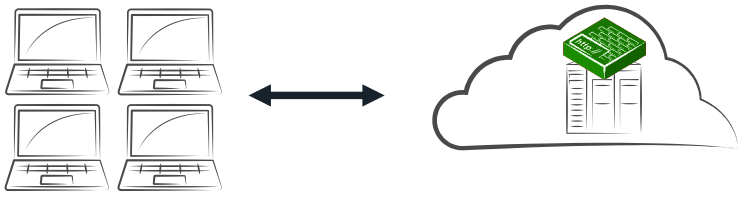

Figure 2: Pulse Secure vWAF plug-in modules deployed on the Web server.

One-Armed Deployment

In a one-armed deployment, Pulse Secure vWAF is deployed in the same VLAN/network as Web/application servers, and the single interface on the device connects to the internal network.

As depicted in the Figure 4, traffic flow for this deployment mode is as follows:

1. The FQDN for the application that needs to be protected resolves to an external IP address on the Traditional ADC. The client makes a TCP connection to this IP address.
2. The traditional ADC is configured to load balance HTTP traffic across one or more Pulse Secure vWAF instances.
3. Pulse Secure vWAF analyzes incoming traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the incoming traffic is forwarded to the application Web/applications servers. (Note: If any response needs to go back through the traditional ADC, either the ADC must also function in full-proxy mode or source-NAT needs to be configured on the ADC, or the vWAF default-gateway should be the ADC*).*
4. The Web server processes the request, and send the response to Pulse Secure vWAF via the ADC.
5. Pulse Secure vWAF analyzes outgoing traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the outgoing traffic is sent to the client via the ADC.

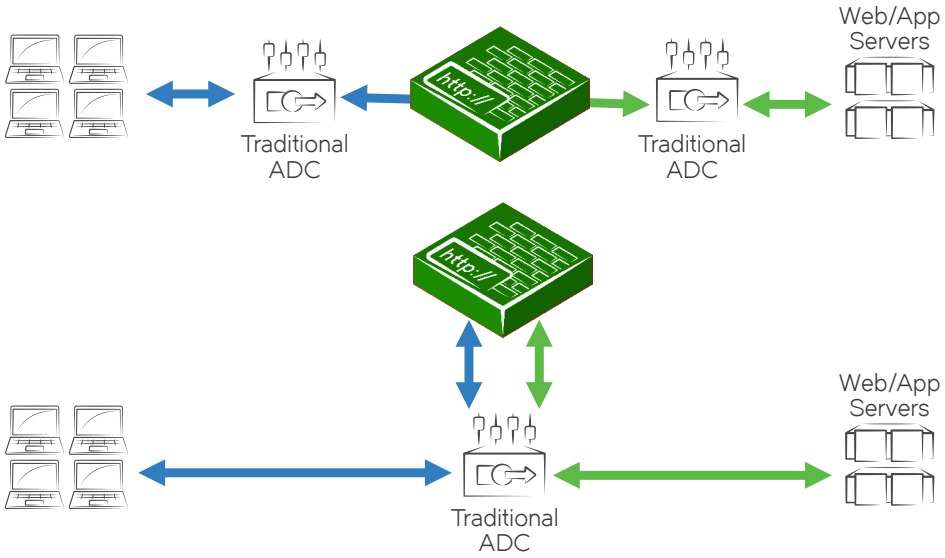

Figure 3: Logical "sandwich" view of deployment (top) and typical "trombone" deployment (bottom) that eliminates the need for two layers of ADCs.

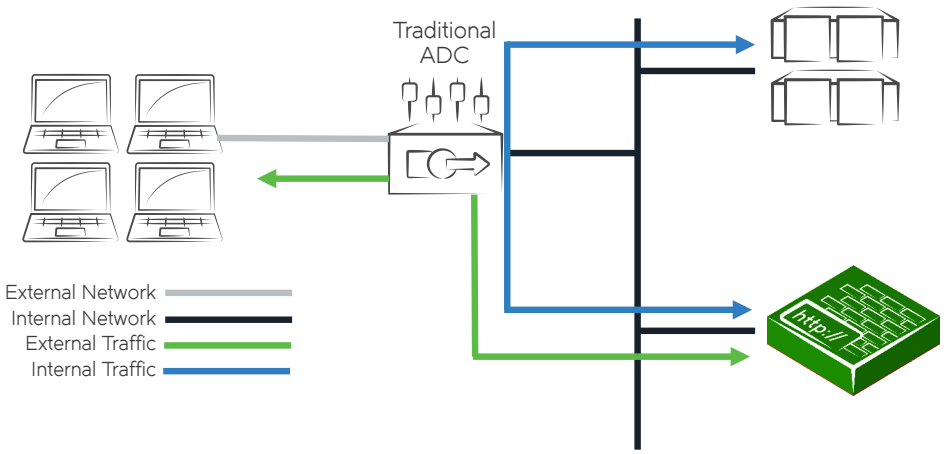

Figure 4: Deployment alongside an existing ADC or load balancer: One-armed Deployment.

Two-Armed Deployment

In this mode of deployment, Pulse Secure vWAF is connected to the external and internal network as depicted in Figure 5.

Traffic flow for this deployment mode is as follows:

1. The FQDN for the application that needs to be protected resolves to an external IP address on the Traditional ADC. The client makes a TCP connection to this IP address.
2. The traditional ADC is configured to load balance HTTP traffic to Pulse Secure vWAFl or across a pool of Pulse Secure vWAF devices with external IP addresses.
3. Pulse Secure vWAF analyzes incoming traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the incoming traffic is forwarded to the application Web/applications servers. (Note: that if any response needs to go back through the traditional ADC, either the ADC must also function in full-proxy mode or source-NAT needs to be configured on the ADC, or the Pulse Secure vWAFdefault- gateway should be the ADC.)
4. The Web server processes the request, and sends the response to Pulse Secure Web Application Firewall via the ADC.
5. Pulse Secure Web Application Firewall analyzes outgoing traffic for potential threats, against both "Detect" and "Protect" policies, and if permitted, the outgoing traffic is sent to the client via the ADC.

If necessary, an additional management interface can be configured on Pulse Secure Web Application Firewall and then connected to a separate management VLAN or network.

Pulse Secure Web Application Firewall Scalability

The ADC may load-balance traffic across multiple independent Pulse Secure Web Application Firewall nodes. The ADC should apply session persistence so that all traffic from the same client is directed to the same Pulse Secure Web Application Firewall instance.

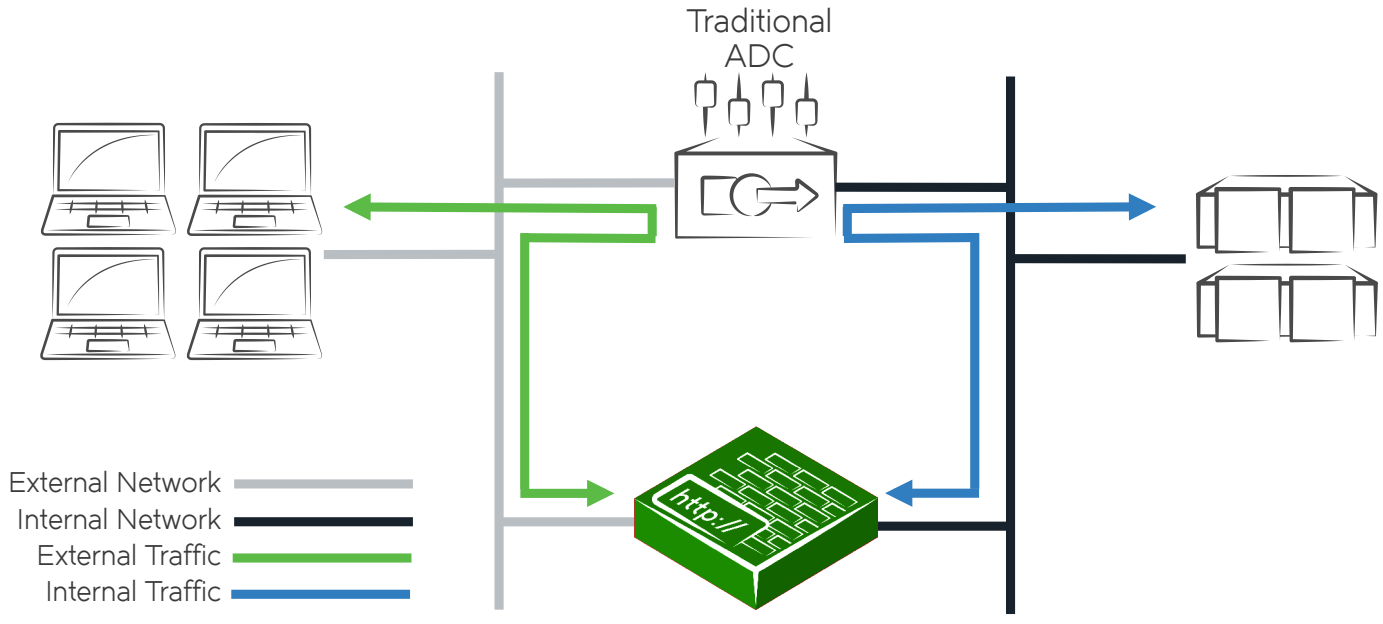

Figure 5: Deployment alongside an existing ADC or load balancer: Two-armed Deployment.

Pulse Secure vWAF Deployed without a Local ADC or Load-Balancer

In some scenarios, a local ADC or load balancer may not be present. The Web Application may be served from a single web server, or a technique like round robin DNS may be used to distribute traffic across the servers. In this situation, Pulse Secure vWAF is deployed as a proxy, receives external traffic, and then forwards it on to the Web servers.

Some configuration changes to the DNS need to be made in order to ensure that the traffic would be directed to Pulse Secure vWAF. Otherwise an IP address reassignment is necessary.

Deploying Pulse Secure vWAF with a Single Web Server

Pulse Secure vWAF is configured as a simple proxy with a single virtual server and pool. Incoming traffic is routed to the Pulse Secure vWAF virtual server and the pool forwards it to the back-end server. Either a one-armed or a two-armed deployment may be used (See Figure 6).

Deploying Pulse Secure vWAF with a Group of Web Servers

In this scenario, a load balancer or an ADC is needed to forward traffic to a group of Web servers. However, in limited cases, a load balancer or DNS round robin solution may be in use. But without administration privileges or if the load balancer is not local, it may not be possible to use the configuration described in the previous section. In such cases, the stand-alone device can be deployed with multiple virtual server and pool pairs, one for each back-end Web server (See Figure 7).

Once again, either a one-armed or two-armed deployment model may be used.

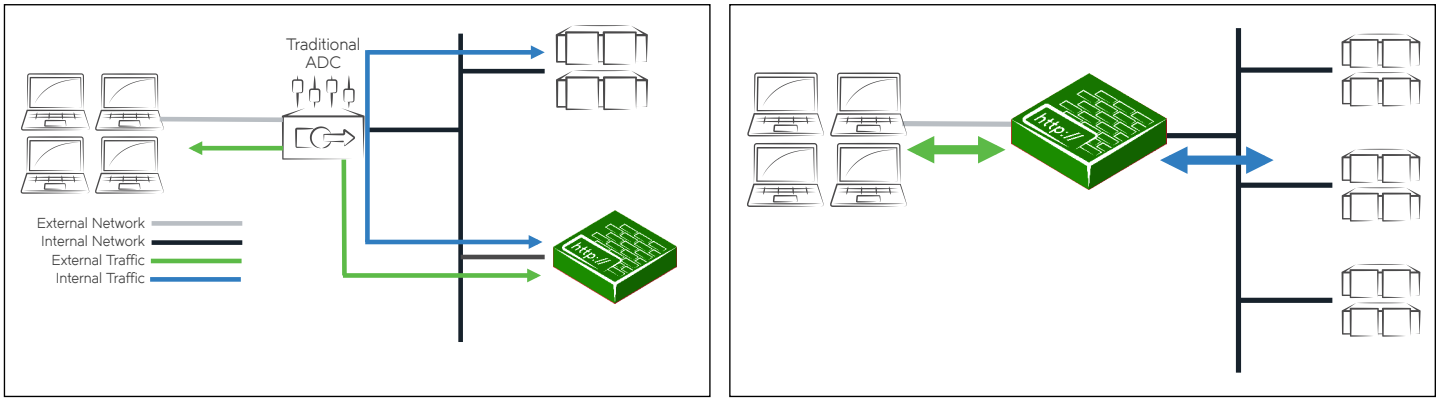

Figure 6: Deploying Pulse Secure vWAF with a single Web server.

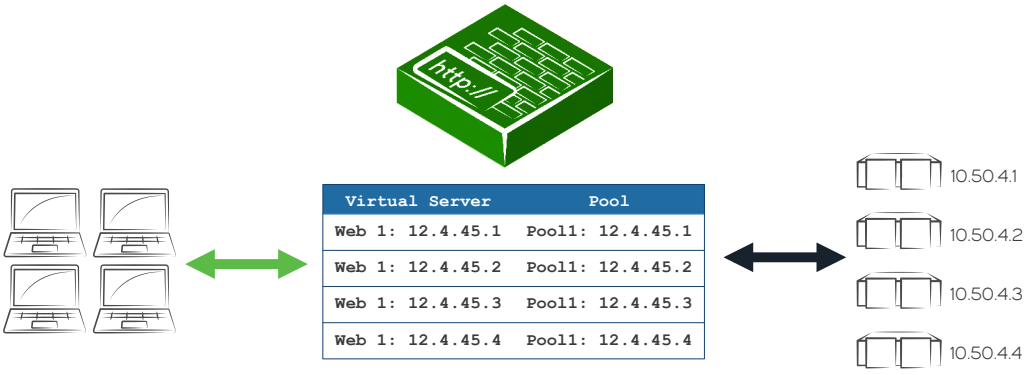

Figure 7: Deploying Pulse Secure vWAF with a group of Web servers.

Pulse Secure vWAF Scalability

Pulse Secure vWAF may be deployed in a fault-tolerant cluster consisting of two or more devices. Pulse Secure vWAF clusters manage a floating set of IP addresses (called "Traffic IPs") and ensure that the cluster manages traffic directed to those IP addresses, even in the event of a Pulse Secure vWAF failure. For high scalability needs, the cluster may be run in an Active/Active fashion, allowing for linear scalability of capacity.

Conclusion

The range of Pulse Secure Web Application Firewall platforms and deployment options make it possible to apply vWAF optimizations to almost any Web-based application:

- Pulse Secure vWAF add-on for Pulse Secure vTM may be added to an existing Pulse Secure vTM ADC
- Pulse Secure vWAF web-server plug-ins may be deployed for maximum scalability in global applications
- Pulse Secure vWAF proxy solutions may be deployed to augment an existing load-balanced or single-server environment

Pulse Secure vWAF platforms support multiple network topologies and can be provisioned as both software and a packaged virtual appliance, making it easy to accelerate existing enterprise or online applications and free development teams from the burden of content optimization and testing.

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

Pulse Secure®