GateDefender Performa updates from a local Web server

Table of contents

1. Installation and configuration of the Web server

This manual explains the procedure for installing and configuring an Apache Web server for Linux and MS-Windows.

In the case of Linux there are several installation and configuration procedures. This manual focuses on the simplest of them. Specifically, it explains the case of the Linux distributions: Debian and Ubuntu.
For other distributions, the procedure is similar.

1.1 Linux HTTP server (Ubuntu and Debian distributions)

1.1.1 Installation of Apache and SSL

Before starting you must check if there has been a previous installation. To do this, run the following command using the **root** user:

- **dpkg -l apache2**

If the there has been a previous installation, go to point 1.1.2

To carry out a new installation of the Apache packet, run the following command:

- **apt-get install apache2**

If you have problems with this installation, make sure the following two lines are in the file: **/etc/apt/sources.list**:

- **deb ftp://ftp.debian.org/debian sarge main contrib non-free**
- **deb-src ftp://ftp.debian.org/debian sarge main contrib non-free**

1.1.2 Get a valid domain name

This domain name must be included in the file **/etc/** along with the local IP address, for example:

127.0.0.1 localhost
172.16.128.18 webserver.example.com webserver

1.1.3 Directory for file downloads

In the process of installing Apache, the apache2-default directory is created automatically in **/var/www**. By default, this directory stores the downloaded files.

In this case a directory called **files** is created in **/var/www/**.
This directory stores **Pav.zip** and **Pavsig.txt***, which are copied from a server connected to the Internet, where the files have been downloaded from Panda Security servers in order to update Panda GateDefender Performa.

1.1.4 Configuring the Apache server

Once you have reached the point, you can start the configuration:

Steps to follow:

1. Configure the connection with the server through port 80.
   To do this, edit the following file:

   /etc/apache2/ports.conf

   And add the following line:

   Listen 80

2. Create a new site in the directory **/etc/apache2/sites-available/**, adding the following lines to a newly created file called, for example, http:

   ```
   NameVirtualHost *:80
   <VirtualHost *:80>
   ServerAdmin webmaster@localhost
   DocumentRoot /var/www/
   <Directory /var/www/>
   Options FollowSymLinks
   RedirectMatch ^/$ /files/
   </Directory>
   </VirtualHost>
   ```

3. Load the new site, with the command:

   a2ensite http

4. Run the following command again with the configuration updated:

   /etc/init.d/apache2 force-reload

1.1.5 Check the connection with the Web server

To check this connection, enter the URL **http://webserver.example.com** in a browser. This domain must be included in the file /etc/hosts or must be accessible through a DNS.

Once you have checked the connection, the server is ready to download local updates for Panda GateDefender Performa.

1.2 Linux HTTPS server (Ubuntu and Debian distributions)

1.2.1 Installation of Apache and SSL

Before starting you must check if there has been a previous installation. To do this, run the following command using the root user:

- **dpkg -l apache2**
- **dpkg -l openssl**

If there has been, go to point 1.2.2

To carry out a new installation of the Apache and SSL packets, run the following command:

apt-get install apache2 openssl

If you have problems with this installation, make sure the following two lines are in the file: /etc/apt/sources.list:

- **deb ftp://ftp.debian.org/debian sarge main contrib non-free**
- **deb-src ftp://ftp.debian.org/debian sarge main contrib non-free**

If both packets are installed, go to point 1.2.2
If you have Apache without SSL, reinstallation is required.

1.2.2 Get a valid domain name

This domain name must be included in the file **/etc/** along with the local IP address, for example:

127.0.0.1 localhost
172.16.128.18 webserver.example.com webserver

1.2.3 Generating certificates

Now you have to create a certificate. To do this, use the script apache2-ssl-certificate. This script will be in the **/usr/sbin** directory after installation of Apache.
This script is just a small shell with **openssl** commands. A series of configuration parameters are required. Most of the parameters can be left with the default values, However, it is important to correctly enter the name of the domain in the **Common Name** parameter.

1.2.4 Directory for file downloads

The **HTTP** and **HTTPS** servers can be on the same computer, creating one directory in /var/www, for example, the directory **files**.
This directory stores **Pav.zip** and **Pavsig.txt**, which are copied from a server connected to the Internet, where the files have been downloaded from Panda Security servers in order to update Panda GateDefender Performa.

1.2.5 Configuring the Apache server

Once you have reached the point, you can start the configuration:

Steps to follow:

5. Configure the connection with the server through port 443.
   To do this, edit the following file:

   /etc/apache2/ports.conf

   And add the following line:

   Listen 443

6. Create a new site in the directory /etc/apache2/sites-available/, adding the following lines to a newly created file called, for example, ssl:

   ```
   NameVirtualHost *:443
   <VirtualHost *:443>
   ServerAdmin webmaster@localhost
   DocumentRoot /var/www/
   <Directory /var/www/>
   Options FollowSymLinks
   RedirectMatch ^/$ /files/
   </Directory>
   SSLEngine On
   SSLCertificateFile /etc/apache2/ssl/apache.pem
   </VirtualHost>
   ```

7. Load the new site with the command:

   a2ensite ssl

8. Enable the SSL module

   a2enmod ssl

9. Run the following command again with the configuration updated:

   /etc/init.d/apache2 force-reload

1.2.6 Check the connection with the Web server

To check this connection, enter the URL **https://webserver.example.com** in a browser. This domain must be included in the file **/etc/hosts** or must be accessible through a DNS.

Once you have checked the connection, the server is ready to download local updates for Panda GateDefender Performa.

1.3 MS Windows server

There are several ways on installing and configuring a Web server on MS Windows.
This section looks at installing Apache, a free server.
You can also install other Web servers, such as IIS.

1.3.1 Getting Apache

You can download the latest version of Apache for MS-Windows from:

http://ftp.udc.es/apache-dist/httpd/binaries/win32/apache_2.2.8-win32-x86-openssl-0.9.8g.msi

1.3.2 Installing Apache

The same file downloaded in the previous section contains a wizard for installation.
It is advisable to follow the wizard and use the default values during the installation process.
Is important to correctly enter the domain name and the server name when prompted:

Domain name-> example.com
Server name -> webserver.example.com

Once you have reached this point, the installation process will require a user mode, either for a local user or for all users, using port 80. Choose the second option.

In a typical installation, Apache is installed by default in:

C:\Program Files\Apache software foundation\Apache2.2

You can check that Apache has been installed correctly by going to the URL **http://localhost**

If you get the message: **It works!** It has been correctly installed.
If the Apache process is not active, it can be started in:
Control Panel, in **Administrative Tools**, **Services** if Apache is started or not.

1.3.3 Customizing Apache

The only thing left to do is to copy the **Pav.zip** and **Pavsig.txt** files to:
C:\Program Files\Apache software foundation\Apache2.2\htdocs

2. Configuring the Web server

Finally, once the Web server is operating correctly, configure the updating of Panda GateDefender Performa in **Local mode**.

This configuration can be made through the Web console, in **Updates**, **Update settings** and selecting **Local mode**. In this mode you can enter the URL and the path where the **pav.zip** and **pavsig.txt** files have been saved.

For example:

Linux: If the Web server has the following URL: webserver.example.com
and the files have been copied to **/var/www/** files, the URL is:

https://webserver.example.com/files for HTTPS and
http://webserver.example.com/files for HTTP.

MS-Windows: If the files have been copied to **C:\Program Files\Apache software foundation\Apache2.2\htdocs\files**, the URL is

http://webserver.example.com/files

Once the updates have been configured in local mode, services must be reset for the changes to take effect.

***Note:** You can obtain pavsig.txt file from the following URL:

http://acs.pandasoftware.com/member/pavsig/pavsig.txt