

Zabbix Monitoring PFSense using Agent

Would you like to learn how to do monitor PFSense using Zabbix? In this tutorial, we are going to show you how to install and configure the Zabbix agent software on a computer running PFSense and how to monitor a PFSense firewall using the Zabbix server.

Hardware List:

- Zabbix server 4.2.6 with IP address: 192.168.15.10
- Pfsense 2.4.4-p3 with IP address: 192.168.15.11

PFSense - Zabbix Agent Installation


First, we need to install the Zabbix agent on the PFSense server.

Open a browser software, enter the IP address of your Pfsense firewall and access web interface.

In our example, the following URL was entered in the Browser:

- <https://192.168.15.11>

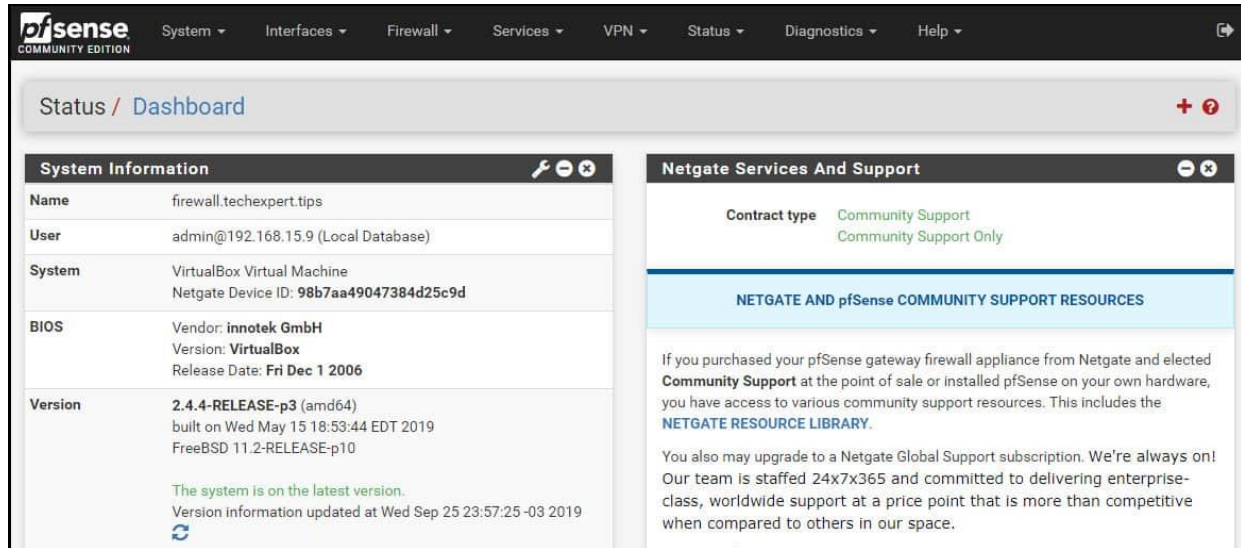
The Pfsense web interface should be presented.



On the prompt screen, enter the Pfsense Default Password login information.

- Username: admin
- Password: pfsense

After a successful login, you will be sent to the Pfsense Dashboard.



Access the Pfsense System menu and select the Package Manager option.



On the package manager screen, access the Available packages tab.

On the Available packages tab, search for zabbix-agent and install the Zabbix agent package.

There are multiple agent versions available, make sure you select the same version of your Zabbix server.

Search

Search term

zabbix-agent

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
zabbix-agent42	1.0.4_2	<p>Zabbix agent is deployed on a monitoring target to actively monitor local resources and applications (hard drives, memory, processor statistics etc). The agent gathers operational information locally and reports data to Zabbix server for further processing. In case of failures (such as a hard disk running full or a crashed service process), Zabbix server can actively alert the administrators of the particular machine that reported the failure. Zabbix is an enterprise-class open source distributed monitoring solution.</p> <p>Package Dependencies:</p> <p>zabbix42-agent-4.2.1</p>	<div>+ Install</div>

In our example, we have a Zabbix server version 4.2.6.

In our example, we installed the Zabbix agent package named: zabbix-agent42

Wait the Zabbix agent installation to finish.

Access the PfSense Services menu and select the Zabbix Agent option.

Services

Auto Config Backup

Captive Portal

DHCP Relay

DHCP Server

DHCPv6 Relay

DHCPv6 Server & RA

DNS Forwarder

DNS Resolver

Dynamic DNS

IGMP Proxy

Load Balancer

NTP

PPPoE Server

SNMP

SNMP (NET-SNMP)

SNMP Trap Daemon (NET-SNMP)

Wake-on-LAN

Zabbix Agent 4.2

On the General tab, enable the Zabbix agent service and perform the following configuration:

- Server - The IP address of the Zabbix server
- ServerActive - The IP address of the Zabbix server
- Hostname - The hostname of the PfSense firewall
- Listen IP - Use 0.0.0.0 to listen on All IP addresses
- Listen Port - Zabbix agent default port 10050

Zabbix Agent Settings	
Enable	<input checked="" type="checkbox"/> Enable Zabbix Agent service.
Server	<input type="text" value="192.168.15.10"/> List of comma delimited IP addresses (or hostnames) of ZABBIX servers.
Server Active	<input type="text" value="192.168.15.10"/> List of comma delimited IP:port (or hostname:port) pairs of Zabbix servers.
Hostname	<input type="text" value="PFSENSE-FIREWALL"/> Unique, case sensitive hostname. Required for active checks and must match the one in the Zabbix server configuration.
Listen IP	<input type="text" value="0.0.0.0"/> Listen IP for connections from the server. (Default: 0.0.0.0 - all interfaces)
Listen Port	<input type="text" value="10050"/> Listen port for connections from the server. (Default: 10050)
Refresh Active Checks	<input type="text" value="120"/> The agent will refresh list of active checks once per this number of seconds.
Timeout	<input type="text" value="3"/> Do not spend more than N seconds on getting requested value. Note: The agent does not kill timeouted User Parameters processes! (Default: 3. Valid range: 1-30)
Buffer Send	<input type="text" value="5"/> Do not keep data longer than N seconds in buffer. (Default: 5. Valid range: 1-3600)
Buffer Size	<input type="text" value="100"/>

On the TLS-RELATED Parameters area, you need to perform the following configuration:

- TLS Connect - PSK
- TLS Accept - PSK
- TLS PSK IDENTITY - key-pfsense-01
- TLS PSK - fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff
(Create your own key)

TLS-RELATED Parameters	
TLS Connect	<div>psk</div> <div>How the agent should connect to server or proxy. Used for active checks. Only one value can be specified: unencrypted - connect without encryption psk - connect using TLS and a pre-shared key cert - connect using TLS and a certificate</div>
TLS Accept	<div>unencrypted psk cert</div> <div>What incoming connections to accept. Multiple values can be specified: unencrypted - connect without encryption psk - connect using TLS and a pre-shared key cert - connect using TLS and a certificate</div>
TLS CA	<div>none</div> <div>Top-level CA certificate for peer certificate verification.</div>
TLS CA System	<input type="checkbox"/> Use the CA certificate list from the operating system. This option overri
TLS CRL	<div>none</div> <div>List of revoked certificates.</div>
TLS Cert	<div>none</div> <div>Agent certificate.</div>
TLS PSK Identity	<div>key-pfsense-01</div> <div>Unique, case sensitive string used to identify the pre-shared key.</div>
TLS PSK	<div>fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff</div>

If you need help to create a PSK key, you may use websites like:

<https://www.browserling.com/tools/random-hex>

After finishing the configuration, click on the Save button on the bottom part of the screen.

In our example, we used the following configuration:

- The Zabbix server has the IP address: 192.168.15.10.
- The PFSense firewall has the IP address: 192.168.15.11.
- The Pfsense firewall hostname is: PFSENSE-FIREWALL
- The PSK Identification key was named: key-pfsense-01
- The communication will be encrypted using the following key:
fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff

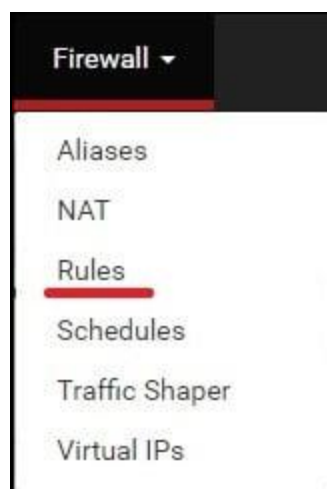
You have successfully installed the PFSense Zabbix agent!

PFSense - Zabbix Firewall Configuration

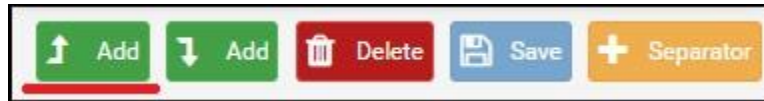
By default, the PFSense firewall does not allow external Zabbix connections to the WAN interface.

In our example we are going to create a firewall rule to allow the Zabbix communication.

Access the Pfsense Firewall menu and select the Rules option.



Click on the Add button to add a rule to the Top of the list.



On the Firewall rule creation screen, perform the following configuration:

- Action - Pass
- Interface - WAN
- Address family - IPV4
- Protocol - TCP

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (...) whereas with block the packet is dropped silently. In either case, the origin	
Disabled	<input type="checkbox"/> Disable this rule
Set this option to disable this rule without removing it from the list.	
Interface	WAN
Choose the interface from which packets must come to match this rule.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	TCP

On the Source configuration screen, you need to define the Zabbix server IP address.

This IP address should be allowed to communicate with the Zabbix agent installed on the PfSense firewall.

In our example, only the computer using the IP address 192.168.15.10 will be able to communicate with the PFsense Zabbix agent.

On the Firewall destination screen, perform the following configuration:

- Destination - Wan address
- Destination port range- From (Other) 10050 to (Other) 10050

On the Firewall Extra options screen, you may enter a description to the firewall rule.

Click on the Save button, you will be sent back to the Firewall configuration screen.

Now, you need to reload the firewall rules to apply the Zabbix communication firewall rule.

Click on the Apply changes button to reload the firewall configuration.

You have finished the PFsense firewall configuration to allow the Zabbix server communication using the WAN interface.

PfSense - Testing the Zabbix Agent Configuration

To test the PfSense Zabbix agent configuration, access the command-line of your Zabbix server.

First, we need to create a file containing the PSK key to encrypt the communication.

Create a temporary PSK key file on the Zabbix server.

Insert the PSK Key previously defined inside this file.

```
touch /tmp/key-pfsense-01
vi /tmp/key-pfsense-01
fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff
```

Use the following command to test the communication between the Zabbix server and the Zabbix agent.

If everything worked, the Zabbix agent should report the agent version installed on the PfSense server.

```
zabbix_get -s 192.168.15.11 -k "agent.version" --tls-connect=psk --tls-psk-identity="key-pfsense-01" --tls-psk-file=/tmp/key-pfsense-01

4.2.1
```

Keep in mind that you need to change the Zabbix agent IP address, the PSK identification name and the PSK key value to reflect your environment.

You have successfully performed a communication test between the Zabbix server and the Zabbix agent installed on the PfSense firewall.

Congratulations!

You have installed the Zabbix agent on a computer running PfSense!

You can now use the Zabbix server dashboard to add this computer to the network monitoring service.

Tutorial - Zabbix Monitoring PFSense

Now, we need to access the Zabbix server dashboard and add the Pfsense server as a Host.

Open your browser and enter the IP address of your web server plus /zabbix.

In our example, the following URL was entered in the Browser:

- <http://192.168.15.10/zabbix>

On the login screen, use the default username and default password.

- Default Username: Admin
- Default Password: zabbix



The image shows the Zabbix login interface. At the top is the ZABBIX logo in a red box. Below it are two input fields: 'Username' and 'Password'. Under the password field is a checkbox labeled 'Remember me for 30 days'. At the bottom is a blue 'Sign in' button. Below the button is the text 'or sign in as guest'.

ZABBIX

Username

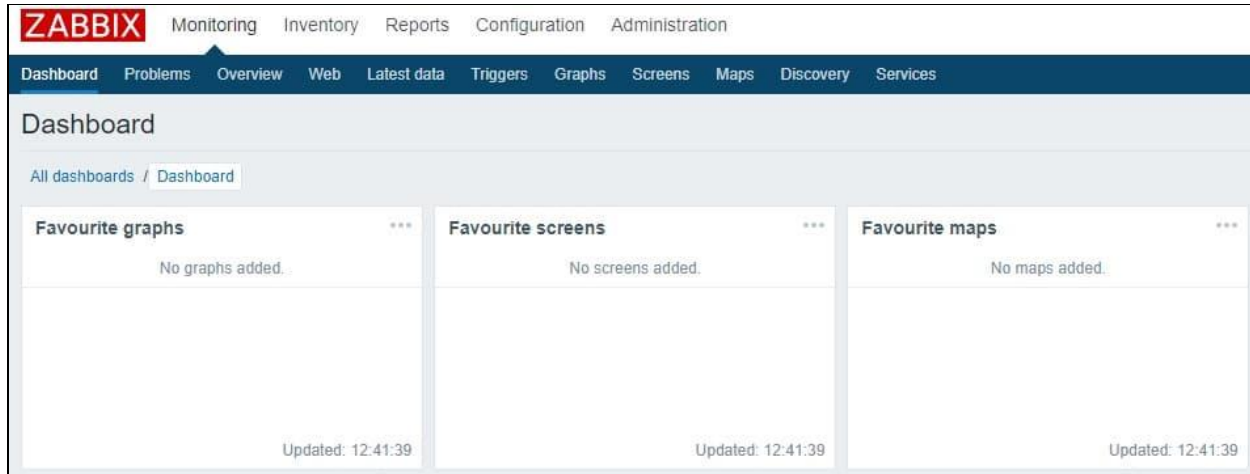
Password

☒ Remember me for 30 days

Sign in

or sign in as guest

After a successful login, you will be sent to the Zabbix Dashboard.



On the dashboard screen, access the Configuration menu and select the Host option.



On the top right of the screen, click on the Create host button.



On the Host configuration screen, you will have to enter the following information:

- Host Name - Enter a Hostname to identify the PFSense server.
- Visible Hostname - Repeat the hostname.
- New group - Enter a name to identify a group of similar devices.
- Agent Interface - Enter the IP address of the PFsesne server.

Here is the original image, before our configuration.

This screenshot shows the Zabbix host configuration page in its default state. The 'Host name' and 'Visible name' fields are empty. The 'Groups' section shows an empty 'In groups' list and a list of 'Other groups' including 'Discovered hosts', 'Hypervisors', 'Linux servers', and various templates. The 'New group' field is highlighted with a green border. The 'Agent interfaces' section contains one entry with IP address '127.0.0.1', DNS name empty, 'Connect to' set to 'IP', 'Port' set to '10050', and 'Default' checked. Below this are sections for 'SNMP interfaces', 'JMX interfaces', and 'IPMI interfaces', each with an 'Add' button.

Here is the new image with our configuration.

This screenshot shows the Zabbix host configuration page after configuration. The 'Host name' and 'Visible name' fields are both filled with 'PFSENSE-FIREWALL'. The 'Groups' section now shows 'Pfsense Firewall (new)' selected in the 'In groups' list, with a 'Select' button next to it. A red asterisk indicates a required field. Below this, a red message states '* At least one interface must exist.' The 'Agent interfaces' section now shows the IP address changed to '192.168.15.11'. The 'SNMP interfaces' section remains empty with an 'Add' button.

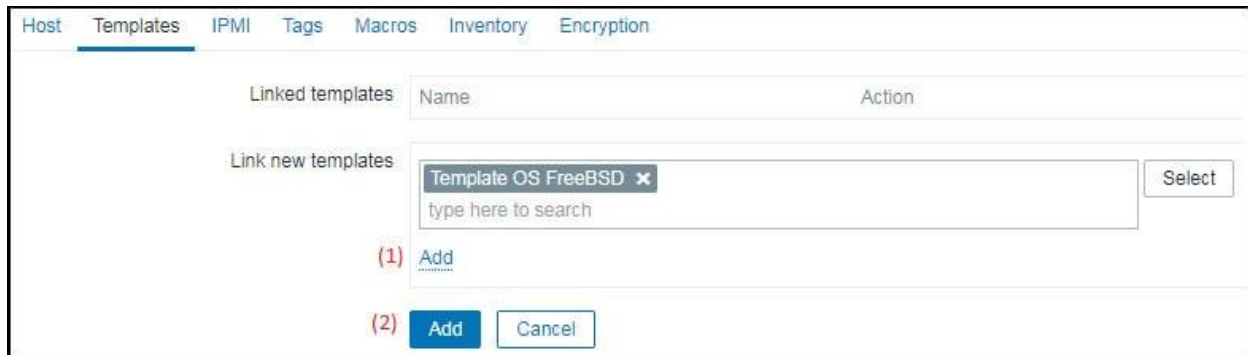
Next, we need to associate the host with a specific network monitor template.

By default, Zabbix comes with a large variety of monitoring templates.

Access the Templates tab on the top of the screen.

Click on the Select button and locate the template named: **Template OS FreeBSD**

Click on the Add option (1).



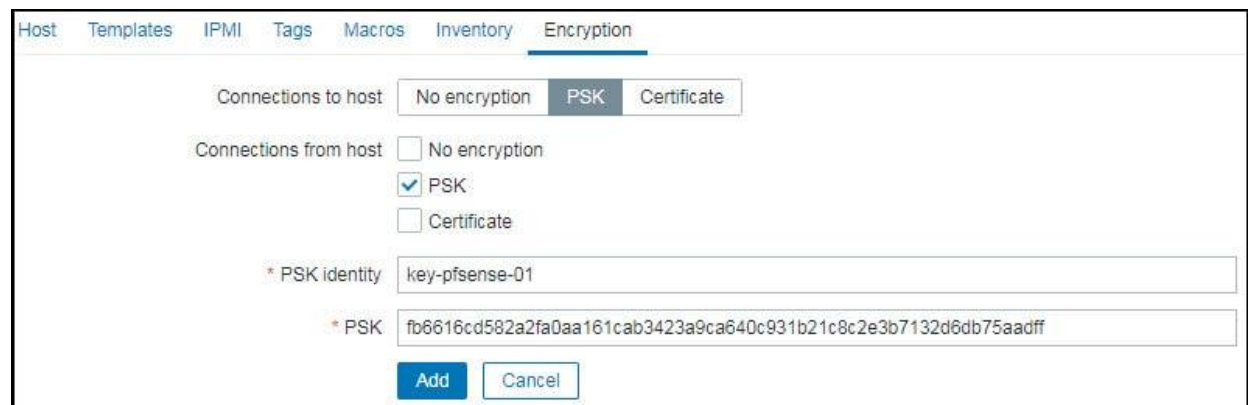
The screenshot shows the Zabbix web interface with the 'Templates' tab selected. In the 'Link new templates' section, a search box contains the text 'Template OS FreeBSD' and a 'Select' button is to its right. Below the search box, there is a red '(1)' next to an 'Add' button. At the bottom of the section, there is a red '(2)' next to 'Add' and 'Cancel' buttons.

Next, we need to encrypt the communication between the Zabbix server and the PfSense firewall.

Access the Encryption tab on the top of the screen and perform the following configuration:

- Connections to host - PSK
- Connections from host - PSK
- PSK identity - key-pfsense-01
- PSK - fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff

Click on the Add button to finish the configuration.



The screenshot shows the Zabbix web interface with the 'Encryption' tab selected. In the 'Connections to host' section, the 'PSK' button is selected. In the 'Connections from host' section, the 'PSK' checkbox is checked. The '* PSK identity' field contains the text 'key-pfsense-01' and the '* PSK' field contains the long hexadecimal string 'fb6616cd582a2fa0aa161cab3423a9ca640c931b21c8c2e3b7132d6db75aadff'. At the bottom, there are 'Add' and 'Cancel' buttons.

After a few minutes, you will be able to see the initial result on the Zabbix Dashboard.

The final result will take at least one hour.

By default, Zabbix will wait 1 hour to discover the number of interfaces available on the Pfsense server.

By default, Zabbix will wait 1 hour before collect information from the network interfaces.

In order to test your configuration, access the Monitoring menu and click on the Graphs option.



On the top right of the screen, select the group named ALL.

Select your PFSense computer host name.

Select the graph named: CPU UTILIZATION

Group Host Graph View as

You should be able to see the graphic of CPU utilization.



Congratulations!

You have configured the Zabbix server to monitor a PFSense computer!

LNC 22082020