Security Gateway Manual

Microsoft Azure

© Copyright 2020 Rubicon Communications LLC

Mar 12, 2020
The pfSense® Firewall/VPN/Router for Microsoft Azure is a stateful firewall, VPN and security appliance. It is suitable for use as a VPN endpoint both for site-to-site VPN tunnels and as a remote access VPN server for mobile devices. Native firewall functionality is available as are many additional features such as bandwidth shaping, intrusion detection, proxying, and more via pfSense packages.

pfSense for Azure is available in the Azure Marketplace.

Getting Started
LAUNCHING AN INSTANCE WITH A SINGLE NIC

An instance of pfSense® for Azure that is created with a single NIC can be used as a VPN endpoint to allow access into a virtual network. These instances can be created in the Azure management portal.

In the Azure Management Portal, launch a new instance of the pfSense firewall and VPN appliance from Netgate®.

1. From the Azure portal Dashboard, click on Marketplace

2. Search for and select the Netgate Appliance for Azure
3. Set the name of the instance, username, password, resource group, and region. The username typically used to administer pfSense is admin, but admin is a reserved name that is not allowed to be set by the Azure provisioning wizard. The username entered will be created as a valid pfSense account upon bringup and will be able to log into the web GUI. Additionally, the admin user will also have it’s password set to the value that’s entered.
4. Choose the instance size.
5. Choose the disc type, and network settings (virtual network, subnet, public IP address, network security group). In order to manage the Netgate pfSense appliance, you should ensure that the security group contains rules to allow ports 22 (SSH) and 443 (HTTPS) to access the command line and Web GUI. If you plan to allow other traffic, you will need to add additional endpoints. For IPsec, you would allow UDP port 500 (IKE) and UDP port 4500 (NAT-T). For OpenVPN, you would allow UDP port 1194. Click on Network security group and make additions as needed.
6. Confirm your selections on the Summary page and click OK. Note the price on the purchase page and click Purchase. Once the VM launches and the Azure portal shows that it has come up, you can access the web interface. Use the password you set during the provisioning process and the admin user. You should now be able to access the appliance.
LAUNCHING AN INSTANCE WITH MULTIPLE NETWORK INTERFACES

An instance of pfSense® for Azure that has multiple NICs that is to be used as a firewall or gateway cannot be provisioned in the Azure portal websites. In order to provision an instance with multiple network interfaces, you must use PowerShell, the Azure CLI, or an ARM template to perform the tasks required.

These procedures are documented in Microsoft’s azure documentation. Some links that illustrate this process:

- Deploy with PowerShell under the classic deployment model
- Deploy with PowerShell under the Resource Manager deployment model
- Deploy with Azure CLI under the Resource Manager deployment model
- Deploy with templates under the Resource Manager deployment model
SUPPORT FOR THE AZURE BOOT DIAGNOSTICS EXTENSION

The Azure Boot Diagnostics extension may not function properly with the pfSense® for Azure appliance from Netgate. Problems were reported with this functionality during certification testing of the appliance. Subsequent testing indicated that it appeared to work under some circumstances. You are free to attempt to enable boot diagnostics, but it is not officially supported.

As such, please do not initiate support calls or tickets if you find that the Boot Diagnostics extension is not functioning properly with your Netgate pfSense for Azure VM. This is a known limitation and no remedy is available from Azure’s customer support team or Netgate’s.

References
FREQUENTLY ASKED QUESTIONS

• 1. Should I set a password or use an SSH key during Azure user provisioning?
• 2. Is a live update of the pfSense software supported?

4.1 1. Should I set a password or use an SSH key during Azure user provisioning?

It is recommended to set a password. This will grant access to the web GUI, whereas an SSH key will only allow you access to the SSH command prompt. Most configuration items in pfSense® are typically controlled via the web GUI. If you accidentally use an SSH key instead, you can select the option to reset the admin password at the text menu that appears when you ssh to your instance. Then the web GUI password will be reset to “pfsense”. You should immediately update the admin password to a more secure value once you have successfully logged into the web GUI.

4.2 2. Is a live update of the pfSense software supported?

Versions in the 2.2.x range should not attempt to have a firmware upgrade executed. In the future (pfSense 2.3 or later), this may be possible, but it is currently untested and unsupported. Since a real system console is not available, a definitive recovery process for failures during upgrades would be difficult to define. The currently recommended process for upgrades is to backup your pfSense config from your existing instance and restore it on a new instance when an upgrade is available.
5.1 Commercial Support

In order to keep prices low, the software is not bundled with a support subscription. For users who need commercial support, Netgate Global Support can be purchased at https://www.netgate.com/support.

5.2 Community Support

Community support for pfSense® software is available through the Netgate Forum.
6.1 Netgate Training

Netgate training offers training courses for increasing your knowledge of pfSense® products and services. Whether you need to maintain or improve the security skills of your staff or offer highly specialized support and improve your customer satisfaction; Netgate training has got you covered.

https://www.netgate.com/training

6.2 Resource Library

To learn more about how to use your pfSense appliance and for other helpful resources, make sure to browse our Resource Library.

https://www.netgate.com/resources

6.3 Professional Services

Support does not cover more complex tasks such as CARP configuration for redundancy on multiple firewalls or circuits, network design, and conversion from other firewalls to pfSense®. These items are offered as professional services and can be purchased and scheduled accordingly.

https://www.netgate.com/our-services/professional-services.html

6.4 Community Options

If you elected not to get a paid support plan, you can find help from the active and knowledgeable pfSense community on our forums.

https://forum.netgate.com/