Security Gateway Manual

Microsoft Azure

Jan 09, 2021

CONTENTS

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.

CHAPTER

ONE

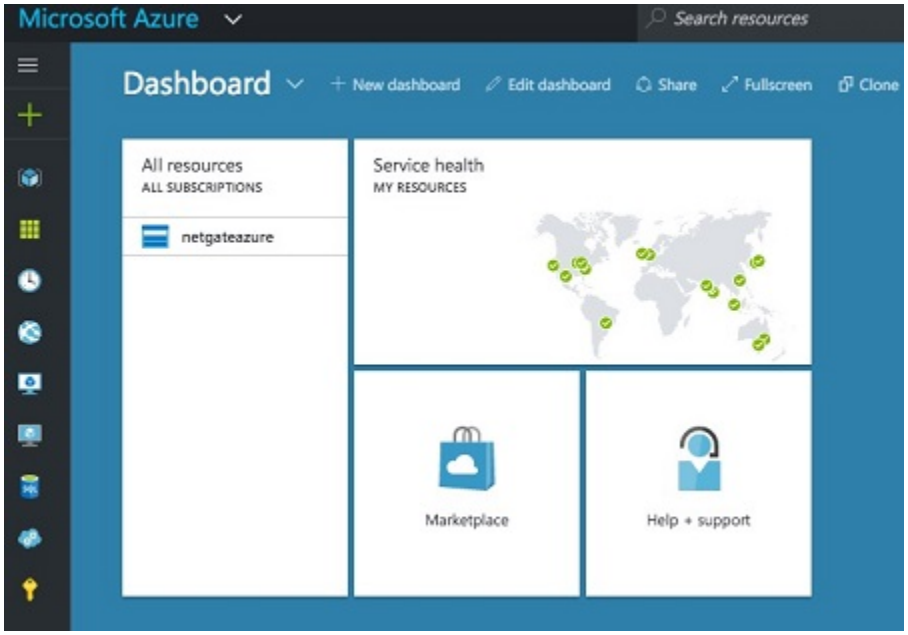
GETTING STARTED

1.1 Launching an Instance with a single NIC

An instance of Netgate® pfSense® for Azure that is created with a single NIC can be used as a VPN endpoint to allow access into an Azure Virtual Network (VNet). The single NIC pfSense virtual machine (VM) only creates a WAN interface, but still provides a public and private IP within Azure.

In the Azure Management Portal, launch a new instance of the Netgate pfSense Firewall/VPN/Router appliance.

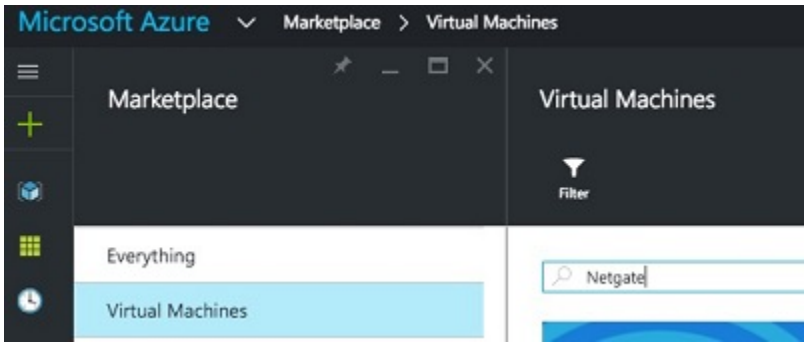
1. From the Azure portal Dashboard, click on **Marketplace**

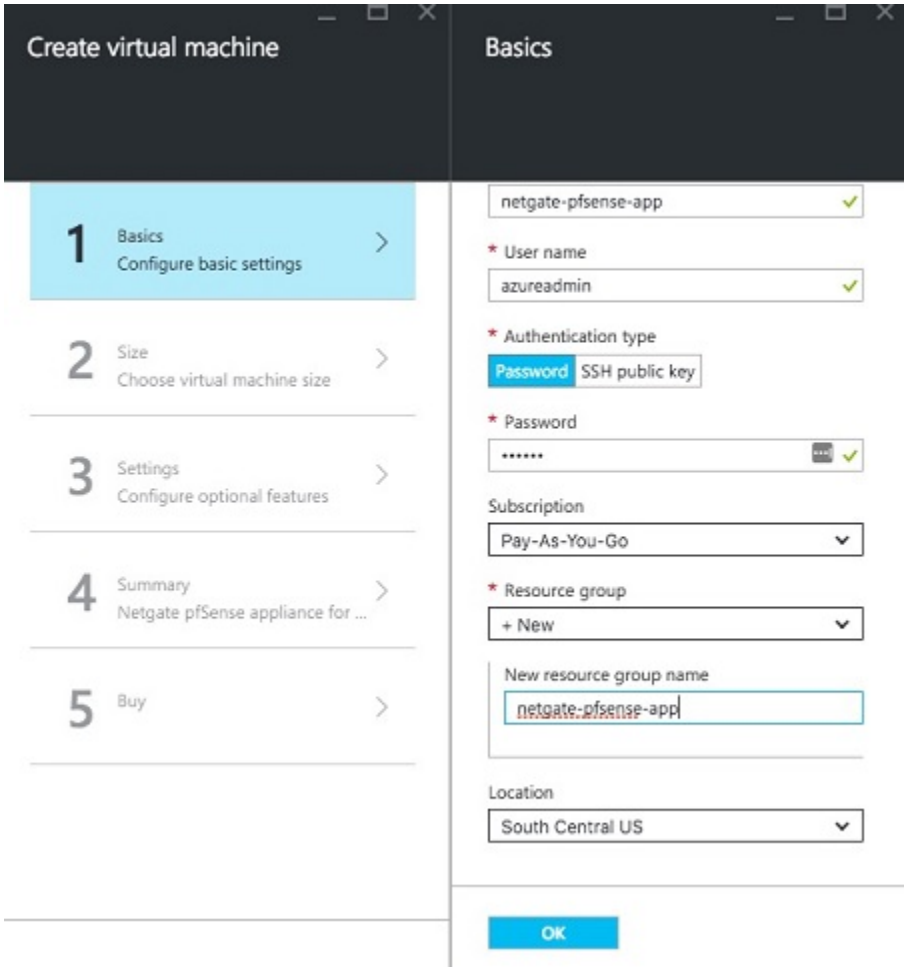


2. Search for and select the **Netgate Appliance for Azure**
3. Set the **name** of the instance as well as **username**, **password**, **resource group**, and **region**.

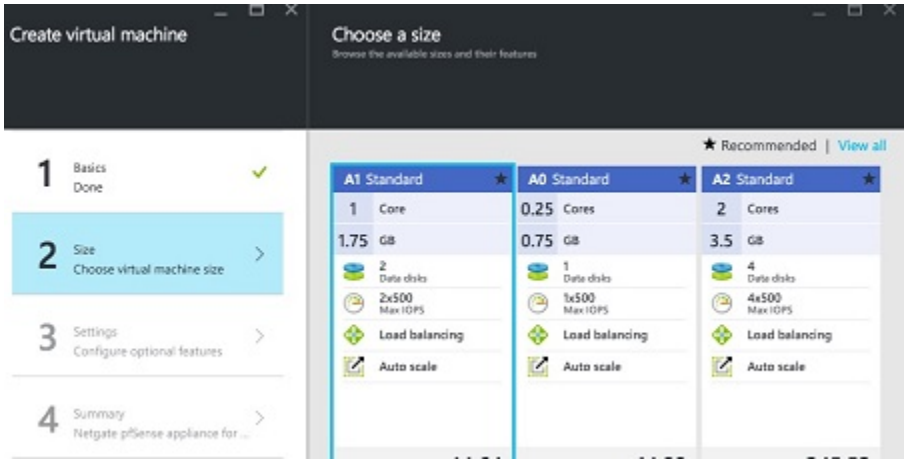
   The username entered will be created as a valid pfSense account upon boot and will be able to log into the webGUI. Additionally, the admin user will also have it's password set to the value that's entered.

> **Warning:** 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. Also for cloud security, it is considered best practice to limit access for the root user, so `root` is locked by default.


Microsoft Azure
Marketplace
Virtual Machines
Marketplace
Virtual Machines
Filter
Everything
Virtual Machines
Netgate


Create virtual machine
Basics
1 Basics
Configure basic settings
2 Size
Choose virtual machine size
3 Settings
Configure optional features
4 Summary
Netgate pfSense appliance for ...
5 Buy
netgate-pfsense-app
* User name
azureadmin
* Authentication type
Password
SSH public key
* Password
Subscription
Pay-As-You-Go
* Resource group
+ New
New resource group name
netgate-pfsense-app
Location
South Central US
OK

4. Choose the **instance size**.



5. Choose the **disc type**, and **network settings** (virtual network, subnet, public IP address, network security group).

   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, add additional endpoints.

   For **IPsec**, allow UDP port `500` (IKE) and UDP port `4500` (NAT-T).

   For **OpenVPN**, allow UDP port `1194`.

   Click on **Network security group** and make additions as needed.

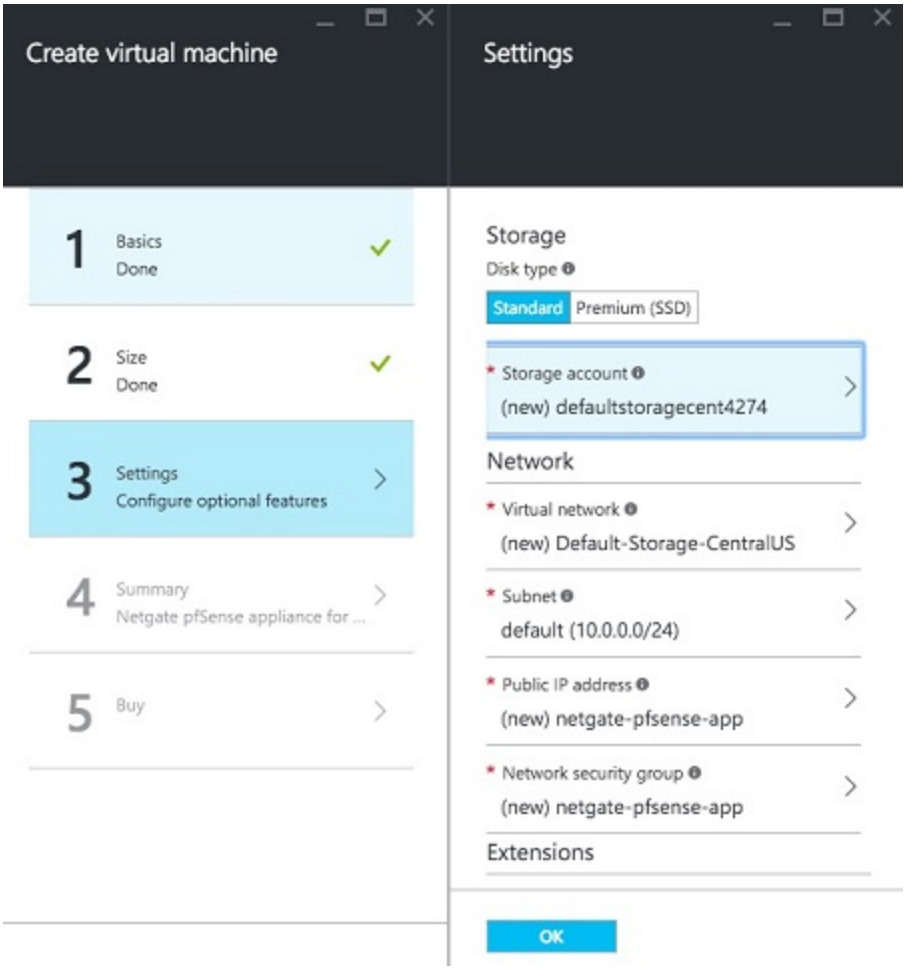
6. Confirm your selections on the Summary page and click **OK**.
7. Note the price on the purchase page and click **Purchase**.
8. Once the VM launches and the Azure portal shows that it has come up, you can access the web interface. Use the password you set during the provisioning process and the admin user. You should now be able to access the appliance.

1.2 Launching an Instance with Multiple Network Interfaces

An instance of Netgate® 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


Create virtual machine
1 Basics
Done
2 Size
Done
3 Settings
Configure optional features
4 Summary
Netgate pfSense appliance for ...
5 Buy
Settings
Storage
Disk type
Standard
Premium (SSD)
* Storage account
(new) defaultstoragecent4274
Network
* Virtual network
(new) Default-Storage-CentralUS
* Subnet
default (10.0.0.0/24)
* Public IP address
(new) netgate-pfsense-app
* Network security group
(new) netgate-pfsense-app
Extensions
OK

1.3 Support for the Azure Boot Diagnostics Extension

The Azure Boot Diagnostics extension may not function properly with the Netgate® pfSense® software for Azure appliance.

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.

CHAPTER

TWO

REFERENCES

2.1 Regional Market Availability

The tables below represent the current availability by regional market. If the desired regional market is not listed, refer to the Microsoft Regions availability or submit a support ticket directly to Microsoft Azure.

Table 1: Microsoft Azure Available Regions

Market	pfSense
Armenia	Available
Australia	*
Austria	Available
Belarus	Available
Belgium	Available
Brazil	Available
Canada	Available
Croatia	Available
Cyprus	Available
Czechia	Available
Denmark	Available
Estonia	Available
Finland	Available
France	Available
Germany	Available
Greece	Available
Hungary	Available
India	Available
Ireland	Available
Italy	Available
Korea	Available
Latvia	Available
Liechtenstein	Available
Lithuania	Available
Luxembourg	Available
Malta	Available
Monaco	Available
Netherlands	Available
New Zealand	Available
Norway	Available

continues on next page

Table 1 – continued from previous page

Market	pfSense
Poland	Available
Portugal	Available
Puerto Rico	Available
Romania	Available
Russia	Available
Saudi Arabia	Available
Serbia	Available
Slovakia	Available
Slovenia	Available
South Africa	Available
Spain	Available
Sweden	Available
Switzerland	Available
Taiwan	Available
Turkey	Available
United Arab Emirates	Available
United Kingdom	Available
United States	Available

* Australia is a Microsoft Managed Country for sales through all customer purchase scenarios except the Enterprise Agreement customer purchase scenario.

2.2 Frequently Asked Questions

2.2.1 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 WebGUI, whereas an SSH key will only allow you access to the SSH command prompt. Most configuration items in Netgate® pfSense® software are typically controlled via the WebGUI. 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 WebGUI 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 WebGUI.

2.2.2 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.

2.3 Support Resources

2.3.1 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.

2.3.2 Community Support

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

2.4 Additional Resources

2.4.1 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

2.4.2 Resource Library

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

https://www.netgate.com/resources

2.4.3 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 software. These items are offered as professional services and can be purchased and scheduled accordingly.

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

2.4.4 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/

