INFOBLOX GUIDE FOR MICROSOFT AZURE SITE-TO-SITE VPN

Infoblox Guide: Site-to-Site VPN for Microsoft Azure
## Contents

Introduction.......................................................................................................................... 3
Prerequisites ............................................................................................................................. 3
Limitations ............................................................................................................................... 3
Concepts .................................................................................................................................. 4
  Introduction to Site-to-Site VPN for Microsoft Azure ......................................................... 4
  pfSense and VPN Basics ..................................................................................................... 4
Setting up the PoC Environment ......................................................................................... 4
  Overview .............................................................................................................................. 4
  Configuring the on-premise environment .......................................................................... 5
    On-premise pfSense .......................................................................................................... 5
  Optional Setup ................................................................................................................... 8
Setting up the PoC Environment in Microsoft Azure ......................................................... 9
  Resource Group .................................................................................................................. 9
  Virtual Network (vNet) and Subnet ................................................................................... 10
  Network Security Group (NSG) ......................................................................................... 11
  Route Table ....................................................................................................................... 12
Deploying pfSense in Microsoft Azure .............................................................................. 13
  Create the pfSense Virtual Machine .............................................................................. 13
  Verify IP Address Configuration ..................................................................................... 19
pfSense in Azure ................................................................................................................ 19
  Connect to the web interface for your pfSense instance ................................................. 19
  Initial Setup ....................................................................................................................... 20
  Enable VPN Tunnel ......................................................................................................... 21
Local (on-prem) pfSense configuration ........................................................................... 24
  Verify the VPN status ....................................................................................................... 26
Guidelines for creating instances in Microsoft Azure .................................................. 26
  The Usage Calculator ....................................................................................................... 26
Additional Resources ......................................................................................................... 26
Introduction

The goal of this document is to provide a guide for creating a VPN connection to a Microsoft Azure vNet. This allows the demonstration of hybrid cloud deployments using vNIOS both in Microsoft Azure and on-premise.

Using a demonstration system in your office, you can deploy a virtual Grid Master. You can then deploy a pfSense virtual machine to act as the VPN endpoint for the on-premise side, deploy a Netgate (pfSense) instance in Microsoft Azure vNet as the other VPN endpoint and create a secure VPN tunnel between them. When this is complete, you can deploy a TE or CP appliance to operate as a grid member or Grid Master Candidate (GMC) in Microsoft Azure, linking it to your Grid Master running in your on-premise environment/network.

This represents a hybrid cloud deployment and can be used for vDiscovery demonstrations and proof of concepts. Figure 1 shows the end state of this procedure.

Prerequisites

You will need the following in order to set this up:

- A virtual cloud environment – This can be a simple ESXi deployment with a vNIOS instance running as a Grid Master
- Version 8.0 – This is something you will need to check on when first deploying. Ideally, the on-premise version should match the version of NIOS for the vNIOS for Azure instance that you are deploying in the Microsoft Azure public cloud. If a version mismatch is detected when joining your vNIOS for Azure instance to your on-premise Grid, it will automatically synchronize the NIOS software from the Grid Master during the join process. This will involve a large data transfer and will affect your data transfer usage, resulting in additional costs.
- A Microsoft Azure account and active subscription – this could be company supplied or a personal account. Services and resources (including any virtual machine (instances), storage and data usage) used in Microsoft Azure have associated costs so it would be advisable to stop instances and delete any storage data when no longer needed.
- Appropriate permissions to create a virtual machine in your vNet (this should be allowed by default when using the base/default account).
- Netgate pfSense Instance image – this is the image used in Microsoft Azure. This can be easily found by searching for “pfsense” in the Azure Marketplace.

Limitations

Operating pfSense in Microsoft Azure will incur a cost which will vary depending on the machine size used, along with data and storage consumption. For lab or testing environments where the VPN tunnel is not required to be operating regularly, you can halt the pfSense instance; however, you should use care to not completely stop it in Azure if using a dynamic public IP address (PIP) as the PIP will change the next time the pfSense instance is started.

If this happens, you would need to reconfigure your VPN tunnel to reflect the new PIP before resuming operations. A static PIP can also be used but you will continue to incur costs on the PIP even while the pfSense instance has been stopped. If you halt pfSense but do not completely stop it in Azure, you will also continue to incur compute costs so you may need to review what may be a more cost effective solution for you (paying for a static PIP or the compute costs for a halted instance).
Concepts

Introduction to Site-to-Site VPN for Microsoft Azure

Microsoft Azure provides its own Virtual Network (vNet) service that any virtual machine instances deployed in Azure will use for network connectivity. These instances will have their own private IP address which can communicate within the vNet or across other vNets if routing is enabled. A public IP address (PIP) can also be assigned to instances to enable connectivity to them across the Internet (assuming that the required rules have been allowed in the Network Security Group assigned to the vNet).

To enable secure connectivity between an on-prem network / data center and your vNets in Azure, administrators will commonly setup a VPN tunnel between their local networks and Azure vNets. For environments hosted in a supporting data center, the Azure Express Routes feature can also be used. Express Routes provide the benefit of being a secure connection, providing better performance and at a reduced cost structure for data transmission into the Azure cloud.

pfSense and VPN Basics

Before implementing pfSense for Azure, an administrator must understand common terms or objects available in Azure related to the implementation of pfSense and the VPN. The following are common objects and terms:

**Resource Group**: A container which holds objects created for any services or applications that you deploy (including virtual machines).

**vNet**: Virtual Network, comparable to a VPC (Virtual Private Cloud) in Amazon AWS, a vNet provides network services for your objects and applications that you may be running in Azure.

**Subnet**: The actual network that any virtual machines and applications would reside on and use for network communications.

**Network Security Group (NSG)**: The object in Azure which allows you to configure firewall rules that will be applied for your subnet(s).

**Express Route**: A dedicated MPLS circuit established between a network operating in a supported data center or ISP and Microsoft Azure. These provide fast and direct connections to the Azure cloud.

Setting up the PoC Environment

Overview

Setting up this environment will be done in 3 steps:

- Configuring on-premise environment – Configure the pfSense router and vNIOS instance in a private cloud at your facility
- Configuring the public cloud environment – Configure a vNet, subnet, Network Security Group, Internet gateways and routing tables. Then deploy the Netgate pfSense instance.
- Configuring the VPN tunnel – Create the secure VPN tunnel between the two pfSense instances.

For more information regarding pfSense, visit https://pfsense.org/.
Configuring the on-premise environment

On-premise pfSense

You can find the pfSense iso at the following URL: https://www.pfsense.org/download/

Download the latest version of the AMD64 “Live CD with Installer” image. At the time of this writing, the image is pfSense-CE-2.3.2-RELEASE-amd64.iso.

1. Place the pfSense ISO in a datastore on your ESXi server.

2. Create a new VM for pfSense. The VM settings for CPU, memory, and disk are not critical for the PoC but ensure your new VM has two network adapters which can be on the same vSwitch. Configure the CD/DVD drive to connect to the iso in the location from step 1 and select the Connect at power on check box. Figure 1 shows the virtual machine properties for the pfSense VM.

![Figure 1](image)

3. Boot the VM and run the installation of pfSense by pressing i at the prompt as shown in figure 2.

![Figure 2](image)
4. Accept the default configuration then select Quick/Easy Install. This will install pfSense on the virtual disk. Select Standard Kernel when prompted. The installer will prompt for a reboot and boot from the virtual disk.

5. When pfSense boots from disk, answer N to the “Do you want to set up VLANs first?” prompt. Enter “vmx0” for the WAN interface, “vmx1” for the LAN interface, then press Enter at the “Optional 1 interface name” prompt. pfSense will then finish its configuration.

6. Use the menu (option 2) to set the LAN interface IP address to an address on your home lab network (Example: 192.168.0.0/23) or the local subnet. This document uses 192.168.0.10/24. Do not set an IPv6 address, enable DHCP, or revert to HTTP at the prompts.

7. On a workstation attached to the same network as the VMware host, open a web browser to the LAN IP. Example: https://192.168.0.10

8. Log in with the default credentials (admin/pfsense). Click Next through the introduction screens.

9. Specify a hostname and DNS server as shown in figure 3. Uncheck the Override DNS checkbox, then click Next.

10. Set your time zone and click Next.

11. Click Next at the Configure WAN Interface page as this interface will be disabled.

12. Check the LAN IP address and click Next.

13. Set a password for the admin user and click Next.

14. Click the Reload button to save the configuration.

15. When the reload completes, click the “Click here to continue on to pfSense webConfigurator” link.

16. Select WAN from the Interfaces dropdown. Deselect the Enable Interface checkbox as shown in figure 4, then click Save.
17. Click the **Apply** changes button.
18. Select **Routing** from the System menu.
19. Click the + icon in the **Gateways** tab to configure the default gateway.
20. As shown in figure 6, select **LAN** from the Interface drop-down box, give the gateway a name, specify the default gateway address for your network, and select the **Default Gateway** checkbox.

21. Click **Save** and when prompted, click **Apply Changes**.
Optional Setup

To help with troubleshooting, it is also recommended to complete the following steps:

1. Click on the pfSense logo in the upper left hand corner of the window to return to the main dashboard.
2. Click + to expand the Available Widgets panel.
3. Add the “Firewall Logs” and “Installed Packages” widgets.

4. Expand the System menu at the top of the page and select Package Manager.

5. Toggle to the Available Packages tab.
6. Scroll down to Open-VM-Tools and click on the Install button.
Setting up the PoC Environment in Microsoft Azure

Resource Group

The Resource Group acts as a container or basket which holds all of the objects that are created for any services or applications that you deploy (including virtual machines). These objects can be placed in a single Resource Group, or in their own individual Resource Groups. For the purposes of this guide, a single Resource Group will be used.

1. Log in to the Azure portal.
2. Expand the toolbar on the left hand side of the page and click More services.
3. In the filter box, type Resource groups and click Resource groups in the search results.

4. Click Add.
5. Enter a descriptive Resource group name.
6. Select the proper Subscription if you have more than available; otherwise, leave this set to the default.
7. Select the Resource group location. This sets the default location where your resources will be deployed from.
8. Click Create.
Figure 10

Virtual Network (vNet) and Subnet

1. In the Azure portal, expand the toolbar on the left hand side of the page and click More services.
2. In the filter box, type Virtual networks and click on Virtual networks in the search results.

Figure 11

3. In the Virtual networks panel, click on the Add button.
4. Enter a descriptive name for the vNet. In this document we will use the name “pfC001-172.18-vnet”. Specify a /16 CIDR block. In this document we will assume you will use 172.18.0.0/16.

Figure 12
5. Enter a descriptive Subnet name (**pfC001-172.18.1-subnet**) and a /24 CIDR subnet block (**172.18.1.0/24**).

6. Select the proper Subscription if you have more than one to choose from; otherwise, leave this set to the default.

7. For Resource group, toggle the radio button to **Use existing** and select the Resource Group that was created in the previous steps. Alternatively, you can create a new Resource Group here as well. Enter a descriptive name if creating a new Resource Group.

8. Select the location where you want to deploy this vNet (or leave set to the default).

9. Click **Create**.

![Network Security Group (NSG)](image)

**Figure 13**

**Network Security Group (NSG)**

1. In the Azure portal, expand the toolbar on the left hand side of the page and click **More services**.

2. In the filter box, type **Network security groups** and click on Network security groups in the search results.

![Network security groups](image)

**Figure 14**

3. Click **Add**.
4. Type a descriptive name.

5. Select the proper Subscription if you have more than one to choose from; otherwise, leave this set to the default.

6. For Resource group, toggle the radio button to **Use existing** and select the Resource Group that was created in the previous steps.

7. Select the location where you want to deploy this vNet (or leave set to the default).

8. Click **Create**.

![Create network security...](image)

**Figure 15**

**Route Table**

1. In the Azure portal, expand the toolbar on the left hand side of the page and click **More services**.

2. In the filter box, type **Route tables** and click on **Route tables** in the search results.

![Route tables](image)

**Figure 16**

3. Click **Add**.
4. Enter a descriptive name
5. Select the proper Subscription if you have more than one to choose from; otherwise, leave this set to the default.
6. For Resource group, toggle the radio button to **Use existing** and select the Resource Group that was created in the previous steps.
7. Select the location where you want to deploy this vNet (or leave set to the default).
8. Click **Create**.

![Create route table](image)

**Figure 17**

Note: Entries in the route table will be added once the pfSense instance has been deployed.

**Deploying pfSense in Microsoft Azure**

**Create the pfSense Virtual Machine**

1. In the Azure Portal, expand the toolbar on the left hand side of the page and click **More services**.
2. In the filter box, type **Marketplace** and click on **Marketplace** in the search results.

![Marketplace search](image)

**Figure 18**

3. In the filter box, type **pfSense for Azure** and press **Enter** or click on the auto-fill text.
4. Click on **pfSense for Azure** from Netgate in the search results.

5. Review the product information and click **Create**.
6. In step 1 (Configure basic settings), enter a descriptive name and a user name (for example: azureadmin). Note: The user name is not applied to the pfSense instance at the time of this writing.
7. Set the **Authentication type** to **Password** and type matching passwords in the two text boxes for the password and password confirmation.

8. Select the proper **Subscription** if you have more than one to choose from; otherwise, leave this set to the default.

9. For **Resource group**, toggle the radio button to **Use existing** and select the Resource Group that was created in the previous steps.

10. Select the location where you want to deploy this VM (or leave set to the default).

11. Click **OK**.

12. In step 2 (Choose virtual machine size), click on the box for the smallest size available for your location (the machine size with the smallest estimated monthly cost).
Note: This will be a smaller machine size than is recommended by the vendor but will be suitable for a lab or testing environment with minimal activity. For environments with higher load or for production use, verify the appropriate machine size to use in order to adequately handle the services that you may be running and expected activity/traffic.

![Choose a size](image)

**Figure 26**

13. Click **Select**.

14. In step 3 (Configure optional features), accept the storage account automatically created for you or create a new one. This must be a premium type storage account.

![Storage](image)

**Figure 27**

15. Under Network, click on the Virtual network bar and make sure that the vNet that you created previously is selected.

16. Click on **Subnet** and verify that the subnet that you created previously is selected.
17. Verify that a new Public IP address is being created as this will be required for connectivity to your on-prem pfSense server.

18. Click on **Network security group (firewall)** and select the NSG that you created previously.

![Network](image)

**Figure 28**

19. Leave the remaining settings default. Click **OK**.

20. Review the Summary screen and verify that all resources assigned correctly. Click **OK**.

![Validation passed](image)

**Figure 29**
21. Review the Purchase information, including pricing and terms of use. Click Purchase to begin the deployment process for your pfSense virtual machine instance. This process may take 3-4 minutes to complete.

![Deployment succeeded](image)

**Figure 30**

**Verify IP Address Configuration**

1. In the Azure Portal, expand the toolbar on the left hand side of the page and click **More services**.
2. In the filter box, type **Virtual machines** and click on **Virtual machines** in the search results.

![Virtual machines](image)

**Figure 31**

3. Click on the name for your pfSense instance

![Virtual machines](image)

**Figure 32**

4. Switch to the Network interfaces panel
5. Take note of the PIP and private IP address. Example:

<table>
<thead>
<tr>
<th>NAME</th>
<th>PUBLIC IP ADDRESS</th>
<th>PRIVATE IP ADDRESS</th>
<th>SECURITY GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>pfco01-vm177</td>
<td>23.99.25.175</td>
<td>172.18.1.4</td>
<td>pfsense-sec-group</td>
</tr>
</tbody>
</table>

**Figure 33**

**pfSense in Azure**

**Connect to the web interface for your pfSense instance**

1. In a new window or tab in your web browser, connect to [https://<PIP>/](https://<PIP>/) (replace `<PIP>` with the public IP address for your pfSense instance. Accept any warnings that may be displayed.
2. Login using the user name **admin** and the password that you specified when creating the pfSense instance.
Initial Setup

Firewall Rules
1. In the pfSense web interface, expand the Firewall menu and select Rules.

![Firewall menu expanded](image)

Figure 34

2. Click on the Delete button (garbage can) for the Port 80 (HTTP) rule. Click OK when prompted.

3. Click Add.

4. In the Protocol drop-down menu, select UDP

5. In the Destination section, set the drop-down menus for Destination port range to (other). In the text boxes, type 1196.

![Destination port range](image)

Figure 35

6. Under Extra Options, enable the check box to log packets that are handled by this rule.

![Extra Options](image)

Figure 36

7. For Description, type "Firewall rule to allow OpenVPN traffic".

8. Click Save.

![Extra Options](image)

Figure 37
9. Click ![Add](https://example.com).  

10. In the **Protocol** drop-down menu, select TCP/UDP.  

11. In the **Destination** section, set the drop-down menus for **Destination port range** to **DNS (53)**.  

12. Under **Extra Options**, enable the check box to **log packets that are handled by this rule**.  

13. For **Description**, type “**Firewall rule to allow DNS traffic**”.  

14. Click **Save**.  

15. Click **Apply Changes**.

![Dashboard Widget – Firewall logs](https://example.com)  

Dashboard Widget – Firewall logs  
1. Click on the pfSense logo to return to the status dashboard.  

2. Click the + icon to add a widget to the main dashboard and select Firewall Logs.  

![Enable VPN Tunnel](https://example.com)  

Enable VPN Tunnel  
1. Expand the VPN menu and select OpenVPN.  

![Figure 38](https://example.com)  

![Figure 39](https://example.com)  

![Figure 40](https://example.com)
2. Toggle to the **Servers** tab and click **Add**.

![Server configuration screen](image1.png)

**Figure 41**

3. In the **Server mode** drop-down menu, select **Peer to Peer (Shared Key)**.

![Server mode options](image2.png)

**Figure 42**

4. Change the **Local port** to **1196**.

![Local port input field](image3.png)

**Figure 43**

5. In the **Description** text box, type “**VPN tunnel to on-premise network**”.

6. Set the **Encryption Algorithm** to **AES-256-CBC (256-bit)** and the **Auth digest algorithm** to **RSA-SHA256 (256-bit)**.

![Cryptographic settings](image4.png)

**Figure 44**
7. As shown in figure 45, type \textbf{192.168.112.0/24} in the \textit{IPv4 Tunnel Network} box and \textbf{192.168.0.0/23} in the \textit{IPv4 Remote Network(s)} box.

![Figure 45]

8. Set \textit{Concurrent connections} to \textbf{1}.

![Figure 46]

9. Click the \textit{Save} button.

10. Click the \textit{Edit Server} (pencil) icon for the VPN server connection that was just created.

![Figure 47]

11. Scroll down to the \textbf{Cryptographic Settings} section and copy all of the text from the \textit{Shared Key} box as shown in figure 48 (the last line will read "-----END OpenVPN Static key V1-----"). Paste this data to a text editor as this will be used later to configure the OpenVPN Client connection on the local (on-prem) pfSense instance.

![Figure 48]
Local (on-prem) pfSense configuration

1. Open a new web browser tab and connect to the web interface for your local pfSense instance as set up earlier (https://192.168.0.10/ in this documentation).

2. Expand the VPN drop-down menu and select OpenVPN.

![Figure 49](image)

3. Toggle to the Clients tab and click Add.

4. Set the Server mode drop-down menu to Peer to Peer (Shared Key) and verify that Interface is set to LAN. Type the PIP for your pfSense for Azure instance in the Server host or address box and change the value for Server port to 1196.

![Figure 50](image)

5. Disable the checkbox for Automatically generate a shared key and paste in the key data that was saved from the steps in the previous section of this guide to the Shared Key box.
Figure 51

6. Set the **Encryption algorithm** drop-down menu to **AES-256-CBC (256-bit)** and the **Auth Digest Algorithm** drop-down menu to **RSA-SHA256**.

Figure 52

7. For **IPv4 Tunnel Network**, type **192.168.112.0/24**. Specify the network address of the Azure pfC001-172.18.1-subnet (**172.18.1.0/24**) subnet in the **IPv4 Remote Network(s)** box.

Figure 53

8. Enable the **Disable IPv6** checkbox and then click **Save**.

Figure 54
Verify the VPN status

9. Select OpenVPN from the Status pulldown. The Status should be "up" as shown in figure 58. The pfSense for Azure instance should also show "up" status.
10. Click the Log icon in the upper right of the status window to open the OpenVPN log. Scroll to the bottom of the log (most recent entries) and verify the "Initialization Sequence Completed" message as shown in figure 59.
11. Add a static route to a workstation on your local network to the 172.18.1.0/24 network via the 192.168.0.10 gateway (the local pfSense instance).
12. Ping the LAN side of the pfSense for Azure instance (172.18.0.10) and ensure you can contact the remote private network.
13. Once you create other instances in the Azure environment, you should be able to ping them from the local workstation with the static route to the Azure environment. Note that no static route is required on the Azure VM instances. When the pfpriv-rt-green route table was created earlier in this procedure a default route was set to the LAN interface on the pfSense for Azure instance. All traffic in the pfC001-priv-green subnet (172.18.0.0/17) will be sent to the pfSense instance for routing.
14. You should be able to ping back and forth between the remote side of pfSense in Azure, 172.18.0.10, and your client. Ping is under the Diagnostics pulldown in pfSense.

Guidelines for creating instances in Microsoft Azure

Once you have the VPN setup you will want to generate multiple instances for multiple scenarios. The following are some general guidelines and best practices to be aware of when creating instances.

The Usage Calculator

Usage is the cost to your account for running instances in Azure. This cost is based on the 4 main components:

- Instance size – The larger the machine size, the higher the costs will be as more vCPU and more vMemory will be consumed.
- Data Storage – This can be one of the easiest ways to have your costs get out of control. In general, always use Magnetic storage when costs are a concern and performance is not as critical (such as when deploying instances for test purposes where load should be minimal). SSD primarily provides read performance and as such, very few applications require it. SSD will generally double your instance costs.
- Network data transfer – This is the lowest of costs and usually not a major factor until you hit the TB of data.
- Any associated objects like elastic IPs – These tend to be very low cost but if you have a lot of them costs can add up.
- Vendor usage costs – These are per hour pricing that are charged for using a vendor’s product from the marketplace. You should always review these before running an instance as it can double or triple the overall cost of running an instance.

Additional Resources

Additional guides, including the Infoblox Installation Guide for Azure, NIOS Administrators Guide, can be found at https://www.infoblox.com/.