Table of Contents

1. Overview ................................................................................................................................................. 2
   1.1 Use Cases .............................................................................................................................................. 2

2. Proofs of Concept and Lab Usage .................................................................................................................. 2
   2.1 General Requirements .............................................................................................................................. 2
   2.2 Solution Overview ................................................................................................................................... 2
       2.2.1 Azure Side ........................................................................................................................................ 2
       2.2.2 On-premises side .............................................................................................................................. 3

3. Azure Side Deployment .................................................................................................................................. 3
   3.1 Post Deployment information gathering ................................................................................................. 6

4. On-Premises Side ........................................................................................................................................... 6
   4.1 On-Premises pfSense Virtual Machine Setup .......................................................................................... 6
       4.1.1 pfSense ISO Download ...................................................................................................................... 7
       4.1.2 Verify VPN Connectivity .................................................................................................................. 23

5. Configuring Zerto Components ...................................................................................................................... 24
   5.1 Configuring ZVM ..................................................................................................................................... 24
   5.2 Configuring VRA’s .................................................................................................................................... 25

6. References ...................................................................................................................................................... 27
1. Overview

This document provides an outline of how to use Zerto Virtual Replication (ZVR) with Azure VPN Gateway service. This guide includes step-by-step instructions on how to configure a pfSense-based IPSec VPN solution to Azure as well as notes on how to configure it with other IPSec compatible devices.

The configuration steps are intended for virtual machine administrators that want to do a quick VPN configuration for a Proof of Concept (POC) or Lab without requiring significant corporate network changes with dedicated networking resources.

1.1 Use Cases

The VPN solution included in this guide allows you to deploy quickly and establish secure connections for testing and lab usage. For production use cases, Zerto recommends using a commercial VPN solution on-premises in combination with the Azure VPN Service.

The target use cases covered in this manual include:

• Proofs of Concept or Labs – Quickly establish a VPN for validation testing.
• Lab Usage – Build ZVR to Azure lab without making any network changes.

2. Proofs of Concept and Lab Usage

For short term functionality testing of ZVR to Azure such as a proof of concept, open source VPNs are a perfect solution. They provide robust performance without having to modify or purchase commercial VPN licenses for limited use, limited duration need.

2.1 General Requirements

The IPSec VPN solution highlighted in this guide requires the following:

1. An Azure subscription - Microsoft offers a free Azure trial subscription that provides everything necessary to do a POC or short-term lab.
2. A hypervisor capable of running pfSense (FreeBSD) in the on-premises side.
3. Available IP addresses for networking components.

The links to the Azure and other trials are in the References sections of this guide.

2.2 Solution Overview

This VPN solution consists of two sides, the Azure side and the on-premises side. The Azure side is delivered as SaaS and the on-premises side is delivered as a virtual machine.

2.2.1 Azure Side
For the Azure side, we will be deploying all needed components via an Azure Deployment Template. It contains all components listed in the diagram below.

The components include:

- A **Linux Virtual Machine** - for test purposes (must be deleted before pairing to on-premises)
- An **Azure Vnet** – a Vnet is like a VLAN. When you create a Vnet you tell azure what subnet you want to use in that VLAN as well
- An **Azure VPN Gateway** – this is the virtual VPN device that will terminate your VPN connection into your Azure Vnet
- An **Azure Gateway public IP** – the IP address that your on-premises VPN device connects to
- A **local gateway configuration object** – this object is just a configuration file so to speak. It contains your on-premises IP address so Azure knows where to connect to

We will deploy the Azure side of our VPN first as the deployment process takes some time, and it will allow us to configure the on-premises side while the Azure side is completed.

### 2.2.2 On-premises side

In this guide, we will use a pfSense virtual appliance to terminate the VPN. However, you could use any IPSec compatible device. More information on other supported VPN devices can be found on the Azure support portal here:


For the pfSense virtual appliance, we will need to create a 1vCPU 1GB RAM virtual machine with two NICs. One public IP address is also required. More on deploying the pfSense virtual appliance is discussed in section 4 of this guide.

### 3. Azure Side Deployment

The quickest way to configure the Azure side is to use an Azure Deployment Template. These templates are available at


Once you navigate to that template click on the Deploy to Azure button.

If you are not already logged into Azure you will be asked to authenticate. If you are already logged in you will see the variables page. On this page, we need to configure all our Azure VPN variables. Keep in mind that if you are new to Azure, most of the settings that have default can be left at those defaults.

We will need to know the following information about your Local Area Network:

- On-Premises Public IP address (ex. 66.102.58.21)
- On-Premises LAN Subnet (ex. 10.10.1.0/24)

The following parameters can be customized by you on the variables page:

- Azure Resource Group (create a new one if you don’t have one)
- Location (where would you like your VM’s to be replicated to)
- LocalGatewayName – just an object name for your on-premises configuration info
- Azure Vnet name – just a name for your Azure “VLAN”/subnet
- Azure Vnet Address prefix – this needs to be a /16 subnet that doesn’t exist on your LAN
- Azure Vnet Subnet – an IP subnet for your VM’s (should be a /24 inside of the subnet listed above)
- Gateway Subnet Prefix – a /29 subnet inside of your VNet Address prefix /16
- Pre-Shared Key (ex. AzureSite2SiteVPN1234567890)

In the screenshot below the settings have been configured for the test environment used in this lab. Many of the settings will need to be customized for your environment so make sure to review each field.
Once you have all the variables configured, click the “I agree” box at the bottom and then click Purchase.

This will start the deployment process. This process takes between 30-45 minutes to complete. You can monitor the process by clicking on the bell icon in the top ribbon and then click on Deployment in progress. This will open the blade (that is what Azure calls the little windows inside its web page) that shows detailed deployment progress. If you scroll to the bottom you will see the Operation details section. This section will list out what is currently being deployed. Deployment is completed when the status in the top section of this blade says complete.

3.1 Post Deployment information gathering

Once the template has been deployed we need to figure out what our Azure VPN Gateway’s public IP address is.

To do this, look for the Azure gateway IP object in the “All resources” blade. Then on the overview section, you will see the public IP address. Write this IP down so that when you are deploying your on-premises appliance you have it.

Once the template has deployed you have finished the Azure side of your configuration.

4. On-Premises Side

pfSense is a powerful firewall distribution, based on FreeBSD, that is created and maintained by Netgate. It is open source and distributed under the Apache 2.0 license. More information on the history of the pfSense project is located here: [https://www.pfsense.org/about-pfsense](https://www.pfsense.org/about-pfsense).

4.1 On-Premises pfSense Virtual Machine Setup
This guide assumes you are using VMware vSphere on-premises, however, the steps can be easily adapted if you are using Microsoft Hyper-V. The goal of this section is to deploy a FreeBSD based virtual machine into your corporate network which will act as a VPN client to the Azure pfSense appliance we just configured in the last section. This on-premises VPN client will also act as the default gateway for your Zerto Virtual Replication (ZVR) components so they can talk to the Azure based ZVR components across the VPN.

4.1.1 pfSense ISO Download

The pfSense ISO image is required to complete this section of the guide. It is available free for download from pfSense.org. Make sure to select “Install” as the file type and “CD Image (ISO) Installer” as the platform.

After downloading the ISO upload it to one of your VMware datastores so that we can select it as the installation ISO in the next section.

4.1.1.1 Deployment Procedure

1. Login to your hypervisor management console and start a new virtual machine deployment wizard. Select “New Virtual Machine.”
2. Name the virtual machine and place it in your virtual infrastructure where appropriate.
3. Once you get to the Guest OS Type, select family type “Other” then select version “FreeBSD (64-bit)”

4. You can customize the basic hardware to include 1 or 2 vCPU’s and 1 or 2 GB of RAM

5. Set the CD/DVD Drive to the pfSense ISO image that you uploaded to a datastore in the previous section

6. Add an additional Network Adapter to the virtual machine for a total of two. Set the top network adapter to a VLAN with access to a public IP address. The second network adapter should be assigned to the port group where you intend to install your ZVM and VRAs.

   Note: If you do not have a port group (such as a DMZ) where you could assign public IP’s to a VM then try putting the first NIC in a port group where you can do Port address translation. Make sure to open the required ports for
IPSec traffic.

7. Click Next and then Finish to create the virtual machine.

8. Power on the virtual machine and wait for it to boot from the ISO image.
9. Once the installer comes up you should accept the console defaults.

10. Select the “Quick/Easy Install” type.
11. Select “OK” on the confirmation screen.

13. Once the installation is completed, select “Reboot”

14. Installation is now complete. Next, we will configure pfSense.

4.1.1.2 pfSense Configuration

In this section, we will configure the on-premises pfSense virtual machine with a static IP address and the required information to form a VPN with our Azure VPN Gateway. When you are finished with this section you will be able to pass traffic between your LAN and the Azure network.

1. On the console of the pfSense virtual machine, you will see the WAN and LAN IP addresses listed. In most cases the LAN IP will default to 192.168.1.1; however, we will need to change that to match whatever subnet your LAN
is. Select option 2 to start this process and follow the prompts.

```plaintext
generating RAD graphs...done.
starting syslog...done.
starting CRON... done.
pfSense (pfSense) 2.3.2-RELEASE amd64 Tue Jul 19 12:41:43 CDT 2016
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (tty0)

*** Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense ***

WAN (wan) → eth0
LAN (lan) → eth1 → v4: 192.168.1.1/24

0) Logout (SSH only)  9) pfTop
1) Assign Interfaces  10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system  14) Enable Secure Shell (sshd)
6) Halt system  15) Restore recent configuration
7) Ping host  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

2. Make sure to say “No” to enable DHCP services as your LAN already has DHCP services running.

```plaintext
2 - LAN (eth1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.254.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
E.g. 255.255.255.0 = 24
     255.255.0.0  = 16
     255.0.0.0   =  8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y

Disabling IPv4 DHCP...Disabling IPv6 DHCP...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```
3. You should now have a LAN IP address listed that you can reach from your web browser.

   https://192.168.254.2/

   Press <ENTER> to continue.

   Welcome to pfSense 2.3.2-RELEASE (amd64 full-install) on pfSense

   WAN (wan)  -> em0  
   LAN (lan)  -> em1  

   0) Logout (SSH only)  
   1) Assign Interfaces  
   2) Set Interface(s) IP address  
   3) Reset webConfigurator password  
   4) Reset to factory defaults  
   5) Reboot system  
   6) Halt system  
   7) Ping host  
   8) Shell

   Enter an option:

   Message from syslogd@pfSense at Aug 9 13:41:55 ...

4. In a web browser navigate to https://<IP address of pfSense VM> and bypass any security warnings to are displayed. You should then see the pfSense login page. The default credentials are admin/pfsense

5. After logging in the initial wizard will start. Click “Next” through the first few pages until you get to the “General Information” screen.
6. The only thing you must customize on the “General Information” page is the primary and secondary DNS servers.

7. On the “Time Server Information” page configure your time zone.
8. On the “Configure WAN Interface” page you can set a static IP address if you have not already done so.

9. The last step is to set the admin WebGUI password. Customize this as needed then click Next.

10. Finally, click the Reload button to apply the changes.

4.1.1.3 IPSec Configuration

Now that pfSense on-premises has been configured, we can configure the OpenVPN Client to connect to our Azure OpenVPN server. Most of the configuration details are the standard settings, but you will need the private SSL key from the Azure pfSense side as well as the public IP address, both of which we documented in during the Azure pfSense virtual appliance deployment.
1. Navigate to the “IPSec configuration” page in the top ribbon. (VPN -> IPSec)

![IPSec configuration page]

2. Click on the “Add P1” button.

3. Set Key Exchange version to IKEv2
   Set the Remote Gateway to the public IP address of your Azure VPN Gateway (documented earlier)

![VPN / IPSec / Tunnels / Edit Phase 1]

4. The “Authentication Method” should be set to “Mutual PSK”, then paste in your Pre-Shared key. (Same one you entered on your Azure Deployment Template)
   Encryption should be set to “AES 256 bit”, the Hash algorithm is “SHA1”, and select “DH Group 2”. Lastly, set
Lifetime to “10800” seconds.

5. The remainder of the settings on the page can be left at their default values. Then click “Save”.

6. Click “Add P2” under the Phase 1 entry you just created.
7. On the General Information section, we need to set the Remote Network to the Azure Vnet ip range. In this example, it was 10.3.1.0/24

![VPN / IPsec / Tunnels / Edit Phase 2](image)

8. The Encryption Algorithm on this page is set to “AES 128-bit”. Hash Algorithm is “SHA1”, PFS key Group is “2 (1024bit)”, and lastly Lifetime is “3600” seconds.

![Phase 2 Proposal (SA/Key Exchange)](image)

9. Click Save
10. You should now have a P1 and P2 entry.

11. The last step is to allow VPN traffic through the pfSense Firewall. To do this click Firewall -> Rules in the top ribbon.

12. Click the “IPSec” tab at the top, then click “Add”.

13. On the new rule page, we want to set the Action to “Pass” on Interface “IPSec”. The Address family is IPv4 and Protocol is “Any”. See the example below, we are allowing any type of traffic over the IPSec Interface.
14. You should now have a rule under IPsec that lists “IPv4 *” as the protocol with asterisks in the other columns.
4.1.2 Verify VPN Connectivity

At this point, both sides of our VPN are configured and the VPN connection are established. This section will walk you through the process of verifying that there is connectivity between sites and that the VPN is passing traffic.

1. From the top ribbon click “Status” then click “IPsec.” The Client Instance Statistics page will appear, and your VPN connection should list the status as “Established.”

![Client Instance Statistics page]

2. If the status is not “Established” click the “Connect” button on the right.

3. Once the VPN status column is in the “established” state, try to ping the Azure side LAN address from the on-premises pfSense console.

4. Select option 7 in the menu “Ping host”, then enter the Azure pfSense virtual appliance internal IP

```
2) Set interface(s) IP address
3) Reset webConfiguration password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option: 7

Enter a host name or IP address: 172.16.100.5

PING 172.16.100.5 (172.16.100.5): 56 data bytes
64 bytes from 172.16.100.5: icmp_seq=0 ttl=64 time=42.217 ms
64 bytes from 172.16.100.5: icmp_seq=1 ttl=64 time=42.217 ms
64 bytes from 172.16.100.5: icmp_seq=2 ttl=64 time=42.217 ms

--- 172.16.100.5 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 42.217/42.217/42.217/0.000 ms
```

Press ENTER to continue.
5. If the address pings, you have a working VPN connection and you are ready to start your Zerto Virtual Replication deployment.

5. Configuring Zerto Components

Now that we have a working VPN connection we can configure the on-premises ZVM and VRA’s to use the on-premises pfSense virtual appliance as its default gateway.

5.1 Configuring ZVM

Once you deploy the Windows virtual machine that ZVM will run on, you must set a static IP address on its NIC. Unlike the rest of your servers on your LAN, you will want to set its default gateway to use the on-premises pfSense virtual appliance. In this guide, we used 10.10.1.66 as the on-premises LAN address for pfSense, so ZVM network connectivity should look like this.

![Internet Protocol Version 4 (TCP/IPv4) Properties](image)

Note that the default gateway has been set to the pfSense appliance IP address, but all other settings should be configured just like any other host on your LAN.

Click “OK” to save the settings then verify that ZVM can get to Azure by running a ping and a traceroute to the Azure pfSense LAN IP.
5.2 Configuring VRAs

The configuration of Zerto VRAs is done from the Zerto GUI after installation of the ZVM software.

1. Login to ZVM
2. Navigate to the Setup tab
3. Click the “New VRA” link on the top right side of the interface
4. When filling out the static IP information set the pfSense LAN IP as the default gateway.
5. Click OK to deploy the VRA.

Note: If you have existing VRAs deployed you can edit their settings and switch the default gateway to the new address and click Save. The changes will take effect after clicking Save.
6. References


Zerto Virtual Replication - https://www.zerto.com/