

Pulse Connect Secure Virtual Appliance on Microsoft Azure

Deployment Guide

Pulse Secure, LLC 2700 Zanker Road, Suite 200 San Jose CA 95134

https://www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Connect Secure Virtual Appliance on Microsoft Azure Cloud - Deployment Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.pulsesecure.net/product-service-policies/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

Revision and Date	Added/Updated /Removed	Remarks
3.1 October 2019	None	Cosmetic changes
3.0 July 2019	Added the " <u>Backing up</u> <u>Configs and Archived</u> <u>Logs on Azure Storage</u> " section. Limitations section is updated.	
2.0 April 2019	Updated FAQ section with Source NATTING feature.	
1.2 March 2019	Updated the "Overview", "Deploying PCS Active- Active Cluster using Virtual Traffic Manager in Microsoft Azure" and "Limitations" sections.	
1.1 December 2018	Added " <u>Deploying PCS</u> <u>Active-Active Cluster using</u> <u>Virtual Traffic Manager in</u> <u>Microsoft Azure</u> " section.	
1.0, September 2018	None	No changes to the document from the previous release.

Table of Contents

Revision History	3
Overview	6
About This Guide	6
Assumptions	6
Pulse Connect Secure on Azure Marketplace	7
Prerequisites and System Requirements on Azure Marketplace	7
Deploying Pulse Connect Secure on Azure Marketplace	7
Basic Configuration	
Network Settings	9
Instance Configuration	10
Summary Step	11
Pulse Connect Secure on Microsoft Azure Cloud	12
Prerequisites and System Requirements on Azure	13
Steps to Deploy Pulse Connect Secure on Azure	13
Upload Pulse Connect Secure Virtual Appliance Image to Azure Web Portal	13
Upload Azure Resource Manager Template to Azure Account	15
Deploying Pulse Connect Secure on Azure using Azure Portal	17
Deploying PCS on New Virtual Network	17
Deployment on VM with Three NIC Cards	17
Deployment on VM with Two NIC Cards	21
Deploying PCS on an Existing Virtual Network	24
Deployment on VM with Three NIC Cards	
Deployment on VM with Two NIC Cards	
Deploying Pulse Connect Secure on Azure using Azure CLI	
Pulse Connect Secure Provisioning Parameters	
Provisioning Pulse Connect Secure with Predefined Configuration	
Configuring Licenses on the Pulse Connect Secure Appliance	
Pulse License Server in Corporate Network	35
Pulse License Server in Cloud Network	
Adding Authentication Code in PCS Admin Console	
Including Authentication Code in ARM Template	
Deploying PCS Active-Active Cluster using Virtual Traffic Manager in Microsoft Azure	
Deploying Two PCS EC2 instances Using ARM Template	
Forming the Active-Active Cluster	
Deploying Virtual Traffic Manager EC2 Instance in the External Subnet of PCS in Microsoft Azure	
Setting Up and Configuring vTM for External Users	
Accessing the Pulse Connect Secure Virtual Appliance	
Accessing the Pulse Connect Secure Virtual Appliance as an Administrator	
Accessing the Pulse Connect Secure Virtual Appliance as an End User	
Accessing the Pulse Connect Secure Virtual Appliance using SSH Console	
On Linux and Mac OSX	49

On Windows	
System Operations	51
Network Configuration	51
IP Address Assignment for Internal, External and Management Interfaces	51
IP Addressing Modes	51
Modifying Network Parameters After Deployment	52
Controlling the Selection of Internal, External and Management Interfaces	52
Backing up Configs and Archived Logs on Azure Storage	54
Configuring Backup Configs and Archived Logs via PCS Admin Console	54
Configuring Backup Configs and Archived Logs via REST	55
Setting Azure as Archive Logs Backup	55
Decommissioning Pulse Connect Secure	55
Delete Entire Resource Group that the Pulse Connect Secure Is In	55
Delete Pulse Connect Secure and Resource It Uses, but not the Other Resources in Resource Group	56
Pricing	57
Limitations	57
Not Qualified	57
Troubleshooting	
Frequently Asked Questions	59
FAQ1: I am unable to connect to my backend resources through L3 VPN	59
Testing the Connection to CentOS System	61
Testing the Connection to On-premise Resource	64
FAQ2: Users are unable to access internet resources when connected to a VPN tunnel on an Azure-bas	ed PCS
Appendix A: Network Security Group (NSG)	66
Appendix B: Pulse Connect Secure Resource Manager Template	70
parameters	70
variables	73
resources	74
outputs	77
Appendix C: Pulse Connect Secure Resource Manager Template for an Existing Virtual Network	78
parameters	78
variables	81
resources	82
outputs	84
References	85
Requesting Technical Support	85

Overview

About This Guide

This guide helps in deploying the Pulse Connect Secure Virtual Appliance on Microsoft Azure. Beginning 9.0R3 release, Pulse Connect Secure is made available in Azure Marketplace. The PCS 9.1R1 image is now available in Azure Marketplace.

This document also describes how a Pulse Connect Secure administrator manually upload the Pulse Connect Secure Virtual Appliance image into Microsoft Azure storage account. And, once the image is available in the Azure storage account, how the Pulse Connect Secure administrator can deploy Pulse Connect Secure on Microsoft Azure.

Assumptions

The basic understanding of deployment models of Pulse Connect Secure on a data center and basic experience in using Microsoft Azure is needed for the better understanding of this guide.

Pulse Connect Secure on Azure Marketplace

Prerequisites and System Requirements on Azure Marketplace

To deploy the Pulse Connect Secure Virtual Appliance on Azure Marketplace, you need the following:

- A Microsoft Azure account
- Access to the Microsoft Azure portal (<u>https://portal.azure.com</u>)
- Pulse Connect Secure licenses *

🕖 Note:

* Pulse Connect Secure Virtual Appliance, by default, has two-users license. This release supports licensing with License server located at corporate network and licensing through Pulse Cloud Licensing Service (PCLS) server. For licensing through PCLS, administrator needs to obtain Authentication Code from Pulse Secure Support and apply it in the Pulse Connect Secure admin console.

🕖 Note: From release 9.0R1 onwards, PCS supports VM with 2-NICs model and 3-NICs model for deployment.

Deploying Pulse Connect Secure on Azure Marketplace

1. Log into Azure portal and navigate to Azure Marketplace by clicking Create a resource.

Figure 1: Marketplace

*	Home > New		
+ Create a resource	New	∎ ×	
· = _ All		A	
All services	♀ Pulse Secure	×	1
	/		4
— 🛧 FAVORITES —————	Azure Marketplace See all Popular		
	reare manacipiade Topular		

2. Search with keyword Pulse Secure.

Figure 2: Published Pulse Secure Images

Home > New > Marketplace > Everythin	ıg			
Marketplace	* ×	Everything		
My Saved List 🧿	<u> </u>	▼ Filter		
Everything	=	Pulse Secure		
Compute		NAME	PUBLISHEK	CATEGORY
Networking		S Pulse Connect Secure - BYOL 2 NIC	Pulse Secure	Compute
Storage		S Pulse Connect Secure - BYOL 3 NIC	Pulse Secure	Compute

Azure Marketplace contains the following two Pulse Connect Secure SKUs:

- Pulse Connect Secure-BYOL 2 NIC
- Pulse Connect Secure BYOL 3 NIC

3. Select **Pulse Connect Secure BYOL 3 NIC** and click **Create**. In this section, 3-NICs model is chosen as example.

Basic Configuration

- 4. In the Basic Configuration step, enter the following parameters and click **OK**:
- VM name: Name of the Pulse Connect Secure to be deployed. Virtual name can be only lowercase letters and numbers, and must be 1-9 characters long.
- **SSH public key**: Copy and paste an RSA public key in the single-line format or the multi-line PEM format. This key is used to access PCS via SSH. The SSH keys are generated using ssh-keygen on Linux and OS X, or PuTTyGen on Windows. For details about generating the SSH key pairs, refer:

For Windows: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows</u> For MacOS and Linux: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys</u>

• **Resource group**: Name of the resource group to be deployed.

Figure 3: Basic Configuration Settings

			onnect Secure - BYOL 3 NIC (Staged) Create Pulse Connect Secu
Creat	te Pulse Connect Secur	e - B 🗡	Basics
1	Basics Configure basic settings	>	* Pulse Connect Secure VM Name demotest ✓
2	Network Settings Configure Virtual Network	>	* SSH public key 1 //DquwQM+Eg2h6OcYw6JjtxyyQ //jcrzU+sGBITAAt8fqWDyujixIXOQB2pBI4sltt rpIKSxG1Kt69MHfH2v4uj6att1Oh3jYrV3Ehu
3	Instance Configuration Configure Instance settings	>	Subscription Visual Studio Premium with MSDN ✓ * Resource group ①
4	Summary Pulse Connect Secure - BYO	> L 3	Create new Use existing demotest
5	Buy	>	South India V
			ОК

Network Settings

- 5. In the Network Settings configuration step, enter the following parameters:
- Virtual Network:
 - Select an existing virtual network from the list or
 - Create a new virtual network. Specify the virtual network name and the address space.

Figure 4: Virtual Network

Create virtual network	
Create virtual network	×
L	
* Name	_
demopcs-vnet	
* Address space	_
10.0.0/16	
10.0.0.0 - 10.0.255.255 (65536 addresses	;)
ОК	

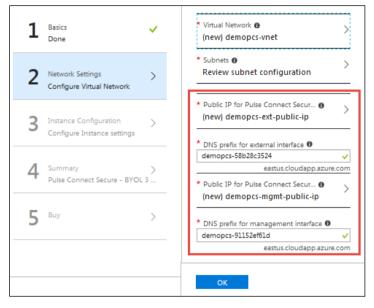
• **Subnets**: Four subnets – external, internal, management and tunnel subnets - are autopopulated with names and address prefix values. Make any changes if required.

Figure 5: Subnets

NIC > Network Settings > Subnets Subnets		
* Internal Subnet name		
InternalSubnet	~	
* Internal Subnet address prefix		
10.0.0/24	~	
* External Subnet name		
ExternalSubnet	~	
* External Subnet address prefix		
10.0.1.0/24	~	
* Management Subnet name		
ManagementSubnet	~	
* Management Subnet address prefix		
10.0.2.0/24	~	
* Tunnel Subnet name		
TunnelSubnet	~	
* Tunnel Subnet address prefix		
10.0.3.0/24	~	
ОК		

 Public IP name and DNS prefix for the External and Management interfaces are autopopulated. Make any changes if required.
 Note that in a 2-NICs model, Public IP name and DNS prefix name for the External and Internal interfaces are auto-populated.

Figure 6: Network Settings



Instance Configuration

- 6. In the Instance Configuration step, enter the following parameters:
- Pulse Connect Secure VM Size: Specify the size of VM. By default, 1x Standard DS3-v2 is set for 3-NICs model and 1x Standard DS2-v2 is set for 2-NICs model.
- Diagnostic storage account: Storage account for the Virtual Machine's diagnostics
- Pulse Connect Secure Config Data: Provisioning parameters in an XML format. Refer the section "<u>Pulse Connect Secure Provisioning Parameters</u>"

 $^{\prime\prime}$ Note: Ensure that the attribute "accept-license-agreement" in pulse-config is set to "y".

Figure 7: Instance Configuration

Create	Pulse Connect Secure -	BY ×	Instance Configuration \square ×
1	Basics Done	~	* Pulse Connect Secure VM Size > 1x Standard DS3 v2
2	Network Settings Done	~	* Diagnostic storage account (new) demopcs7e97996fe4
3	Instance Configuration Configure Instance settings	>	* Pulse Connect Secure Config Data ① <pre><pre><pre><pre><pre><pre><pre><p< th=""></p<></pre></pre></pre></pre></pre></pre></pre>
4	Summary Pulse Connect Secure - BYOL	> 3	
5	Buy	>	
			ок

Summary Step

7. In the Summary step, once the final validation is complete, click **OK**.

Figure 8: Configuration Validation

Create Puls	e Connect Secure - I	вү ×	Summary		
1 Basic	-c		Validation passed		
L Don		`			
			Basics	MSDN Platforms	
			seescheren		
2 Netw	vork Settings	Image: A second seco	2	demopcs	
🗲 Don	e		Location	East US	
			Pulse Connect Secure VM Na	demopcs	
			SSH public key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDCB+jsW6f.	
Insta	nce Configuration				
5 Don	-	×	Network Settings		
Don	e			demopcs-vnet	
				InternalSubnet	
			Internal Subnet address prefix External Subnet	ExternalSubnet	
4	mary	>	External Subnet address prefix		
 Pulse 	e Connect Secure - BYOL 3	3		ManagementSubnet	
			Management Subnet address	-	
			-	TunnelSubnet	
🗖 Buy		>	Tunnel Subnet address prefix		
5			Public IP for Pulse Connect S		
			DNS prefix for external interfa		
			Public IP for Pulse Connect S		
			DNS prefix for management i	demopcs-91152ef61d	
			Instance Configuration		
			Pulse Connect Secure VM Size	Standard DS3 v2	
			Diagnostic storage account	demopcs7e97996fe4	
			Pulse Connect Secure Config	<pulse-config><primary-dns>8.8.8.8</primary-dns><seco.< td=""><td></td></seco.<></pulse-config>	
			OK Download tem	plate and parameters	

8. Finally, in the Terms of Use page, accept the terms and click **Create**.

Create Pulse Connect Secure - B \times	Create 🗖	3
1 Basics	Pulse Connect Secure by Pulse Secure	
L Done	Terms of use privacy policy	
2 Network Settings 🗸	Deploying this template will result in various actions being performed, which may include the deployment of one of more Azure resources or Marketplace offerings and/or transmission of the information you provided as part of the deployment process to one or more parties, as specified in the template. You are responsible for reviewing the text of the template to determine which actions will be performed and which resources or offerings will be deployed,	
3 Instance Configuration	and for locating and reviewing the pricing and legal terms associated with those resources or offerings.	
Done	Current retail prices for Azure resources are set forth here and may not reflect discounts applicable to your Azure subscription.	
4 Summary ✓ Pulse Connect Secure - BYOL 3 NIC	Prices for Marketplace offerings are set forth here, and the legal terms associated with any Marketplace offering may be found in the Azure portal; both are subject to change at any time prior to deployment.	
5 Buy >	Neither subscription credits nor monetary commitment funds may be used to purchase non- Microsoft offerings. These purchases are billed separately. If any Microsoft products are included in a Marketplace offering (e.g., Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.	
	Template deployment is intended for advanced users only. If you are uncertain which actions will be performed by this template, which resources or offerings will be deployed, or what prices or legal terms pertain to those resources or offerings, do not deploy this template.	
	Terms of use	
	By clicking "Create", I (a) agree to the legal terms and privacy statement(a) provided above as well as the legal terms and privacy statement(a) associated with each Marketplace offering that will be deployed using this template, if any; (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(a), including applicable taxes, with the same billing frequency as my Azure abscription, until I discontinue use of the offering(a); and (c) agree that Microsoft may share my contact information and transaction details with any third-party sellers of the offering(a). Microsoft assumes no responsibility for any	
	Create	

Figure 9: Terms of Use

9. Wait for a few minutes while it creates all the resources. This completes deploying PCS on Azure Marketplace.

Figure 10: Deployment in Progress

demopcs							*
Resource group	«	+ Add 📰 Edit columns 🏛 Delete resource group ひ	Refresh 🔿 Move 🏼 🏶 Assign Tag	5			
(Overview	<u>^</u>	Subscription (drange) Subscription ID MSDN Platforms a953001f-92f3-4903-811 Tags (drange)	Deployments a-8de66a9 1 Succeeded				
Activity log		Click here to add tags		â			
🝰 Access control (IAM)				8			
🥒 Tags		Filter by name	All types	~	All locations	~	No grouping
		13 items 🗹 Show hidden types 0					
SETTINGS		NAME 💱		TYPE 14	LOCATION 1		
📣 Quickstart		demopcs		Virtual machine	East US		
Resource costs		demopcs7e97996fe4		Storage account	East US		
📩 Deployments	=	demopos-external-nic		Network interface	East US		
Policies		demopes-external-nsg		Network security grou	p East US		
		demopes-ext-public-ip		Public IP address	East US		
Properties	_	demopes-internal-nic		Network interface	East US		
Locks		demopes-internal-nsg		Network security grou	p East US		
Automation script		demopes-mgmt-nic		Network interface	East US		
MONITORING		demopcs-mgmt-nsg		Network security grou	p East US		
		demopes-mgmt-public-ip		Public IP address	East US		
Matrics		🗌 署 demopes-osdisk		Disk	East US		
👭 Alerts (classic)		demopes-UDR		Route table	East US		
Diagnostics logs		demopcs-vnet		Virtual network	East US		

Note: For L3 connectivity, make sure that "<PCS VM name>-UDR" is properly associated with the subnet where Backend/Protected resources are connected. For example:

- If PCS internal, external and management interfaces are connected to subnet1, subnet2 and subnet3 respectively and Backend/Protected resources are in subnet5, then we need to associate <PCS VM name>-UDR to subnet5.
- If Backend/Protected resources are in Datacenter or in different virtual network, then associate <PCS VM name>-UDR to GatewaySubnet.

Pulse Connect Secure on Microsoft Azure Cloud

As depicted in the below diagram, a remote user can use Pulse Connect Secure to securely access cloud resources as well as corporate resources. To access corporate resources, the Pulse Connect Secure administrator needs to ensure that site-to-site VPN is already established between Azure and corporate network.

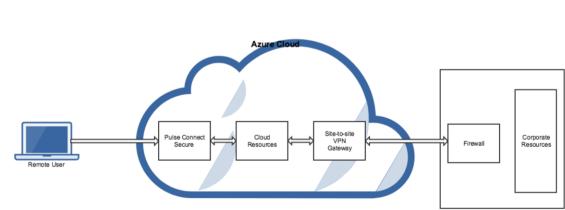


Figure 11: Pulse Connect Secure on Microsoft Azure

Prerequisites and System Requirements on Azure

To deploy the Pulse Connect Secure Virtual Appliance on Azure, you need the following:

- A Microsoft Azure account
- Access to the Microsoft Azure portal (https://portal.azure.com)*
- Pulse Connect Secure Virtual Appliance Image (.vhd file)
- Azure Resource Manager template (ARM template)
- Pulse Connect Secure licenses **
- Site-to-Site VPN between Azure and the corporate network (optional)

 $rac{1}{2}$ Note: This is needed only if the Pulse Connect Secure users need to access corporate resources.

- Pulse License Server (optional)**
 - Located at corporate network, accessible through site-to-site VPN
- Pulse Connect Secure configuration in XML format (optional)
- The following systems are qualified in 9.0R1 release:
 - DS2 2-core
 - DS3 4-core
 - DS4 8-core

🕖 Note:

* Pulse Connect Secure Virtual Appliance can be deployed only through Azure Resource Manager (ARM) style. It does not support deployment in classic style.

** Pulse Connect Secure Virtual Appliance, by default, has two-users license. This release supports licensing with License server located at corporate network and licensing through Pulse Cloud Licensing Service (PCLS) server. For licensing through PCLS, administrator needs to obtain Authentication Code from Pulse Secure Support and apply it in the Pulse Connect Secure admin console.

🕖 Note: From release 9.0R1 onwards, PCS supports VM with 2-NICs model and 3-NICs model for deployment.

Steps to Deploy Pulse Connect Secure on Azure

Below are the one-time activities to be followed to deploy Pulse Connect Secure on Azure.

- Upload Pulse Connect Secure Virtual Appliance Image to Azure Web Portal
- Upload Azure Resource Manager Template to Azure Account

Below are the steps to be followed for each deployment of Pulse Connect Secure.

- Deploying Pulse Connect Secure on Azure using Azure Portal
- Deploying Pulse Connect Secure on Azure using Azure CLI

Upload Pulse Connect Secure Virtual Appliance Image to Azure Web Portal

This section shows the steps to upload the Pulse Connect Secure Virtual Appliance image to Azure web portal. To upload Pulse Connect Secure Virtual Appliance image to Azure web portal, do the following:

- 1. Visit the Pulse Secure support site <u>www.pulsesecure.net</u> and download the Azure PCS image file (**ps-pcs**azure-psa-v-<releaseno>-<buildno>-package.zip) which is in the zipped format.
- 2. Unzip the file and look for the Pulse Connect Secure Virtual Appliance vhd image.
- 3. Log in to the Azure portal.

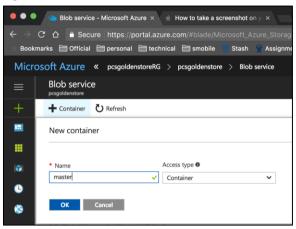
4. Click **New** and create a storage account named 'pcsgoldenstore' under the resource group named 'pcsgoldenstoreRG'.

Figure 12:	Storage Accou	nt - pcsgoldenstore



5. Inside the pcsgoldenstore storage account, click on **Blobs** and create a container with access type as 'Container' named 'master'.

Figure 13: Container master



6. Inside the 'master' blob, click on **upload** to upload the Pulse Connect Secure Virtual Appliance image. Inside the 'Upload blob', select the Blob type as Page blob and click on **Upload**.

Figure 14: Upload Pulse Connect Secure Virtual Appliance Image

-	-			
👼 / 🍝	Upload blob - Microsoft 🛛 🗙 🔽			_ 0 X
\leftrightarrow \Rightarrow \diamond	Carter Attps://portal.azure.com			4d-a770-15457f592e7a%2FresourceGroups%2Fpcsgoldenstr 🛠 🧿
Micros	soft Azure « posgoldenstore >	Blob servi	ice > master > Upload blob P Search resources ×	LP >_ 🚳 😳 🕐 johnavali sesteure (defa.
=	Blob service	×х	master 1	Upload blob 3
+	+ Container 💍 Refresh		🐺 Upload 🖉 efresh 🗴 Delete container 🗄 Properties 🏓 Access policy	* Files 0
	Essentials 👻		Location: master	"VA-SPE-SA-58109.1-SERIAL-hyperv.vhd"
	, Search containers by prefix		, Search blobs by prefix (case-sensitive)	
	NAME		NAME	Blob type Page blob
٩	master		No blobs found.	Upload .vhd files as page blobs (recommended)
8				Block size 4 MB
<u>.</u>				4 MB
8				Upload 5

Upload Azure Resource Manager Template to Azure Account

The Azure Resource Manager (ARM) template is a JSON-based file, which has instructions for Azure Fabric on all the resources that need to be created on Azure while running this script. More details on the ARM template can be found at https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-create-first-template.

Pulse Secure provides two sample Azure template files each for three NIC cards and two NIC cards, namely "pulsesecure-pcs-3-nics.zip" and "pulsesecure-pcs-3-nics-existing-vnet.zip", and "pulsesecure-pcs-2-nics.zip" and "pulsesecure-pcs-2-nics-existing-vnet.zip". Users can modify the template to make it suitable for their need. Here are the steps to upload the template to Azure Portal.

- 1. Unzip the pulsesecure-pcs-3-nics.zip file / pulsesecure-pcs-2-nics.zip file to get azuredeploy.json.
- 2. Log in to the Azure portal.
- 3. Click on More services and select Templates.

Figure 15: Templates

Microsoft Azure Resource	groups	Ъ Ф	>_	ŝ	:	?	skindlay.a@pulsesecur PULSE SECURE, LLC
≡		Shi	t+Space t	o togale	e favorite	×	* ×
+ New							
🚸 Azure Active Directory 🔷	By category ~				*	^	✓ No grouping ✓
🕒 Monitor	 Service Health 			PREV	/IEW 🤺		
🗣 Advisor	I Tags				*		
Security Center	Templates			PREV	/IEW 🔺		
8 Billing	Time Series Insights	environments		PREV	/iew 🤺		
Pelp + support	∃ Time Series Insights	event sources		PREV	/iew 🤺	~	~
More services >	_	<u>Help im</u>	prove the	e servio	e meni	<u>11</u>	

4. In the Templates page, click **Add** to add template.

Figure 1	Figure 16: Add Template									
Micro	osoft Azure Templates	୍ନ ପ ≻_ 🀯 🤅) (?) :xkrx;Liyu;@pulsesecur PULSE SECURE, LLC							
	Templates Pulse Secure, LLC - PREVIEW		* ×							
+	➡ Add == Columns ひ Refresh									
•	Directory: Pulse Secure, LLC		^							
0		All locations	Vo grouping							
	0 items									
•	·									
0										
2		JSON	~							
>										

5. Provide a suitable name and description for the template.

Figure 17: Template – General Information

General $ ho$ Se		resources	×	Ċ,	>_	្ដែរ	\odot	0	julius annu
Add template	□ ×	General						I	×
* General Add general information • ARM Template Add template	>	* Name TestPCSDeploy * Description Testing PCS Deployment							٤ د
ADU		on Google chrome							

6. Copy the contents of **azuredeploy.json** and paste it in the template section.

Figure 18: Add ARM Template

ARM Template	>> Search re	sources	× \$ > \$ 0 0
Add template	□ ×	ARM Template	□ ×
* General TestPCSDeploy	>	1	1
* ARM Template Add template	>		
Add		OK Google Chrome	

Deploying Pulse Connect Secure on Azure using Azure Portal

Before proceeding with the deployment, refer the following sections:

- Upload Pulse Connect Secure Virtual Appliance Image to Azure
- Upload Azure Resource Manager Template to Azure Account

Pulse Connect Secure can be deployed on:

- <u>a new Virtual network</u> or
- an already existing Virtual network

Deploying PCS on New Virtual Network

This section describes deployment with three NIC cards and two NIC cards.

Deployment on VM with Three NIC Cards

To deploy PCS on Azure using the Azure portal, do the following:

1. Select the template file created in section 'Upload Azure Resource Manager Template to Azure account' and click **Deploy**.

Note: Before proceeding with deployment, ensure that the attribute "accept-license-agreement" in pulse-config is set to "y".

/licro	osoft Azure Templates > t	estpcsdeploy >	Custom deployment	
≡	testpcsdeploy Template - PREVIEW	* 🗆 X	Custom deployment Deploy from a custom template	
F	🖆 Deploy 🖍 Edit	••• More		
-	DESCRIPTION		TEMPLATE	
	Testing PCS Deployment		11 resources	Edit template Edit parame Learn more
	PUBLISHER		BASICS	
	orman@pulsesecure.net		* Subscription	Visual Studio Enterprise with MSDN
3	MODIFIED		* Resource group	Create new Use existing
2	8/4/2017		instance group	TestPCSDeploymentRG
	View Template		the section	
3	view remplate		* Location	Central US V
			SETTINGS	
			PCS Storage Account Name 🛛	pcsgoldenstorage
			PCS Storage Account Resource Group Name 🛛	GoldenImageRG
			PCS Image Location URI	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure.vhd
			PCSVM Name	PCSAzureVA
			PCS Config 🖲	<pulse-config><primary-dns>8.8.8.8</primary-dns><secondary-dns>88.8.9</secondary-dns></pulse-config>
			* SSH Public Key	
			Dns Label Prefix Ext	mycloudpcsext
			Dns Label Prefix Mgmt 🛛	mycloudpcsmgmt
			Vnet Address Space 0	10.20.0.0/16
			Internal Subnet 🖲	10.20.1.0/24
			External Subnet	10.20.2.0/24
			Management Subnet	10.20.3.0/24
			Tunnel Subnet 🛛	10.20.4.0/24
			TERMS AND CONDITIONS	
			Pin to dashboard	
			Purchase	

Figure 19: Custom Deployment on VM with Three NIC Cards – New Virtual Network

- 2. Fill or modify the following parameters:
 - **Resource group:** Specify the resource group name in which Pulse Connect Secure needs to be deployed
 - Location: Region where resource group needs to be created
 - **PCS Storage Account Name:** Storage account name where the Pulse Connect Secure Virtual Appliance image is available
 - **PCS Storage Account Resource Group:** Resource group of where the Pulse Connect Secure Virtual Appliance image is copied
 - PCS Image Location URI: URI to Pulse Connect Secure Virtual Appliance Image
 - PCSVM Name: Name of the Pulse Connect Secure Virtual instance
 - **PCS Config:** Provisioning parameters in an XML format. Refer the section '<u>Pulse Connect Secure</u> <u>Provisioning Parameters</u>'
 - SSH Public Key: This key is used to access PCS via SSH. The SSH keys are generated using ssh-keygen on Linux and OS X, or PuTTyGen on Windows. For details about generating the SSH key pairs, refer:

For Windows: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows</u> For MacOS and Linux: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys</u>

- DNS Label Prefix Ext: Prefix for the external interface DNS label
- DNS Label Prefix Mgmt: Prefix for the management interface DNS label
- Vnet Address Space: Virtual network address space
- Internal Subnet: Subnet from which Pulse Connect Secure internal interface needs to lease IP
- External Subnet: Subnet from which Pulse Connect Secure external interface needs to lease IP
- Management Subnet: Subnet from which Pulse Connect Secure management interface needs to lease IP
- **Tunnel Subnet:** Subnet which will be configured as tunnel IP pool in the Pulse Connect Secure VPN Profile
- 3. Agree to the Azure licensing terms and click **Purchase**.
- 4. Watch for the deployment succeeded message after 3 to 5 minutes.

Figure 20: Deployment Succeeded

:	TestPCSDeploymentRG				* ×
		$+$ Add $\equiv \equiv$ Columns \equiv Delete \circlearrowright Refresh \rightarrow	Move		
	(n) Overview	Essentials ^ Subscription name (change) Visual Studio Premium with MSDN	Deployments 1 Succeeded		
	Activity log Access control (IAM)	Subscription ID + 7 activities - 1094 - 40494 - 11172 - data - 2 that Demot	1 Succeded		
	Tags	Filter by name All types	✓ All locations	✓ No grouping	~
	SETTINGS	11 items NAME V	Type $$	location \vee	
	🕰 Quickstart	Backend2PCSRoute	Route table	South India	
	Resource costs	NSGExternalSubnet	Network security group	South India	
	Deployments	NSGInternalSubnet	Network security group	South India	
	Policies	-			
	Properties	VSGManagementSubnet	Network security group	South India	
	Locks	PCSAzureVA	Virtual machine	South India	
	Automation script	PCSExternalNIC	Network interface	South India	
	Mutomation script	PCSExternalPublicIP	Public IP address	South India	
	MONITORING	PCSInternalNIC	Network interface	South India	
	iii Metrics	PCSManagementPublicIP	Public IP address	South India	

- 5. Go to the resource group in which the Pulse Connect Secure Virtual Appliance was deployed to see the resources created.
- 6. Navigate to the resource group and click **PCS Management Public IP**. Make a note of the PCS Management Public IP and DNS name (FQDN) to access PCS for admin page.

Figure 21: PCS Management Public IP											
Micr	rosoft Azure « TestPCSDeploymentRC	5 PCSManagementPublicIP	,⊅ Search resources	×	Q	>_	ŝ	٢	0		
+	, Search (Ctrl+/)		Delete								
	Overview	Essentials A Resource group (change)		IP address					<u> </u>		
	Activity log	TestPCSDeploymentRG Location		13.71.121.15 DNS name							
	Access control (IAM)	South India Subscription name (change)	l	mycloudpcsmgmt.sou Associated to	thindia.	cloudap	op.azure	e.com	J		
٢	🛷 Tags	Visual Studio Premium with MSDN Subscription ID		PCSMangementNIC Virtual machine PCSAzureVA							
8	SETTINGS	 Heritate - The mode after any staged bases 		PCSAZUREVA							
*	Configuration										
* 	Properties										
	Locks Automation script										
*											
 ↔	SUPPORT + TROUBLESHOOTING										
- × /	Terr subbristed age										

7. Click PCS External Public IP and note down the PCS External Public IP and DNS name (FQDN) to access PCS for end user page.

Figure 22: PCS External Public IP

Micro	osoft Azure Resource groups	TestPCSDeploymentRG PCSExternalPublicIP	O Search resources	×	û ≻ 🐯	0				
≡	PCSExternalPublicIP									
+	Search (Ctrl+/)		Delete							
	Overview	Essentials ^								
	Activity log	Resource group (change) TestPCSDeploymentRG Location	(IP address 13.71.127.197 DNS name						
	Access control (IAM)	South India Subscription name (change)	l	mycloudpcsext.southindia.cloudapp.azure.com						
۲	🛷 Tags	Visual Studio Premium with MSDN Subscription ID		PCSExternalNIC Virtual machine						
8	SETTINGS	c hourists - this altant drift dath diffastitione		PCSAzureVA						
e	Configuration									
100	Properties									
•	Locks	_								
-	😃 Automation script									

🕖 Note: Azure allows static as well as dynamic assignment of IP addresses to the network interfaces. The mode of IP assignment (static/dynamic) can be mentioned in the Azure Resource Manage template file. The current JSON template uses the dynamic method of allotting IP addresses to the network interfaces.

Deployment on VM with Two NIC Cards

To deploy Pulse Connect Secure on Azure using the Azure portal, do the following:

1. Select the template file created in section 'Upload Azure Resource Manager Template to Azure account' and click **Deploy**.

Note: Before proceeding with deployment, ensure that the attribute "accept-license-agreement" in pulse-config is set to "y".

Figure 23: Custom Deployment on VM with Two NIC Cards – New Virtual Network

Micro	soft Azure Templates > testp	csdeploy >	Custom deployment	
	testpcsdeploy Template - PREVIEW	* ¤ ×	Custom deployment Deploy from a custom template	
+	📫 Deploy 💉 Edit	••• More		
	DESCRIPTION		TEMPLATE	
	Testing PCS Deployment		11 resources	Edit template Edit parame Learn more
٢	PUBLISHER		BASICS	
3	johnav@pulsesecure.net	1		
0	MODIFIED		* Subscription	Visual Studio Enterprise with MSDN
Q	8/4/2017		* Resource group	Create new Use existing
				TestPCSDeploymentRG 🗸
	View Template		* Location	Central US V
8			SETTINGS	
*			PCS Storage Account Name	pcsgoldenstorage
<u>a</u>			PCS Storage Account Resource Group Name 0	GoldenImageRG
			PCS Image Location URI 0	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure.vhd
-			PCSVM Name	PCSAzureVA
			PCS Config 0	<pulse-config> <primary-dns>8.8.8.8 </primary-dns> <secondary-dns>8.</secondary-dns></pulse-config>
			* SSH Public Key 🛛	
•			Dns Label Prefix Ext 🖲	mycloudpicsext
0			Vnet Address Space 🛛	10.20.0.0/16
			Internal Subnet 🖲	10.20.1.0/24
•			External Subnet O	10.20.2.0/24
0			Tunnel Subnet 🛛	10.20.4.0/24
2				
•			Pin to dashboard	
>			Purchase	

- 2. Fill or modify the following parameters:
 - **Resource group:** Specify the resource group name in which Pulse Connect Secure needs to be deployed
 - Location: Region where resource group needs to be created
 - **PCS Storage Account Name:** Storage account name where the Pulse Connect Secure Virtual Appliance image is available
 - PCS Storage Account Resource Group: Resource group of where the Pulse Connect Secure Virtual Appliance image is copied
 - PCS Image Location URI: URI to Pulse Connect Secure Virtual Appliance Image
 - PCSVM Name: Name of the Pulse Connect Secure Virtual instance

- **PCS Config:** Provisioning parameters in an XML format. Refer the section '<u>Pulse Connect Secure</u> <u>Provisioning Parameters</u>'
- SSH Public Key: This key is used to access PCS via SSH. The SSH keys are generated using ssh-keygen on Linux and OS X, or PuTTyGen on Windows. For details about generating the SSH key pairs, refer:

For Windows: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows</u> For MacOS and Linux: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-kevs</u>

- DNS Label Prefix Ext: Prefix for the external interface DNS label
- Vnet Address Space: Virtual network address space
- Internal Subnet: Subnet from which Pulse Connect Secure internal interface needs to lease IP
- External Subnet: Subnet from which Pulse Connect Secure external interface needs to lease IP
- **Tunnel Subnet:** Subnet which will be configured as tunnel IP pool in the Pulse Connect Secure VPN Profile
- 3. Agree to the Azure licensing terms and click **Purchase**.
- 4. Watch for the deployment succeeded message after 3 to 5 minutes.

Figure 24: Deployment Succeeded

				* ×
, Search (Ctrl+/)	of the test of te	Move		
(in) Overview	Essentials ^ Subscription name (change)	Deployments		
Activity log	Visual Studio Premium with MSDN Subscription ID	1 Succeeded		
🚔 Access control (IAM)	s Tanfallis s 198-4948-9175 dails Elbertheor			
🥔 Tags	Fifter by name All types	✓ All locations	✓ No grouping	~
SETTINGS	11 items NAME ∽	түре 🗸	LOCATION V	
📣 Quickstart	Backend2PCSRoute	Route table	South India	
 Resource costs 	SGExternalSubnet	Network security group	South India	
Deployments	NSGInternalSubnet		South India	
Policies		Network security group		
Properties	PCSAzureVA	Virtual machine	South India	
Locks	PCSExternalNIC	Network interface	South India	
Automation script	PCSExternalPublicIP	Public IP address	South India	•••
- conversion average	PCSInternalNIC	Network interface	South India	

5. Go to the resource group in which the Pulse Connect Secure Virtual Appliance was deployed to see the resources created.

6. Click **PCS External Public IP** and note down the **PCS External Public IP and DNS name (FQDN)** to access PCS for end user page.

Micros	soft Azure Resource groups	TestPCSDeploymentRG PCSExternalPublicIP P Search resources	× ↓ >_ 🕸 😳 🗿			
	PCSExternalPublicIP Public IP address					
+	Search (Ctrl+/)					
	Cverview	Essentials	IP address			
	Activity log	Resource group (dwnge) TestPCSDeploymentRG Location	13.71.127.197 DNS name			
	Access control (IAM)	South India Subscription name (change)	mycloudpcsext.southindia.cloudapp.azure.com Associated to			
8	🥔 Tags	Visual Studio Premium with MSDN Subscription ID	PCSExternalNIC Virtual machine			
2	SETTINGS	c how/initial → this, etheris, d= 1%, double/diffusione	PCSAzureVA			
• ••	Gonfiguration					
1	Properties					
•	Locks					
- 🔥 👘	😃 Automation script					

Figure 25: PCS External Public IP

Note: Azure allows static as well as dynamic assignment of IP addresses to the network interfaces. The mode of IP assignment (static/dynamic) can be mentioned in the Azure Resource Manage template file. The current JSON template uses the dynamic method of allotting IP addresses to the network interfaces.

Deploying PCS on an Existing Virtual Network

This section describes deployment with three NIC cards and two NIC cards.

Deployment on VM with Three NIC Cards

To deploy Pulse Connect Secure on Azure using the Azure portal, do the following:

1. Select the template file "pulsesecure-pcs-3-nics-existing-vnet" created in the section '<u>Upload Azure Resource</u> <u>Manager Template to Azure account</u>' and click **Deploy**.

() Note: Before proceeding with deployment, ensure that the attribute "accept-license-agreement" in pulse-config is set to "**y**".

Figure 26: Custom Deployment on VM with Three NIC Cards – Existing Virtual Network

Micro	Microsoft Azure Templates > testpcsdeploy > Custom deployment					
	testpcsdeploy Template - PREVIEW	* 🗆 ×	Custom deployment Deploy from a custom template			
+	🚹 Deploy 💉 Edit	••• More				
	DECONSTICUT		TEMPLATE			
	DESCRIPTION Testing PCS Deployment		11 resources			
	resting res beployment			Edit template Edit parame Learn more		
(*)	PUBLISHER		BASICS			
9	ochriman@pulsesecure.net					
8	MODIFIED		* Subscription	Visual Studio Enterprise with MSDN		
0	8/4/2017		* Resource group	Create new Use existing		
				TestPCSDeploymentRG 🗸		
_	View Template		* Location	Central US 🗸		
8			SETTINGS			
\$			PCS Storage Account Name	pcsgoldenstorage		
<u>a</u>			PCS Storage Account Resource Group			
			Name	GoldenimageRG		
-			PCS Image Location URI 🛛	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure.vhd		
			PCSVM Name 🖲	PCSAzureVA		
			PCS Config 🛛	<pre><pre><pre><pre>config><primary-dns>8.8.8.8</primary-dns><secondary-dns>8.8.8.9</secondary-dns></pre></pre></pre></pre>		
1			* SSH Public Key			
•			Dns Label Prefix Ext 🛛	mycloudpcsext		
0			Dns Label Prefix Mgmt ® Resource Group Name Of Existing Virtual	mycloudpcsmgmt		
Ó			Network 0	ExistingVnetRG		
			Existing Vnet Name O	virtualNetwork		
0			Existing Internal Subnet 0 Existing External Subnet 0	subnet1		
			Existing Management Subnet	subnet2 subnet3		
٠			Existing Tunnel Subnet O	subnet4		
>			TRANK HUD CONDITIONS			
			Pin to dashboard			
			Purchase			

- 2. Fill or modify the following parameters:
 - **Resource group:** Specify the resource group name in which Pulse Connect Secure needs to be deployed
 - Location: Region where resource group needs to be created
 - **PCS Storage Account Name:** Storage account name where the Pulse Connect Secure Virtual Appliance image is available
 - **PCS Storage Account Resource Group:** Resource group of where the Pulse Connect Secure Virtual Appliance image is copied
 - PCS Image Location URI: URI to Pulse Connect Secure Virtual Appliance Image
 - PCS VM Name: Name of the Pulse Connect Secure Virtual instance
 - PCS Config: Provisioning parameters in XML format. Refer '<u>Pulse Connect Secure Provisioning</u> <u>Parameters'</u>
 - SSH Public Key: This key is used to access PCS via SSH. The SSH keys are generated using ssh-keygen on Linux and OS X, or PuTTyGen on Windows. For details about generating the SSH key pairs, refer:

For Windows: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows</u> For MacOS and Linux: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys</u>

- DNS Label Prefix Ext: Prefix for the external interface DNS label
- DNS Label Prefix Mgmt: Prefix for the management interface DNS label
- **Resource Group Name of Existing Virtual Network:** Resource Group name of the Virtual network
- Existing Vnet Name: Virtual network name
- Existing Internal Subnet: Subnet from which the Pulse Connect Secure internal interface needs to lease IP
- Existing External Subnet: Subnet from which the Pulse Connect Secure external interface needs to lease IP
- Existing Management Subnet: Subnet from which the Pulse Connect Secure management interface needs to lease IP
- Existing Tunnel Subnet: Subnet which will be configured as the tunnel IP pool in the Pulse Connect Secure VPN Profile
- 3. Agree to the Azure licensing terms and click **Purchase**.

4. Watch for the deployment succeeded message after 3 to 5 minutes.

Figure 27: De	ployment Succeeded
	pioyment Succeded

TestPCSDeploymentRG Resource group				,
, Search (Ctrl+/)	🕂 Add 📰 Columns 🛍 Delete 💍 Refresh 🕂	Move		
(iii) Overview	Essentials			
Activity log	Subscription name (change) Visual Studio Premium with MSDN Subscription ID	Deployments 1 Succeeded		
Access control (IAM)	k TineBille o 1990-40480-41172-0123-41840Dame			
🥔 Tags	Filter by name All types	✓ All locations	✓ No grouping	,
SETTINGS	11 items	TYPE 🗸	LOCATION V	
📣 Quickstart				
Resource costs	M backend2PC5Route	Route table	South India	
Deployments	NSGExternalSubnet	Network security group	South India	
Policies	NSGInternalSubnet	Network security group	South India	
Properties	PCSAzureVA	Virtual machine	South India	
Locks	PCSExternalNIC	Network interface	South India	
Automation script	PCSExternalPublicIP	Public IP address	South India	
MONITORING	PCSinternalNIC	Network interface	South India	
iii Metrics	PCSManagementPublicIP	Public IP address	South India	

- 5. Go to the resource group in which the Pulse Connect Secure Virtual appliance was deployed to see the resources created.
- 6. Navigate to the resource group and click **PCS Management Public IP**. Make a note of the PCS Management Public IP and DNS name (FQDN) to access PCS for admin page.

Figure 28: PCS Management Public IP

Micro	soft Azure « TestPCSDeploymentRG	PCSManagementPublicIP	𝒫 Search resources	x	Û	>_	\$ C	0
=	PCSManagementPublicIP							
+	,O Search (Ctrl+/)		Î Delete					
	Overview	Essentials ^						
	Activity log	Resource group (change) TestPCSDeploymentRG Location		IP address 13.71.121.15 DNS name				
	Access control (IAM)	South India Subscription name (change)	l	mycloudpcsmgmt.southindia.cloudapp.azure.com Associated to			.azure.com	
۲	🥔 Tags	Visual Studio Premium with MSDN Subscription ID		PCSMangementNIC Virtual machine				
8	SETTINGS	charfalls with energy with the effective		PCSAzureVA				
-	Configuration							
10 0	Properties							
•	Locks							
•	Automation script							
-	SUPPORT + TROUBLESHOOTING							
\Leftrightarrow	New support request							

7. Click PCS External Public IP and note down the PCS External Public IP and DNS name (FQDN) to access PCS for end user page.

Micro	soft Azure Resource groups	TestPCSDeploymentRG PCSExternalPublicIP Dearch resources	× ↓ >_ 🕸 😳 Ø
	PCSExternalPublicIP Public IP address		
+	Search (Ctrl+/)	$\mathscr{E}^{?}$ Associate \bigstar Dissociate \rightarrow Move \square Delete	
	Overview	Essentials ^	(IP address
	Activity log	Resource group (change) TestPCSDeploymentRG Location	13 address 13.71.127.197 DNS name
	Access control (IAM)	South India Subscription name (change)	mycloudpcsext.southindia.cloudapp.azure.com Associated to
8	🥐 Tags	Visual Studio Premium with MSDN Subscription ID	PCSExternalNIC Virtual machine
2	SETTINGS	C % cardinal = 1988. dimit: dir 1% chain-diffusione	PCSAzureVA
e	🚔 Configuration		
100	Properties		
	Locks	_	
- 🚓	Le Automation script		

Figure 29: PCS External Public IP

Note: Azure allows static as well as dynamic assignment of the IP addresses to the network interfaces. The mode of IP assignment (static/dynamic) can be mentioned in the Azure Resource Manage template file. The current JSON template uses dynamic method of allotting IP addresses to the network interfaces.

Deployment on VM with Two NIC Cards

To deploy Pulse Connect Secure on Azure using the Azure portal, do the following:

1. Select the template file "pulsesecure-pcs-2-nics-existing-vnet" created in the section '<u>Upload Azure Resource</u> <u>Manager Template to Azure account</u>' and click **Deploy**.

Note: Before proceeding with deployment, ensure that the attribute "accept-license-agreement" in pulse-config is set to "y".

Figure 30: Custom Deployment on VM with Two NIC Cards – Existing Virtual Network

Microsoft Azure Templates > testpcsdeploy > Custom deployment					
	testpcsdeploy Template - PREVIEW	* 🗆 ×	Custom deployment Deploy from a custom template		
+	🛍 Deploy 💉 Edit	••• More			
	DESCRIPTION		TEMPLATE	1 1 0	
	Testing PCS Deployment			Edit template Edit parame Learn more	
	PUBLISHER	B	BASICS		
•		-	* Subscription	Visual Studio Enterprise with MSDN	
©	MODIFIED		* Resource group	Create new Use existing	
<u>.</u>	8/4/2017			TestPCSDeploymentRG 🗸	
	View Template		* Location	Central US 🗸	
			SETTINGS		
*			PCS Storage Account Name 🛛	pcsgoldenstorage	
<u>-</u>			PCS Storage Account Resource Group Name O	GoldenimageRG	
			PCS Image Location URI	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure.vhd	
-			PCSVM Name 0	PCSAzureVA	
=			PCS Config 🛛	<pre>config><primary-dns>8.8.8.8</primary-dns><secondary-dns>8.8.8.9</secondary-dns></pre>	
			* SSH Public Key 🛛		
			Dns Label Prefix Ext 0	mycloudpcsext	
0			Resource Group Name Of Existing Virtual Network O	ExistingVnetRG	
			Existing Vnet Name 0	virtualNetwork	
•			Existing Internal Subnet O	subnet1	
0			Existing External Subnet O	subnet2	
2			Existing Tunnel Subnet O	subnet4	
-			Pin to dashboard		
>			Purchase		

- 2. Fill or modify the following parameters:
 - Resource group: Specify the resource group name in which Pulse Connect Secure needs to be deployed
 - Location: Region where resource group needs to be created
 - **PCS Storage Account Name:** Storage account name where the Pulse Connect Secure Virtual Appliance image is available
 - **PCS Storage Account Resource Group:** Resource group of where the Pulse Connect Secure Virtual Appliance image is copied
 - PCS Image Location URI: URI to Pulse Connect Secure Virtual Appliance Image
 - PCS VM Name: Name of the Pulse Connect Secure Virtual instance

- PCS Config: Provisioning parameters in XML format. Refer '<u>Pulse Connect Secure Provisioning</u>
 <u>Parameters'</u>
- SSH Public Key: This key is used to access PCS via SSH. The SSH keys are generated using ssh-keygen on Linux and OS X, or PuTTyGen on Windows. For details about generating the SSH key pairs, refer:

For Windows: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/ssh-from-windows</u> For MacOS and Linux: <u>https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-kevs</u>

- DNS Label Prefix Ext: Prefix for the external interface DNS label
- **Resource Group Name of Existing Virtual Network:** Resource Group name of the Virtual network
- Existing Vnet Name: Virtual network name
- Existing Internal Subnet: Subnet from which the Pulse Connect Secure internal interface needs to lease IP
- Existing External Subnet: Subnet from which the Pulse Connect Secure external interface needs to lease IP
- Existing Tunnel Subnet: Subnet which will be configured as the tunnel IP pool in the Pulse Connect Secure VPN Profile
- 3. Agree to the Azure licensing terms and click **Purchase**.
- 4. Watch for the deployment succeeded message after 3 to 5 minutes.

Figure 31: Deployment Succeeded

TestPCSDeploymentRG				* ×
, Search (Ctrl+/)	+ Add ≣≣ Columns III Delete 🖑 Refresh → M	Nove		
(🔊) Overview	Essentials Subscription name (change)	Deployments		
Activity log	Visual Studio Premium with MSDN Subscription ID	1 Succeeded		
Access control (IAM)	CONTRACTOR OFFICE STOTE CARACTERISTIC			
🥔 Tags	Filter by name All types	✓ All locations	✓ No grouping	~
SETTINGS	11 items NAME V	түре 🗸	LOCATION V	
📣 Quickstart	Backend2PCSRoute	Route table	South India	
 Resource costs 	NSGExternalSubnet	Network security group	South India	
Deployments	+			
Policies	VSGInternalSubnet	Network security group	South India	
Properties	PCSAzureVA	Virtual machine	South India	
	PCSExternalNIC	Network interface	South India	
Locks	PCSExternalPublicIP	Public IP address	South India	
Automation script	PCSInternalNIC	Network interface	South India	
MONITORING	PCSInternalNIC	Network interface	South India	

- 5. Go to the resource group in which the Pulse Connect Secure Virtual appliance was deployed to see the resources created.
- 6. Click PCS External Public IP and note down the PCS External Public IP and DNS name (FQDN) to access PCS for end user page.

Micro	osoft Azure Resource groups	TestPCSDeploymentRG PCSExternalPublicIP	\wp Search resources	× 🗘 >_ 🕸 😳 🕐
≡				
+	Search (Ctrl+/)		🗓 Delete	
	Overview	Essentials ^		
	Activity log	Resource group (change) TestPCSDeploymentRG Location		IP address 13.71.127.197 DNS name
	Access control (IAM)	South India Subscription name (change)		mycloudpcsext.southindia.cloudapp.azure.com
۲	Iags 🖉	Visual Studio Premium with MSDN Subscription ID		PCSExternalNIC Virtual machine
2	SETTINGS	Chronibbe - mie athan dir m dathabitana		PCSAzureVA
e	量 Configuration			
1	Properties			
•	Locks			
-	4 Automation script			

🕖 Note: Azure allows static as well as dynamic assignment of the IP addresses to the network interfaces. The mode of IP assignment (static/dynamic) can be mentioned in the Azure Resource Manage template file. The current JSON template uses dynamic method of allotting IP addresses to the network interfaces.

Figure 32: PCS External Public IP

Deploying Pulse Connect Secure on Azure using Azure CLI

Before proceeding with the deployment, refer Upload Pulse Connect Secure Virtual Appliance Image to Azure.

- 1. Download and Install Azure CLI from https://azure.github.io/projects/clis.
- 2. Visit <u>www.pulsesecure.net</u> and download the ps-pcs-azure-psa-v-<releaseno>-<buildno>-package.zip file.
- 3. Unzip the file and look for the **pulsesecure-pcs-3-nics.zip** file. Unzip the file to get **azuredeploy.json**
- 4. Ensure that parameters section has correct default values:
 - **PCS Storage Account Name:** Storage account name where the Pulse Connect Secure Virtual Appliance image is available
 - **PCS Storage Account Resource Group:** Resource group where the Pulse Connect Secure Virtual Appliance image is copied
 - PCS Image Location URI: URI to the Pulse Connect Secure Virtual Appliance Image
 - PCS VM Name: Name of the Pulse Connect Secure Virtual instance
 - **PCS Config:** Provisioning parameters in an XML format. Refer "Pulse Connect Secure Provisioning Parameters"
 - DNS Label Prefix Ext: Prefix for the external interface DNS label
 - DNS Label Prefix Mgmt: Prefix for the management interface DNS label
 - Vnet Address Space: Virtual network address space
 - Internal Subnet: Subnet from which the Pulse Connect Secure internal interface needs to lease IP
- 5. To deploy Pulse Connect Secure using Azure CLI, run the following commands

\$ az login

\$ az group create -l <location> -n <resource group name>

\$ az group deployment create -g <resource group name> --template-file <json file name>

For example:

\$ az login

\$ az group create - I southindia -n TestPCSDeploymentRG

```
TestPCS:Desktop TestPCS$ az group create -1 southindia -n TestPCSDeploymentRG
{
    "id": "/subscriptions/TestPCS6-9175-9175-southindiaee/resourceGroups/TestPCSDeploymentRG",
    "bocation": "southindia",
    "managedBy": null,
    "name": "TestPCSDeploymentRG",
    "provisioningState": "Succeeded"
    },
    "tags": null
}
TestPCS:Desktop TestPCS$
```

\$ az group deployment create -g TestPCSDeploymentRG --template-file azuredeploy.json

```
{
        "id": null,
        "namespace": "Microsoft.Compute",
        "registrationState": null,
        "resourceTypes": [
          {
            "aliases": null,
            "apiVersions": null,
            "locations": [
              "southindia"
            1,
            "properties": null,
            "resourceType": "virtualMachines"
          }
       1
     }
    1,
    "provisioningState": "Succeeded",
    "template": null,
    "templateLink": null,
    "timestamp": "2017-08-06T17:19:20.227838+00:00"
  },
  "resourceGroup": "TestPCSDeploymentRG"
7
```

Pulse Connect Secure Provisioning Parameters

Provisioning parameters are those parameters which are required during the deployment of a virtual appliance. Pulse Connect Secure accepts the following parameters as provisioning parameters in the XML format.

"<pulse-config>

<primary-dns>8.8.8.8</primary-dns></primary-dns>8.8.8.8</primary-dns>

</pulse-config>",

The below table depicts the details of xml file.

#	Parameter Name	Туре	Description
1	primary-dns	IP address	Primary DNS for Pulse Connect Secure
2	secondary-dns	IP address	Secondary DNS for Pulse Connect Secure
3	wins-server	IP address	Wins server for Pulse Connect Secure
4	dns-domain	string	DNS domain of Pulse Connect Secure
5	admin-username	string	admin UI user name
6	admin-password	string	admin UI password
7	cert-common-name	string	Common name for the self-signed certificate
8	cert-random-text	string	generation. This certificate is used as the device certificate of Pulse Connect Secure
9	cert-organization	string	Random text for the self-certificate generation Organization name for the self-signed certificate generation
10	config-download-url	String URL	Http based URL where XML based Pulse Connect Secure configuration can be found. During provisioning, Pulse Connect Secure fetches this file and comes up with preloaded configuration. XML based configuration can be present in another VM in Azure cloud or at corporate network which is accessible for Pulse Connect Secure through site to site VPN between Azure and corporate data center
11	config-data	string	base64 encoded XML based Pulse Connect Secure configuration
12	auth-code-license	string	Authentication code that needs to be obtained from Pulse Secure
13	enable-license-server	string	If set to 'y , PCS will be deployed as a License server.

			If set to ' n ', PCS will be deployed as a normal server.
14	accept-license-agreement	string	This value is passed to the instance for configuration at the boot time. By default, this value is set to ' n '. This value must be set to 'y .
15	enable-rest	string	If set to ' y , REST API access for the administrator user is enabled.

Vote: In the above list of parameters, **primary dns, dns domain, admin username, admin password, certrandom name, cert-random text, cert-organization** and **accept-license-agreement** are mandatory parameters. The other parameters are optional parameters.

Provisioning Pulse Connect Secure with Predefined Configuration

The Pulse Connect Secure Virtual Appliance can be provisioned on Azure with a pre-defined Pulse Connect Secure configuration. The provisioning can be done in the following two ways:

 Pulse Connect Secure administrator needs to provide the location of the XML-based configuration as a provisioning parameter. Refer '<u>Pulse Connect Secure Provisioning</u> <u>Parameters</u>' for details about the Pulse Connect Secure specific provisioning parameters.

Pulse Connect Secure configuration can be kept on Azure VM or on a machine located in the corporate network. If it is in the corporate network, the Pulse Connect Secure administrator needs to ensure that site-to-site VPN between Azure to corporate network is already established so that Pulse Connect Secure can access the machine located in the corporate network.

• Pulse Connect Secure administrator provides the configuration data encoded in the base64 encoded xml in the ARM template.

Azure Cloud

Figure 33: Pulse Configuration Server in Corporate Network

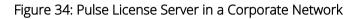
Configuring Licenses on the Pulse Connect Secure Appliance

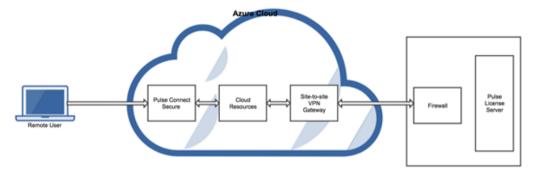
By default, two-user licenses are provided. To add more licenses, the Pulse Connect Secure administrator needs to leverage the Pulse License server.

The Pulse License server can be made available in:

- <u>corporate network</u>
- <u>cloud network</u>

Pulse License Server in Corporate Network





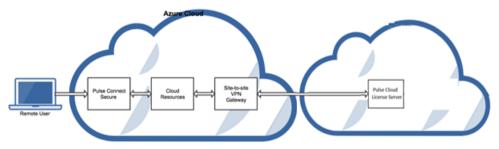
Pulse License Server in Cloud Network

In Pulse Connect Secure 8.3R3, the Pulse Connect Secure virtual machines (VM) are enabled to provision licenses through the Pulse Cloud Licensing Service (PCLS). For this, administrator needs to obtain an Authentication code from Pulse Secure Support and apply it in Download Licenses page of PCS admin console. The PCS also periodically sends heartbeat messages to PCLS for auditing purposes.

The Authentication code can also be specified in the ARM template. When PCS comes up, it automatically fetches the Authentication code.

- Adding Authentication Code in PCS Admin Console
- Including Authentication Code in ARM Template

Figure 35: Pulse License Server in Cloud Network



Adding Authentication Code in PCS Admin Console

To add Authentication code:

- 1. Go to System > Configuration > Licensing > Download Licenses.
- 2. Under On demand license downloads, enter the Authentication code in the text box.
- 3. Click on Download and Install.

Figure 36: Enter Authentication Code

SPULSe Secure system Authentication Administrators Users Maintenance	Vizards Default Network CO						
Configuration + Licensing > Deveload License							
Download License							
See Configuration							
Kiteway Pulse One Browsky Centificates DM Agent HCP Bursans Client.Types 1 Mosile VPN Turneling Telenetry	Pulse Collaboration Virtual Decidages INEx2 SAML						
Same Sereary Contact Series							
W Dicesse downloads settings Use his setCon to ins049 extrusts settings for (Konse sense) Performal Notions: Material Material Material State Changes							
♥ On demand lonne downloads							
Enter Aufbreeffication Code in the below text box. The of contact Para Search is demonstrated with Desearch or the mathem. Conversional and Install							
W Last contact time autous							
Last Contact Time: 10:45:43 AM on Jul 20, 2017							

Including Authentication Code in ARM Template

To include Authentication code in the ARM template:

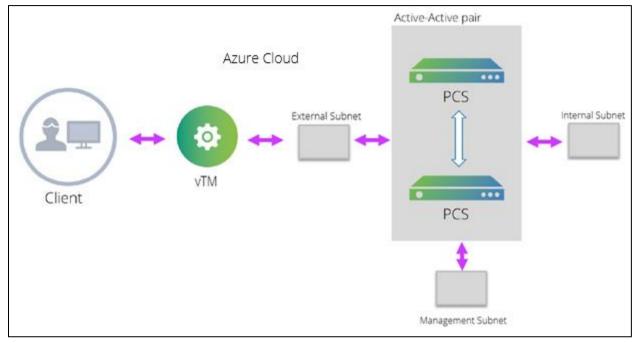
- 1. In the ARM template, go to the PCSConfig section.
- 2. For the element <auth-code-license>, enter the Authentication code as the content.
- 3. Save the template.

For details about the license configuration, refer to License Configuration Guide.

Deploying PCS Active-Active Cluster using Virtual Traffic Manager in Microsoft Azure

This section describes deploying PCS A-A cluster with vTM load balancer in Microsoft Azure.

Figure 37: Deploying PCS A-A Cluster Topology Diagram



The deployment process involves the following steps:

- Deploying Two PCS EC2 instances Using ARM Template
- Forming the Active-Active Cluster
- Deploying Virtual Traffic Manager EC2 Instance in the External Subnet of PCS in
- Setting Up and Configuring vTM for External Users

Deploying Two PCS EC2 instances Using ARM Template

PCS can be deployed in Azure using ARM template in a 3-armed model. Based on the need, deploy two PCS instances using the json template from one of the following zip files:

- pulsesecure-pcs-3-nics.zip
- pulsesecure-pcs-3-nics-existing-vnet.zip

Forming the Active-Active Cluster

Once the two PCS instances are initialized, form the Active-Active cluster between them. For details about creating PCS clusters, refer to <u>PCS Administration Guide</u> published in the Pulse Secure Techpubs site.

Figure 38: PCS A-A Cluster Status

ŜР	ulse Secure	System Authentication Admir	nistrators Users Maintenance	e Wizards	1. 18 1	Pulse Connect Secure on PCS2	1.
Clustering > C							
Cluster Sta	atus						
Status	Properties						
Cluster Name							
Type: Configuration	PSA-V n: Active/Active						
Add Memt		lemove					
	 records per page 					Search:	
	Member Name	Internal Address	External Address	Status	Notes	Sync Rank Update	
0	PCS1	10.251.1.214/24	10.251.2.180/24	٥	Enabled	0	
0	• PCS2	10.251.1.238/24	10.251.2.143/24	٥	Leader	0	
						- Previous 1	Next \rightarrow

Deploying Virtual Traffic Manager EC2 Instance in the External Subnet of PCS in Microsoft Azure

Virtual Traffic Manager can be deployed through either Azure Marketplace or Azure CLI. Deploying Virtual Traffic Manager through Marketplace includes the following steps:

To deploy through Marketplace, follow the below steps:

1. Search and select **Pulse Secure vTM** in Azure Marketplace.

Figure 39: Azure Marketplace > Pulse Secure vTM

Microsoft Azure			✓ market	Ļ	>_	្ដែរ	\odot	?	Ŗ	Chelonie	PULSE SE	CURE, LLC	
Create a resource	Home > Marketplace > Everything Marketplace	×	Everything								*	•×	
⋮ All services	My Saved List 🔍		T Filter										
★ FAVORITES	Everything		Pulse Virtual Traffic Manager									×	
🖪 Dashboard	Compute		Results										
All resources	Networking		NAME		PUBLIS	HER			CATEGOR	Y			
Resource groups	Storage		S Pulse Virtual Traffic Manager		Pulse S	Secure			Comput	p	(\heartsuit	
💿 App Services	Web		Pulse Virtual Traffic Manager with WAF		Pulse S				Comput			×	
Function Apps	Mobile												
👼 SQL databases	Containers		S Pulse Virtual Web Application Firewall		Pulse S	secure			Comput	e			
🥒 Azure Cosmos DB	Databases												
Virtual machines	Analytics												
🚸 Load balancers	Al + Machine Learning												
Storage accounts	Internet of Things												
↔ Virtual networks	Integration												

2. Select the required deployment model and click **Create**.

Figure 40: vTM Editions Available in Azure Marketplace

Pulse Virtual Traffic Manager	*		×
Pulse Secure			
HA via active-active deployment. 3. Integration with DevOps tools: Use the REST API to integrate with your choice of orchestration tools.	of Devo	ps and	I
Pricing of available editions			
This template gives you access to 8 different versions of Pulse vTM. Search for Pulse Se Marketplace to see editions of Pulse vTM with Web Application Firewall or standalone Application Firewall.		n the	
1. Pulse Virtual Traffic Manager Dev/BYOL – 1Mbps. Free edition. Server inst Azure pricing	ance as	s per	
2. Pulse Virtual Traffic Manager – Essential 10Mbps. \$0.15 USD per hour 3. Pulse Virtual Traffic Manager – Essential 100Mbps. \$0.21 USD per hour 4. Pulse Virtual Traffic Manager – Essential 300Mbps. \$0.35 USD per hour			
5. Pulse Virtual Traffic Manager – Standard 10Mbps. \$0.44 USD per hour 6. Pulse Virtual Traffic Manager – Standard 200Mbps. \$0.76 USD per hour 7. Pulse Virtual Traffic Manager – Standard 1Gbps. \$1.16 USD per hour			
8. Pulse Virtual Traffic Manager – Enterprise 1Gbps. \$1.70 USD per hour			
Other currencies are available. See the Pulse Secure vTM & WAF Licensing Guide for de features available with each edition.	etails of	the	
BYOL			
The Dev/BYOL edition of Pulse vTM can be used as the host for a license key purchased Pulse Secure's Partners. Please see the Cloud Services Installation and Getting Started of license deployment process.			
icense deployment process.			
Pulse (previously Brocade) Virtual Traffic Manager (Pulse vTM) is a software-base application delivery controller. Designed to run in public or private clouds or virt			
environments			
Select a deployment model 🚯			
Resource Manager			
Create			

- 3. In the wizard that follows, provide the required configuration details:
 - Cluster name
 - License type
 - Authentication details
 - Virtual Network and Subnet settings
 - Resource group
 - Location information

In the **Network Settings** tab, select the Virtual Network and Traffic Manager Subnet matching PCS's Vnet and External Subnet.

Home > Marketplace > Everything > Pulse Virtual Traffic Create Pulse Virtual Traffic Mana ×		Basics					
1 Basics > Configure basic settings	* Cluster Name vtmlb License	~					
2 Service Configuration > Configure settings for the servi	Developer Edition or BYOL	~					
3 Network Settings > Configure Virtual Network	* Instance Count		eate Pulse Virtual Traffic Ma Basics Done	ana ×	Network Settings * Virtual Network @ pcs1-vnet	×	Subnet
4 Instance Configuration > Configure Instance settings	Authentication type Password SSH public key Password		2 Service Configuration Done	~	* Subnet Review subnet configuration	•	
5 Summary > Pulse Virtual Traffic Manager	Confirm password	✓	 3 Network Settings Configure Virtual Network 4 Instance Configuration Configure Instance settings 	>			
6 ^{Buy} >	Subscription MSDN Platforms	~	5 Summary Pulse Virtual Traffic Manager	>			
	* Resource group ① Create new Use existing RG3	~	6 виу	>			
	* Location East US	~					
	ок	on/Re	sources/resourceType/Microsoft.Resou	urces%2Fresou	OK		ОК

Create Pulse Virtual Traffic Mana... imesSummary 1 Validation passed Basics 1 ~ Done Basics MSDN Platforms Subscription Resource group RG3 Service Configuration 2 > Location East US Configure settings for the servi... Cluster Name vtmlb License Developer Edition or BYOL Version 17.4 3 Network Settings 1 Instance Count 1 Done ********* Password Service Configuration IP Address Name vtmlb Instance Configuration 4 \checkmark DNS Label vtmlb Done Service Port Number 80 Service Protocol TCP Summary Network Settings 5 >Pulse Virtual Traffic Manager Virtual Network pcs1-vnet Traffic Manager Subnet ExternalSubnet Traffic Manager Subnet addres... 10.0.1.0/24 Buy Instance Configuration 6 Virtual Traffic Manager VM Size Standard A3 First port number for SSH access 50000 First port number for administr... 50100 First port number for REST acce... 50200 Standard_LRS Storage Account Type Storage Account Prefix vtmlb Storage account count 1 ОК Download template and parameters

Figure 41: Configuration Wizard

Adding Load Balancing and Inbound Network Security Rules

To manage an additional service in your Traffic Manager cluster, or if the existing service uses multiple ports or protocols, add load balancer and network security rules after creating the cluster.

To add load balancing rule, perform the following steps:

- 1. Navigate to your resource group.
- 2. Click the Load Balancer resource name (typically named "<clustername>-vtmLB").
- 3. From the load balancer settings pane, click Load balancing rules.
- 4. Click Add.

Figure 42: Add Load Balancing Rule

Add load balancing rule SSL Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP • Name SSP </th <th>Home > Resource groups > RG3 > vtmlb-vtmLB - Load balancing rules > Add load balancing rule</th> <th>Home > Resource groups > RG3 > vtmlb-vtmLB - Load balancing rules > SSL</th>	Home > Resource groups > RG3 > vtmlb-vtmLB - Load balancing rules > Add load balancing rule	Home > Resource groups > RG3 > vtmlb-vtmLB - Load balancing rules > SSL
ESP • IP Version • IP Version • IP Nember 10 • Protocol • Port 4500 • Backend port • • Statemer Backend • Backend port • • Backend po	Add load balancing rule	
 IP Version IP Version IP Net IPA6 Frontend IP address ● 40.117.152.174 (LoadBalancerFrontEnd) Protocol ICP UDP Port 4500 Sackend port ● Font Backend port ● LoadBalancerBackend VinAdminProbe (TCP:9000) Session persistence ● Client IP Foating IP (direct server return) ● Disabled Enabled K 	* Name	🕞 Save 🗶 Discard 🛅 Delete
 IP Version IP Version IP Normend IP address ● 40.117.152.174 (LoadBalancerFrontEnd) Protocol IP OP Port 4500 Seakend port ● 4500 Backend port ● 4500 Backend port ● InddBalancerEackend VarnAdminProbe (ICP:990) Session pensistence ● Client IP Foating IP (direct server return) ● Ditabled Enabled K K Image: Set in the set of the set	ESP 🗸	
* Frontend IP address @ * Frontend IP address @ 40.117.152.174 (LoadBalancerfrontEnd) Protocol • Port 4500 * Backend port @ 4500 * Backend port @ 4500 • Backend port @ 4500 • Port 4500 • Det • Backend port @ • LoadBalancerFlackend • MadminProbe (TCP-9090) • Backend pool @ Client IP Potabled Enabled Session persistence @ Client IP None Ide timeout (minutes) @	* IP Version	U opdaung
 Frontend IP address @ Invited IP address @ IP Version IP Version	● IPv4	
Protocol Prot 4500 Backend port • 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4500 4510 4510 4510 4510 4510 4510 4510 4510 4510 4510 4510 5ession persistence • 10110 101100 101100 101100 101100 101100 101100 1011000 1011000 1011000 1011000 1011000 1011000 1011000 1011000 10110000 10110000 10110000 10110000 101100000 <t< td=""><td>* Frontend IP address 🚯</td><td>SSL</td></t<>	* Frontend IP address 🚯	SSL
Protocol Port 4500 * Backend port • 4500 Backend pool • LoadBalancerBackend wtmAdminProbe (TCP:9090) Session persistence • Client IP Floating IP (direct server return) • Disabled Enabled CK	40.117.152.174 (LoadBalancerFrontEnd)	* IP Version
 CP ● UPP Port 4500 Backend port ● 4500 Backend port ● 4500 Backend port ● LoadBalancerBackend VrnAdminProbe (TCP:9090) Session persistence ● Client P Floating IP (direct server return) ● Disabled Enabled K 	Protocol	
 Port 4500 Backend port ● 4500 Backend pool ● LoadBalancerBackend VtmAdminProbe (TCP:9090) Session persistence ● Client IP Floating IP (direct server return) ● Disabled Enabled OK 		* Frontend IP address 🕦
 * Backend port @ * Backend port @ 4500 Backend pool @ LoadBalancerBackend * Mackend port @ * Backend pool @ LoadBalancerBackend * Backend pool @ LoadB	* Port	40.117.152.174 (LoadBalancerFrontEnd)
 * Backend port ① 4500 Backend pool ① LoadBalancerBackend * Mackend port ① * Backend port ② * Backend port ② * Backend port ② * Backend port ③ * Backend port ④ * Backend port ● * Backend port ●<td>4500 🗸</td><td>Protocol</td>	4500 🗸	Protocol
4500 Backend pool ① LaadBalancerBackend Health probe ① VtmAdminProbe (TCP:9090) Session persistence ① Client IP Floating IP (direct server returm) ① Disabled Enabled OK	* Backend port 🙃	
backend pool • • LoadBalancerBackend • Health probe • • vtmAdminProbe (TCP:9090) • Session persistence • • Client IP • Floating IP (direct server returm) • • Disabled Enabled • OK Idle timeout (minutes) •		* Port
Health probe ① Interview of the section of the secting of the secting of the secting of the sect	Backend pool 🚯	443
Health probe ① vtmAdminProbe (TCP:9090) Session persistence ④ Client IP Floating IP (direct server return) ① Disabled Enabled OK 443 Backend pool ④ LoadBalancerBackend VtmAdminProbe (TCP:9090) VtmAdminProbe ① Session persistence ④ None Idle timeout (minutes) ④	LoadBalancerBackend V	* Backend port 🙃
Session persistence ① Backend pool ① Client IP ✓ Floating IP (direct server return) ① ✓ Disabled Enabled ✓ OK Idle timeout (minutes) ①	Health probe 🕐	
Session persistence ① IoadBalancerBackend ~ Client IP ~ Floating IP (direct server return) ① ~ Disabled Enabled OK Idle timeout (minutes) ①	vtmAdminProbe (TCP:9090) V	Backend pool
Floating IP (direct server return) ① Health probe ① Disabled Enabled OK Idle timeout (minutes) ①	Session persistence 🕦	
Floating IP (direct server return) ① vtmAdminProbe (TCP:9090) v Disabled Enabled Session persistence ① None v OK Idle timeout (minutes) ①	Client IP V	
Disabled Enabled Session persistence () None OK Idle timeout (minutes) ()	Floating IP (direct server return) 🙃	
OK None		
OK Idle timeout (minutes) 🛛		
OK OK		None
	OK .	Idle timeout (minutes) 🚯
		4

- 5. Configure the following settings for ESP and SSL traffic modes, and click **OK**:
 - Name: Type a descriptive name for this rule.
 - **Protocol**: Select your traffic protocol.
 - **Port**: Enter the port number for your traffic.
 - Backend Port: Set to the same value as Port.
 - Session Persistence: Select "None".
 - Idle Timeout (minutes): Set to a timeout value suitable for your service.
 - Floating IP (direct server return): Select "Disabled".
- 6. In the resource group, click the name of the Network Security Group resource (typically named "<clustername>-vtmNSG").
- 7. Click Inbound Security Rules and then click Add.

me > Resource groups > RG3 > vtmlb vtmlb-vtmNSG - Inbound Network security group		y rules						* >
♀ Search (Ctrl+/)	« 🕂 Add 🗞	Default rules						
🔋 Overview	Updating							
Activity log	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
Access control (IAM)	1000	🔺 allow-ssh	22	тср	Any	Any	Allow	
Tags	1100	allow-service	80	тср	Any	Any	Allow	
X Diagnose and solve problems	1200	allow-admin	9090	ТСР	Any	Any	Allow	
ETTINGS	1300	allow-rest	9070	тср	Any	Any	Allow	
- Inbound security rules	1310	Port_443	443	Any	Any	Any	Allow	
Outbound security rules	1320	Port_4500	4500	UDP	Any	Any	Allow	
Network interfaces	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	
Subnets	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalan	Any	Allow	
Properties	65500	DenyAllInBound	Any	Any	Any	Any	O Deny	

- 8. Configure the following settings:
 - Name: Type a descriptive name for this rule.
 - **Priority**: Enter the desired priority number. The higher the priority number, the lower the priority over other rules.
 - Source: Select "Any".
 - **Protocol**: Select your traffic protocol.
 - Source Port Range: Leave this setting as the default "*".
 - Destination: Select "Any".
 - Destination Port Range: Enter the port number or range for your traffic.
 - Action: Select "Allow".
- 9. Click **OK** to save the rule.

Pulse Secure Virtual Traffic Manager Initial Configuration

A newly created Virtual Traffic Manager requires some basic information to function normally. Use the Initial Configuration wizard by entering the URL of the Admin UI into your Web browser. Provide the following details:

- Administrator password for the instance
- Confirmation to the terms and conditions
- Time zone settings for the appliance
- Login credentials for master admin user to log in to the Administration server and SSH console
- Licensing option

Figure 44: Pulse Secure vTM Initial Configuration Wizard

C 🖉 C 🔺 Not Secure https://40.117.152.174:50100/apps/zxtm/wizard.fcgi?section=Wizard:Startup	🖈 🌀 <u>ଲ</u> :
👯 Apps 🗁 Citrix 🗁 Tools_related 🗁 AWS 🌎 sbi 🗁 PCS - CLNT 📄 SMB	Cther Bookmark
nitial configuration, step 1 of 7	
1. Welcome to your Pulse Secure Virtual Traffic Manager	
The following pages will guide you through the process of setting up your Pulse Secure Virtual Traffic Manager Azure Appliance for basic operation. This should only take a few minutes.	
	■Back Next ►

Initial configuration, step 2 of 7	
2. Enter administrator password	
Please enter the administrator password for this instance.	
If you did not specify a password when you launched the instance, connect to the instance with SSH and set a password using z-reset-password.	
Password:	
	< Back Next ►
Initial configuration, step 3 of 7	
3. Pulse Secure Terms and Conditions of Sale	
Use of this software is subject to the Pulse Secure Terms and Conditions of Sale.	
Please review these terms, published at https://www.pulsesecure.net/support/eula before proceeding.	
I accept the license agreement	■ Back Next ▶
	a Daux Next
Initial configuration, step 4 of 7	
4. Date and Time Settings	
Please specify the time settings for this appliance.	
Time Zone: America/Los Angeles	
Date: 31 July + 2018	
Time: 03 : 02 : 20	
	< Back Next ►
Initial configuration, step 5 of 7	
5. Security	
A master 'admin' user is created that you can use to log in to the Administration Server and SSH console. Please choose a password for this user.	
Enter Password: •••••••	
Confirm Password: •••••••	
Pulse Secure vTM Appliances come with a tool pre-installed to help prevent brute-force SSH attacks. This will block remote hosts that have made multiple failed connection attempts for a set time. The specific parameters,	
including the time spent blocked and the number of permissible failed attempts, can be configured on the Security page when you have completed the initial configuration.	
Would you like to enable this tool now? Enable SSH Intrusion Prevention	
	✓ Back Next ►
Initial configuration, step 6 of 7	
6. License Key	
To use the traffic manager, you will need a valid license key. You have the following licensing options:	
Upload a license key for this traffic manager Register for flexible licensing using Services Director. This option is available for KVM, VMware and EC2.	
platforms only	
platforms only Skip licensing for now (traffic manager will run in Developer mode until licensing is configured)	
platforms only	

For additional details, and to deploy vTM though Azure CLI, follow the steps in the section "Creating a Traffic Manager Instance on Azure EC2" in <u>Pulse Secure Virtual Traffic Manager: Cloud Services Installation and Getting</u> <u>Started Guide</u>. Make sure that vTM is deployed on the external network of PCS.

Setting Up and Configuring vTM for External Users

Once the vTM EC2 instance is deployed, set up the instance using the Initial Configuration wizard. For details, refer <u>Pulse Secure Virtual Traffic Manager: Cloud Services Installation and Getting Started Guide</u>. The Pulse Secure vTM Administrator login prompt appears.

Figure 45: Pulse Secure vTM Login Page

S Pulse Se	CUIC Virtual Traffic Manager Appliance 500 L 10 17.4
Login	Pulse Secure vTM Administration Server
	Software: Virtual Traffic Manager Appliance 17.4
	Use of this software is subject to the Pulse Secure Terms and Conditions of Sale.
	Please review these terms, published at Pulse Secure Terms and Conditions of Sale before proceeding.
	Login to 10.251.2.152
	Enter a username and password to access the administration server.
	Your session timed out. Please login.
	Username:
	Password:
	Login

Next step is to set up the vTM for the external users using traffic pools and load balancing virtual servers. Traffic pool is the group that will bind to virtual server for load balancing. In an Active-Active Cluster scenario, traffic pool comprises cluster nodes. We need to create two separate traffic pools, each for SSL(L7) and ESP(L3) traffic modes.

Create Service Pool

In the **Services** tab, select **Pools** and create new pool by adding external IPs of cluster nodes along with port number. Also, select appropriate monitor from the drop-down options.

Complete these steps for SSL and UDP. For details, refer to the section "Creating PCS Pools" in <u>Load Balancing</u> <u>PCS with vTM Deployment Guide</u>.

Figure 46: Create Traffic Pool

^					10.251.2.152 (ad	min/admin) Logout
Security Pulse Secu	Jre virtual	Traffic Manager Appliance 500 L 10 17.	4		Cluster: OK	840.0 b/s
🕈 Home 🚱 Ser	vices 🛄 Cat	talogs 🖇 Diagnose 🖗 Activity 🖌 System	m	Wizards	¢Q	Help
Configuring:	Traffic IP G	roups Virtual Servers Pools Config S	ummary			
Pools	Pools				Unf	old All / Fold All
	A pool man	ages a group of server nodes. It routes traffic	to the most appropriate node, based on load balancing and session persistence criteria.			
	🕨 🖌 (nt	OP-testing-ESP-pool (UDP - Streaming, 2	nodes)			🖊 Edit
	► 🗸 S	SL-testing-SSI-pool (SSL (HTTPS), 2 node	s)			🖊 Edit
	Create a n	ew Pool				
	Pool Name:	SSL-Pool				
	Nodes:	10.251.2.143:443,10.251.2.180:443				
	Monitor:	Ping \$				
	Create Pool					

By default, they use Round Robin method of traffic distribution without any session persistency. Make a note of protocol type and port numbers that has been used for this use case.

Figure 47: SSL and UDP Pools

N					10.251.2.152 (a	dmin/admin) Logol
S Pulse Sec	UIC' Virtual Traffic Manager Appliance 50	OL10 17.4			Cluster: OK	1.6 kb/s
Home 😔 Se	ervices 🛄 Catalogs 🤌 Diagnose 🚈 Activi	ty 🗲 System		Wizards	¢) [Q	Hel
Configuring:	Traffic IP Groups Virtual Servers Pool	Config Summary				
Pools	Pools				U	nfold All / Fold A
	A pool manages a group of server nodes. It	outes traffic to the most	appropriate node, based on load balancing and session persistence crite	ria.		
	¥ 💉 ESP-pool (UDP - Streaming, 2 no	des)				Z Ec
	Protocol: UDP - Streaming	Used by virtual serve	rs: ESP-pool			
	Nodes: 10.251.2.143 10.251.2.180	Traffic distribution:	Round Robin, no session persistence			
	Port: 4500	Monitored by:	Ping			
	SSL: II	Bandwidth:	22			
	🔻 💉 SSI-pool (SSL (HTTPS), 2 nodes)					<u>/</u> Ec
	Protocol: SSL (HTTPS)	Used by virtual serve	rs: SSL-Vserver			
	Nodes: 10.251.2.143 10.251.2.180	Traffic distribution:	Round Robin, no session persistence			
	Port: 443	Monitored by:	Ping			
	SSL: II	Bandwidth:	22			

Choose an IP-based Session Persistence Class

In the **Services** tab, select **Pools.** In the pool edit page, locate the Session Persistence section and enable the **Session Persistence** class. Session persistency is required for ESP-based VPN tunnels.

Figure 48: Session Persistency Class

Seculse Secu	JTC ⁴ Virtual Traffic Manager Appliance 500 L 10 17.4
f Home 🚱 Sei	rvices 🛄 Catalogs 🖇 Diagnose 🖉 Activity 🖌 System
Configuring:	Traffic IP Groups Virtual Servers Pools > VA-ESP > Session Persistence Config Summary
Edit Session	Pool: VA-ESP (UDP - Streaming, 2 nodes)
Persistence	Session Persistence ensures that all requests from a client will always get sent to the same node.
	Session Persistence Catalog
	Choose Session Persistence Class
	The default Session Persistence class this pool uses, if any.
	Name Type
	persistence: None
	Persistency IP-based persistence Edit Update

Create Virtual Servers

In the **Services** tab, select **Virtual Servers** and create a new virtual server by selecting protocol type and traffic pools. You need to create separate virtual servers to handle both SSL and UDP traffic. Each virtual server balances traffic across the pool of the same protocol type.

For details, refer to the section "Creating Virtual Server" in Load Balancing PCS with vTM Deployment Guide.

Figure 49: Create Virtual Server

A				10.251.2.152 (admin/admin) Logout				
S Pulse Sec	UIC Virtual Traffic M	anager Appliance	500 L 10 17.4				Cluster: OK	800.0 b/s
ft Home 😪 Se	ervices 🛄 Catalogs 🦧	Diagnose 🗠 Act	ivity 🗜 System			Wizards	\$ 9	Help
Configuring:	Traffic IP Groups	/irtual Servers Po	ols Config Summary					
Virtual Servers	Virtual Servers						Unf	fold All / Fold All
Servers	A virtual server accept	ts network traffic an	d processes it. It normally giv	ives each connection to a pool; the pool t	hen forwards the traffic to a ser	ver node.		
	► 🖌 🖻 SSL-Vser	ver (SSL (HTTPS),	port 443)					🖊 Edit
	► ✓ ESP-pool (U	DP - Streaming, po	ort 4500)					🖉 Edit
	Create a new Virtue	al Server						
	Virtual Server Name:	SSL-Server						
	virtual server name:							
	Protocol:		•					
			•					

Figure 50: Virtual Servers to Handle SSL and UDP Traffic

Que la c		10.251.2.152 (admi	in/admin) Logout
SPulse Secure' Virtual Traffic Manager Appliance 500 L 10 17.4		Cluster: OK	1.6 kb/s
Home Services Catalogs & Diagnose Activity & System	Wizards	¢	Help
Configuring: Traffic IP Groups Virtual Servers Pools Config Summary			
Virtual Virtual Servers			
Servers		Untol	id Ali / Fold Ali
A virtual server accepts network traffic and processes it. It normally gives each connection to a pool; the pool then forwards the traffic	to a server node.		
▼ 🛷 🚔 SSL-Vserver (SSL (HTTPS), port 443)			🖊 Edit
Balancing: SSL (HTTPS), port 443 Rules: 😂 Service protection class: 😂			
Listening on all IP addresses SLM class: S Bandwidth class:			
On to pool: SSI-pool Logging: 🗸			
V V ESP-pool (UDP - Streaming, port 4500)			🖊 Edit
Balancing: UDP - Streaming, port 4500 Rules: 🛤 Service protection class: 🛤			
Listening on all IP Addresses SLM class: Bandwidth class: B			
On to pool: ESP-pool Logging: 🗸			
Create a new Virtual Server			
Virtual Server Name:			
Protocol:			
Port: 80			
Default Traffic Pool			
Create Virtual Server			

Once the configuration is complete, go to home page and verify the configurations.

Figure 51: Pulse Secure vTM Home Page Showing Services and Event Logs

			10.251.2.152 (admin/admin) Logos		
S Pulse Sec	CUTE' Virtual Traffic Manager Appliance 5	00L10 17.4		Cluster: OK	1.6 kb/s
ft Home 🚱 S	ervices 🛄 Catalogs 🖇 Diagnose 🕍 Activ	ity 🖌 System	Wizards	۹.	He
	igin by admin: 2017-12-13 10:36:43 -0800 from npts since then: none.	121.244.123.150 (UI) on 10.251.2.152.			
Traffic Managers	10.251.2.152				
Services	SSL-Vserver SSL (HTTP5) (443)	SSI-pool Default Pool			
	ESP-pool UDP - Streaming (4500)	ESP-pool Default Pool			
Event Log	✓ 13/Dec/2017:20:04:36 -0800 INFO P	ool ESP-pool, Node 10.251.2.180:4500: Node 10.251.2.180 is working again		8	10.251.2.152
	✓ 13/Dec/2017:20:04:36 -0800 INFO P	ool SSI-pool, Node 10.251.2.180:443: Node 10.251.2.180 is working again			10.251.2.152
	✓ 13/Dec/2017:20:04:35 -0800 INFO M	onitor Ping: Monitor is working for node '10.251.2.180'.		9	10.251.2.152
	✓ 13/Dec/2017:20:04:35 -0800 INFO P	ool SSI-pool: Pool now has working nodes		8	10.251.2.152
	✓ 13/Dec/2017:20:04:35 -0800 INFO P	ool SSI-pool, Node 10.251.2.143:443: Node 10.251.2.143 is working again		8	10.251.2.152
				٩	Examine Logs

Accessing the Pulse Connect Secure Virtual Appliance

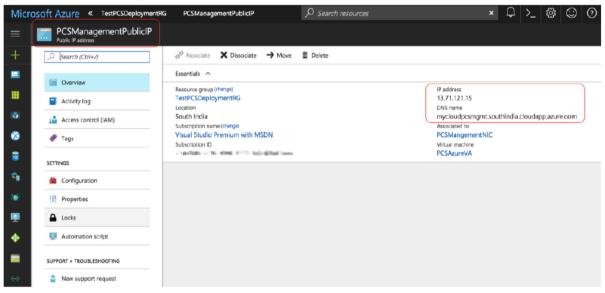
The Pulse Connect Secure appliance can be accessed:

- <u>as an administrator</u>
- <u>as an end user</u>
- using SSH console

Accessing the Pulse Connect Secure Virtual Appliance as an Administrator

To access the Pulse Connect Secure Virtual Appliance as an administrator, copy the IP address from the Pulse Management Interface resource.

Figure 52: Pulse Management Interface



Use the credentials provided in the provisioning parameters to log in as the administrator. The default PCS admin Ul user configured in the azuredeploy.json config file is: user 'admin' and password 'password'.

The administrator can configure Active Directory located in the corporate network for user authentication. The Pulse Connect Secure Virtual Appliance administrator can check troubleshooting tools provided in the Pulse Connect Secure admin UI (System->Maintenance->Troubleshooting), to verify whether Pulse Connect Secure is able to reach other cloud resources as well as corporate resources. For this, Azure network administrator needs to ensure that all other resources have Pulse Connect Secure Internal interface as its default gateway.

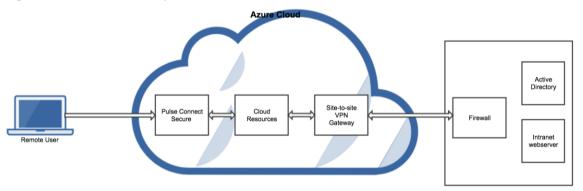
Accessing the Pulse Connect Secure Virtual Appliance as an End User

To access the Pulse Connect Secure Virtual Appliance as an end user, copy the IP address from Pulse External Interface resource.

Figure 53: Pulse External Interface

Micro	OSOft Azure Resource groups	TestPCSDeploymentRG PCSExternalPublicIP $ ho$ Se	earch resources	×	Û	>_	ŝ	\odot	?
≡	PCSExternalPublicIP								
+	Search (Ctrl+/)	$\mathscr{C}^{\mathcal{P}}$ Associate \bigstar Dissociate \rightarrow Move $ ilde{ ext{ II }}$ Delet	te						
	Overview	Essentials A Resource group (change)		IP address					
	Activity log	TestPCSDeploymentRG		13.71.127.197					
	Access control (IAM)	South India Subscription name (change)	L	mycloudpcsext.southi Associated to	ndia.clo	udapp.a	zure.com	n	
٢	I Tags	Visual Studio Premium with MSDN Subscription ID		PCSExternalNIC Virtual machine					
3	SETTINGS	Chicaelinin: - 1181 - 45403 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 - 511 -		PCSAzureVA					
۹	Gonfiguration	-							
1	Properties								
	Locks								
	Automation script								

Figure 54: Resource in Corporate Network



Accessing the Pulse Connect Secure Virtual Appliance using SSH Console

To access the Pulse Connect Secure Virtual Appliance using the SSH console, copy the Public IP address from the PCSManagementPublicIP resource.

On Linux and Mac OSX

Execute the following command:

ssh -i <rsa-private-key-file> <PCS-Management-Interface-PublicIP> -p 6667

On Windows

- 1. Launch the Putty terminal emulator.
- 2. In the Session category:
 - Enter the host name or IP address.
 - Enter the port number.
 - Select the connection type as SSH.

Figure 55: Putty Co	nfiguration – Basic Options	
🕵 PuTTY Configuration		8
Category:		
Session Logging Terminal Keyboard Bell Features Window	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 13.71.121.15 6667 Connection type: Raw Telnet Rlogin SSH Se	rial
Appearance Behaviour Translation Colours Connection Data Proxy Telnet Rlogin Serial	Load, save or delete a stored session Saved Sessions Default Settings Default Settings Delete	;
About	Close window on exit: Always Never Only on clean exit Open Cancer	el

3. Select **Connection > SSH > Auth**. Click **Browse** and select the private key file for authentication.

Figure 56: Putty Configuration – SSH Authentication

🕵 PuTTY Configurat	ion		?	\times			
Category:							
- Teminal	^	Options controlling SSH authentication					
Keyboard Bell Features		Display pre-authentication banner (SSH Bypass authentication entirely (SSH-2 of					
 Window Appearance Behaviour Translation Selection 	l	Authentication methods Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH					
Colours Connection Data Proxy Telnet	l	Authentication parameters Allow agent forwarding Allow attempted changes of usemame Private key file for authentication:	in SSH-2	_			
Rlogin ⊡ SSH Kex Host keys		C:\Users\ops\myPrivateKey.ppk	Browse				
···· Flost Reys ···· Cipher ···· TTY ···· X11	*						
About	Help	Open	Cance	4			

System Operations

The Azure VA portal provides Start, Restart and Stop operations to control the Virtual Appliance connection.

Figure 57: System Operations

≡	PCSAzureVA Virtual machine	
+	Search (Ctrl+/)	
	Q Overview	Essentials 🔿
	Activity log	Resource group (change) Computer name upgradetest PCSAzureVA
	Access control (IAM)	Status Operating system Running Linux
8	🛷 Tags	Location Size South India Ch Standard DS3 v2 (4 vcpus, 14 GB memory)
2	X Diagnose and solve problems	Subscription (change) Public IP address Visual Studio Premium with MSDN 52.172.34.62
.	SETTINGS	Subscription ID Virtual network/subnet c7def686-c196-4946-9175-0d2d28a03eee PCSVirtualNetwork/PCSInternalSubnet
18 7	Availability set	DNS name mycloudpcsint.southindia.cloudapp.azure.com

On the Azure portal top menu bar:

- Click **Start** to start a VM
- Click **Stop** to stop the VM
- Click **Restart** to restart the VM

The corresponding CLI commands are: Start a VM az vm start --resource-group myResourceGroup --name myVM

Stop a VM

az vm stop --resource-group myResourceGroup --name myVM

Restart a VM

az vm restart --resource-group myResourceGroup --name myVM

Network Configuration

IP Address Assignment for Internal, External and Management Interfaces

Each interface in Azure can have private and public IP addresses. Sample Azure Templates provided by Pulse Connect Secure creates the Pulse Connect Secure Virtual Appliance with public and private IP addresses for external and management interfaces and only private IP address for internal interface. More details about IP address types on Azure can be seen at: <u>https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network/virtual-network/virtual-network-ip-addresses-overview-arm</u>

IP Addressing Modes

When Pulse Connect Secure gets deployed by using the sample templates provided by Pulse Secure, Pulse Connect Secure comes up with multiple interfaces. If you take an example of a template "pulsesecure-pcs-3-nics.zip" provided by Pulse Secure, you notice the following things.

PCS external interface and PCS management interface are having both Public and Private IP addresses. In the below code snippet, observe the network interface getting created with two IP addresses - private IP address and public IP address. Highlighted section points to private IP allocation method and Public IP address getting assigned to NIC.

- 1. "type": "Microsoft.Network/networkInterfaces",

If you want to have control on the IP assigned to Network Interface, then you need to change the attribute "privateIPAllocationMethod" from "Dynamic" to "Static". Also, you need to add an attribute called "privateIPAddress" which holds the static IP address. When you are assigning static IP address, make sure that it is not in the reserved IP category.

```
    "ipConfigurations": [{
    "name": "ipconfig2",
    "properties": {
    "privatelPAllocationMethod": "Static",
    "privatelPAddressVersion": "IPv4",
    "privatelPAddress": "[variables('privatelPExternal')]",
    }
    }]
```

Modifying Network Parameters After Deployment

Since Networking Infrastructure is provided by Azure, a PCS admin cannot change Networking configuration after deployment. Hence, both admin UI and ssh does not support changing network configuration.

Controlling the Selection of Internal, External and Management Interfaces

Sample Azure Template, provided by Pulse Secure, requests Azure fabric to create three Network Interfaces. While running this template, Azure fabric creates interfaces named eth0, eth1 and eth2 and attaches them to PCS Virtual Interface.

So, the question is, among eth0, eth1 and eth2 which network interface will become external, internal or management interface? Below table answers this question.

Interface Name	PCS Interface
eth0	internal interface
eth1	external interface
eth2	management interface

Then, question is how you can control the order of network interfaces named eth0, eth1 and eth2 created through Azure Template?. Azure supports two types of interfaces: primary and secondary. Only one primary interface can be present on a VM.

For more details of primary and secondary interface, see <u>https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-interface-addresses</u>.

The Pulse Connect Secure Virtual Appliance is qualified with internal interface as primary and other two are secondary. In the following code snippet, three network interfaces get assigned to VM. These three NICs with ID "nic1", "nic2" and "nic3" are internally mapped to 'eth0', 'eth1', and 'eth2' respectively.

1.	"networkProfile": {
2.	"networkInterfaces": [{
3.	"id": "nic1",
4.	"properties": {
5.	"primary": true
6.	}
7.	}, {
8.	"id": "nic2",
9.	"properties": {
10.	"primary": false
11.	}
12.	}, {
13.	"id": "nic3",
14.	"properties": {
15.	"primary": false
16.	}
17.	}]
18.	},

PCS converts eth0 to int0, eth1 to ext0 and eth2 to mgmt0. This means, the network interface with ID nic1 will be internal interface, nic2 will be external interface and nic3 will be management interface. The below table depicts this scenario well:

Interface Name	PCS Interface	Network ID
eth0	internal interface (int0)	nic1
eth1	external interface (ext0)	nic2
eth2	management interface (mgmt0)	nic3

Suppose if you make 'nic2' as primary, then the order may not be maintained, and it is difficult to predict which interface will become internal interface of PCS. As a best practice, always assign 'primary' to the first network interface which will become internal interface of PCS.

Backing up Configs and Archived Logs on Azure Storage

Pulse Connect Secure supports pushing configs and archived logs to the servers that support SCP and FTP protocols. In the Azure deployment, Pulse Connect Secure now supports pushing configs and archived logs to the Azure storage.



Configuring Backup Configs and Archived Logs via PCS Admin Console

To configure backing up configs and archived logs:

- 1. Log into the Pulse Connect Secure admin console.
- 2. Navigate to Maintenance > Archiving > Archiving Servers.
- 3. In the Archive Settings section, select the **Azure Storage** option and configure Storage Name, Storage Key, Container Name and Destination Path Prefix.

Figure 58: Azure Archive Settings

★ Archive Settings		
Method:		S S3 🧿 Azure Storage
*Storage Name:	pcsgoldenstorage	Azure storage account name
*Storage Key:		Secret access key to storage
*Container Name:	testaz	Container name in storage account
Dest Path Prefix:		Path to copy files under container,eg: folder1/folder2
Test Connection		
* indicates required field		

Parameter	Description
Storage Name	 To create an Azure V2 Storage account: In the Azure portal, select All services. From the list of resources, select Storage Accounts. In the Storage Accounts window, click Add. Select the subscription in which to create the storage account. Under the Resource group field, select Create new and enter a name for the new resource group. Next, enter a unique name, between 3 and 24 characters length, for the storage account. For the procedure to create storage account, refer https://docs.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account?tabs=azure-portal
Storage Key	 To view storage key, In the Azure portal, locate the storage account (see Storage Name description). In the Settings section, select Access keys. The account access keys and the complete connection string for each key appear. Find the Key value under key1 and click the Copy button to copy the account key. For more details, refer https://docs.microsoft.com/en-

us/azure/storage/common/storage-account-manage#view-and-copy-access-	
Container Name	Container name in the storage account.
Dest Path Prefix (Optional)	Path to copy files under container.

Configuring Backup Configs and Archived Logs via REST

Setting Azure as Archive Logs Backup

REQUEST PUT /api/v1/configuration/system/maintenance/archiving/settings HTTP/1.1 Content-Type: application/json
{ "archive-path": "folder1/folder2", "method": "AZURE", "Password-cleartext": "fasfdsfsdasfas", "server": "mystorage", "user-name": "mycontainer"
}

Mapping of keys in POST body:

archive-path	Destination path Prefix
method	method (AZURE)
Password-cleartext	Storage Key
server	Storage Name
user-name	Container Name

Decommissioning Pulse Connect Secure

When deploying Pulse Connect Secure, if you have selected the option "Use existing resource group", then follow the steps mentioned in the section Delete Pulse Connect Secure and Resource It Uses, but not the Other Resources in Resource Group. Else if you have selected the option "New resource group" then follow the steps mentioned in the section Delete Entire Resource Group that the Pulse Connect Secure Is In.

Delete Entire Resource Group that the Pulse Connect Secure Is In

- 1. Log into Azure portal.
- 2. Navigate to Resource Groups.
- 3. Click on the resource group where Pulse Connect Secure is in.
- 4. Click on the **Delete resource group** button. In the confirmation page type in resource group name and click **Delete**.

Search (Ctrl+/)	➡ Add ◆ Assign Tags ■■ Columns	Delete resource group	\bigcirc Refresh \rightarrow Move	
	Essentials			
(*) Overview	Subscription name (change)	Deployments		
Activity log	Visual Studio Premium with MSDN	1 Succeeded		
Access control (IAM)	Subscription ID c7def686-c196-4946-9175-0d2d28a03eee			
Tags	Filter by name All types	✓ All locations	✓ No grouping	
ETTINGS	11 items	түре 🔨	LOCATION 1	
🗳 Quickstart	Backend2PCSRoute	Route table	South India	
• Resource costs	SGExternal	Network security gro		
↑ Deployments	NSGInternal	Network security gro	. South India	
Policies	NSGManagement	Network security gro	. South India	
Properties	PCSExternalNIC	Network interface	South India	•
	PCSExternalPublicIP	Public IP address	South India	•
	PCSInternalNIC	Network interface	South India	•
Automation script	PCSManagementPublicIP	Public IP address	South India	•
IONITORING	PCSMangementNIC	Network interface	South India	•
Metrics	📃 💆 РСЅРОС	Virtual machine	South India	

Figure 59: Delete Resource Group

- 5. Navigate to the storage account where the Pulse Connect Secure VHD image is stored.
- 6. In the storage account, click on **Blobs**. Find boot diagnostic folder and delete it. Boot diagnostic folder name will have the pattern "bootdiagnostics-<pcs-name>-<random-ascii-characters>".
- 7. In the storage account, click on **Blobs**. Find and click on the **vhds** folder. Find and delete file size named "rcsOSDisk.vhd".

Delete Pulse Connect Secure and Resource It Uses, but not the Other Resources in Resource Group

- 1. Log into Azure portal.
- 2. Navigate to Resource Groups.
- 3. Click on the resource group where Pulse Connect Secure is in.
- 4. Delete the following resources:
 - PCS Virtual Machine
 - Virtual Network named PCSVirtualNetwork
 - PCSInternalNIC, PCSExternalNIC and PCSManagementNIC
 - PCSExternalPublicIP and PCSManagementIP
 - Three Network Security Groups named NSGInternal, NSGExternal and NSGManagement
 - User-defined Routing table named Backend2PCSRoute
- 5. Navigate to the storage account where the Pulse Connect Secure VHD image is stored.
- 6. In the storage account, click on **Blobs**. Find boot diagnostic folder and delete it. Boot diagnostic folder name will have the pattern "bootdiagnostics-<pcs-name>-<random-ascii-characters>".
- 7. In the storage account, click on **Blobs**. Find and click on the **vhds** folder. Find and delete file size named "rcsOSDisk.vhd".

Pricing

The cost of running this product is combination of License cost and Azure infrastructure cost. It will be very difficult to find out Azure infrastructure cost for this product as it may vary with Regions/Country/Time. Hence, it is recommended to use "Azure Calculator", which is available online, to calculate the cost of running this product.

Here are resources that are created during deployment.

Resources	Category	Chargeable
PCS VM (Standard_DS3_V2)	Compute	Yes
Virtual Network with four subnets	Networking	No
Three NIC cards named PCSInternalNIC, PCSExternalNIC and PCSManagementNIC	Networking	No
Two static Public IPs name PCSExternalPublicIP and PCSManagementIP	Networking	Yes
Three Network Security Groups named NSGInternal, NSGExternal and NSGManagement.	Networking	No
User Defined Routing table named Backend2PCSRoute	Networking	No
Boot diagnostic file under existing storage account (Less than 5MB)	Storage	Yes
File size of 40GB in the existing storage account under Blobs and container VHDs named " <pcs-name><13 digit unique string>pcsOSDisk.vhd"</pcs-name>	Storage	Yes

Limitations

The following list of Pulse Connect Secure features are not supported in this release:

- VLAN tagging
- IPv6 capabilities
- Layer 3 Tunnel IP pool assignment via DHCP
- Layer 2 functionality like ARP Cache and ND Cache
- Virtual Ports
- Multicast capabilities
- Bandwidth management

Not Qualified

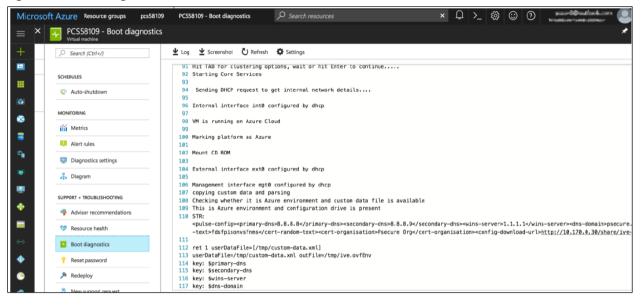
The following list of Pulse Connect Secure features are not qualified in this release:

- Pulse Connect Secure and Pulse One interaction
- Pulse Connect Secure and PWS interaction
- IF-MAP support

Troubleshooting

Pulse Connect Secure emits booting logs at a specified storage. You can check the storage details of the boot diagnostic logs as shown below:

Figure 60: Boot Diagnostics



Frequently Asked Questions

This section provides solution for the frequently asked questions.

FAQ1: I am unable to connect to my backend resources through L3 VPN

Solution: The solution describes the configuration required in the Azure Virtual Network and PCS to connect to the On-premise network through the L3 VPN connection.

The following network topology shows two networks, Azure Virtual Network and On-premise network, with Site-to-Site connectivity between them.

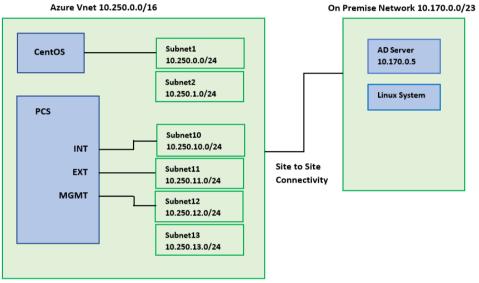


Figure 61: Pulse Connect Secure on Microsoft Azure

Before proceeding with the configuration, prepare a configuration checklist that will be handy during the configuration.

Azure Virtual Network	Resource group name: OnPremRG
	Virtual Network name: VirtualNetwork
	Virtual Network address space: 10.250.0.0/16
	Subnets:
	Subnet1: 10.250.0.0/24
	Subnet2: 10.250.1.0/24
	Subnet3: 10.250.2.0/24
	Subnet4: 10.250.3.0/24
	Subnet10: 10.250.10.0/24
	Subnet11: 10.250.11.0/24
	Subnet12: 10.250.12.0/24
	Subnet13: 10.250.13.0/24
	PCS Internal interface connected to Subnet10 (10.250.10.0/24)
	PCS External interface connected to Subnet11 (10.250.11.0/24)
	PCS Management interface connected to Subnet12 (10.250.12.0/24)
	PCS VPN pool connected to Subnet13 (10.250.13.0/24)

	CentOS system IP address: 10.250.0.4 connected to Subnet1 (10.250.0.0) Public IP address: 104.211.245.193 VPN Pool address space: 10.250.13.0/24
On-premise network	On-premise Network address space: 10.170.0.0/23 AD Server IP address: 10.170.0.5

The Azure Vnet with address space 10.250.0.0/16 has four subnets - Subnet10 to Subnet12 - connected to PCS's Internal, External and Management interfaces respectively, and Subnet13 connected to PCS VPN pool. The CentOS system is connected to Subnet1.

Figure 62: Virtual Network in a Resource Group (OnPremRG)

Microsoft Azure				× 🗘 >_ 🎕 😳	
+ Create a resource	Home Resource groups OnPremRG Virt				* ×
All services		O Refresh → Move			
★ FAVORITES	\Leftrightarrow Overview	Resource group (thing) OnPremRG Location		Address space 10.250.0.0/16 DNS servers	
🧮 Dashboard	Activity log	South India Subscription (change)		Azure provided DNS service	
All resources	Access control (IAM)	Visual Studio Premium with MSDN Subscription ID c7def686-c196-4946-9175-0d2d28a03eee			
Resource groups	🥔 Tags	c/def686-c196-4946-91/5-0d2d28803eee		*	
S App Services	X Diagnose and solve problems	Connected devices			
🥃 SQL databases	SETTINGS	Search connected devices DEVICE	туре	1 IP ADDRESS	SUBNET †.
📬 SQL data warehouses	Address space	PCSExternalNIC	Network interface	10.250.11.4	subnet11
🧟 Azure Cosmos DB	 Connected devices 	PCSMangementNIC	Network interface	10.250.12.4	subnet12
Virtual machines	<-> Subnets	PCSInternalNIC	Network interface	10.250.10.4	subnet10
🚸 Load balancers	DNS servers	VnetGateway	Virtual network gateway	-	GatewaySubnet
Storage accounts	Service endpoints	centosycs129	Network interface	10.250.0.4	subnet1
↔ Virtual networks	Properties				
Azure Active Directory	Locks				
🧿 Monitor					

Figure 63: Subnets in the Virtual Network

Microsoft Azure		,	earch resources, services and docs	× 🖧 >_	Si C O outlook	
+ Create a resource	Home Resource groups OnPremRG Virtu <-> VirtualNetwork - Subnets Virtual network					* ×
EAVORITES	, Search (Ctrl+∕)	+ Subnet + Gatewa	y subnet			
Dashboard	Overview Activity log	NAME	°↓ ADDRESS RANGE	AVAILABLE ADDRESSES		°4
All resources	Access control (IAM)	subnet2	10.250.1.0/24	251	-	
 Resource groups App Services 	 Tags Diagnose and solve problems 	subnet4	10.250.3.0/24	251 250		
sQL databases	SETTINGS	subnet12	10.250.12.0/24	250	-	
SQL data warehouses Azure Cosmos DB	Address space Connected devices	subnet14	10.250.14.0/24	251	-	
Virtual machines	<> Subnets	subnet6	10.250.5.0/24	251	-	
 Load balancers Storage accounts 	DNS servers	subnet13 subnet10	10.250.13.0/24	251		
Storage accounts Virtual networks	Service endpoints	GatewaySubnet	10.250.255.0/27	26	-	•••
Azure Active Directory	Locks	subnet1	10.250.0.0/24	250	-	

Log in to PCS admin console and configure the VPN tunneling connection profile. The VPN pool has the range 10.250.13.10 to 10.250.13.20 in subnet13.

Figure 64: VPN Tunneling Connection Profile

Access Control Connection Profiles Split-tunneling Networks	Bandwidth Management			
Show profiles that apply to: All roles 🗘 🔍 Update				
iew/Modify VPN Tunnel Server side configuration				
New Profile Duplicate Delete 🛨 🖡			Save C	hanges
Profiles	IPv4 Addresses	IPv6 Addresses	DNS Settings	Appli to ro
1. vpn pool	10.250.13.10-10.250.13.20		No proxy server Default Search client DNS servers first	All roles

Create a user for this VPN tunnel policy and define the role mapping rule.

Figure 65: Use Role Mapping

lse Connect Secur	•		Help Guidance Switch to New UI Sign Out
System Status + Configuration + Network + Clustering + Traffic Segregation +	Uter Realms > Users > Role Mapping General Authentication Policy Role Mapping		
IF-MAP Federation + Log/Monitoring +	Specify how to assign roles to users when they sign in. Users that are not	assigned a role will not be able to sign in.	
Reports () Authentication	New Rule Duplicate Delete 🕇 🖡		Save Changes
Signing In + Endpoint Security +	When users meet these conditions	assign these roles	Rule Name Stop
Auth. Servers	C 1. username is "*"	→ Users	rule 0
Administrators Admin Realms			
Admin Roles → Users	When more than one role is assigned to a user: Merge settings for all assigned roles 		
Jser Realms >	User Roles st select from among assigned roles		
Resource Profiles			
Resource Policies	1. Users		

Testing the Connection to CentOS System

1. Note down the public IP address / FQDN of PCS's External interface.

Figure 66: Public IP of PCS External Interface

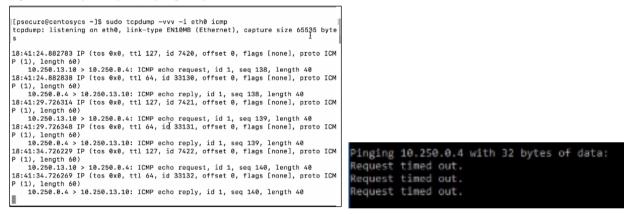
Microsoft Azure		$\mathcal P$ Search resources, services and docs	× 🗘 >_ 🍩 😳 Ø	ycsunil@outlook.com
+ Create a resource	Home Resource groups pcs83r3 PCSE PCSExternalPublicIP Public IP address	xtems Public P		* ×
i All services ★ FAVORITES	Search (Ctrl+/) Overview			
🔲 Dashboard	Activity log	Resource group (change) pcs83ar3 IP address	Location South India Subscription name (change)	
All resources	Access control (IAM)	52.172.29.21 DNS name mycloud12pcsext.southindia.cloudapp.azure.com	Visual Studio Premium with MSDN Subscription ID c7def686-c196-4946-9175-0d2d28a03eee	
 Resource groups App Services 	SETTINGS	Associated to PCSExternalNIC Virtual machine		
SQL databases	e Configuration	pcs83r3		

2. From client, connect to PCS.

Figure 67: Client Connection

3. Once connected, on the CentOS system run tcpdump to capture the icmp traffic. And from the client system, ping to CentOS system.

Figure 68: tcpdump and ping responses



The following is observed:

- The CentOS system shows echo request and echo reply messages.
- The ICMP request is from 10.250.13.10, which is the tunnel IP.
- The client system shows the "Request timed out" messages.
- The packet is sent out from the CentOS system, but it is not forwarded to the PCS Internal interface.

The solution is to add a route that forwards any packet in the tunnel IP address range 10.150.13.0/24 to PCS Internal interface. And associate the route to subnet (Subnet1) connected to the CentOS system.



Microsoft Azure		\mathcal{P} Search resources, services and docs	× 🗘 >_ 🏐 😳 🧿	ycsunil@outlook.com
+ Create a resource	Home Resource groups pcs83r3 Backer			* ×
i ⊟ All services	Search (Ctrl+/)	→ Move		
★ FAVORITES	Cverview	Essentials A	Associations	
Dashboard	 Activity log 	pcs83r3 Location	0 subnet associations	
All resources	Access control (IAM)	South India Subscription name (change)		
Resource groups	🥔 Tags	Visual Studio Premium with MSDN Subscription ID		
App Services	X Diagnose and solve problems	c7def686-c196-4946-9175-0d2d28a03eee		
🧧 SQL databases	SETTINGS	Search routes NAME ADDRESS PREFix		°↓
🔓 SQL data warehouses	Configuration	BackEndToPCS 10.250.13.0/24	10.250.10.4	
1 m m	Pouter			

Figure 70: Subnet Association

Microsoft Azure		ho Search resources, services and d	locs × 🖓		unil@outlook.com
+ Create a resource	Home Resource groups pcs83r3 Backen <-> Backend2PCSRoute - Subnet Route table				* ×
All services	Search (Ctrl+)	Associate Search subnets			
🔲 Dashboard	Cverview	NAME	VIRTUAL NETWORK	⇒ SECURITY GROUP -	•.
All resources	Access control (IAM)				

Wait for some time and observe that the packets are transmitted successfully.

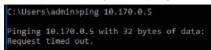
Figure 71: Successful Packets Transmission

Pinging 18.258.8.4 with	h 32 byte	s of data:	
Request timed out.			
Reply from 10.250.0.4:	bytes=32	time=11ms	TTL=63
Reply from 10.250.0.4:			

Session time remaining:	54m 12s
Session duration:	5m 48s
Tunnel type:	VPN
VPN type:	ESP
Assigned IPV4:	10.250.13.10
Bytes in:	660
Bytes out:	9468
Connection source:	User-added

Testing the Connection to On-premise Resource

1. From the client system, ping the on-premise resource, AD server whose IP address is 10.170.0.5.



The output shows "Request timed out" messages. The packet in the return traffic stops at the Azure gateway subnet.

The solution is to add a route that forwards any packet at the gateway subnet to tunnel IP address range 10.150.13.0/24, and associate the route to gateway subnet.

Figure 72: Route Table

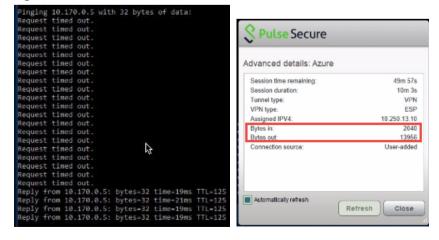
Microsoft Azure		$\mathcal P$ Search resources, services and docs	× 🗘 >_ 🏽 🖸 O) ycsunil@outlook.com YCSUNILOUTLOOK (DEFAULT
+ Create a resource	Home Resource groups pcs83r3 Backen			* ×
i Ξ All services	Search (Ctrl+/)	Move Delete ssentials		
 FAVORITES Dashboard 	Overview Activity log	Resource group (dunge) pcs83r3 Location	Associations 0 subnet associations	
All resources	Access control (IAM)	South India Subscription name (change) Visual Studio Premium with MSDN		
 Resource groups App Services 	Tags Tags Diagnose and solve problems	Subscription ID c7def686-c196-4946-9175-0d2d28a03eee		
SQL databases	SETTINGS	Search routes ADDRESS PREFix		^
📬 SQL data warehouses	Configuration	BackEndToPCS 10.250.13.0/24	10.250.10.4	

Figure 73: Subnet Association

Microsoft Azure		P Set	arch resources, services and docs	× 🗘	>_ 🎲 😳 🔿 ycsu	nil@outlook.com
+ Create a resource	Home Resource groups pcs83r3				Saved route table for subnet	6:48 PM ×
E All services	Search (Ctrl+/)	+ Associate			Successfully saved route table for subn	rt 'GatewaySubnet'.
★ FAVORITES	Cverview	Search subnets				
Dashboard	Activity log	NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP	
All resources	Access control (IAM)	subnet1	10.250.0.0/24	VirtualNetwork		
Resource groups	🛷 Tags	GatewaySubnet	10.250.255.0/27	VirtualNetwork	43	

Wait for some time and observe that the packets are transmitted successfully.

Figure 74: Successful Packets Transmission



FAQ2: Users are unable to access internet resources when connected to a VPN tunnel on an Azure-based PCS

Cause: When end user launches Pulse Client, connects to PCS in Azure and tries to access internet, PCS forwards the received packets (src ip: tunnel-ip, dest-ip: internet) through its internal interface. These packets reach Azure hidden Network Load Balancing (NLB). Azure hidden NLB drops these packets because it sees there is no NIC in the VNET with source IP as tunnel IP, the src-ip of the packet coming out of PCS is 'Client tunnel IP'. **Solution**: Pulse Connect Secure must be able to SNAT these packets to the Internal interface IP which belongs to a subnet within the VNET.

To NAT endpoint tunnel IP to Internal interface IP, do the following:

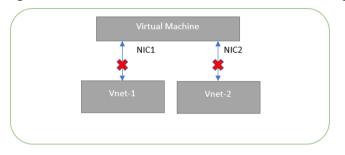
- 1. Log in to Pulse Connect Secure admin console.
- 2. Navigate to System > Network > VPN Tunneling.
- 3. Enable Source NATTING. By default, Source NATTING is disabled.

Source NATTING	
 Enable Disable 	Save

Appendix A: Network Security Group (NSG)

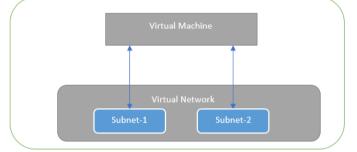
Microsoft Azure has a limitation where virtual machine with multiple network interfaces cannot connect to different Virtual Networks (VNETs). For example, a VM with two NIC cards, NIC1 and NIC2, will not be able to connect to Vnet1 and Vnet2 respectively.

Figure 75: Virtual Machine with two NIC cards Connecting to VNet1 and Vnet2



Microsoft Azure supports a virtual machine with multiple NICs to connect to different Subnets under a same Virtual Network. For example, a VM with two NICs, NIC1 and NIC2, can connect to 'Subnet1' and 'Subnet2' where these subnets exist under a same Virtual Network respectively.





Azure provides isolation between different Vnets. But it does not provide the same kind of isolation when it comes to subnets in the same Vnet. For example, consider a Vnet has two subnets, Subnet1 and Subnet2. And consider two VMs, VM-1 and VM-2, which are connected to Subnet1 and Subnet2 respectively. In this scenario VM-1 can access the resources from VM-2 and vice versa.

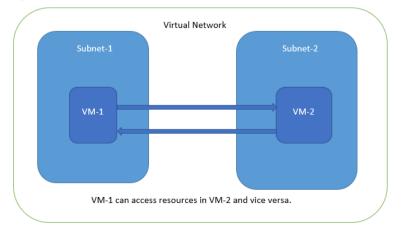


Figure 77: Virtual Machine VM-1 can Access Resources in VM-2 and Vice Versa

Application isolation is an important concern in enterprise environments, as enterprise customers seek to protect various environments from unauthorized or unwanted access. To achieve the traffic isolation between subnets, go for an option of filtering traffic using "Network Security Group" provided by Azure.

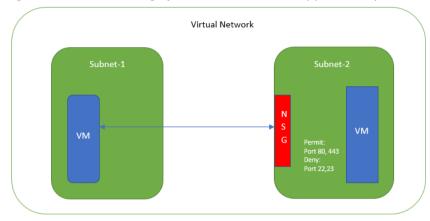


Figure 78: Traffic Filtering by MS Azure Network Support Group

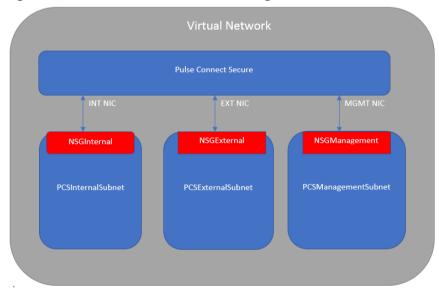
Pulse Connect Secure, when provisioned through the ARM template provided by Pulse Secure, creates four subnets under a virtual network named "PCSVirtualNetwork". The four Subnets are:

- 1. PCSInternalSubnet
- 2. PCSExternalSubnet
- 3. PCSManagementSubnet
- 4. PCSTunnelVPNPoolSubnet

Along with above mentioned subnets, create the following three Network Security Groups (NSG) policies:

- 1. NSGExternalSubnet
- 2. NSGInternalSubnet
- 3. NSGManagementSubnet

Figure 79: NSG External, Internal and Management Subnets



In Network Security Group (NSG) we need to create policies for Inbound and outbound traffic.

1. The list of NSG Inbound/Outbound rules created "NSGExternalSubnet" are:

Figu	ure 80: NSG External -	Inbound I	Rules					
×	NSGExternal - Inbound securit	y rules						
	Search (Ctrl+/)	🕇 Add 💿 [Default rules					
-	🌍 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
	Activity log	100	allowHTTP	80	Any	Any	Any	Allow
	Access control (IAM)	200	allowHTTPS	443	Any	Any	Any	Allow
	Tags	300	allowPTP	11000-11099	Any	Any	Any	Allow
	X Diagnose and solve problems	400	allowESP	4500	Any	Any	Any	Allow
	SETTINGS	500	allowIKEv2	500	Any	Any	Any	Allow
	→ Inbound security rules	4000	denyAll	Any	Any	Any	Any	🕴 Deny
		65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
	Network interfaces	65001	AllowAzureLoadBalancerInBo	Any	Any	AzureLoadBala	Any	Allow
	<-> Subnets	65500	DenyAllInBound	Any	Any	Any	Any	🕴 Deny

Figure 81: NSG External - Outbound Rules

Search (Ctrl+/)	🕂 Add 👁	Default rules					
🔋 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
Activity log	100	denyInternalSubnet	Any	Any	Any	10.20.1.0/24	🕴 Deny
Access control (IAM)	200	denyManagementSubnet	Any	Any	Any	10.20.3.0/24	😣 Deny
Tags	300	denyPoolRange	Any	Any	Any	10.20.4.0/24	8 Deny
X Diagnose and solve problems	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
SETTINGS	65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
Jubound security rules	65500	DenyAllOutBound	Any	Any	Any	Any	8 Deny
Outbound security rules							

2. The list of NSG Inbound/Outbound rules created "NSGInternalSubnet" are:

Figure 82: NSG Internal - Inbound Rules

*		ty rules						
	Search (Ctrl+/)	🕇 Add 👁 D	efault rules					
	🔋 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
	Activity log	100	denyExternalSubnet	Any	Any	10.20.2.0/24	Any	8 Deny
	Access control (IAM)	200	allow-custom-ssh	6667	Any	Any	Any	Allow
	🥔 Tags	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
	X Diagnose and solve problems	65001	AllowAzureLoadBalancerInBo	Any	Any	AzureLoadBala	Any	Allow
s	SETTINGS	65500	DenyAllInBound	Any	Any	Any	Any	8 Deny
	⇒ Inbound security rules							
	Outbound security rules							
	Network interfaces							
	<-> Subnets							

Figu	ure 83: NSG Internal -	Outbound	d Rules					
, ;-	NSGInternal - Outbound se	ecurity rules			-			
L	Search (Ctrl+/)	🕇 Add 👁	Default rules					
L	Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
	Activity log	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
L	Access control (IAM)	65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
L	Jags	65500	DenyAllOutBound	Any	Any	Any	Any	😣 Deny
L	X Diagnose and solve problems							
L	SETTINGS							
L	Linbound security rules							
L	Outbound security rules							
	Network interfaces							

3. The list of NSG Inbound/Outbound rules created "NSGManagementSubnet" are:

Figure 84: NSG Management - Inbound Rules

NSGManagement - Inbound s	security rules						
	🕇 Add 👁 D	efault rules					
🌍 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
Activity log	100	allowHTTPS	443	Any	Any	Any	Allow
Access control (IAM)	200	allowHTTP	80	Any	Any	Any	Allow
🥔 Tags	300	allowCustomSSH	6667	Any	Any	Any	Allow
X Diagnose and solve problems	400	allowDMI	830	Any	Any	Any	Allow
SETTINGS	4000	denyAll	Any	Any	Any	Any	8 Deny
Inbound security rules	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
 Outbound security rules 	65001	AllowAzureLoadBalancerInBo	Any	Any	AzureLoadBala	Any	Allow
Network interfaces	65500	DenyAllInBound	Any	Any	Any	Any	😣 Deny
<-> Subnets							

Figure 85: NSG Management - Outbound Rules

Search (Ctrl+/)	Add 👁 Default rules						
🔋 Overview	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
Activity log	100	denyInternalSubnet	Any	Any	Any	10.20.1.0/24	🕴 Den
Access control (IAM)	200	denyExternalSubnet	Any	Any	Any	10.20.2.0/24	🕴 Den
🛷 Tags	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allov
X Diagnose and solve problems	65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
SETTINGS	65500	DenyAllOutBound	Any	Any	Any	Any	🕴 Denj
Jubound security rules							
Outbound security rules							
Network interfaces							

Appendix B: Pulse Connect Secure Resource Manager Template

Pulse Secure provides sample Azure template files to deploy the Pulse Connect Secure Virtual Appliance on Azure. Users can modify this to make it suitable for their need. Visit <u>https://www.pulsesecure.net</u> and download the pulsesecure-pcs-3-nics.zip file, and unzip it to get **azuredeploy.json**.

This template creates a new PCS with 3 NICs, Vnet, four subnets, NSG policies attached to PCS internal, external and management subnets and user-defined routes on the PCS internal subnet to ensure PCS is used as default gateway for L3 tunnel. All 3 NICs of PCS are configured with dynamic IP configuration and enabled IP forwarding. Public IPs are attached to the PCS external and management NIC.

The template has following sections:

parameters	This section defines the parameters used for deploying PCS on Azure. It contains parameter name, its default value and the mouse-over help text that is displayed when mouse is placed over the parameter in Azure Web portal. The parameters defined here are displayed in the Custom Deployment page of Azure portal.
variables	This section defines variables that will be used in the functions defined in the resources section.
resources	This section defines resource types that are deployed or updated in a resource group.
outputs	This section defines the public IP address and FQDN returned after successful deployment of PCS on Azure.

parameters

Figure 86: Custom Deployment

Custom deployment Deploy from a custom template			
SETTINGS			
PCS Sto Resource group of the ex PCS Sto, age Account Resource gro	kisting storage account where PCS image is uploaded		
Name	GoldenImageRG		
PCS Image Location URI 0	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure-drop5-upgrad		
PCSVM Name	PCSAzureVA		
PCS Config 🛛	<pre><pre>config><primary-dns>8.8.8.8</primary-dns><secondary-dns>8.8.8.9</secondary-dns></pre></pre>		
Dns Label Prefix Ext	mycloudpcsext		
Dns Label Prefix Mgmt 🖲	mycloudpcsmgmt		

PCS Storage Account Name: This is the name of the PCS Storage Account where the PCS Azure vhd image is stored.

```
"parameters": {
    "PCSStorageAccountName": {
    "type": "string",
    "defaultValue": "pcsgoldenstorage",
    "metadata": {
        "description": "Storage account name where PCS image is uploaded"
```

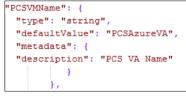
PCS Storage Account Resource Group Name: The is the name of the PCS Storage Account Resource Group where the PCS Azure vhd image is stored.

```
"PCSStorageAccountResourceGroupName": {
    "type": "string",
    "defaultValue": "GoldenImageRG",
    "metadata": {
        "description": "Resource group of the existing storage account where PCS image is uploaded"
    }
}.
```

PCS Image Location URI: The is the URL to the location where PCS Azure vhd image is stored.



PCS VM Name: This is the name given to PCS Virtual Appliance.



SSH Public Key: This is an RSA public key that is used to access Pulse Connect Secure via SSH.



PCS Config: This section contains provisioning parameters that are required during the deployment of a Virtual Appliance. An XML-based configuration file can be present in another Virtual Machine in Azure cloud or in the corporate network which is accessible for Pulse Connect Secure through site-to-site VPN between Azure and the corporate data center.

Pulse Connect Secure accepts the following parameters as provisioning parameters:

- primary-dns
- secondary-dns
- wins-server
- dns-domain
- username
- ssh-publickey
- cert-common-name
- cert-random-text

- cert-organization
- config-download-url
- config-data
- auth-code-license
- enable-license-server
- accept-license-agreement
- enable-rest

For details about these parameters, see Pulse Connect Secure Provisioning Parameters.

"<pulse-config<primary-dns>8.8.8.8</primary-dns>8.8.8.9</secondary-dns><wins-server>1.1.1.1</wins-server><dns-domain>psecure.net</dns-dom
ain><sdmin-username>admin-/admin-username>admin-password>/admin-password>/cert-common-name>val.psecure.net</cert-common-name><cert-random-text>
fdsfpisonvsfims</cert-organisation>config-download-url></config-data</config-data</config-data</config-data</config-data-</cert-code-license></mathcade-license><enable-license-serve
r>n</enable-license-server><accept-license-agreement></accept-license-agreement></mathcade-rest>/cure.psecure

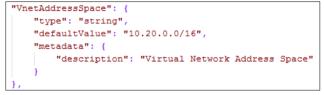
DNS Label Prefix Ext: This is the prefix for External Interface DNS label.



DNS Label Prefix Mgmt: This is the prefix for Management Interface DNS label.

```
"dnsLabelPrefixMgmt": {
    "type": "string",
    "defaultValue": "mycloudpcsmgmt",
    "metadata": {
        "description": "Unique DNS Name for the Public IP used to access PCS"
    }
}
```

VNet Address Space: This is a Virtual Network address space.



Internal Subnet: Subnet from which Pulse Connect Secure Internal Interface needs to lease IP.

```
"InternalSubnet": {
    "type": "string",
    "defaultValue": "10.20.1.0/24",
    "metadata": {
        "description": "PCS internal interface connects to this subnet"
    }
}
```

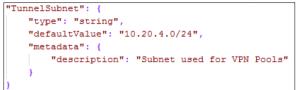
External Subnet: Subnet from which Pulse Connect Secure External Interface needs to lease IP.

```
"ExternalSubnet": {
    "type": "string",
    "defaultValue": "10.20.2.0/24",
    "metadata": {
        "description": "PCS external interface connects to this subnet"
    }.
```

Management Subnet: Subnet from which Pulse Connect Secure Management Interface needs to lease IP.

```
"ManagementSubnet": {
    "type": "string",
    "defaultValue": "10.20.3.0/24",
    "metadata": {
        "description": "PCS management interface connects to this subnet"
    }
```

Tunnel Subnet: Subnet which will be configured as Tunnel IP pool in Pulse Connect Secure VPN profile.



variables

PCS Virtual Network: This is the variable associated with the PCS Virtual Network.

"pcsvnetname" : "PCSVirtualNetwork",

PCS Internal Subnet: This is the variable associated with the Subnet from which Pulse Connect Secure Internal Interface needs to lease IP.

"pcsVnetIntSubnet" : "PCSInternalSubnet",

PCS External Subnet: This is the variable associated with the Subnet from which Pulse Connect Secure External Interface needs to lease IP

"pcsVnetExtSubnet" : "PCSExternalSubnet",

PCS Management Subnet: This is the variable associated with the Subnet from which Pulse Connect Secure Management Interface needs to lease IP.

"pcsVnetMgmtSubnet" : "PCSManagemnetSubnet",

PCS Tunnel VPN Pools Subnet: This is the variable associated with the Subnet which will be configured as Tunnel IP pool in Pulse Connect Secure VPN Profile.

"pcsVnetTunnelPool" : "PCSTunnelVPNPoolSubnet",

Backend to PCS Route: This creates route table for accessing the backend resources in Pulse Connect Secure Internal Interface.

"routeTableName" : "Backend2PCSRoute",

PCS Internal Private IP: This is the private IP address of the Internal IP.

"pcsIntPrivateIP" : "10.20.1.4",

PCS Internal NIC: This is network interface card of PCS Internal network.
"pcsIntNic" : "PCSInternalNIC",

PCS External NIC: This is network interface card of PCS External network.
"pcsExtNic" : "PCSExternalNIC",

PCS Management NIC: This is network interface card of PCS Management network.
"pcsMangementNic"

PCS External Public IP: This is public IP address assigned to PCS External Subnet.
"publicIPAddr1" : "PCSExternalPublicIP",

PCS Management Public IP: This is public IP address assigned to PCS Management Subnet.
"publicIPAddr2" : "PCSManagementPublicIP",]

Public IP Address Type: This variable is defined as static IP.
"publicIPAddressType" : "Static",

NSG Internal Subnet: This variable defines Network Security Group's Internal Subnet policy.
"nsgInt" : "NSGInternalSubnet",

NSG External Subnet: This variable defines Network Security Group's External Subnet policy.
"nsgExt" : "NSGExternalSubnet",

NSG Management Subnet: This variable defines Network Security Group's Management Subnet policy.
"nsgMgmt" : "NSGManagementSubnet",

VM Name: This variable defines PCS Virtual Machine name. "vmName" : "MyPCSVM",

VM Size: This variable defines PCS Virtual Machine size. It is 4 cores, 144MB memory.
"vmSize" : "Standard_DS3_v2",

Virtual Network ID: This variable defines PCS Virtual Network name.

"vnetID" : "[resourceId('Microsoft.Network/virtualNetworks',variables('pcsvnetname'))]",

"subnetRefInt" : "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetIntSubnet'))]",

"subnetRefExt" : "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetExtSubnet'))]",

"subnetRefMgmt" : "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetMgmtSubnet'))]",

API Version

"apiVersion" : "2015-06-15"

resources

publicIPAddresses/publicIPAddr1: This block is responsible for creating public IP address which is static in nature. This is used for external interface IP address of PCS.

"type": "Microsoft.Network/publicIPAddresses", "name": "[variables('publicIPAddr1')]",

publicIPAddresses/publicIPAddr2: This block is responsible for creating public IP address which is static in nature. This is used for management interface IP address of PCS.

"type": "Microsoft.Network/publicIPAddresses", "name": "[variables('publicIPAddr2')]",

virtualNetworks/pcvnetname: This block is responsible for creating PCS Virtual Network name. The creation of

PCS Virtual Network name depends on:

- Backend to PCS route
- NSG Internal Subnet
- NSG External Subnet
- NSG Management Subnet

"type": "Microsoft.Network/virtualNetworks",

"name": "[variables('pcsvnetname')]",

virtualNetworks/pcsVnetIntSubnet: This block is responsible for creating subnet. The created subnet is applied to PCS Internal interface.

"name": "[variables('pcsVnetIntSubnet')]",

virtualNetworks/pcsVnetExtSubnet: This block is responsible for creating subnet. The created subnet is applied to PCS External interface.

"name": "[variables('pcsVnetExtSubnet')]",

virtualNetworks/pcsVnetMgmtSubnet: This block is responsible for creating subnet. The created subnet is applied to PCS Management interface.

"name": "[variables('pcsVnetMgmtSubnet')]",

virtualNetworks/pcsVnetTunnelPool: This block is responsible for creating tunnel pool. The created tunnel pool is applied to PCS Tunnel Pool.

"name": "[variables('pcsVnetTunnelPool')]",

routeTables/routeTableName: This block is responsible for creating route table. The created route table is used for accessing the backend resources in PCS Internal interface.

"type": "Microsoft.Network/routeTables",

"name": "[variables('routeTableName')]",

networkInterfaces/pcsExtNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS External interface. The creation of this network interface depends on:

- PCS Virtual Network name
- Public IP address of External Subnet

```
"type": "Microsoft.Network/networkInterfaces",
"name": "[variables('pcsExtNic')]",
```

networkInterfaces/pcsMgmtNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Management interface. The creation of this network interface depends on:

- PCS Virtual Network name
- Public IP address of Management Subnet

```
"type": "Microsoft.Network/networkInterfaces",
"name": "[variables('pcsMgmtNic')]",
```

networkInterfaces/pcsIntNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Internal interface. The creation of this network interface depends on:

• PCS Virtual Network name

"type": "Microsoft.Network/networkInterfaces", "name": "[variables('pcsIntNic')]",

virtualMachines/PCSVmName: This block is responsible for creating Virtual Machine name. The created Virtual machine name is applied to PCS Virtual Machine. The creation of PCS Virtual Machine name depends on:

- Network Interface Card of PCS Internal interface
- Network Interface Card of PCS External interface
- Network Interface Card of PCS Management interface

"type": "Microsoft.Compute/virtualMachines", "name": "[parameters('PCSVmName')]",

networkSecurityGroups/nsgExt: This block is responsible for creating policy. The created policy is applied to Network Security Group's External interface.

"type": "Microsoft.Network/networkSecurityGroups", "name": "[variables('nsgExt')]",

The following security rules can be defined:

- allowHTTPS
- allowHTTP
- allowPTP
- allowESP
- allowIKEv2
- denyAll
- denyInternalSubnet
- denyManagementSubnet
- denyPoolRange

networkSecurityGroups/nsgMgmt: This block is responsible for creating policy. The created policy is applied to Network Security Group's Management interface.

"type": "Microsoft.Network/networkSecurityGroups", "name": "[variables('nsgMgmt')]",

The following security rules can be defined:

- allowHTTPS
- allowHTTP
- allowCustomSSH
- allowDMI
- denyAll
- denyInternalSubnet
- denyExternalSubnet

networkSecurityGroups/nsgInt: This block is responsible for creating policy. The created policy is applied to Network Security Group's Internal interface.

"type": "Microsoft.Network/networkSecurityGroups", "name": "[variables('nsgInt')]", The following security rules can be defined:

- denyExternalSubnet
- allow-custom-ssh

outputs

The outputs section defines the public IP address and FQDN that is displayed on successful deployment of PCS on Azure.

```
"outputs": {
    "hostname": {
        "type": "string",
        "value": "[reference(variables('publicIPAddr1')).dnsSettings.fqdn]"
```

Appendix C: Pulse Connect Secure Resource Manager Template for an Existing Virtual Network

Pulse Secure provides sample Azure template files to deploy Pulse Connect Secure Virtual Appliance on Azure. Users can modify this to make it suitable for their need. Visit <u>https://www.pulsesecure.net</u> and download the pulsesecure-pcs-3-nics.zip file, and unzip it to get **azuredeploy.json**.

This template creates a new PCS with 3 NICs, Vnet, four subnets, NSG policies attached to PCS internal, external and management subnets and user-defined routes on the PCS internal subnet to ensure PCS is used as default gateway for L3 tunnel. All 3 NICs of PCS are configured with dynamic IP configuration and enabled IP forwarding. Public IPs are attached to the PCS external and management NIC.

The template has following sections:

parameters	This section defines the parameters used for deploying PCS on Azure. It contains parameter name, its default value and the mouse-over help text that is displayed when mouse is placed over the parameter in Azure Web portal. The parameters defined here are displayed in the Custom Deployment page of Azure portal.
variables	This section defines variables that will be used in the functions defined in the resources section.
resources	This section defines resource types that are deployed or updated in a resource group.
outputs	This section defines the public IP address and FQDN returned after successful deployment of PCS on Azure.

parameters

Figure 87: Custom Deployment

Custom deployment Deploy from a custom template		
SETTINGS		
PCS Sto Resource group of the ex	isting storage account where PCS image is uploaded	
Name 0	GoldenImageRG	
PCS Image Location URI	https://pcsgoldenstorage.blob.core.windows.net/master/pcs-azure-drop5-upgrad	
PCSVM Name	PCSAzureVA	
PCS Config 0	<pre><pulse-config><primary-dns>8.8.8.8</primary-dns><secondary-dns>8.8.8.9</secondary-dns></pulse-config></pre>	
Dns Label Prefix Ext	mycloudpcsext	
Dns Label Prefix Mgmt 0	mycloudpcsmgmt	

PCS Storage Account Name: This is the name of the PCS Storage Account where the PCS Azure vhd image is stored.

```
"parameters": {
    "PCSStorageAccountName": {
    "type": "string",
    "defaultValue": "pcsgoldenstorage",
    "metadata": {
        "description": "Storage account name where PCS image is uploaded"
    }
},
```

PCS Storage Account Resource Group Name: The is the name of the PCS Storage Account Resource Group where the PCS Azure vhd image is stored.

```
"PCSStorageAccountResourceGroupName": {
    "type": "string",
    "defaultValue": "GoldenImageRG",
    "metadata": {
        "description": "Resource group of the existing storage account where PCS image is uploaded"
    }
},
```

PCS Image Location URI: The is the URL to the location where PCS Azure vhd image is stored.



PCS VM Name: This is the name given to Pulse Connect Secure Virtual Appliance.



PCS Config: This section contains provisioning parameters that are required during the deployment of a Virtual Appliance. An XML-based configuration file can be present in another Virtual Machine in Azure cloud or in the corporate network which is accessible for Pulse Connect Secure through site-to-site VPN between Azure and the corporate data center.

Pulse Connect Secure accepts the following parameters as provisioning parameters:

- primary-dns
- secondary-dns
- wins-server
- dns-domain
- username
- ssh-publickey
- cert-common-name
- cert-random-text
- cert-organization
- config-download-url
- config-data
- auth-code-license
- enable-license-server
- accept-license-agreement
- enable-rest

For details about these parameters, see Pulse Connect Secure Provisioning Parameters.

"<pulse-config><primary-dns>8.8.8.8</primary-dns>8.8.8.9</secondary-dns><wins-server>1.1.1.1</wins-server><dns-domain>gecure.net</dns-dom ain><admin-username>admin</admin-username><admin-password>password</admin-password><cert-common-name>val.psecure.net</cert-common-name><cert-random-text> fdsfpisopysfnmg</cert-random-text>cert-organisation>Esecure Qrg</cert-organisation>Config-download-url><config-data><auth-code-license><auth-code-license><enable-license-serve r>n</enable-license-server><accept-license-agreement></accept-license-agreement><enable-rest></pulse-config>",

SSH Public Key: This is an RSA public key that is used to access Pulse Connect Secure via SSH.



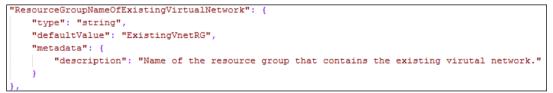
DNS Label Prefix Ext: This is the prefix for External Interface DNS label.

```
"dnsLabelPrefixExt": {
  "type": "string",
  "defaultValue": "mycloudpcsext",
  "metadata": {
    "description": "Unique DNS Name for the Public IP used to access PCS"
    }
}
```

DNS Label Prefix Mgmt: This is the prefix for Management Interface DNS label.

```
"dnsLabelPrefixMgmt": {
    "type": "string",
    "defaultValue": "mycloudpcsmgmt",
    "metadata": {
        "description": "Unique DNS Name for the Public IP used to access PCS"
    }
}
```

Resource Group Name of Exiting Virtual Network: Name of the Resource Group that contains the existing Virtual network.



Existing Virtual Network Name: Name of the existing Virtual network.

```
"existingVnetName": {
    "type": "string",
    "defaultValue": "virtualNetwork",
    "metadata": {
        "description": "Name of existing virtual network"
    }
}.
```

Existing Internal Subnet: Subnet from which Pulse Connect Secure Internal Interface needs to lease IP.

```
"existingInternalSubnet": {
    "type": "string",
    "defaultValue": "subnet1",
    "metadata": {
        "description": "PCS internal interface connects to this subnet"
    }
},
```

Existing External Subnet: Subnet from which Pulse Connect Secure External Interface needs to lease IP.

```
"existingExternalSubnet": {
    "type": "string",
    "defaultValue": "subnet2",
    "metadata": {
        "description": "PCS external interface connects to this subnet"
    }
}
```

Existing Management Subnet: Subnet from which Pulse Connect Secure Management Interface needs to lease IP.

```
"existingManagementSubnet": {
    "type": "string",
    "defaultValue": "subnet3",
    "metadata": {
        "description": "PCS management interface connects to this subnet"
     },
```

Existing Tunnel Subnet: Subnet configured as Tunnel IP pool in Pulse Connect Secure VPN profile.



variables

Backend to PCS Route: This creates route table for accessing the backend resources in Pulse Connect Secure Internal Interface.

"routeTableName" : "Backend2PCSRoute",

PCS Internal NIC: This is network interface card of PCS Internal network.

"pcsIntNic" : "PCSInternalNIC",

PCS External NIC: This is network interface card of PCS External network.
"pcsExtNic" : "PCSExternalNIC",

PCS Management NIC: This is network interface card of PCS Management network.
"pcsMgmtNic" : "PCSMangementNIC",]

PCS External Public IP: This is public IP address assigned to PCS External Subnet.
"publicIPAddr1" : "PCSExternalPublicIP",

PCS Management Public IP: This is public IP address assigned to PCS Management Subnet.
"publicIPAddr2" : "PCSManagementPublicIP",

Public IP Address Type: This variable is defined as static IP. "publicIPAddressType" : "Static",

NSG Internal Subnet: This variable defines Network Security Group's Internal Subnet policy.

 "nsgInt"
 : "NSGInternalSubnet",

NSG External Subnet:	This variable defines Network Security Group's External Subnet policy.
"nsgExt"	: "NSGExternalSubnet",

NSG Management Subnet: This variable defines Network Security Group's Management Subnet policy.
"nsgMgmt" : "NSGManagementSubnet",

VM Size: This variable defines PCS Virtual Machine size. It is 4 cores, 144MB memory. "vmSize" : "Standard_DS3_v2",

Virtual Network ID: This variable defines PCS Virtual Network name.

"vnetID"	: "[resourceId('Microsoft.Network/virtualNetworks',variables('pcsvnetname'))]",
"subnetRefInt"	: "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetIntSubnet'))]",
"subnetRefExt"	: "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetExtSubnet'))]",
"subnetRefMgmt"	: "[concat(variables('vnetID'),'/subnets/',variables('pcsVnetMgmtSubnet'))]",
"subnetRefTunnel"	: "[concat(variables('vnetID'),'/subnets/',parameters('existingTunnelSubnet'))]",
API Version	
"apiVersion"	: "2015-06-15"

resources

publicIPAddresses/publicIPAddr1: This block is responsible for creating public IP address which is static in nature. This is used for external interface IP address of PCS.

"type": "Microsoft.Network/publicIPAddresses", "name": "[variables('publicIPAddr1')]",

publicIPAddresses/publicIPAddr2: This block is responsible for creating public IP address which is static in nature. This is used for management interface IP address of PCS.

"type": "Microsoft.Network/publicIPAddresses", "name": "[variables('publicIPAddr2')]",

networkSecurityGroups/nsgExt: This block is responsible for creating policy. The created policy is applied to Network Security Group's External interface.

"type": "Microsoft.Network/networkSecurityGroups", "name": "[variables('nsgExt')]",

The following security rules can be defined:

- allowHTTPS
- allowHTTP
- allowPTP
- allowESP
- allowIKEv2
- denyAll
- denyInternalSubnet
- denyManagementSubnet

denyPoolRange

networkSecurityGroups/nsgMgmt: This block is responsible for creating policy. The created policy is applied to Network Security Group's Management interface.

"type": "Microsoft.Network/networkSecurityGroups", "name": "[variables('nsgMgmt')]",

The following security rules can be defined:

- allowHTTPS
- allowHTTP
- allowCustomSSH
- allowDMI
- denyAll
- denyInternalSubnet
- denyExternalSubnet

networkSecurityGroups/nsgInt: This block is responsible for creating policy. The created policy is applied to Network Security Group's Internal interface.

```
"type": "Microsoft.Network/networkSecurityGroups",
"name": "[variables('nsgInt')]",
```

The following security rules can be defined:

- denyExternalSubnet
- allow-custom-ssh

routeTables/routeTableName: This block is responsible for creating route table. The created route table is used for accessing the backend resources in PCS Internal interface.

"type": "Microsoft.Network/routeTables", "name": "[variables('routeTableName')]",

networkInterfaces/pcsExtNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS External interface. The creation of this network interface depends on:

- PCS Virtual Network name
- Public IP address of External Subnet

```
"type": "Microsoft.Network/networkInterfaces",
"name": "[variables('pcsExtNic')]",
```

networkInterfaces/pcsMgmtNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Management interface. The creation of this network interface depends on:

- PCS Virtual Network name
- Public IP address of Management Subnet

```
"type": "Microsoft.Network/networkInterfaces",
"name": "[variables('pcsMgmtNic')]",
```

networkInterfaces/pcsIntNic: This block is responsible for creating network interface. The created network interface is applied to network interface card of PCS Internal interface. The creation of this network interface

depends on:

• PCS Virtual Network name

"type": "Microsoft.Network/networkInterfaces", "name": "[variables('pcsIntNic')]",

virtualMachines/PCSVmName: This block is responsible for creating Virtual Machine name. The created Virtual machine name is applied to PCS Virtual Machine. The creation of PCS Virtual Machine name depends on:

- Network Interface Card of PCS Internal interface
- Network Interface Card of PCS External interface
- Network Interface Card of PCS Management interface

"type": "Microsoft.Compute/virtualMachines", "name": "[parameters('PCSVmName')]",

outputs

The outputs section defines the public IP address and FQDN that is displayed on successful deployment of PCS on Azure.

```
"outputs": {
    "hostname": {
        "type": "string",
        "value": "[reference(variables('publicIPAddr1')).dnsSettings.fqdn]"
```

References

Microsoft Azure documentation: <u>https://docs.microsoft.com/en-us/azure/</u>

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

• Product warranties—for product warranty information, visit https://www.pulsesecure.net.