Lab 04 - On-Premises integration with VMC on AWS

Introduction

VMware Cloud on AWS enables customers to have a hybrid cloud platform by running their VMware workloads in the cloud while having seamless connectivity to on-premises and Amazon Web Services (AWS) native services.

Customers can use their existing AWS Direct Connect (DX) or Virtual Private Network (VPN) solutions to connect to their VMware Software-Defined Data Center (SDDC) clusters.

VMware Cloud on AWS uses NSX to control access to this network as part of the SDDC management model, and limits access to only remote traffic required to support features like cross-cluster vMotion. On the top of the underlay, NSX builds overlay networks for logical VMware connectivity. Each SDDC has two types of overlay networks:

- Appliance Subnet used to provide connectivity to SDDC management components like vCenter. This network is created during cluster provisioning with a carved out network range from the Infrastructure or Management subnet. Customers can optionally specify the network range of the Management subnet during cluster creation for the purpose of avoiding conflicts with other networks that will need to connect to the SDDC. Access to this network is controlled by the NSX Management Gateway (MGW) through firewall rules and IPsec tunnels.
- One or more customer-managed logical networks for VM traffic. Those can be either routed locally within the cluster or stretched from remote on-premises clusters with remote gateway for L3 routing. Access to this network is controlled by the NSX Compute Gateway (CGW) through firewall rules and IPsec capabilities to enable customers to connect securely to their remote workloads and the Internet.

IPSec VPN Connectivity to On-Premises



IPSec VPN

IPSec VPN can be used to provide a secure connection to your SDDC over the public Internet or AWS Direct Connect. Route-based and policy-based VPNs are supported. Either type of VPN can connect to the SDDC over the Internet. A route-based VPN can also connect to the SDDC over AWS Direct Connect.

 Route-based VPN - creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.

Route-based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as networks are added and removed. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises) endpoints, then specify tunnel security parameters for the SDDC end of the tunnel.

• **Policy-based VPN** - creates an IPsec tunnel and a policy that specifies how traffic uses it. When you use a policy-based VPN, you must update the routing tables on both ends of the network when new routes are added.

Policy-based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic. To create a policy-based VPN, you configure the local (SDDC) endpoint, then configure a matching remote (on-premises) endpoint. Because each policy-based VPN must create a new IPsec security association for each network, an administrator must update routing information on-premises and in the SDDC whenever a new policy-based VPN is created. A policy-based VPN can be an appropriate choice when you have only a few networks on either end of the VPN, or if your on-premises network hardware does not support BGP (which is required for route-based VPNs).

AWS Cloud Region-1 SDC Unrect Connect

Direct Connect (DX) Connectivity to On-Premises

AWS Direct Connect (DX) provides a dedicated network connection between your onpremises network infrastructure and a virtual interface (VIF) in your AWS VPC. A private VIF provides direct private access to your SDDC. Configure DX over a private VIF to carry workload and management traffic, including VPN and vMotion, between your on-premises data center and your connected VPC. A DX connection over a private VIF can be used for all traffic between your on-premises data center and your SDDC. It terminates in your connected Amazon VPC, provides a private IP address space, and uses BGP to advertise routes in your SDDC and learn routes in your on-premises data center.

If you just want to use DX to access AWS services in a VPC you own, you can do so over a public VIF. You cannot use a public VIF to carry the same kinds of SDDC traffic (such as vMotion) that require a private VIF or Direct Connect Gateway.

The use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

For this lab we will configure our On-Premises to VMware Cloud on AWS using Route-Based IPSec VPN. The On-Premises IPSec VPN Endpoint and session has already been configured.

TASKS

Task 1 - Accessing the On-Premises Environment

- 1. From your Laptop/desktop open a new Google Chrome Incognito window
- 2. Type https://vdi.27virtual.net in the browser address bar
- 3. Click the checkbox "Check here to skip this screen and always use HTML Access"
- 4. Click VMware Horizon HTML Access
- 5. When prompted log in as: (Get the login details from the Student Assignment Spreadsheet)
 - Username: VMCExpert#-XX (where # is the Environment ID and XX is your student number)
 - Password: VMwareNinja1!
- 6. Select the available Desktop pool





Task 2 - Restrict SDDC vCenter access to the On-Premises Environment

Management of workloads in vCenter can currently be done from anywhere due to the current Management Gateway firewall rule that allows any source to access vCenter. With On-premises integration, you may want to restrict access to your VMware on AWS SDDC vCenter from your On-Premises location(s) only. In this task, we will modify the firewall rule to restrict the management of workloads running in VMC on AWS from your On-Premises lab environment only.

- 1. From your VDI Desktop Click the Google Chrome Shortcut on the Desktop,
- 2. Type **whatismyip.com** in the address bar.
- 3. Take note of and record My Public IPv4 Value **i.e. 66.216.10.9** (it should start with 66)



- 4. In the Browser bookmark bar Click the "**VMware Cloud SDDC**" bookmark or type https://vmc.vmware.com/consoles/sddcs
- 5. to access your VMware Cloud on AWS SDDC
- 6. Log into the VMC SDDC Console using your VMC SDDC Student account

- Username = vmcexpert#-xx@vmware-hol.com (where # is the Environment ID & xx is your student number): i.e. vmcexpert1-20@vmware-hol.com
- 8. Password = VMware1!
- 9. Click **View Details** at the bottom of your SDDC Tile (**VMCEXPERT#-XX**, where xx is your student number)
- 10. Click the **Networking & Security** tab
- 11. Click **Groups**
- 12. Click Management Groups
- 13. Click Add Group
- 14. Enter the following values for the New Group settings:
 - Name: On-Prem Mgmt-Net
 - Click Set Members
 - Type 192.168.110.0/24 <Enter> in the IP Addresses Field
 - Also add <your On-Premises Public IP> from step 1 <Enter>
 - Click **APPLY** to close the popup

	-					
verview	Groups	3		Select Members On-Prem Mgmt-Net		×
etwork	Management Gro	Compute Groups		dresses (2)		
Segments					Maximum 400	1 O Search
/PN	ADD GROUP	(4)	/	Actions*	Plantinette 400	Q assici
TAI		\bigcirc		(192 168 10 0/24 x) (66 216 10 41 x) Enter IP		
ier-1 Gateways		Name	Com 6 mber			
ransit Connect			5 Sat North Ser	1		
urity		On-Prem Mgmt-Net	Set Members			
ateway Firewall						
stributed Firewall		Description	escription			
stributed IDS/IPS						
entory		(9)				
oups 2		SAVE CANCEL				
ervices						
rtual Machines	: > 88	ESXi	View Members			
ontext Profiles				Pomer, 2001/0000 0043 0000 0000 0424 03/0 / 334 07 10 12 2 64 20 07 2001 13000 25		\sim
s	> 88	HCX	View Members			CANCEL APPLY
X	: > 22	NSX Manager	View Members	Where Used	Success C	
12.5	/ 00					

Task 2.1 - Modify Gateway Firewall to restrict Access to the On-Premises Environment

We will now disable the current vCenter Inbound rule, which allows access from anywhere and add two new rules restricting access to vCenter and ESXi from the On-Premises Management Network only.

15. Click **SAVE**

- 1. Click Gateway Firewall
- 2. Click Management Gateway
- 3. Hover over the **vCenter Inbound rule** and click the slider on the right side of the row to disable it (it will now be switched to the left and gray instead of right and green)
- 4. Click **ADD RULE** and define the rule as follows:
 - Name: On-Prem to ESXi Inbound
 - Source: On-Prem Mgmt-Net (You will need to hover over the source field and click the pencil. In the popup select the User Defined Groups Radio-button then check the On-Prem Mgmt-Net group) Click Apply
 - Destination: ESXi (same as above except it will be found in System Defined Groups)
 - Services: HTTPS, vMotion, Provisioning & Remote Console
- 5. Click **ADD RULE** to add a 2nd rule, use the instructions above and define it as follows:
 - Name: On-Prem to vCenter Inbound
 - Source: On-Prem Mgmt-Net (Mouse over the source field and click the pencil
 - Destination: vCenter
 - Services: HTTPS, SSO

6. Click Publish

Summary Networking	& Security	Add (Ons Maintenance	Troubleshooting	Settings Support					
Overview	Gatew	ay F	irewall							?
Network	Managem	nent Ga	tewa Compute Gate	eway						6
Segments VPN							(4 Tota	al Unpublished Changes	REVERT	PUBLISH
NAT	+ ADD F	RU 3		DELETE	Unpublished Changes		Success C	Filter by Name, F	Path and more	Ŧ
Transit Connect			Name	ID	Sources	Destinations	Services	Action		
Security Gateway Firew 1	4		On-Prem to vCenter Inb		명이 On-Prem Mgmt-Net 8년 On-Prem Mgmt-Net	2-2 vCenter	HTTPS (TCP 443) SSO (TCP 7444)	Allow ~		© ^
Distributed Firewall Distributed IDS/IPS	:		On-Prem to ESXi		👷 On-Prem Mgmt-Net	88 ESXI	Provisioning & Re VNotion (TCP 80	Allow ~		۵
Groups Services Virtual Machines	:		vCenter Inbound	2026	Any	₽9 vCenter	C SSO C HTTPS	Allow ~	5	۵
Context Profiles	:		ESXi Outbound Rule	2024	22 ESXi	Any	Any	Allow V		@ 🖂
IPFIX Port Mirroring	:		vCenter Outbound Rule	2025	8-8 vCenter	Any	Any	Allow ~		. ⊡
System		ESH								6 Rules

Now Let's confirm we can access vCenter from the Control Center desktop (On-Premises) but not from any other network.

A NOTE: At this time this connection is still going over the Public internet, just restricted from On-Premises Management network. In the Next task we will configure IPSec VPN.

Task 2.2 - Test Connectivity from On-Premises

- 1. Click the **Settings** Tab
- 2. Expand the Default vCenter User and vSphere Client (HTML5) sections
- 3. Take note of and copy the values for:
 - Username
 - Password
 - vSphere Client URL

< ALL SDDCs	
OPEN VCENTER ACT	IONS Y
(Student20 VMware Cloud on AWS (US West (Oregon)	
Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support	
SDDC	
> Management Appliances (N/A)	?
vCenter Information	
Default vCenter User Account	?
User name Password Cloudadmin@vmc.local 🕒	
⊡r/Sphere Client (HTML5)	?
URL https://vcenter.sddc-35-160-79-165.vmwarevmc.com/u 😁 4	
> VCenter Server API Explorer (https://vcenter.sddc-35-160-79-165.vm/apiexplorer/)	?
> PowerCLI Connect Connect-VIServer -Server vcenter.sddc-35-160-79-165 vmwarevmc.com -Protocol https -User cloudadmin@vmc.local -Password ' <password>'</password>	?
Context EQDNI FQDN: https://vcenter.sddc-35-160-79-165.vmwarevmc.com/ Resolution Address: Public IP 35.160.79.165 resolvable from Internet Public IP: 35.160.79.165	?

4. In a new browser tab from within the VDI Desktop paste in the vCenter URL and login using the information you saved from the previous step

U What Is My IP? Quickly See My IP 🗙 🛛 🚾	VMware Cloud - VMCEXPERT3-0 🗙 🛃 🕫	phere - vcenter.sddc-52-28-33 × +						o	- 0	×
← → C 🔒 vcenter.sddc-52-28-3	3-169.vmwarevmc.com/ui/app/folder;nav	h/urn:vmomi:Folder:group-d1:fd86e1		4704-b373-fd724	8d1f43e/s			☆	🔒 Incognito):
📙 VI Management Web01 🌀 Web02	2 📀 NSX 3-Tier App -01a 📀 NSX 3-Tier A	opp - 02a 📀 Planespotter 🔇 VMwar	e Cloud SI	DDC						
\equiv vSphere Client Q Search	n in all environments				C		dadmin@vmc.lo	ocal 🗸	© (? ~
<		33-169.vmwarevmc.cor	n	ACTIONS 🗸						
	Summary Monitor Configure	Permissions Datacenters	Hos	ts & Clusters	VMs	Datastores	Networks			
vcenter.sddc-52-28-33-169.vmwar	Version: 7.0.2						CPU		Free: 69.	5 GHz
✓ ➡ SDDC-Datacenter	Build: 18137590						Used: 13.26 GHz		Capacity: 82.7	6 GHz
✓ []] Cluster-1	[min]						Memory		Free: 347.4	47 GB
10.101.2.4	Clusters: 1						Used: 164.39 GB		Capacity: 511.	86 GB
✓	Hosts: 1						Storage		Free: 9.	29 TB
🔂 webserver01	virtual Machines. It						Used: 1.08 TB		Capacity: 10.	37 TB
webserver02										
값 Win10-Desktop										
	Custom Attributes		~	Tags						~
R NSX-Edge-0	044-i5-uap	Malua		Assisted Tex		Contractor				
RSX-Edge-1	Attribute	Value		Assigned Tag		Category	U	Jescription		
🕅 NSX-Manager-0										
🔂 NSX-Manager-1										
🔂 NSX-Manager-2										
🔂 vcenter										
		No items to disp	lay					N	o items to display	
	Edit			Assign Remo	ove					

5. Now try the same thing from your laptop/desktop and notice you cannot access the SDDC vCenter except through the On-Premises environment. (Sometimes there are caching issues with the browser. You may need to close the entire browser window and try again from a freshly launched window).



Task 3 - Configure IPSec VPN

Task 3.1 - Configure Route-based IPSec VPN in your SDDC

- 1. In your VMC on AWS Console Click the **Networking & Security** Tab Under the **Network** Section
- 2. Click **VPN**
- 3. Click Route Based VPN
- 4. Click ADD VPN
- 5. Enter the following values for the VPN Settings:
 - Name: VMC_to_On-Prem_VPN
 - Local IP Address < Public IP xx.xx.xx> NOTE: Please choose the Public IP (not Private IP).
 - Record this Public IP, you will need it in the next task to modify the on-Premises VPN settings
 - Remote Public IP < On-Premises Public IP > i.e. 66.216.xx.xx
 - BGP Local IP/Prefix: 169.254.111.30/30
 - BGP Remote IP: 169.254.111.29
 - BGP Neighbor ASN: 65002
 - Preshared Key: VMwareNinja1!
 - Remote Private IP: 192.168.151.1
- 6. Click SAVE
- 7. Click **OK**



- Click the arrow next to the VMC_to_On-Prem_VPN you just created and expand the VPN Settings
- 9. Click **DOWNLOAD CONFIG** then click **No** to cancel the Download. We are just showing you how to do it in your own environment but not using it for this lab.

ute Based	Policy Based La	ayer 2					
DD VPN E	DIT LOCAL ASN			COL	LAPSE ALL Filter	by Name, Path and	more
	Name L	ocal IP Address	Remote Public IP	BGP Local IP/Prefix Length	BGP Remote IP	BGP Neighbor ASN	Status
· · @	VMC_to_On- P Prem_VPN	ublic IP1	66.216.	169.254.111.30/30	 169.254.111.29 	65002	● In Progress C ③
	Preshared Key	•••••• 🔘 📋		Remote Private IP	192.168.151.1		
	✓ Advanced Tunne	Parameters					
	> IKE Profile					DOWNLO	AD CONFIG
	> IPSec Profile					VIEW STA	TISTICS
	> DPD Profile					VIEW ROU	JTES
	TCP MSS Clamping	Disabled				DOWNLO	AD ROUTES Y
	Description	Not Set		Tags	0		

Once you've configured IPSec VPN in your VMware Cloud on AWS SDDC, you'll typically download the configuration and hand it to your On-Premises networking team. They can use the values in the document to configure a VPN endpoint On-Premises. IPSec VPN can be configured on any compliant IPSec VPN Gateway device (Physical or Virtual).

Task 3.2 - Configure IPSec VPN On-Premises

The On-Premises lab environment uses NSX-T 3.1, and IPSec VPN has already been configured. However, you'll need to modify the IPSec Session configuration, providing the Public IP address for the IPSec VPN endpoint in your SDDC.

- Note: The IP you'll provide is the Public IP address you recorded in Task 3.1, step 5 (Not your On-Premises Public IP)
- 1. From the Google Chrome Bookmark bar of the VDI Desktop click the VI Management
- 2. Click NSX-T Local Manager bookmark
- 3. If prompted with an SSL Warning message, click **Advanced** and then **Proceed to nsxtmgr-I-01a.vcn.ninja.local**
- 4. Log into NSX-T Manager as:
 - admin
 - VMwareNinja1! Note: You can also use ctrl+m to paste in the password
- 5. Click the **Networking** tab
- 6. Click **VPN** under the **Network Services** Section in the left pane
- 7. Click the IPSEC SESSIONS tab
- 8. Select the 3 vertical dots next to RB-VPN-VMC and Click Edit

vm NSX-T						Q L	(?) ∽ admin
Home Networking Security	Inventory Plan & Troubleshoot	System					POLICY MANAGER
Network Overview	VPN SERVICES IPSEC SESSION	ONS L2 VPN	SESSIONS LOCAL	ENDPOINTS PROFILE	COLLAPSE ALL	Filter by Name, Pa	ath and more =
Connectivity	Edit (4)	Туре	VPN Service	Local Endpoint	Remote IP	Status	Alarms
Tier-O Gateways	Delete Copy path to clipboard	Route Based	On-Prem-IPSec-VPN	On-Prem-IPSec-ENDP	1.1.1.1	🛑 Down 🕕 Ċ	0
 Tier-1 Gateways Segments Network Services VPN 2 NAT Load Balancing Forwarding Policies IP Management IP Management IP Management IP Address Pools 	Copy pair to clipboard Description Compliance suite Authentication Mode Pre-shared Key > Advanced Properties	Not Set None PSK		Admin Status Tunnel Interface Remote ID	 Disabled 169.254.111.29/30 1.111 		VIEW STATISTICS

- 9. Make the following changes:
 - Remote IP: <Your SDDC VPN Public IP> Replace 1.1.1.1 with Public IP1 <Public IP1 from the SDDC VPN Configuration>
 - Admin Status: Enabled (Move the slider to enable the VPN Session)
 - Remote ID: <Your SDDC VPN Public IP> Replace 1.1.1.1 with Public <Public IP1 from the SDDC VPN Configuration>

10. Click **SAVE**

11. Under the Status column, click the **refresh Icon**

vm NSX-T							Q	Ĺ (D~	admin ~
Home Networking Security	Inventory Plan & Troubleshoot	System							POLICY	MANAGER
«	· · · · · · · · · · · · · · · · · · ·									0
🙆 Network Overview	VPN SERVICES IPSEC SESSI	ONS L2 VP	N SESSIONS LOCAL	ENDPOINTS PROFIL	ES					(?)
🔯 Network Topology	DD IPSEC SESSION ¥				COL	LAPSE ALL				=
Connectivity	Name	Туре	VPN Service	Local Endpoint	Remote IP	ذ 1	tatus			Alarms
💤 Tier-O Gateways	RB-VPN-VMC *	Route Based	On-Prem-IPSec-VPN	On-Prem-IF ⊗ ⊻ *	5 84.15					
🔁 Tier-1 Gateways						_	2)		
Segments	Description	Description		Admi	n Status	C Enable	d			
Network Services	0			-						
VPN	Authentication Mode	None	v	Pemo	et internace -	169.254.111.29	9/30		_	
- NAT	Pre-shared Key *		 @ (1)			04.13		-		
Load Balancing	> Advanced Properties									
♦ Forwarding Policies										
IP Management										
III DNS										
DHCP										
😫 IP Address Pools										
Settinas	N REDEQU								1 - 1 of 1	IPSec Sessions

Note: After 30-60 seconds the status should change to Success. You may have to hit refresh or click onto another menu item then click back on VPN to refresh.

Image: Second	
Description Not Set Admin Status Enabled VIEW Compliance suite None Tunnel Interface 169.254.111.29/30 DOWNLO	0 =
Compliance suite None Tunnel Interface 169.254.111.29/30 DOWNLO	STATIST
	AD CON
Authentication Mode PSK Remote ID 54.185.84.15	
Pre-shared Key 👁 📋	
> Advanced Properties	

12. In the Browser tab for your VMC on AWS SDDC Console, Click the **Networking & Security** tab

13. Click **Overview**

14. On the Overview page, view the **graphical dashboard** status of the VPN session. It should show a successful connection



Task 4 - Modify SDDC Firewall and Test VPN Connectivity

We will now confirm connectivity through the IPSec VPN tunnel. In doing this we must first create the required Firewall policy on the Compute and Management Gateways in the SDDC to allow incoming communications. The on-Premises environment is currently set to allow all outgoing and in-coming connections.

Task 4.1 - Configure/Identify Private addressing for vCenter and Workload VMs

- 1. From the VDI Desktop open a new Browser tab and Click VI Management
- Click vSphere Client
 If prompted with an SSL Warning message, click Advanced and then Proceed to vc-I-01a.vcn.ninja.local
- 3. Login in as:
 - Administrator@vsphere.local
 - VMwareNinja1! Note: You can also use ctrl+m to paste in the password
- 4. **Power-on** all the VMs and vApps in the compute Cluster
 - Expand Shinobi-On-Prem DC
 - Select Shotoku Compute01
 - Click the VMs tab
 - Select all Powered-off VMs
 - Right-Click them
 - Click Power --> Power On

- 5. Also take note of the IP addresses of the following VMs (You will reference them later):
 - Web-01a | 172.16.10.11
 - Web-02a | 172.16.10.12
 - App-01a | 172.16.20.11
 - Db-01a | 172.16.30.11

NOTE: We will need to create Gateway firewall rules in the SDDC to allow these VMs access through the tunnel to the web servers in the SDDC

NSX VMware NSX Login	×	🗜 vSphere - Sh	notoku Compute(01 - × +								- E) ×
← → C ▲ Not se	ecure vc-I-01	1a.vcn.ninja.lo	cal/ui/app/clus		momi:ClusterCon	nputeResour					9-428e181 ·	☆ 🔒 Incognito	(2) :
📙 VI Management 🛭 S We	eb01 📀 Web	02 NSX 3	3-Tier App -01a	🕙 NSX 3-Tier A	pp-02a 🚯 Plan	espotter 🕄	VMware	Cloud SDDC	🕙 VCGW	VAMI			
vm vSphere Clien	it Men		C Search in					C	? ~	Adminis	strator@VSPHE	re.local ∨	\odot
		35						<u>.</u>		92			M.
	<u> </u>	🗊 Shoto	oku Com	pute01	ACTIONS \checkmark								
✓ I vc-I-01a.vcn.ninja.loca	al	Summary	Monitor	Configure	Permissions	Hosts	VM ²	Datastores	s Ne	tworks	Updates		
✓ 📑 Shinobi-On-Prem E		-					_						
🗸 📋 Shotoku Compu	ite01	Virtual Ma	chines VI	M Templates	vApps								
esxicomp-01a	a.vcn.ninja												
✓ 🎛 Planespotter												Filter	T
🗗 Planespott	er App	Name		~	State ↑ ~	Status	~ Pro	ovisioned Space	~	Used Space	✓ Host CPU	J v Host Mem	~
🗗 Planespott	er MySQL	T Planes	spotter App		Powered Off	✓ Norma	il 36	.22 GB		1.24 GB	0 H.	0 B	
🗗 Planespott	er Redis	👘 Planes	spotter MySQL		Powered Off	V Norma	I 36	.22 GB		1.29 GB	0 Hz	0 B	
🗗 Planespotte	er Web	📅 Planes	3 r Web	Antines 1			I 36	.22 GB		1.31 GB	0 Hz	0 B	
🗗 app-01a		📅 web-0		Actions - I		Norma	l 2.8	37 GB		561.69 MB	0 Hz	0 B	
📅 db-01a	1	📅 db-01a	3	Power	4	Pov	ver On	5		17 GB	0 Hz	0 B	
🗾 🔓 Tiny-Linux		📅 Planes	spotter Redis	Guest O	s	Pov	ver Off	ct	rl + alt + B	.04 GB	0 Hz	0 B	
📩 web-01a		📅 app-0'	1a							28.01 MB	0 Hz	0 B	
🗗 web-02a		📅 Wordp	oress	Migrate.		Sus	pend		rl + alt + 2	66 GB	0 Hz	0 B	
🗄 Wordpress		📅 web-0		VM Polic	cies	🕨 🗐 Res	et		rl + alt + 1	10.85 MB	0 Hz	0 B	
🗲 🗍 Shotoku Mgmt&	Edge	📅 Tiny-L	inux	Tomplat						1.78 MB	0 H7	0 B	
		VCLS ((3)				i Bown (iuest 03 eti	· · uit · c	8.54 MB	44 MHz	152 MB	
				Compati	ibility	🕨 🚱 Res	tart Gues	t OS ct	rl + alt + F	5			
				Move to	folder								
				Tags & C	Custom Attribute							Export 1	11 items
				Tags & C	Custom Attribute							Export 1	I1 ite

Task 4.1.1 - Enable Private IP address resolution for the SDDC vCenter

- 1. From The VDI desktop access your VMC SDDC and click on the **Setting**s tab
- 2. Expand vCenter FQDN, click Edit
- 3. From the **Resolution address** Drop Down Set the address to **Private IP**
- 4. Click Save

vmw VMware Cloud		· III
*		
A Launchpad	< ALL SDDCs OPEN VCENTER ACTIO	NS V
SDDCs	Student20 VMware Cloud on AWS 🖗 US West (Oregon)	
Subscriptions	Summary Networking & Security Add Ons Maintenance Troubleshooting Setting Support	
i≣ Activity Log		
🖻 Tools	SDDC	
Developer Center	Appliances (N/A)	?
	vCenter Information	SUPPORT
	> Default vCenter User (cloudadmin@vmc.local)	? 《
	VSphere Client (HTML5) (https://vcenter.sdoc-35-160-79-165.vmwarevmc.com/ul)	?
	VCenter Server API (https://vcenter.sdoc-35-160-79-165.vmwarevmc.com/apiexplorer/)	?
	> PowerCLI Connect ViServer - Server vcenter sddc-35-160-79-165.vmwarevmc.com - Protocol https - User cloudadmin@vmc.local - Password '>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	?
	vCenter FODN	?
	VCenter FODN Resolution Address Public IP Private IP https://vcenter.sddc-35-160-79-165.vmwarev. Private IP: 10.120.14.4 35.160.79.165 10.120.14.4 SAVE CANCEL 35.160.79.165 35.160.79.165	

- 5. Click the Networking & Security Tab
- 6. Click **DNS** in the **System** Section
- 7. Click the DNS Zones tab
- 8. Click Add DNS Zones
- 9. Click Add FQDN Zone
- 10. Enter the following Values
- 11. Zone Name: vcn.ninja.local
- 12. Domain: vcn.ninja.local,ninja.local
- 13. DNS Servers: 192.168.110.10
- 14. Click Save

Summary Networking 8	Security Add O	Ons Maintenance	Troubleshooting Settings Suppo	rt		
Transit Connect Security Gateway Firewall	DNS Services	es DNS Zone				(
Distributed Firewall Distributed IDS/IPS	ADD DNS ZO			EXPAN	D ALL Filter by Name, Path	and more
Inventory		Zone Name	Domain	DNS Servers	Source IP	DNS Services
Services Virtual Machines Context Profiles	4	vcn.ninja.lc *	vcn.ninja.local.ninja.local *	192.168.110.10 * Comma Separated Server IPs. Maximum 3 Servers	Enter Source IP	
Tools IPFIX Port Mirroring		Description	Description	Tags	Tag Scor Max 30 allowed. Click (+) to add.	3
System Identity Firewall AD DNS	(5 SAVE CAN	CEL			
DHCP Global Configuration	: > =	Compute Gate	Any	8.8.8.8 View More	Not Set	1
Public IPs Direct Connect	: > :	Management G	Any	8.8.8.8 View More	Not Set	1

- 15. Click DNS Zones Tab
- 16. Select the 3 vertical dots next to **Compute Gateway DNS Forwarde**r
- 17. Click **Edit**
 - Change DNS Servers IP 1 to 192.168.110.10
 - Delete DNS Server IP 2
- 18. Click SAVE
- 19. Select the 3 vertical dots next to Management Gateway DNS Forwarder
- 20. Click Edit DNS Servers IP
 - Change DNS Servers IP to 192.168.110.10
 - Delete DNS Server IP 2
- 21. Click SAVE

DN	S Se	ervic	es					?
DNS	Servi	ces	DNS Zones					
ADD	DNS	ZONE	~			EXPAND ALL	Filter by Name	e, Path and more
		=dit		Domain	DNS Servers		Source IP	DNS Services
:<		Delete Copy P	Path to Clipboard	Any	192.168.110.10		Not Set	1
			Description	Not Set	Tags	0		
÷	>		Management Ga	Any	192.168.110.10		Not Set	1
÷	>	: :	vcn.ninja.local	vcn.ninja.local and 1 More	192.168.110.10		Not Set	0
C F	EFRES	ŝH						1 - 3 of 3 DNS Zones

NS Services	DNS Zones				
	20103				
ADD DNS ZONE Y]		E	Filter by Name, F	Path and more
	Zone Name	Domain	DNS Servers	Source IP	DNS Services
	Compute G.	Any	192.168.110.10	Enter Source IP	
			Comma Separated Server IPs. Max Servers	timum 3	
	Description	Description	Tags	Scop	•
				Max 30 allowed. Click (+) to a	add.
	SAVE CANC	EL			
: > 🔳	Management Ga	Any	192.168.110.10	Not Set	1
: > 🔳	vcn.ninja.local	vcn.ninja.local and 1 More	192.168.110.10	Not Set	0
C REFRESH					1 - 3 of 3 DNS Zor

Now Let's confirm we can still access vCenter from the VDI desktop (On-Premises) but not from any other network. Keeping in mind Private IPs are not accessible from the internet (only Internet addressable IPs).

21. Go to the Setting Tab

22. Expand the Default vCenter User and vSphere Client (HTML5) sections

- 23. Take note of and copy the values for, or get the information form the excel workbook if it was previously saved:
 - Username
 - Password
 - vSphere Client URL
- 24. In a new browser tab from within the VDI desktop paste in the vCenter URL and login using the information you saved from the previous step
- 25. You can also confirm that the vCenter is no longer accessible from external addresses by performing the above steps on your desktop/laptop.

NSX VI	/ware NSX Login	× 🛃	/Sphere - Shotoku Compute	01 - 🗙 🚾 V	/Mware Cloud	- Student20	× 🛃 Login	× -	ŀ	- 0	×
← →	C 🗎 vcenter.sdd	lc-35-160-79	-165.vmwarevmc.com/	ebsso/SAML2/		cal?SAMLReque	est=zZRRb9MwFIXf%	2BRWR3xM7abuuVtOprExl	M2lh 🟠	🔒 Incognito (2) :
📙 VII	Management 🕤 Web01	S Web02	S NSX 3-Tier App -01a	S NSX 3-Tier	App - 02a	3 Planespotter	S VMware Cloud SD	DC 🕤 VCGW VAMI			
	VMware [®]	vSph	ere								
	cloudadmin@vmc.loca	al									
				-							
		LOGIN									

Task 5 - Allow access between On-Premises and SDDC

With the VPN successfully setup, you may need to allow communications between your on-Premises applications and those running in your VMC SDDC. Examples of these could include allowing your VMC workloads Active Directory and DB access where those resources resided On-Premises or vice versa. For this to happen you must modify the firewall policies between your VMC SDDC and your On-Premises Firewall. In this lab task, we will adjust the Firewall setting on the Compute Gateway of the SDDC to allow communications.

5.1 - Create IP Set for On-Premises Applications

- 1. In the VMC SDDC, click Networking & Security
- 2. Click Groups in the Inventory Section
- 3. Select **Compute Groups**
- 4. Click Add Group
- 5. Name the Group "On-Prem 3-Tier App"

6. Click Set Members

- 1. In the Pop Up Select the IP Addresses tab
- 2. Enter the following IP Subnets
 - 172.16.10.0/24
 - 172.16.20.0/24
 - · 172.16.30.0/24
 - Click Apply
- 7. Click Save
- 8. Click Add Group
- 9. Name the Group "SDDC-Workloads"
- 10. Click Set Members
- 11. In the Pop Up Select the Members tab
- 12. For **Category** select **Segments**
- 13. Select all Subnets (Demo-Net, Desktop-Net, SDDC-cgw-network-1)
- 14. Click Apply
- 15. Click Save



Select Members Add Compute Members eit	On-Prem 3	-Tier App	em.				×
Membership Criteria (0)	Members (0)	IP Addresses (3)	MAC Addresses (0)	AD Groups (0)			
ACTIONS ~					Maximum: 4000	Q Search	
8 (172.16.10.0/24 ×) (172.16	20.0/24 X (192.16	.30.0/24 × Inter IP /	Address				
Format: 2001:0db8:85a3:0000	0000-8a2e-0370-733	34 or 10 12 2 64/26 or 200	11-500025				
romat. 2001.0008.8383.0000	0000.0020.0370.73		n.1-000.20			CANCEL	9 AFFLY

5.2 - Create Gateway Firewall rule for Tunnel Communications

- 1. Click Gateway Firewall
- 2. On the Compute Gateway Click Add Rule (Add 3 rules)
- 3. Configure the rules as with the following information (note that we are just creating then disabling them to allow you to feel the interface process, but have another rule that we will be using for this lab):

1. RULE 1

- Name: Allow On-Prem to PhotoApp
- Source: On-Prem 3-Tier App
- Destination: PhotoAppVM
- Service: Any
- Applied To: VPN Tunnel Interfaces (You may need hover over the "All Uplinks" text, click the blue pencil, click the X next to all uplinks, then select from the drop down.
- Action: Allow
- Move the slider to **Disable** this rule

2. RULE 2 (follow the instructions just above)

- Name: Allow PhotoApp to On-Prem
- Source: PhotoAppVM
- Destination: On-Prem 3-Tier App
- Service: Any
- Applied To: VPN Tunnel Interfaces
- Action: Allow
- Move the slider to **Disable** this rule

- 3. **RULE 3 (follow the instructions just above)**
 - Name: Allow SDDC Workloads Outbound HTTP
 - Source: SDDC-Workloads
 - Destination: ANY
 - Service: HTTP, HTTPS, "Office Server Web Services, HTTP,SSL", DNS, DNS-UDP
 - Applied To: All Uplinks
 - Action: Allow
- 4. Change the "Action" dropdown on the **"Default VTI Rule"** to **Allow** instead of **Drop**. This allows all flows over the VPN tunnel in and out of the Compute gateway.
- 5. Click **Publish**

rview	Gatew	/ay F	irewall									
work	Manager	nient Ga	teway Compute G	Gate 3								
gments PN										(1 TO	tal Unpublished Change	REVERT
T	+ add	RU 4	CLONE 5 UT	NDO 🗍 DELETI	E (1 Unpublished Change)					Success C	Filter by Name	, Path and more
ansit Connect			Name	ID	Sources	Destinations		Services	App	ied To	Action	
arity ateway Firew 2 stributed Firewall stributed IDS/IPS	5		Allow SDDC Worklo	1026	88 SDDC WorkI	Any	HTTPS DNS-UDP Office Server Web Services, H_ HTTP	All Uplinks	Allow ~		<u>م</u>	
ntory							O DNS				5	
rvices	3		Allow PhotoApp to	1027	22 PhotoAppVM	88 On-Prem 3-Ti	Any	VPN Tunnel Inter	Allow ~			
ontext Profiles	1		Allow On-Prem to P	1028	22 On-Prem 3-Ti	PhotoAppVM	Any	VPN Tunnel Inter	llow v		¢ 🗠)
5 1X	:		Public In	1015	Any	88 PhotoAppVM	О нттр	All Uplinks	e Allow ~		ð 🕢	
rt Mirroring em entity Firewall AD	1		AWS Outbound	1016	22 PhotoAppVM	88 Connected V	MySQL NFS (UDP) NFS (TCP)	All Uplinks	Allow ~		\$ M	
IS ICP			AWS inbound	1017	22 Connected V	₿8 PhotoApp∨M	Any	All Uplinks	llow ~		<u>م</u>	
bal Configuration lic IPs	\mathcal{O}		Default VTI Rule	1012	Any	Any	Any	VPN Tunnel Inter	Allow) M	
ect Connect	:	Π	Default Uplink Rule		Any	Any	Any	All Uplinks	😑 Drop 🗸			

5.3 - Test Connectivity

- 1. In the browser tab from within the VDI Desktop Click **the VI Management** in the Bookmark bar
- 2. Click vSphere Client (You may need to click proceed if you get a security warning)
- 3. Log in as:
 - administrator@vsphere.local
 - VMwareNinja1! Note: You can also use ctrl+m to paste in the password
- Select web-01a VM (You can find this under vc-l-01a > Shinobi On Prem DC > Shotoku Compute01)
- 5. Click LAUNCH WEB CONSOLE
- In the console for web-01a ping -c3 <webserver01_IP_Address> (10.10.x.11) in your SDDC (Remember that you have to log into vCenter from your VDI machine. If you do not have it written down previously, you can find the IP in your VMC SDDC > SDDC-Datacenter > Cluster-1 > Compute-ResourcePool > Webserver01)

VMware Cloud Services - Log In x 2 Login x Sphere - web-01a - Summary x S web-01a x +									
← → C 🗛 Not secure vc-l-01a.vcn.ninja.local/ui/app/vm:nav=h/um:vmomit/VirtualMachine:vm-3013:e6041af1-4075-4364-a7d9-428e1812b8f4/summary									
📙 VI Management 🔇 Web01 🔇 Web02 🔇 NSX 3-Tier A	ipp - 01a 🔇 NSX 3-Tier App - 02a 🥥 Planespotter 🔇 VMware Cloud SDDC 🔇 VCGW VAMI								
vm vSphere Client Menu V Q S	earch in all environments								
	🕞 web-O1a 📄 🖷 🖶 🖏 🐁 Actions 🗸								
 ✓ @ vc-I-01a.vcn.ninja.local ✓ ∰ Shinobi-On-Prem DC ✓ ∰ Shitobi.compite01 	Summary Monitor Configure Permissions Datastores Networks Snapshots Updates								
 Shotoku Compute01 Shotoku Compute01 stcomp-0ia.vcn.ninja.local stp.0ia app-0ia tiny-Linux web-0ia web-0ia web-02a Wordpress Shotoku Mgmt&Edge 	Guest OS: SUSE Linux Enterprise 11 (64-bit) Compatibility: ESX IS.0 and later (VM version B) VM ware Tools: Running, version:10357 (Upgrade available) MORE INFO DNS Name: web-Ola IP Addresses: 172:16:10:11 VIEW ALL 3 IP ADDRESSES Host: essicomp-Ola.vcn.ninja.local A newer version of VM ware Tools is available for this virtual machine. VM Hardware								
Recent Tasks Alarms									
Task Name V Target	✓ Status ✓ Details ✓ Initiator ✓ Queued For ✓ Start Time								



Conclusion

- A route-based VPN creates an IPsec tunnel interface and routes traffic through it as dictated by the SDDC routing table. A route-based VPN provides resilient, secure access to multiple subnets. When you use a route-based VPN, new routes are added automatically when new networks are created.
- Route based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as networks are added and removed. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises) endpoints, then specify tunnel security parameters for the SDDC end of the tunnel.

With A VPN setup between your On-Premises and VMware Cloud on AWS SDDC, you can begin to take advantage of Hybrid Solution Use-Cases, such as:

- Hybrid Linked Mode
- Cloud Migration
- Disaster Recovery
- Etc...