

Lab 04 - On-Premises integration with VMC on AWS

Introduction

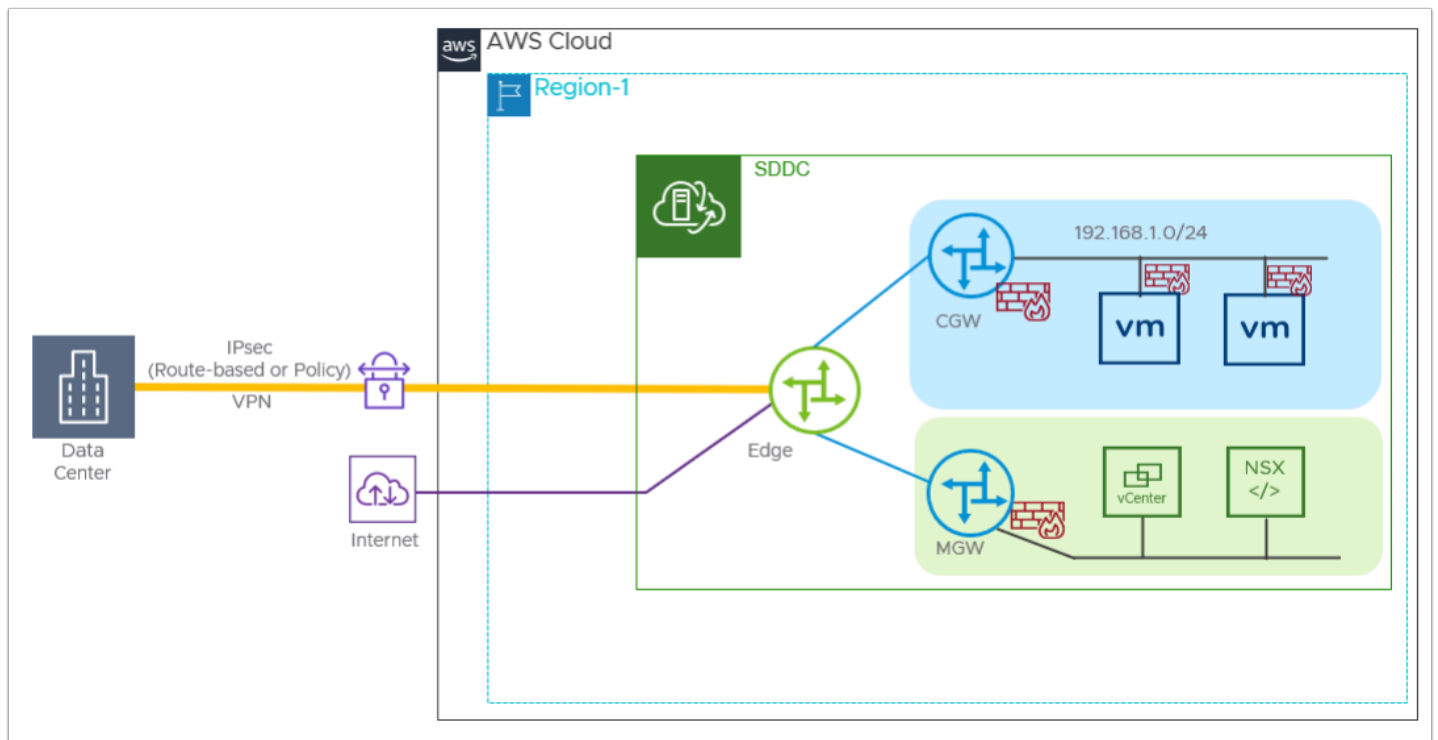
VMware Cloud on AWS enables customers to have a hybrid cloud platform by running their VMware workloads in the cloud while having seamless connectivity to on-premises and Amazon Web Services (AWS) native services.

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.

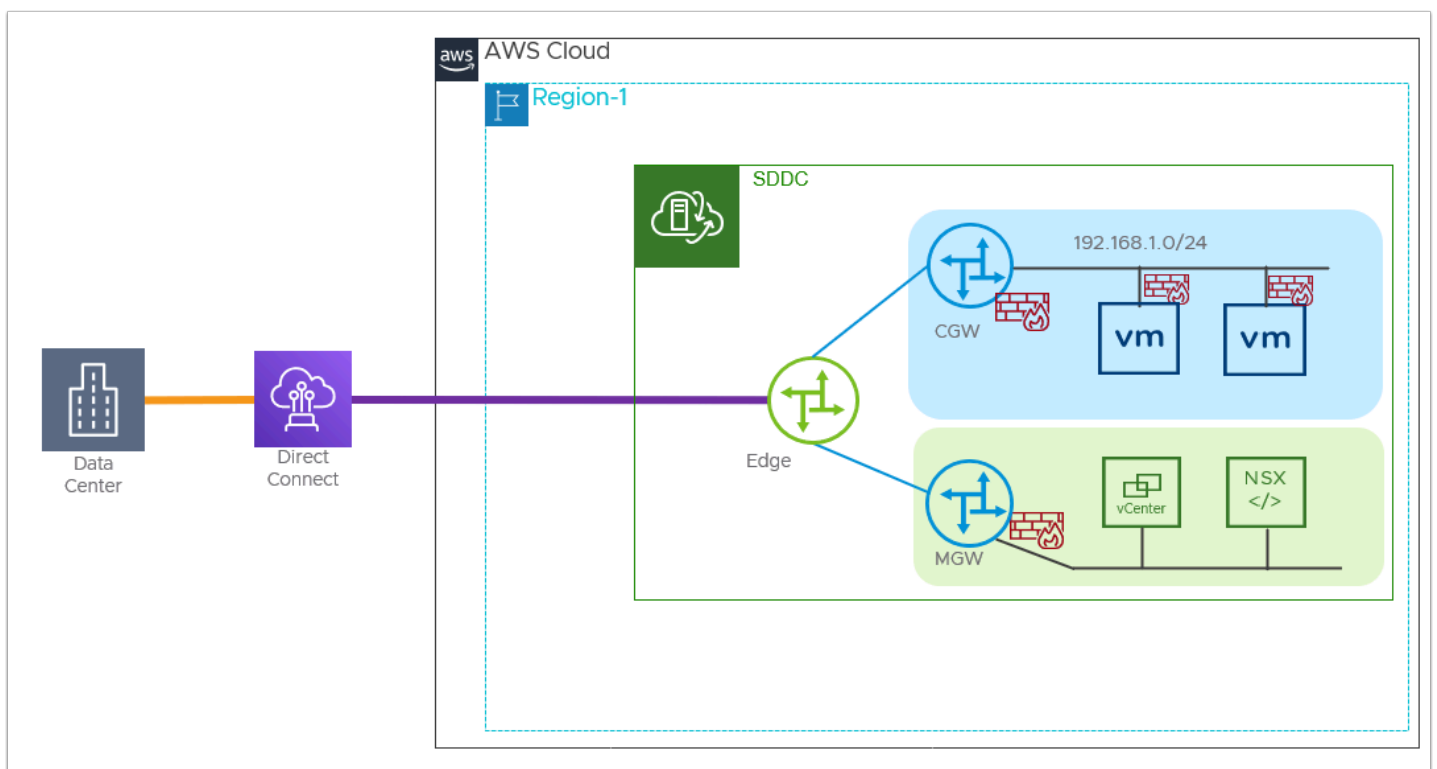
Route-based VPNs in your VMware Cloud on AWS SDDC use an IPsec protocol to secure traffic and the Border Gateway Protocol (BGP) to discover and propagate routes as networks are added and removed. To create a route-based VPN, you configure BGP information for the local (SDDC) and remote (on-premises)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

Direct Connect (DX) Connectivity to On-Premises




AWS Direct Connect (DX) provides a dedicated network connection between your on-premises 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.

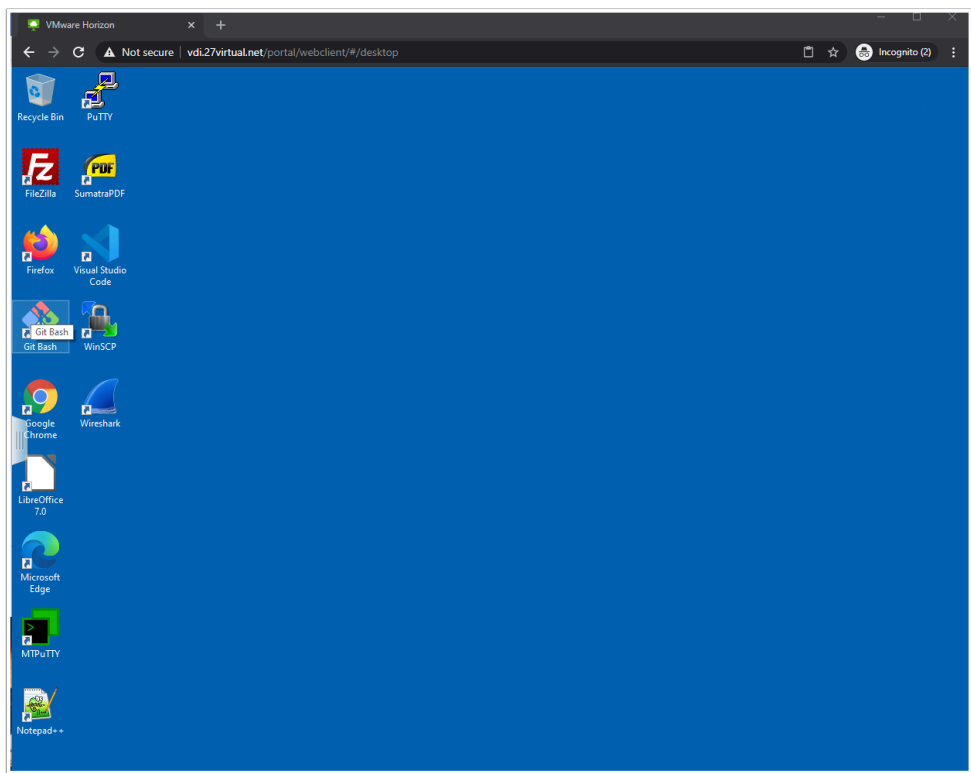
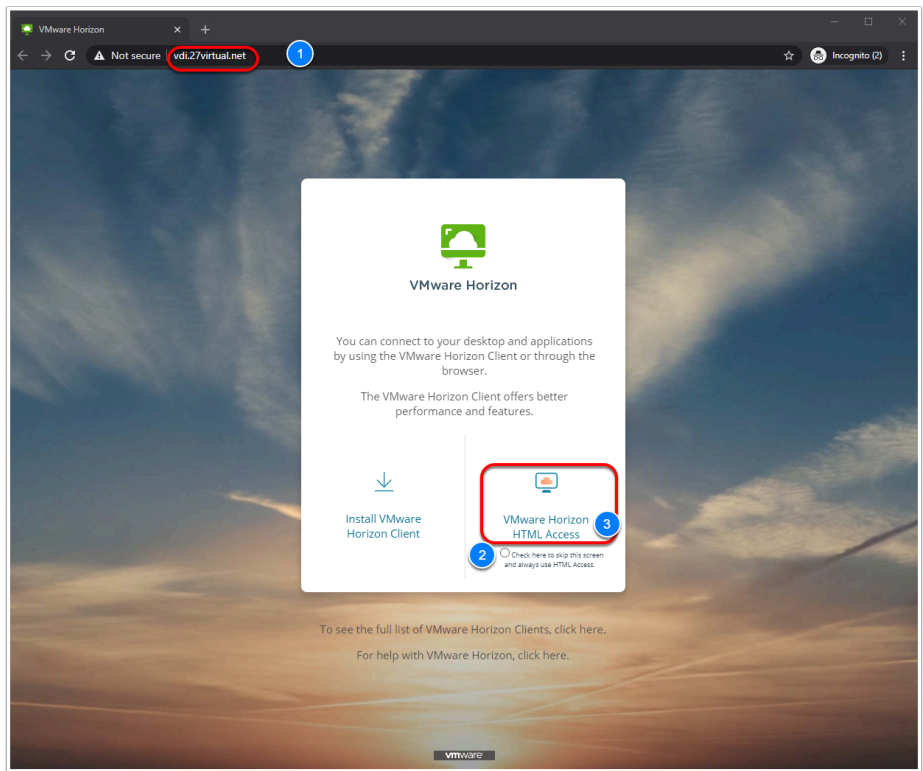
The use of AWS Direct Connect is optional. If traffic between your on-premises network and your SDDC workloads requires higher speeds and lower latency than you can achieve with a connection over the public Internet, configure VMware Cloud on AWS to use AWS Direct Connect.

 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

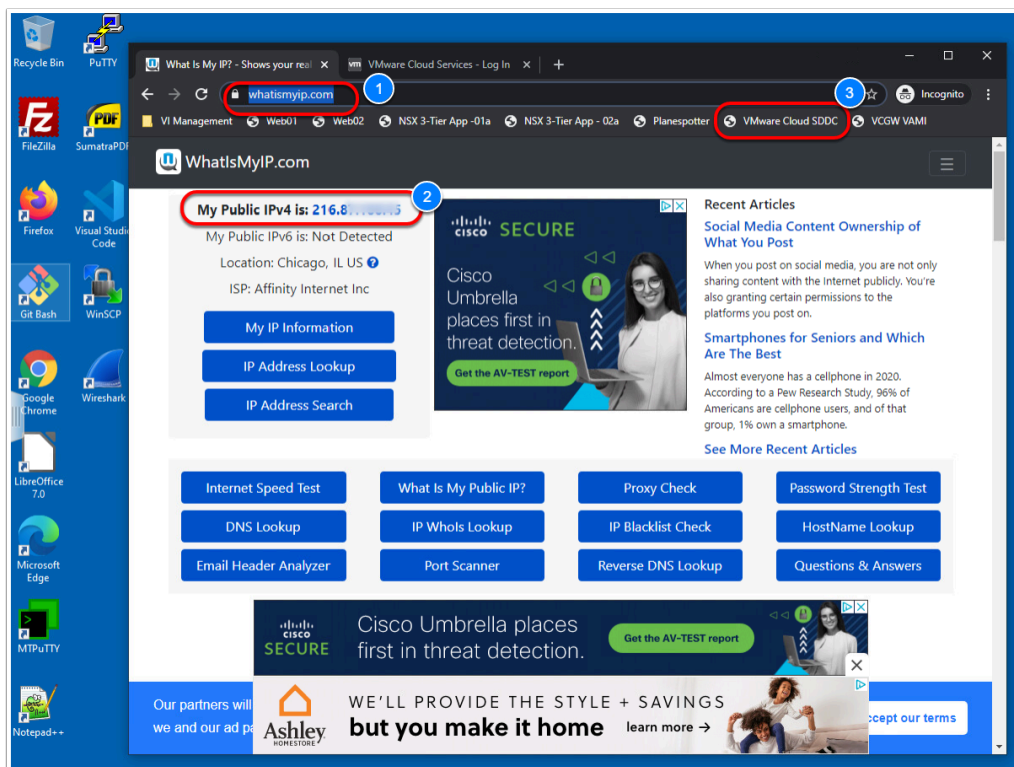
1. From your Laptop/desktop open a new Google Chrome Incognito window
2. Type <https://vdi.27virtual.net> in the browser address bar
3. Click the checkbox "**Check here to skip this screen and always use HTML Access**"
4. Click **VMware Horizon HTML Access**
5. When prompted log in as: **(Get the login 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

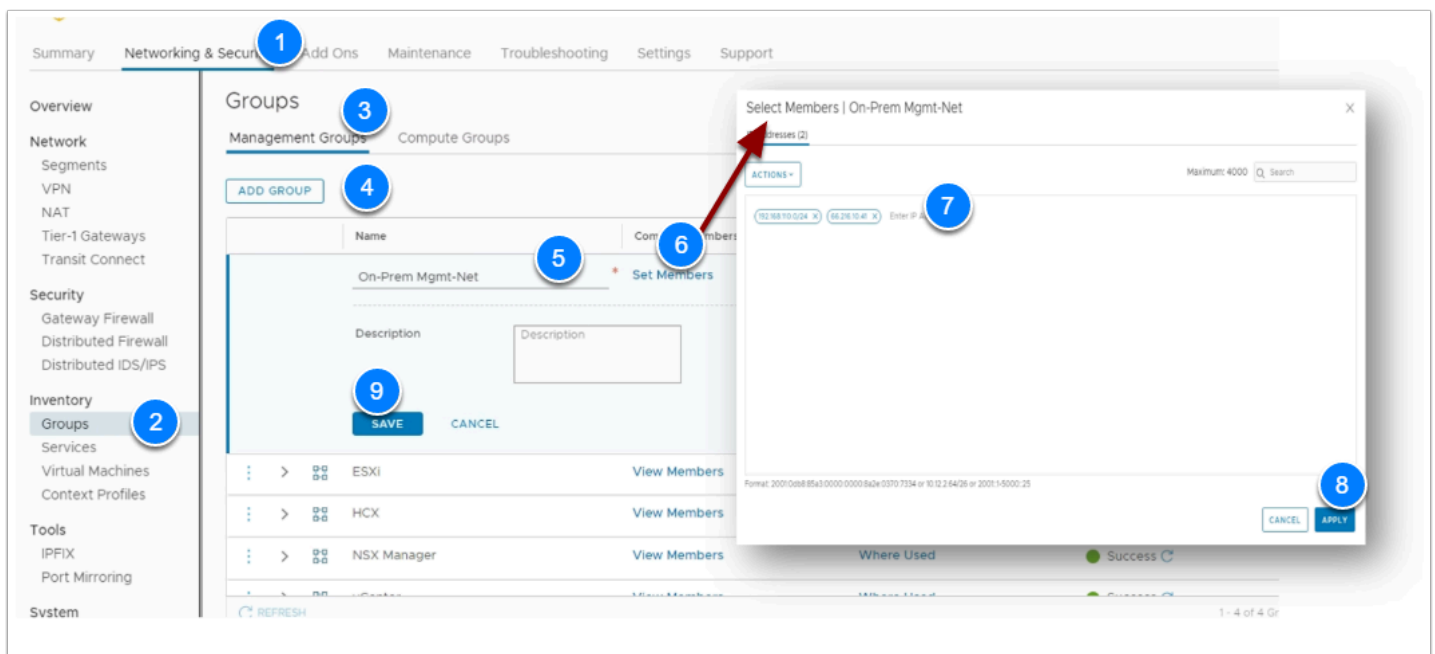
Management of workloads in vCenter can currently be done from anywhere due to the current Management Gateway firewall rule that allows any source to access vCenter. With On-premises integration, you may want to restrict access to your VMware on AWS SDDC vCenter from your On-Premises location(s) only.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

7. 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
15. Click **SAVE**



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

- i** 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.

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**

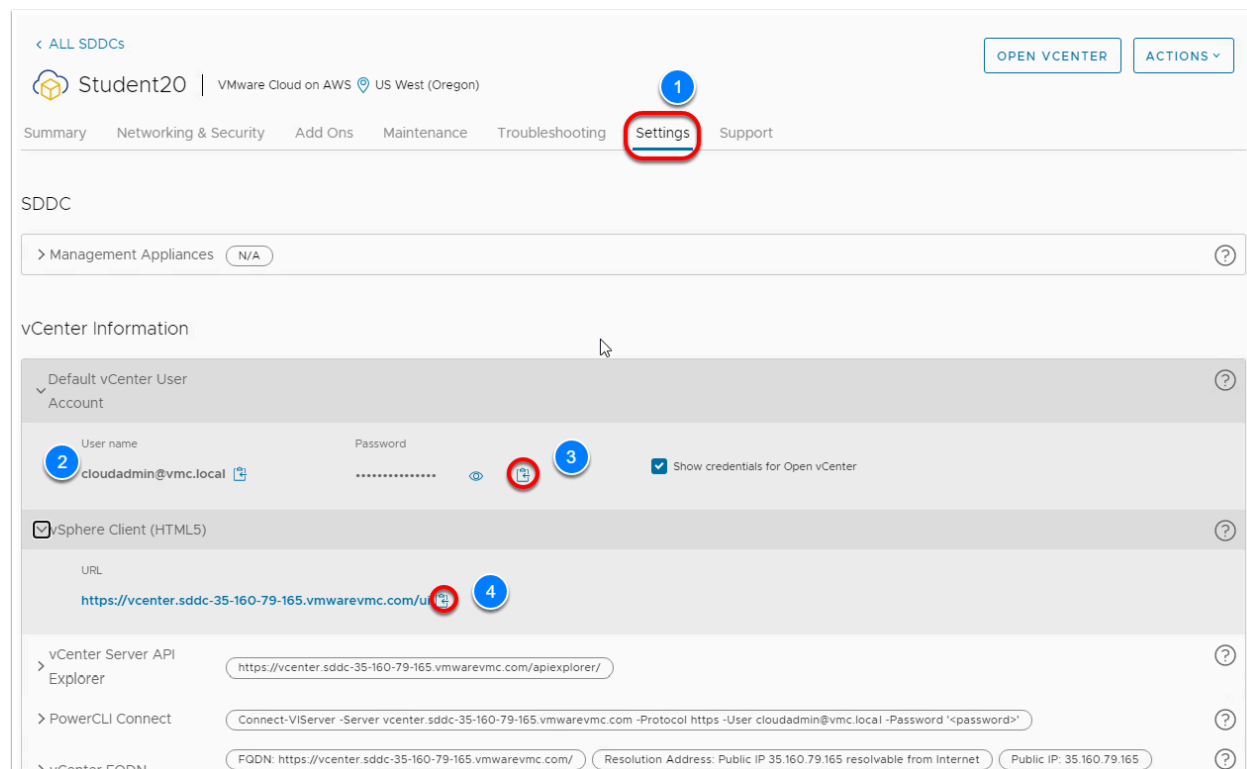
Name	ID	Sources	Destinations	Services	Action
On-Prem to vCenter Inbound		On-Prem Mgmt-Net	vCenter	HTTPS (TCP 443) SSO (TCP 7444)	Allow
On-Prem to ESXi		On-Prem Mgmt-Net	ESXi	Provisioning & Re... vMotion (TCP 80... HTTPS (TCP 443)	Allow
vCenter Inbound	2026	Any	vCenter	SSO HTTPS	Allow
ESXi Outbound Rule	2024	ESXi	Any	Any	Allow
vCenter Outbound Rule	2025	vCenter	Any	Any	Allow

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

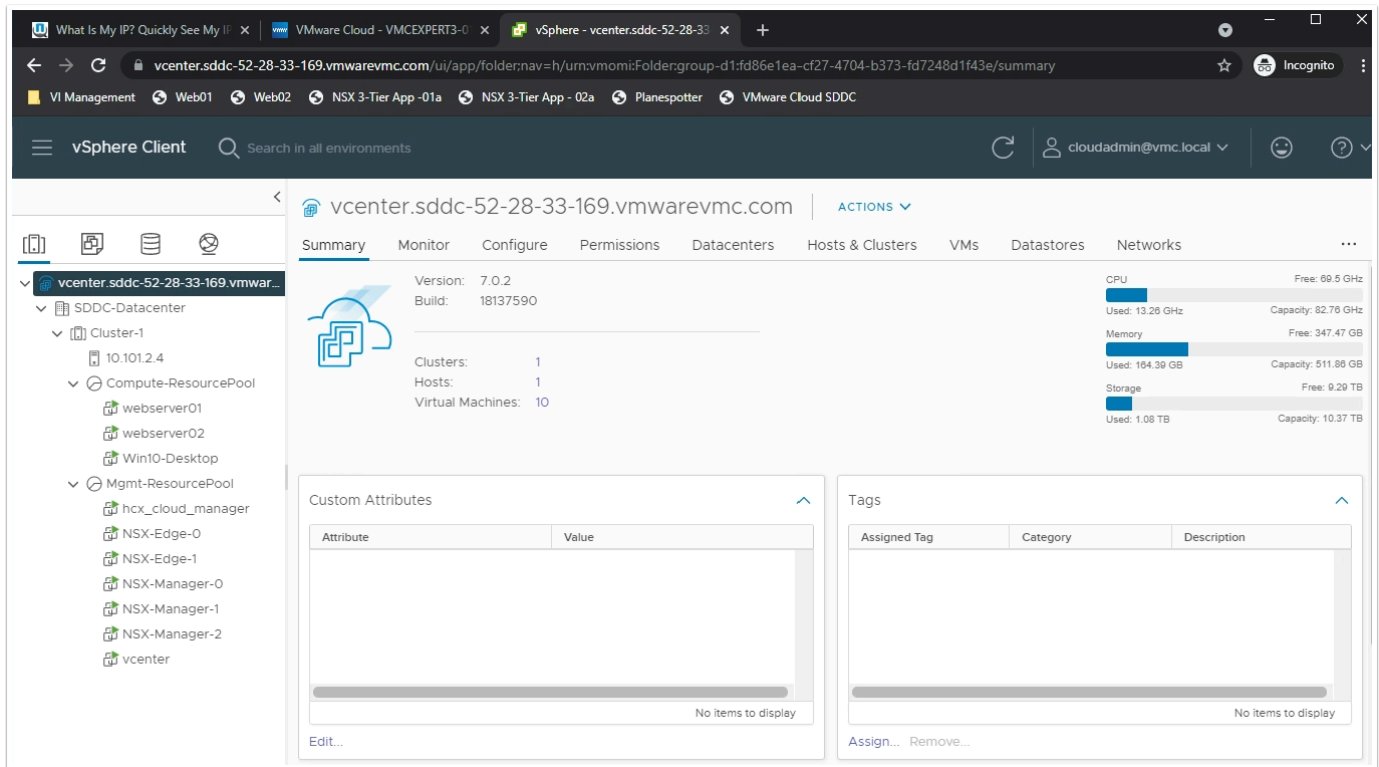
NOTE: At this time this connection is still going over the Public internet, just restricted from On-Premises Management network. In the Next task we will configure IPsec VPN.

Task 2.2 - Test Connectivity from On-Premises

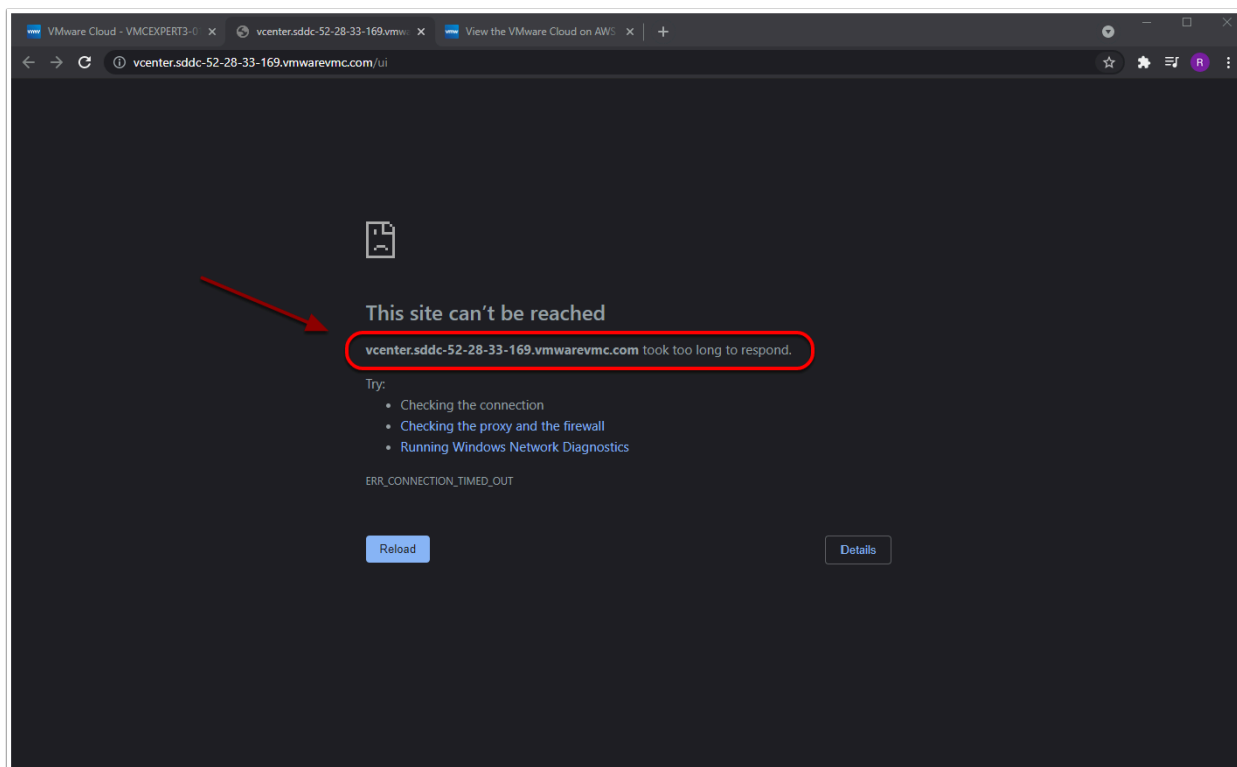
1. Click the **Settings** Tab
2. Expand the **Default vCenter User** and **vSphere Client (HTML5)** sections
3. Take note of and copy the values for:
 - Username
 - Password
 - vSphere Client URL



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



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.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**

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Overview

Network

Segments

VPN

NAT

Tier-1 Gateways

Transit Connect

Security

Gateway Firewall

Distributed Firewall

Distributed IDS/IPS

Inventory

Groups

Services

Virtual Machines

Context Profiles

Tools

IPFIX

Port Mirroring

VPN

Route Based Policy Based Layer 2

ADD VPN EDIT LOCAL ASN

COLLAPSE ALL Filter by Name, Path and more

Name	Local IP Address	Remote Public IP	BGP Local IP/Prefix Length	BGP Remote IP	BGP Neighbor ASN	Status
VMC_	Public IP () .98	66.216	169.254.111.30/30	169.254.111.29	65002	
Preshared Key *		VMwareNinja1!	Remote Private IP	192.168.151.1		

Advanced Tunnel Parameters

Advanced BGP Parameters

Secret

SAVE CANCEL

8. 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.

VPN

Route Based Policy Based Layer 2

ADD VPN EDIT LOCAL ASN COLLAPSE ALL Filter by Name, Path and more

Name	Local IP Address	Remote Public IP	BGP Local IP/Prefix Length	BGP Remote IP	BGP Neighbor ASN	Status
VMC_to_On-Prem_VPN	Public IP1	66.216.	169.254.111.30/30	169.254.111.29	65002	In Progress

Preshared Key Remote Private IP 192.168.151.1

Advanced Tunnel Parameters

- IKE Profile
- IPsec Profile
- DPD Profile

TCP MSS Clamping Disabled

Description Not Set Tags 0

REFRESH 1 - 1 of 1 VPNs

DOWNLOAD CONFIG

VIEW STATISTICS

VIEW ROUTES

DOWNLOAD ROUTES

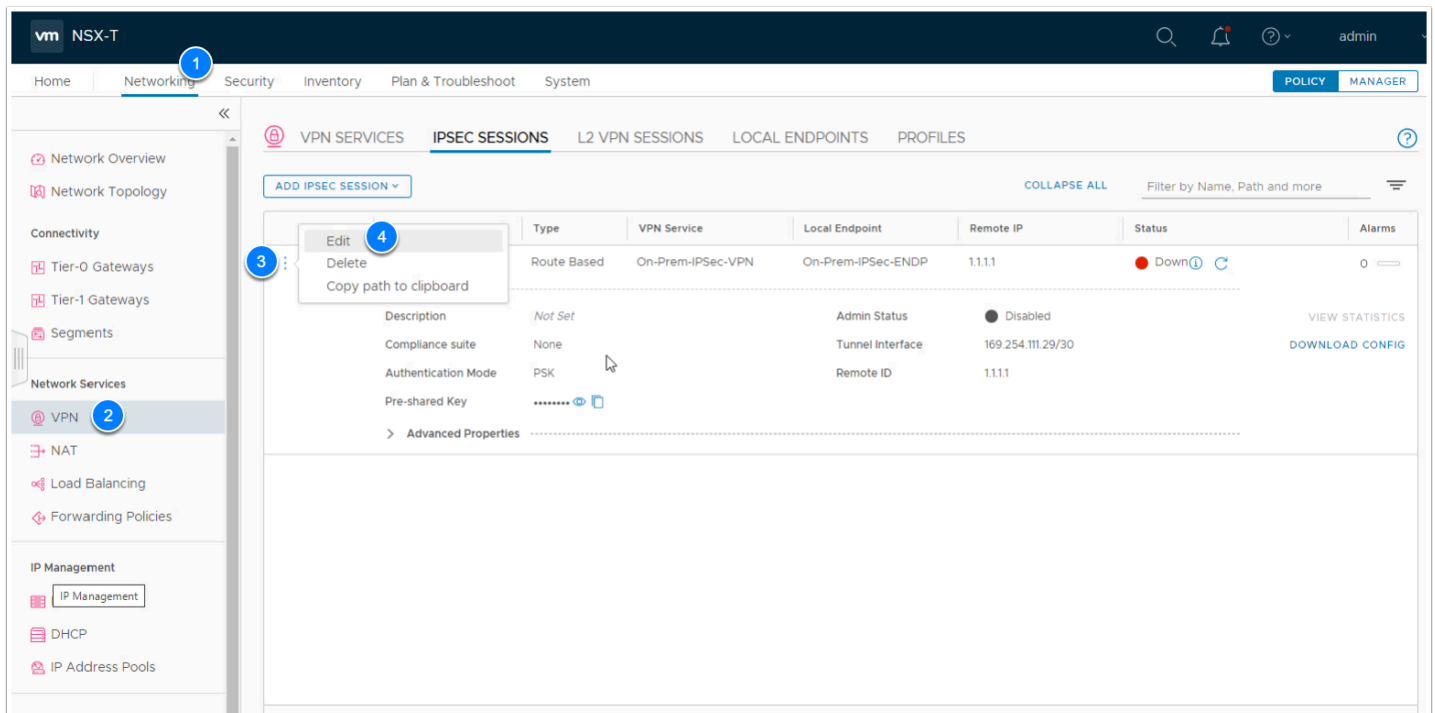
💡 Once you've configured IPsec VPN in your VMware Cloud on AWS SDDC, you'll typically download the configuration and hand it to your On-Premises networking team. They can use the values in the document to configure a VPN endpoint On-Premises. IPsec VPN can be configured on any compliant IPsec VPN Gateway 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-l-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**



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>**

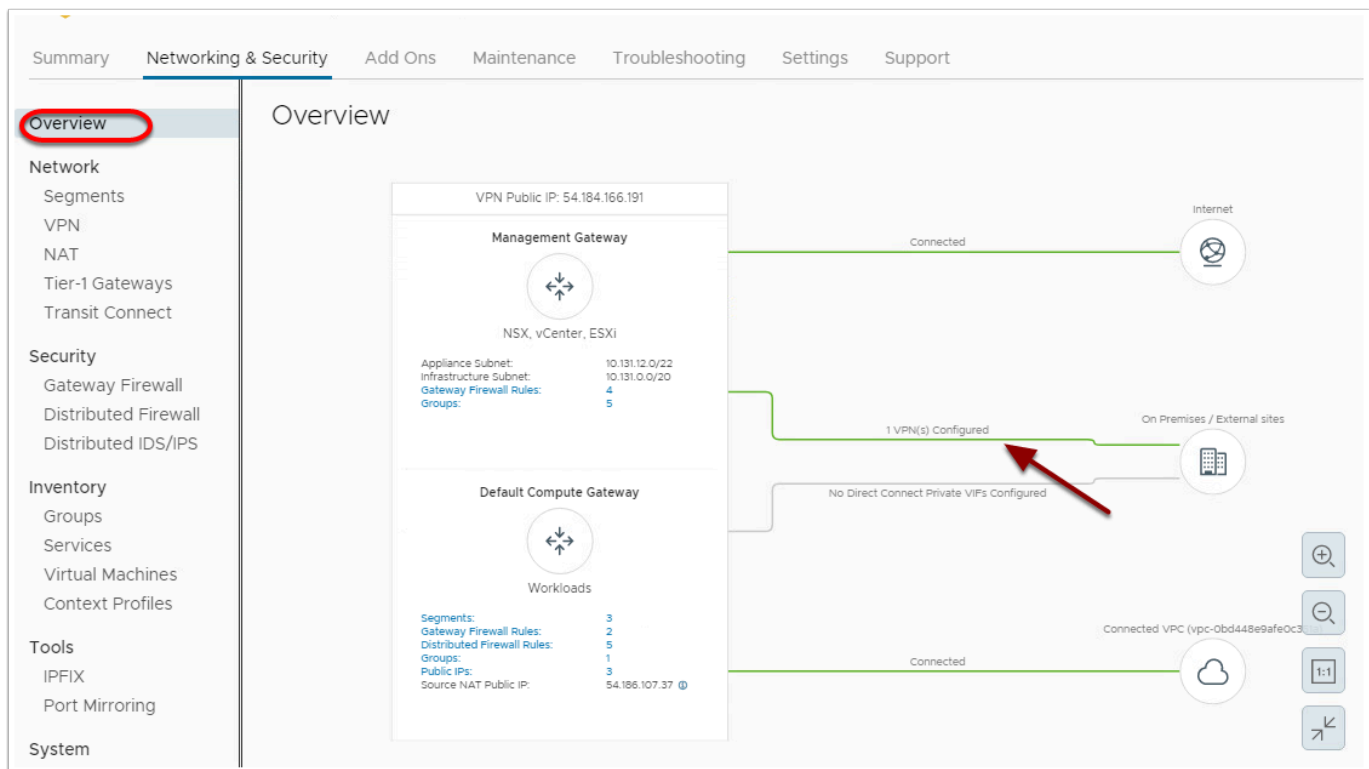
10. Click **SAVE**
11. Under the Status column, click the **refresh icon**

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.

Name	Type	VPN Service	Local Endpoint	Remote IP	Status	Alarms
RB-VPN-VMC	Route Based	On-Prem-IPSec-VPN	On-Prem-IPSec-ENDP	54.185.84.15	Success	0

Description	Not Set	Admin Status	Enabled	VIEW STATISTICS
Compliance suite	None	Tunnel Interface	169.254.111.29/30	DOWNLOAD CONFIG
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 out-going and in-coming connections.

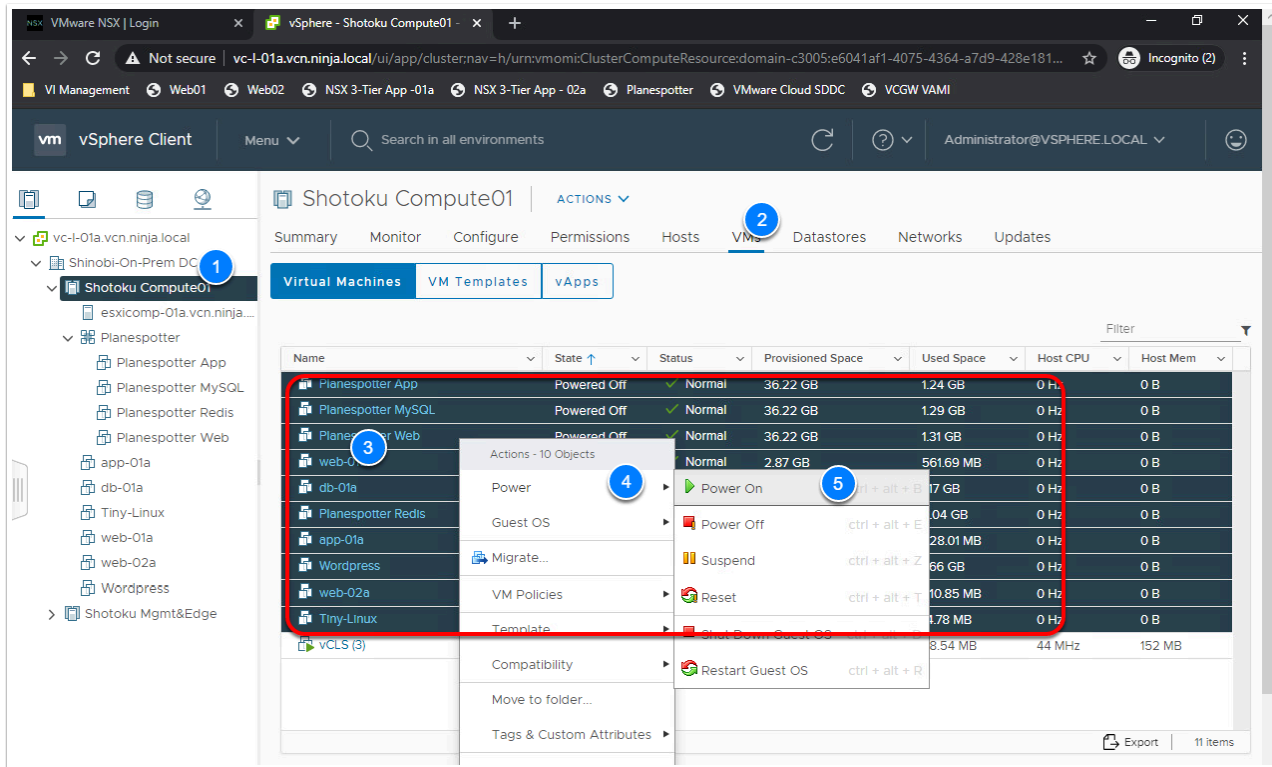
Task 4.1 - Configure/Identify Private addressing for vCenter and Workload VMs

1. From the VDI Desktop open a new Browser tab and Click **VI Management**
2. Click **vsphere Client**
If prompted with an SSL Warning message, click **Advanced** and then **Proceed to vc-l-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**):

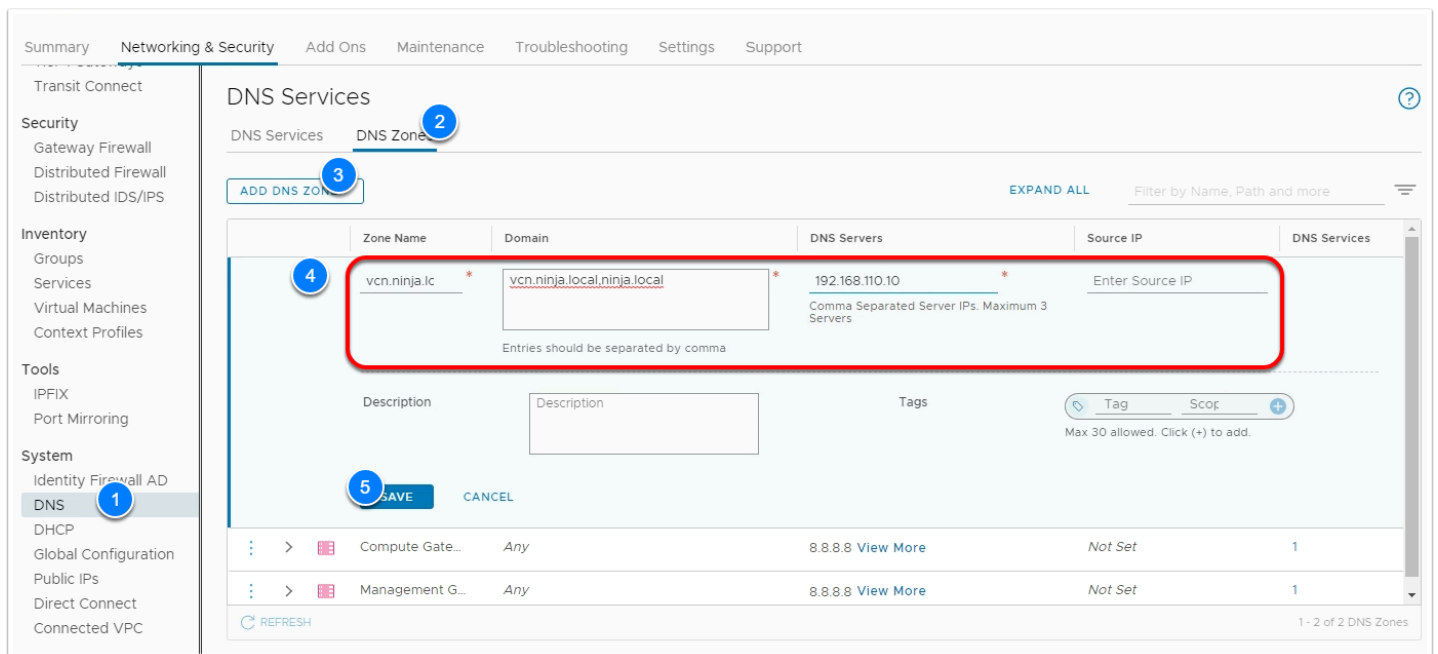
- **Web-01a | 172.16.10.11**
- **Web-02a | 172.16.10.12**
- **App-01a | 172.16.20.11**
- **Db-01a | 172.16.30.11**

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



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 **Settings** tab
2. Expand **vCenter FQDN**, click **Edit**
3. From the **Resolution address** Drop Down Set the address to **Private IP**
4. Click **Save**



15. Click **DNS Zones** Tab
16. Select the 3 vertical dots next to **Compute Gateway DNS Forwarder**
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**

DNS Services

DNS Services DNS Zones

[ADD DNS ZONE](#) EXPAND ALL Filter by Name, Path and more

	Domain	DNS Servers	Source IP	DNS Services
<div> <div>Edit</div> <div>Delete</div> <div>Copy Path to Clipboard</div> </div>	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

[REFRESH](#) 1 - 3 of 3 DNS Zones

DNS Services

DNS Services DNS Zones

[ADD DNS ZONE](#) EXPAND ALL Filter by Name, Path and more

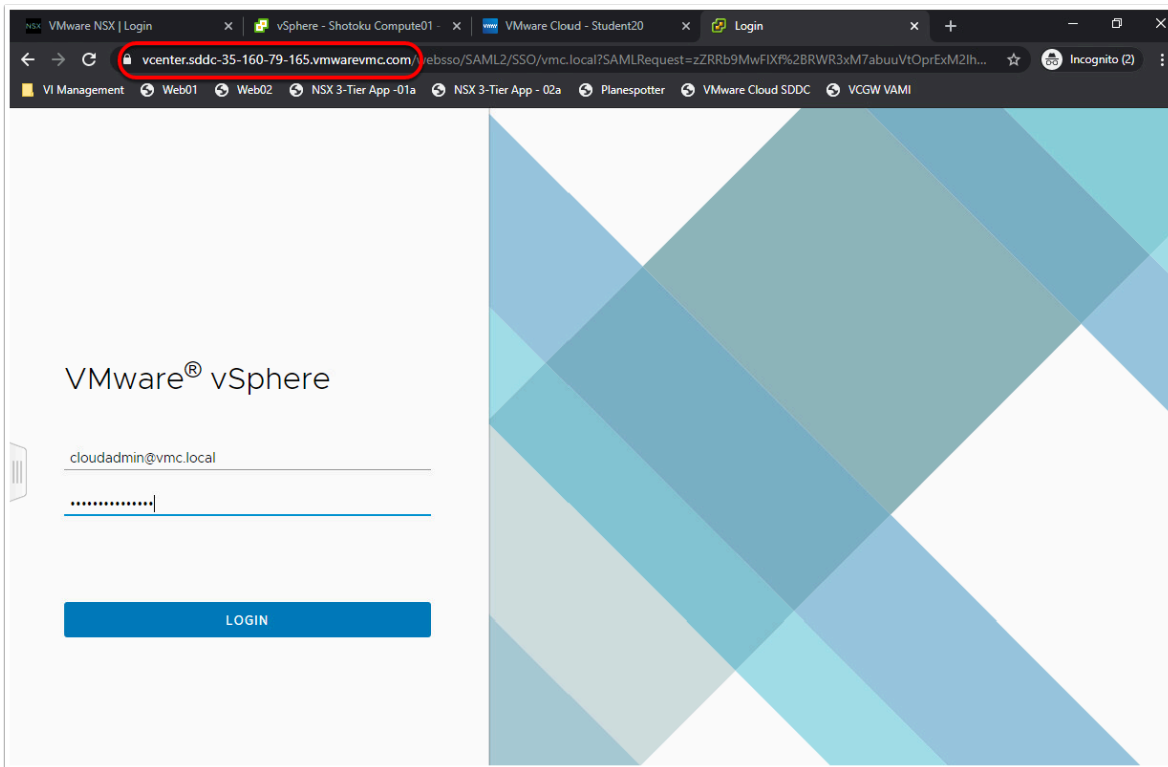
Zone Name	Domain	DNS Servers	Source IP	DNS Services
Compute G. *	Any	<div>1</div> <div>192.168.110.10 *</div> <div>Comma Separated Server IPs. Maximum 3 Servers</div>	Enter Source IP	
Description	Description	Tags	<div>Tag Scop</div> <div>Max 30 allowed. Click (+) to add.</div>	
<div>2</div> <div>SAVE</div> <div>CANCEL</div>				
> 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

[REFRESH](#) 1 - 3 of 3 DNS Zones

💡 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 from 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.



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**

VMC EXPERT3-01 | VMC on AWS EU Central (Frankfurt)

Summary Networking & Security Add Ons Maintenance Troubleshooting Settings Support

Transit Connect

Security

- Gateway Firewall
- Distributed Firewall
- Distributed IDS/IPS

Inventory

- Groups
- Services
- Virtual Machines
- Context Profiles

Tools

- IPFIX
- Port Mirroring

System

- Identity Firewall AD
- DNS
- DHCP
- Global Configuration
- Public IPs
- Direct Connect
- Connected VPC

Groups

Management Groups Compute Groups

ADD GROUP EXPAND ALL Filter by Name, Path and more

Name	Compute Members	Where Used	Status
On-Prem 3-Tier App	Set Members		
Description			
Tags			
Max 30 allowed. Click (+) to add.			
PhotoAppVM	View Members	Where Used	Success
web	View Members	Where Used	Success

SAVE CANCEL

REFRESH

Select Members | On-Prem 3-Tier App ×

Add Compute Members either by creating or by directly adding them.

Membership Criteria (0) Members (0) **IP Addresses (3)** MAC Addresses (0) AD Groups (0)

ACTIONS Maximum: 4000

8 172.16.10.0/24 172.16.20.0/24 192.16.30.0/24

Format: 2001:0db8:85a3:0000:0000:8a2e:0370:7334 or 10.12.2.64/26 or 2001::1-5000::25

CANCEL **9** APPLY

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)

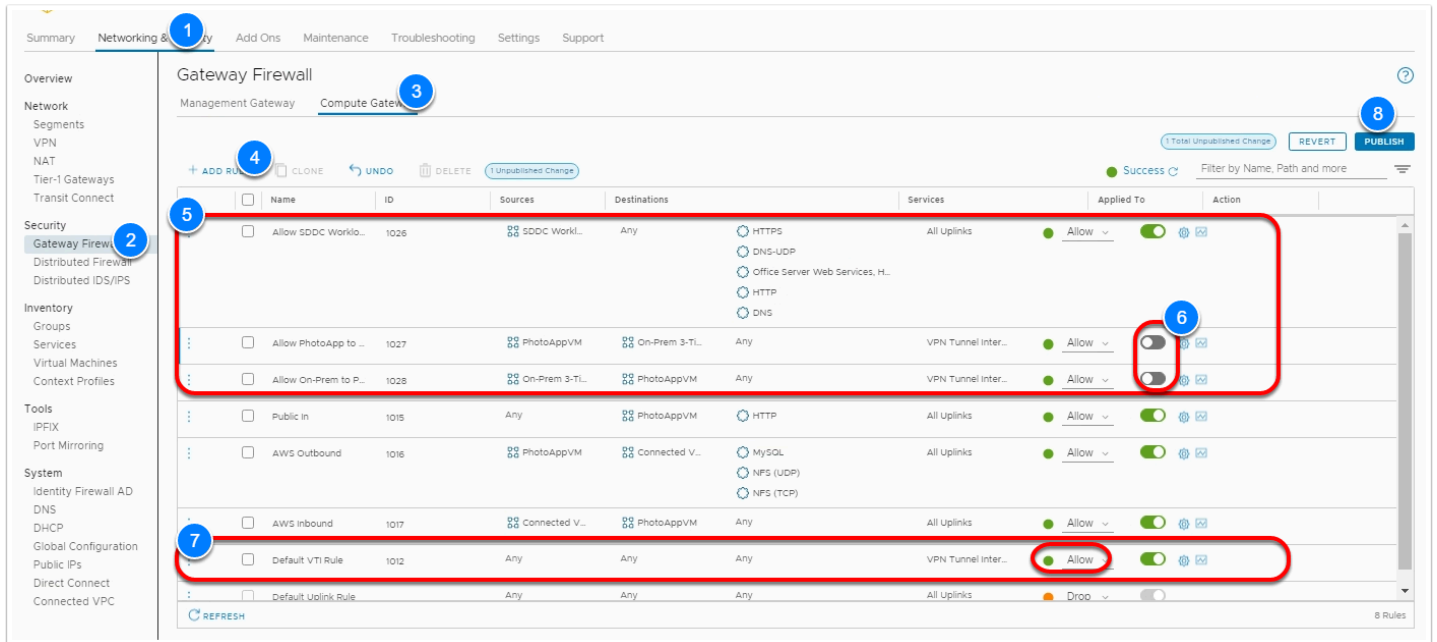
- Name: **Allow PhotoApp to On-Prem**
- Source: **PhotoAppVM**
- Destination: **On-Prem 3-Tier App**
- Service: **Any**
- Applied To: **VPN Tunnel Interfaces**
- Action: **Allow**
- Move the slider to **Disable** this rule

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**

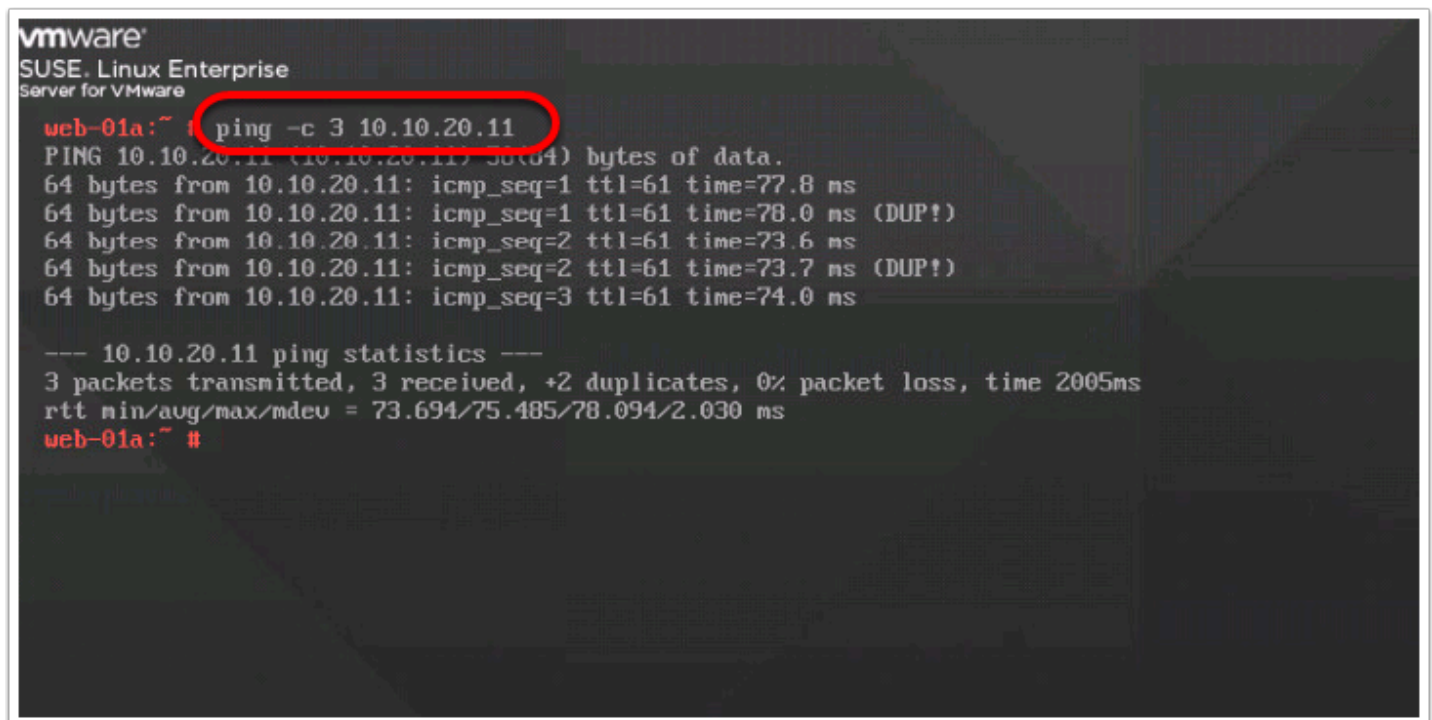
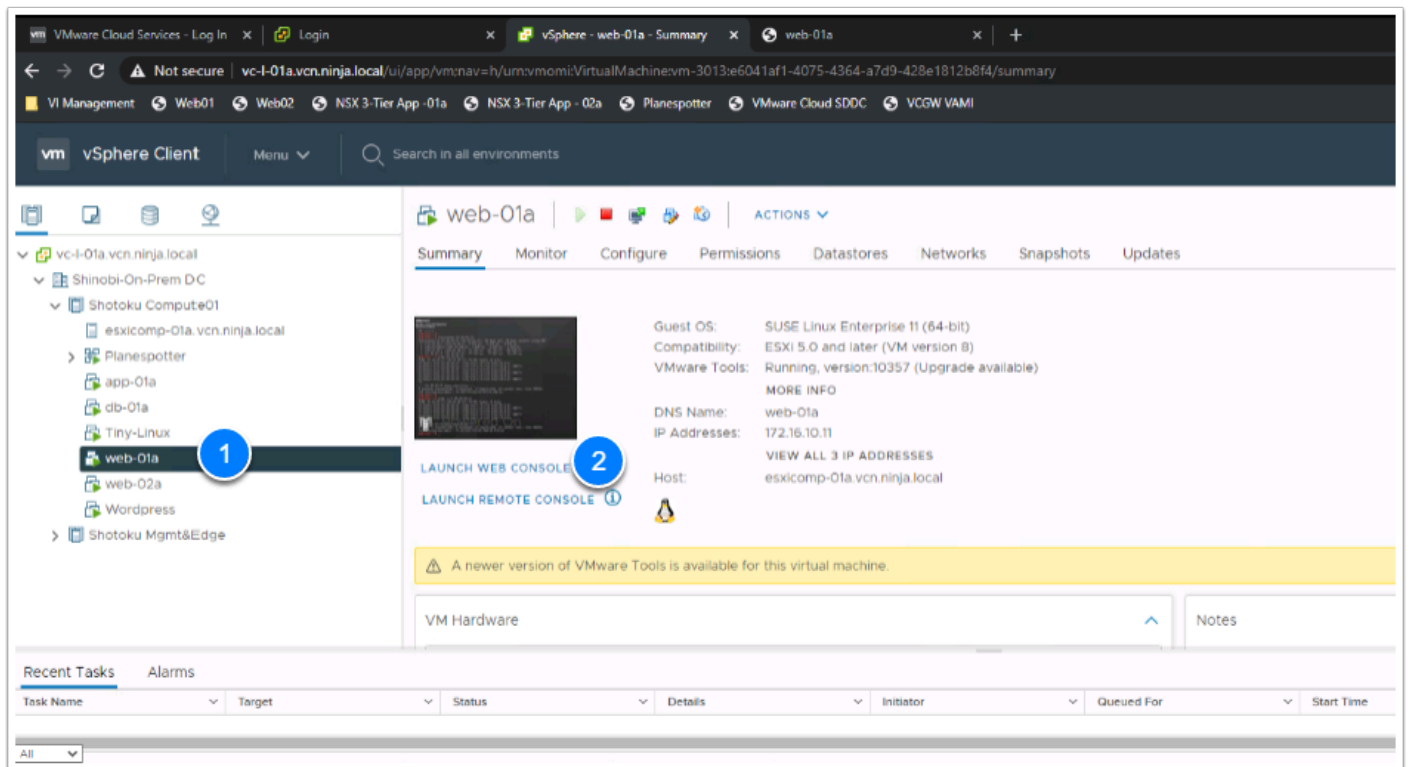
4. Change the "Action" dropdown on the **"Default VTI Rule"** to **Allow** instead of **Drop**. This allows all flows over the VPN tunnel in and out of the Compute gateway.

5. Click **Publish**



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**
4. Select **web-01a** VM (You can find this under vc-l-01a > Shinobi On Prem DC > Shotoku Compute01)
5. Click **LAUNCH WEB CONSOLE**
6. 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-Datcenter > Cluster-1 > Compute-ResourcePool > Webserver01)



Conclusion

i 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.

i 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...