USDC TECHNOLOGY
Smart Data Center

USER GUIDE FOR vFIREWALL AND vLOAD BALANCER SERVICES

INDEX

I. Introduction 2

II. Configure vFirewall 3

1. Configure Network Address Translation (NAT) 5
2. Define Firewall Rules 7
3. Configure IPsec VPN Site to Site 9
4. Configure SSL VPN Client to Site 13

III. vLoad Balancer service 22

1. Import certificate 23
2. Application Profiles 25
3. Server Pool 27
4. Virtual Server 30
5. Test the service 31

I. Introduction

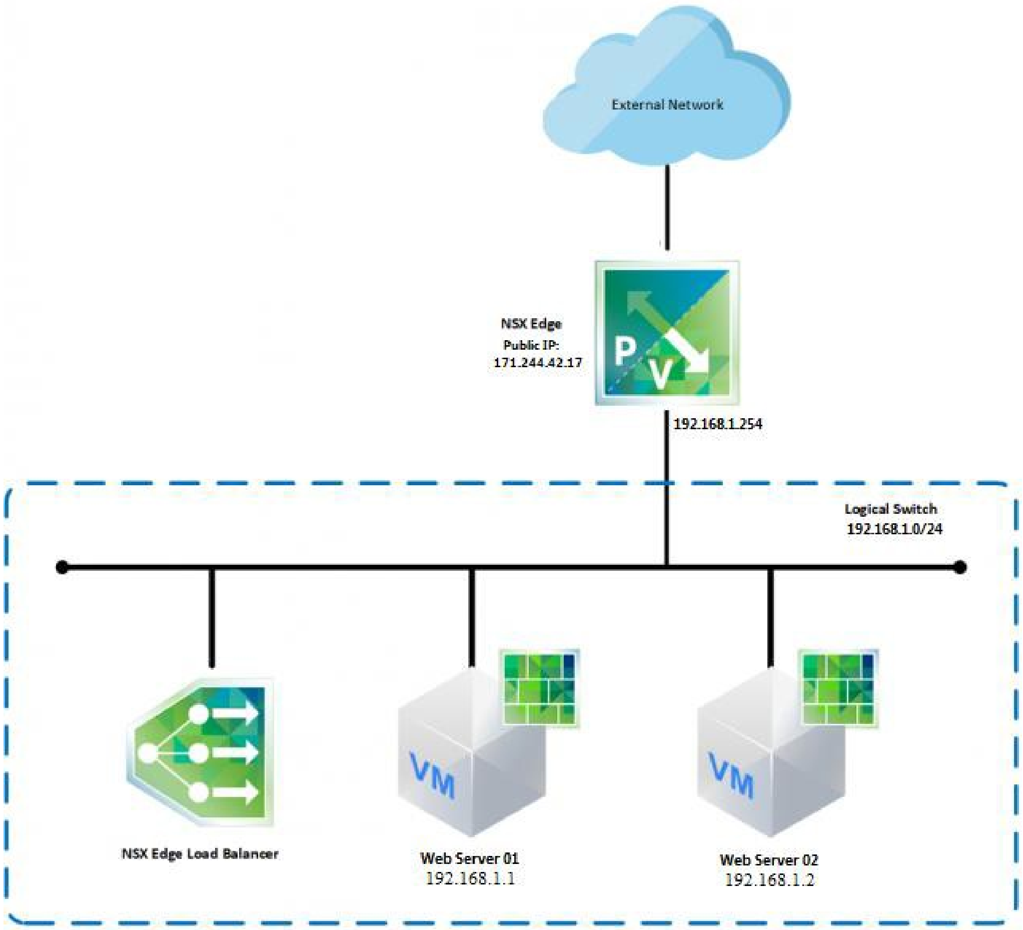
vFirewall and vLoad Balancer are 2 add-on services based on the VMWare NSX solution provided on USDC Technology's Virtual Private Cloud (VPC) service.

USDC Technology provided 2 services to the NSX Edge Gateway Advanced version with many features and improvements compared to the Basic version. To access management page, please log in to vCloud Director Portal with the link and account provided.

Syntax of the login path:

https://vpc.vcpp.vn/tenant/YOUR_ID (HTML5 interface) with YOUR_ID is Customer ID (Tenant) on USDC Technology’s Virtual Private Cloud.

Assume that we need to establish the basic network model as the diagram below:

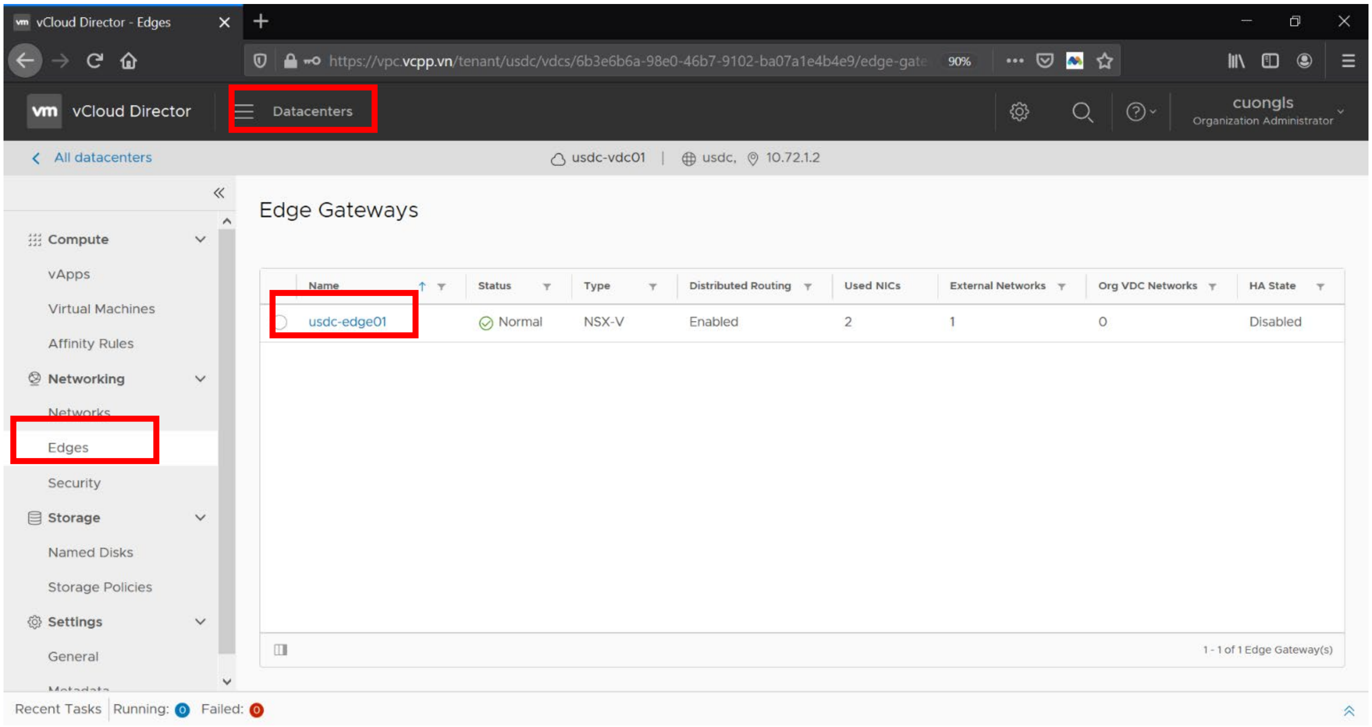


	Private Zone	Public Zone	Mode
NSX Edge (vFirewall)	192.168.1.254	171.244.42.17	NIC direct connection
NSX Edge Load Balancer	1 cluster include 2 members of Web Server below	171.244.42.17	To Internet
Web Server 01	192.168.1.1	171.244.42.111	VIP represent for Cluster
Web Server 02	192.168.1.2	171.244.42.112	NAT on vFirewall

In this model, there are 2 types of Public IP: One is the IP used for representing NSX Edge (vFirewall), virtual IP for vLoad Balancer (called Master IP); Another is the public IP used for NAT 1: 1 for VMs (called NAT IP).

II. Configure vFirewall

After successful login, from main dashboard, choose **Datacenters -> Networking -> Edge Gateway.** The vFirewall's configuration which you rent will be showed here when clicking to the Edge name.



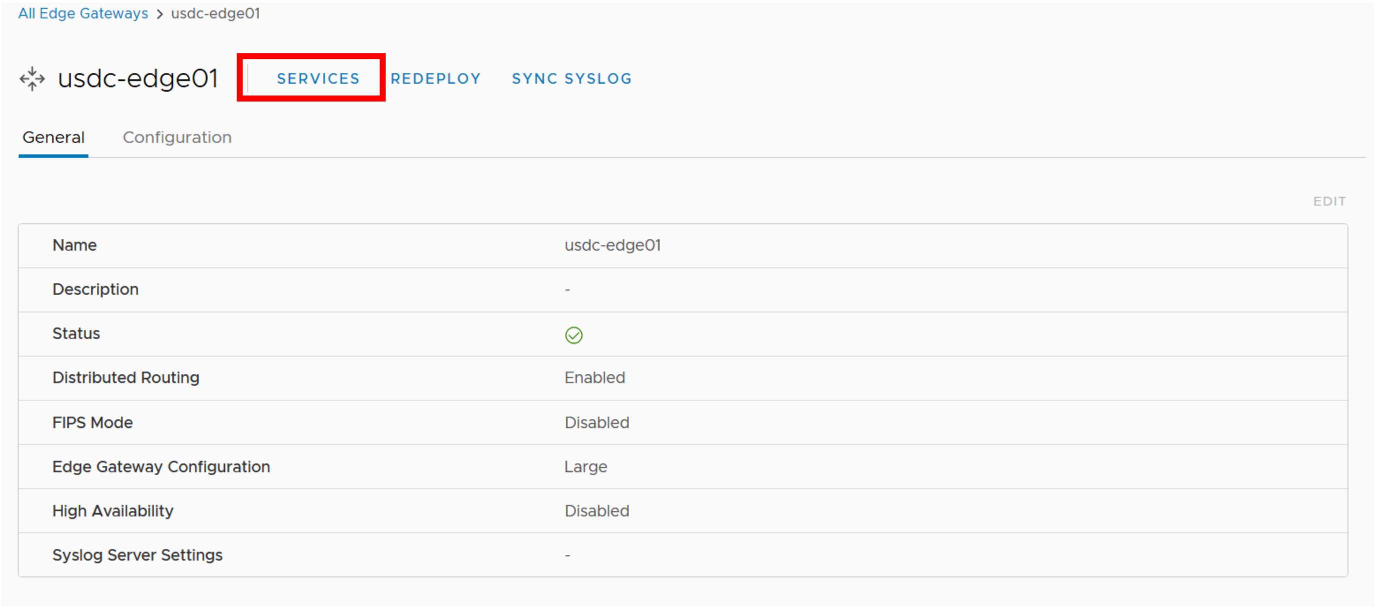
vCloud Director - Edges

https://vpc.vcpp.vn/tenant/usdc/vdcs/6b3e6b6a-98e0-46b7-9102-ba07a1e4b4e9/edge-gate

Edge Gateways

Name	Status	Type	Distributed Routing	Used NICs	External Networks	Org VDC Networks	HA State
usdc-edge01	Normal	NSX-V	Enabled	2	1	0	Disabled

1 - 1 of 1 Edge Gateway(s)



All Edge Gateways > usdc-edge01

usdc-edge01 SERVICES REDEPLOY SYNC SYSLOG

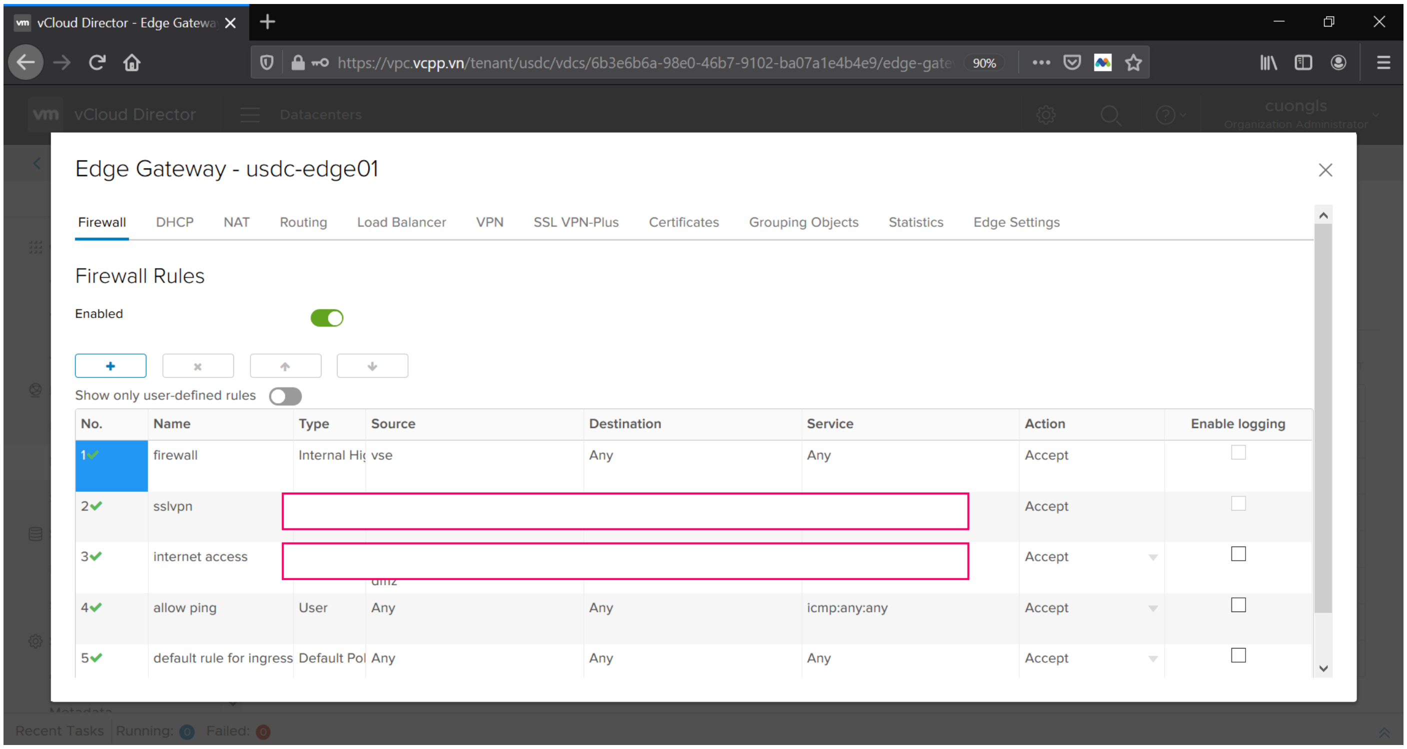
General Configuration

EDIT

Name	usdc-edge01
Description	-
Status	✓
Distributed Routing	Enabled
FIPS Mode	Disabled
Edge Gateway Configuration	Large
High Availability	Disabled
Syslog Server Settings	-

✍ *You can view Edge Policies and Services (Firewall, DHCP, VPN, SSL, etc.):* choose Edge Gateway at the item **Networking -> Edge -> Services**

Note: The NSX Edge configuration screen appears, select **Enable** at the **Firewall tab**



vCloud Director - Edge Gatewa
https://vpc.vcpp.vn/tenant/usdc/vdcs/6b3e6b6a-98e0-46b7-9102-ba07a1e4b4e9/edge-gate
90%
vCloud Director
Datacenters
cuongls
Organization Administrator
Recent Tasks Running: 0 Failed: 0

Edge Gateway - usdc-edge01

Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Certificates Grouping Objects Statistics Edge Settings

Firewall Rules

Enabled ●

+ × ↑ ↓

Show only user-defined rules ○

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1✓	firewall	Internal Hi(	vse	Any	Any	Accept	□
2✓	sslvpn	[redacted]	[redacted]	[redacted]	[redacted]	Accept	□
3✓	internet access	[redacted]	[redacted]	[redacted]	[redacted]	Accept	□
4✓	allow ping	User	Any	Any	icmp:any:any	Accept	□
5✓	default rule for ingress	Default Pol	Any	Any	Any	Accept	□

1. Configure Network Address Translation (NAT)

You must enable Firewall before NAT configuration.

Switch to the **NAT** tab, which will display a list of NAT rules configured. USDC Technology's vFirewall solution supports two main types of NAT: Source-based NAT (SNAT) and destination-based NAT (DNAT) for both IPv4 and IPv6. This guide focuses on IPv4.

To create a new NAT rule, select the icon

☑ SNAT + SNAT RULE **(from IP local translates to IP public)**

- Applied On: Select the network area to execute, the default is the external network layer (External).

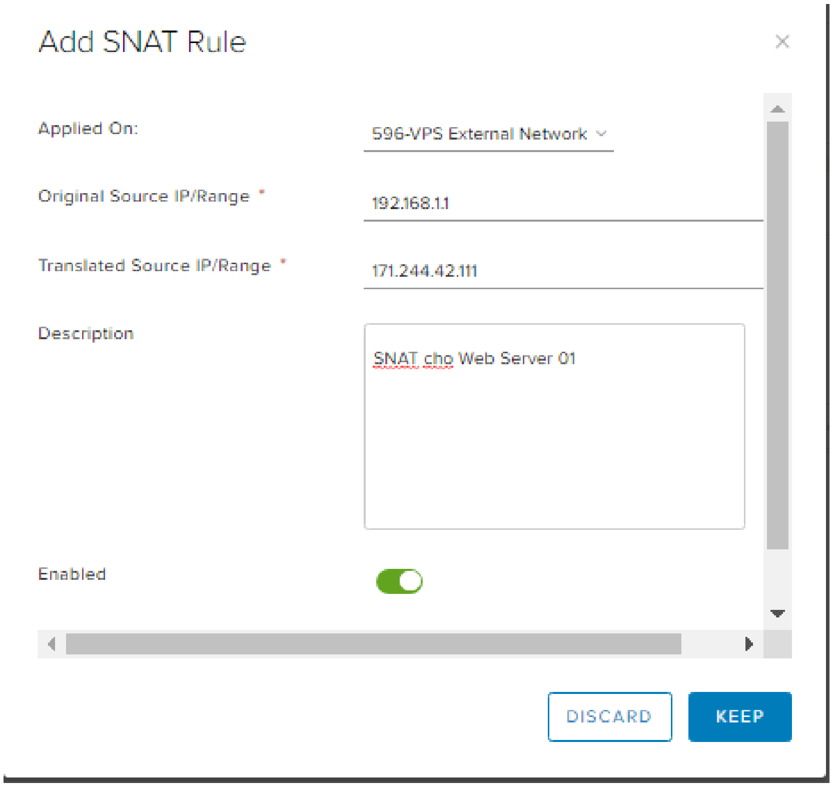
- Original Source IP/Range: enter the original IP (server's private IP)

- Translated Source IP/Range: IP is converted after NAT (it is the Public NAT IPs obtained above)

- Description: Enter a description

- Enable: Select this item to make the rule valid

Click **Keep** after completing fill in parameters.



Add SNAT Rule

Applied On: 596-VPS External Network

Original Source IP/Range *: 192.168.1.1

Translated Source IP/Range *: 171.244.42.111

Description: SNAT cho Web Server 01

Enabled

☑ **DNAT** + DNAT RULE **(from IP public translates to IP local)**

-Applied On: Select the network area to execute, the default is the external network layer (External).

- Original IP / Range: enter the original IP (IP Public, it is the Public NAT IP obtained above)

- Protocol: choose the type of protocol (TCP, UDP, ICMP, Any)

- Original Port: the original port sent by the client

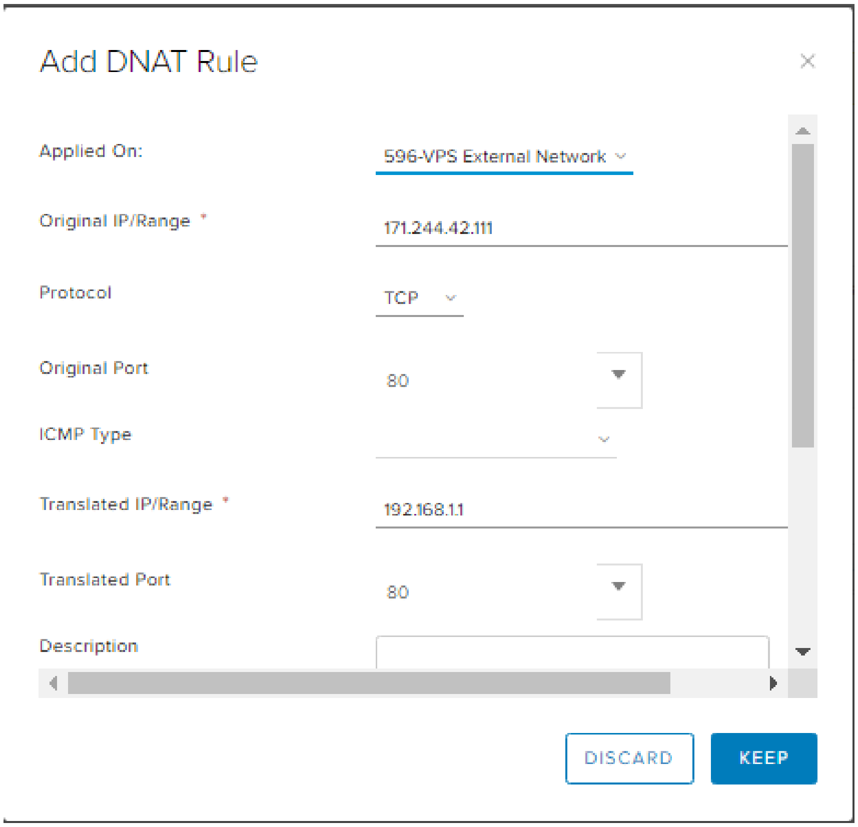
- Description: Enter a description

- Translated IP / Range: The server's private IP is converted after NAT

- Translated Port: Port converted, transferred to server after NAT

- Enable: select it to make rule valid

Click **Keep** after completing the parameters



Add DNAT Rule

Applied On: 596-VPS External Network

Original IP/Range *: 171.244.42.111

Protocol: TCP

Original Port: 80

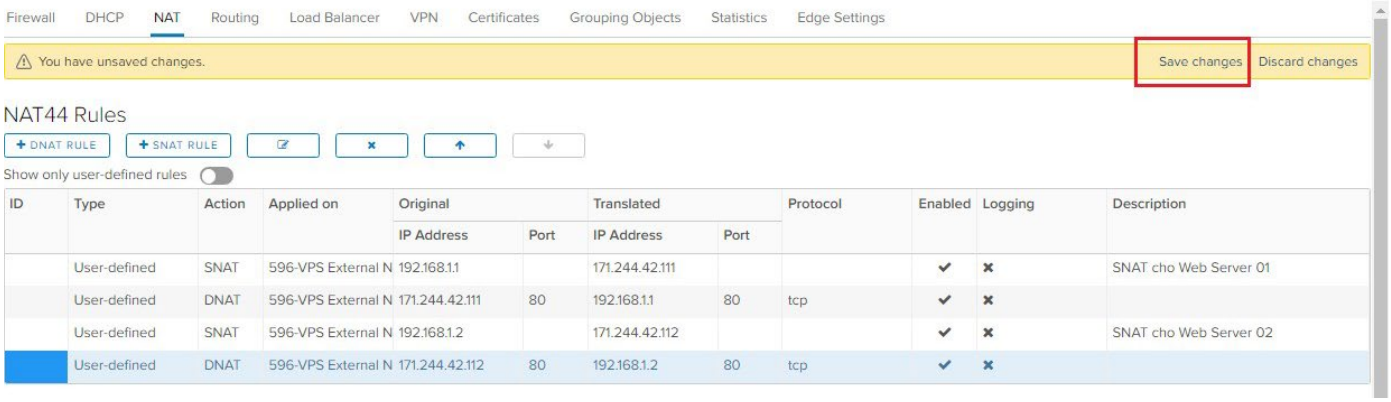
ICMP Type:

Translated IP/Range *: 192.168.1.1

Translated Port: 80

Description:

Do the same for Web Server 02. After you have finished, click the "**Save Changes**" button to save and execute the new configuration:



⚠ You have unsaved changes.

NAT44 Rules

ID	Type	Action	Applied on	Original		Translated		Protocol	Enabled	Logging	Description
				IP Address	Port	IP Address	Port				
	User-defined	SNAT	596-VPS External N	192.168.1.1		171.244.42.111			✓	✖	SNAT cho Web Server 01
	User-defined	DNAT	596-VPS External N	171.244.42.111	80	192.168.1.1	80	tcp	✓	✖	
	User-defined	SNAT	596-VPS External N	192.168.1.2		171.244.42.112			✓	✖	SNAT cho Web Server 02
	User-defined	DNAT	596-VPS External N	171.244.42.112	80	192.168.1.2	80	tcp	✓	✖	

✍ Custom can edit NAT rule which defined before by choosing th button ✎. Click ✖ to delete NAT rule. Choose "Save Changes" to apply new changes.

2. Define Firewall Rules

At **Firewall** tab, Firewall should be "enabled" and turn on option **"Show only user-defined rules"**

+: Create new rule

✖: Delete selected rule

↑: Upgrade the priority order of selected rules

↓: Downgrade the priority order of selected rules

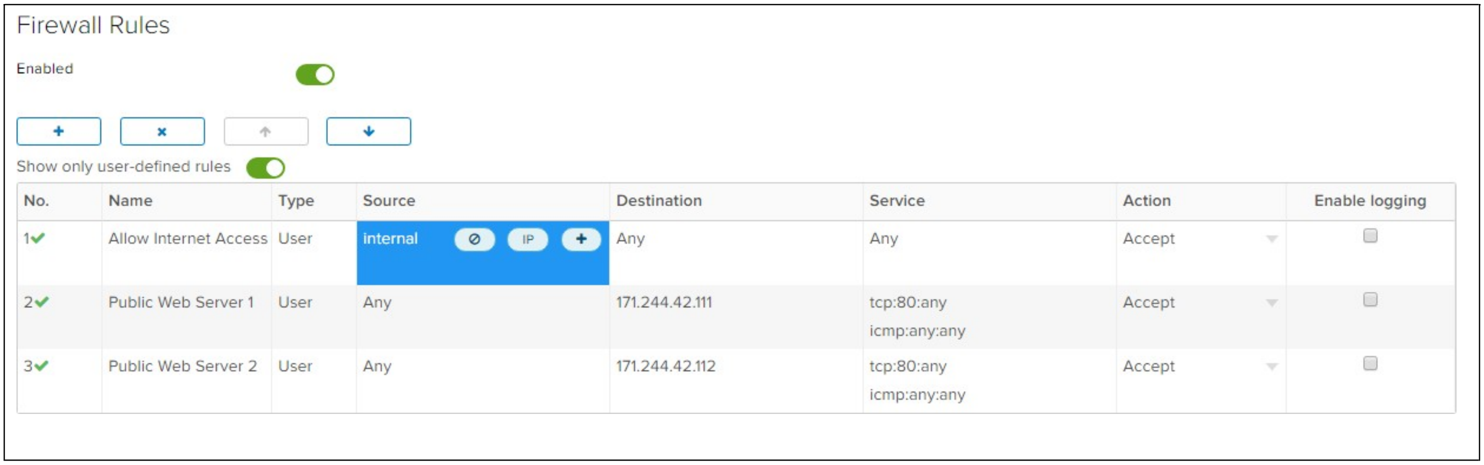
After creating a new rule, it will show a new line which show up with the default information fields (any, any, accept), click on the corresponding box to edit the information needed:

- **No**: Priority of Rules
- **Name**: Name of Rules
- **Type**: System or User create
- **Source**: Source IP, able to click IP to enter IP address or click + to choose available object (internal, external, all..)
- **Destination**: Destination IP.

- **Service**: select protocols (TCP, UDP, ICMP, Any) and port (80, 443, 21) for Source and destination
- **Action**: select action type: Accept - allow or Deny - block

After completing the rules, press the "Save Changes" button to save and apply the new configuration.

🕮 **An example of the original system model in Section I:**



Firewall Rules

Enabled ●

Show only user-defined rules ●

No.	Name	Type	Source	Destination	Service	Action	Enable logging
1✓	Allow Internet Access	User	internal	Any	Any	Accept	□
2✓	Public Web Server 1	User	Any	171.244.42.111	tcp:80:any icmp:any:any	Accept	□
3✓	Public Web Server 2	User	Any	171.244.42.112	tcp:80:any icmp:any:any	Accept	□

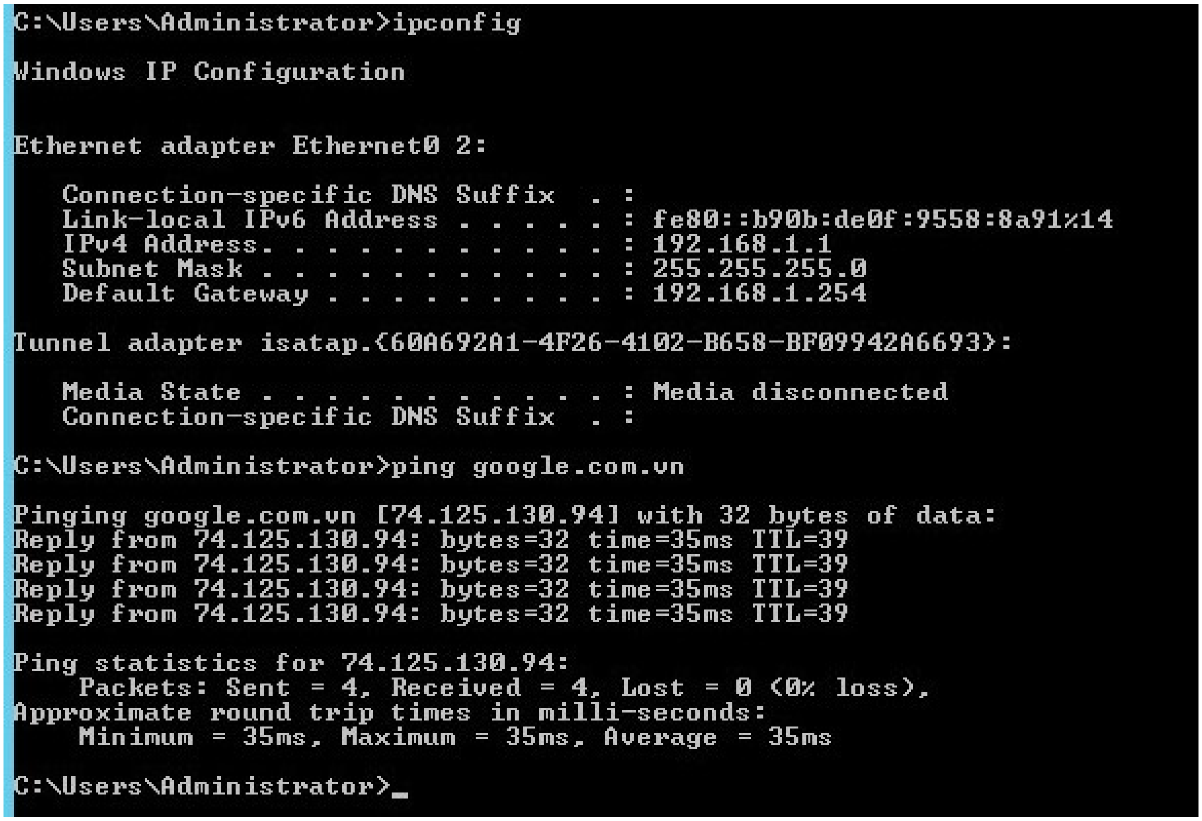
Description:

- Rule No. 1: Allow network traffic from the internal network (192.168.1.x) to all routes (including both external network). The internal network will follow the NAT rule which created before to access the Internet.
- Rule No.2 and No.3: Customer can ping (ICMP) and access web services (http- tcp port 80) of 2 public IP 171.244.42.111 and 171.244.42.112. This is the NAT IP of the two Web servers 192.168.1.1 and 192.168.1.2 Follow as the NAT rule, customer from external networks (internet) can access the web to these two servers.

Network traffics does not match three rules above is blocked by default.

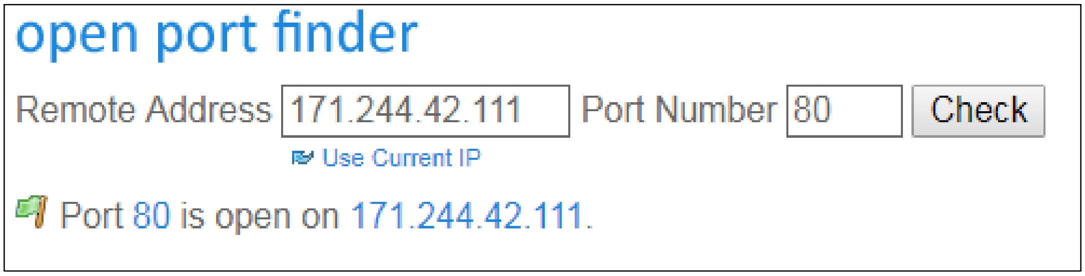
✍ Check the results:

From Web Server 1, ping the internet:



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b90b:de0f:9558:8a91%14
   IPv4 Address. . . . . . . . . . . : 192.168.1.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254

Tunnel adapter isatap.{60A692A1-4F26-4102-B658-BF09942A6693}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>ping google.com.vn

Pinging google.com.vn [74.125.130.94] with 32 bytes of data:
Reply from 74.125.130.94: bytes=32 time=35ms TTL=39
Reply from 74.125.130.94: bytes=32 time=35ms TTL=39
Reply from 74.125.130.94: bytes=32 time=35ms TTL=39
Reply from 74.125.130.94: bytes=32 time=35ms TTL=39

Ping statistics for 74.125.130.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 35ms, Average = 35ms

C:\Users\Administrator>_
```

Check status of service:



open port finder

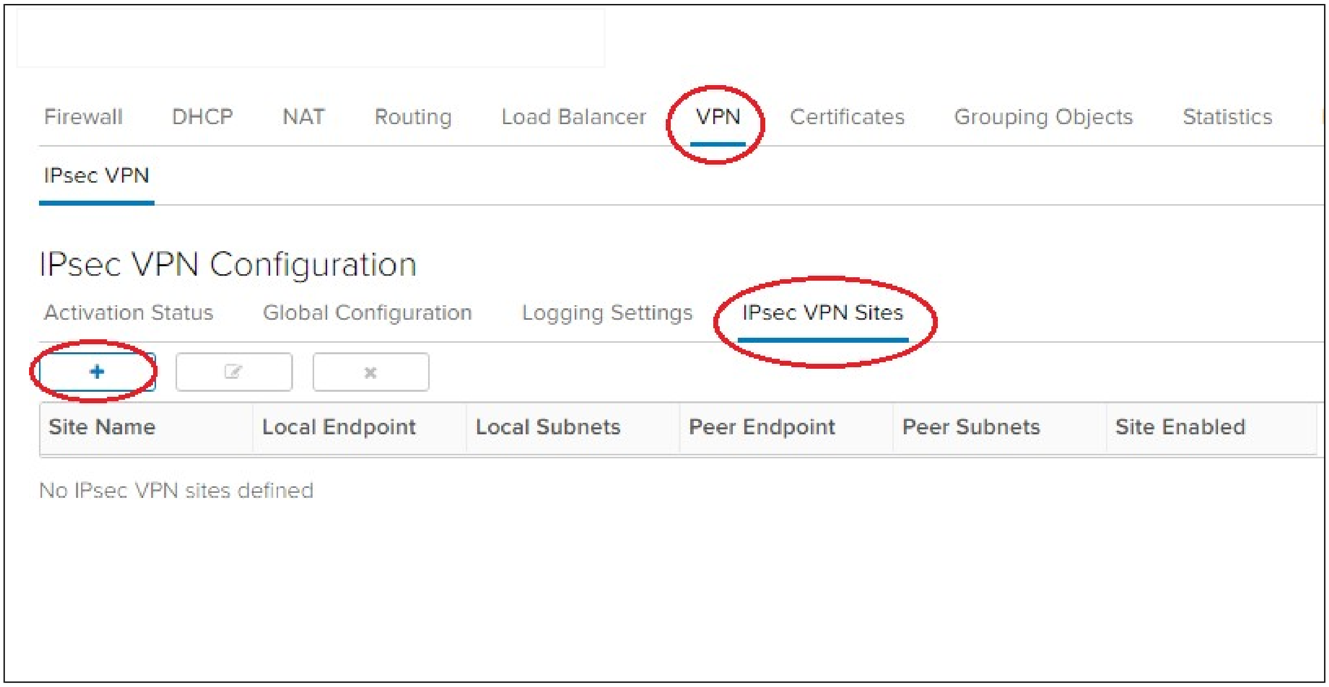
Remote Address: 171.244.42.111

Port Number: 80

Port 80 is open on 171.244.42.111.

3. Configure IPsec VPN Site to Site

In vFirewall service of USDC Technology, we provide the function of setting up VPN Site to Site connection. At administration page, select the **VPN tab** -> **IPsec VPN** -> **IPsec VPN Sites**. Click + to create a new VPN connection.



Site Name	Local Endpoint	Local Subnets	Peer Endpoint	Peer Subnets	Site Enabled

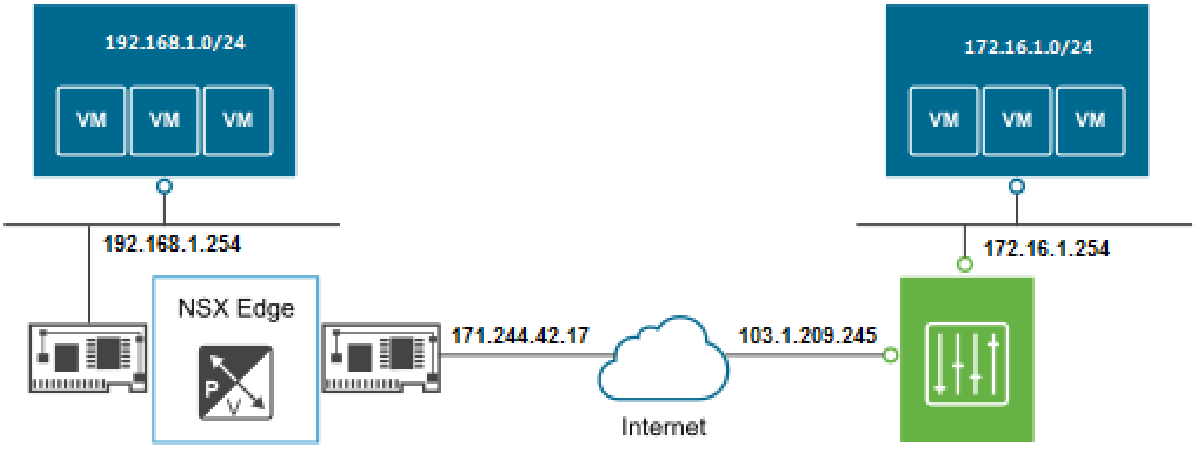
No IPsec VPN sites defined

Configure parameters as follow. Note that these parameters must match the configuration on the remote router / firewall.

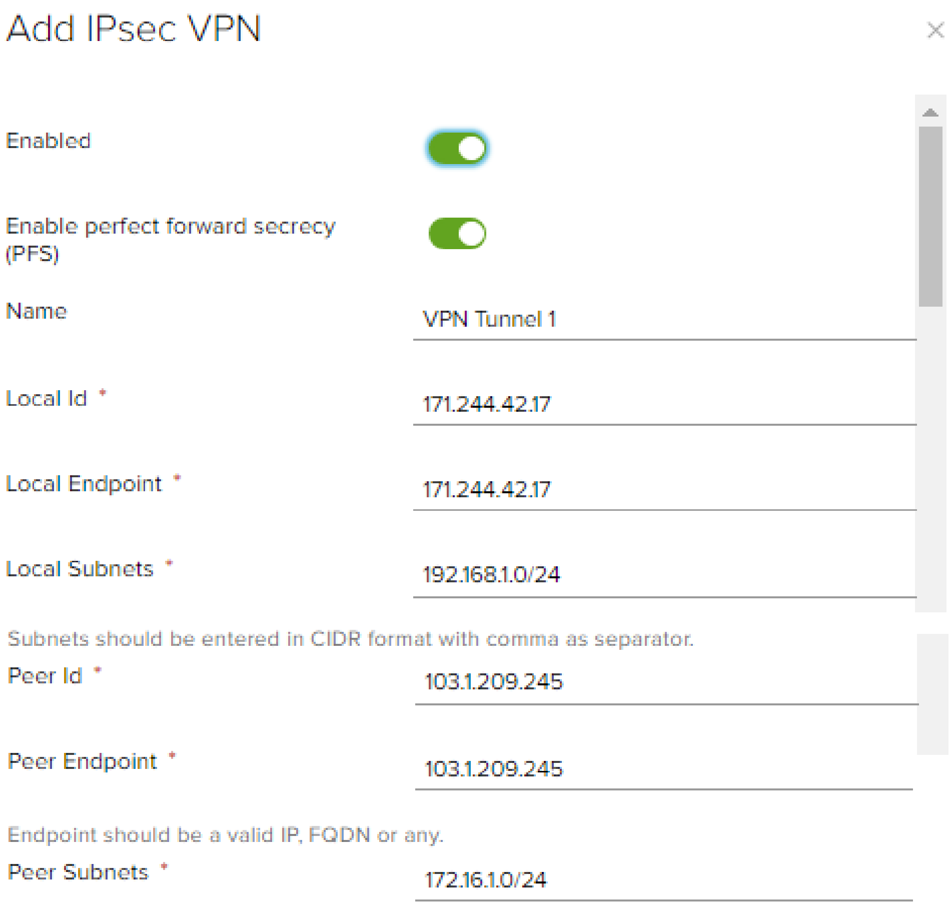
- **Enabled**: enable or disable VPN session.
  - **Enable perfect forward secrecy (PFS):** Allows running PFS mode for higher Connection security (recommended).
  - **Name:** name of the VPN connection
  - **Local Id and Local Endpoint:** enter the Public Master IP address of vFirewall in Section II.1. The case of the simulation is 171.244.42.17
  - **Local Subnets:** the private network range of the local, in this case 192.168.1.0/24
  - **Peer Id and Peer Endpoint:** Public IP of the remote router.
  - **Peer Subnets:** private network range of remote site.
- **Encryption Algorithm**: encryption algorithms, support algorithms: AES, AES256 and 3DES
  - **Authentication:** a form of authentication, usually using a preshare key (PSK)
  - **Pre-Shared Key:** enter preshare key
  - **Diffie-**Hellman **Group:** select key exchange method, support methods: DH2, DH5, DH14, DH15, DH16

Click **Keep** after completing the parameters then select **"Save Changes**" to apply the new changes.

🕮 Assume that we need to set up a VPN connection according to the following model:



Step 1: Configure USDC Technology Cloud side as follows:



Add IPsec VPN

Enabled

Enable perfect forward secrecy (PFS)

Name: VPN Tunnel 1

Local Id *: 171.244.42.17

Local Endpoint *: 171.244.42.17

Local Subnets *: 192.168.1.0/24

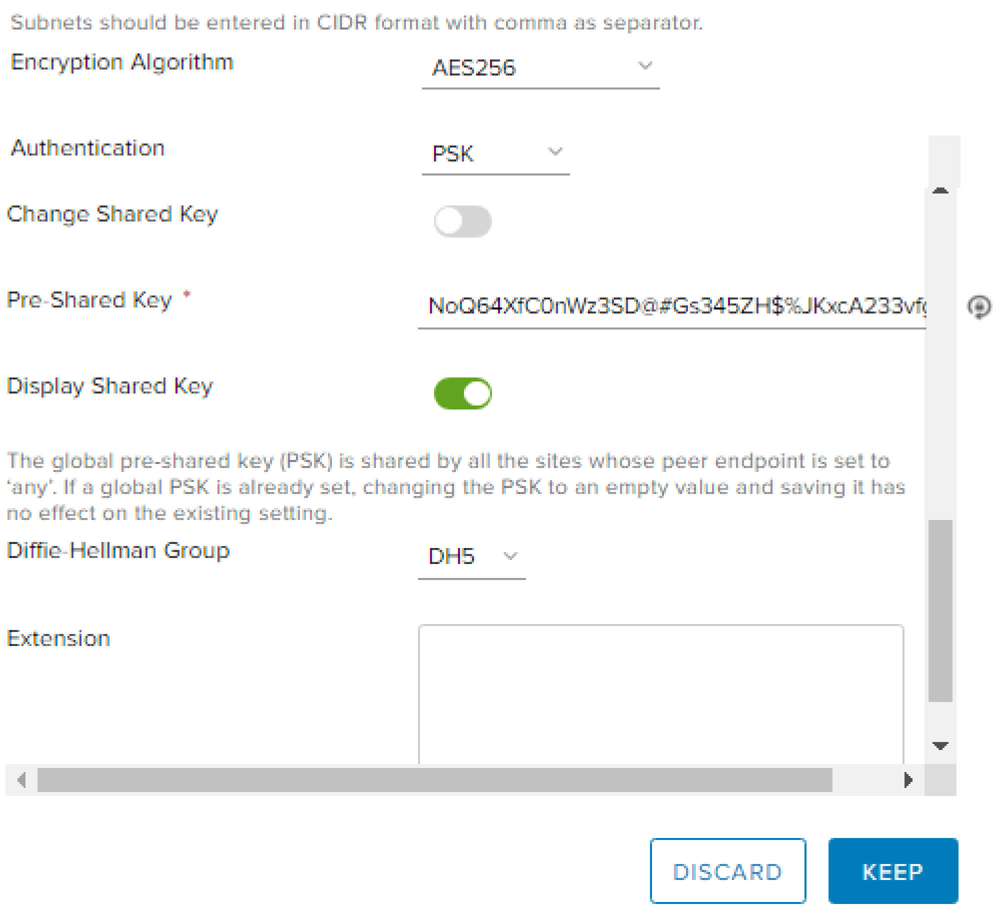
Subnets should be entered in CIDR format with comma as separator.

Peer Id *: 103.1.209.245

Peer Endpoint *: 103.1.209.245

Endpoint should be a valid IP, FQDN or any.

Peer Subnets *: 172.16.1.0/24



Subnets should be entered in CIDR format with comma as separator.

Encryption Algorithm: AES256

Authentication: PSK

Change Shared Key: ○

Pre-Shared Key *: NoQ64XfC0nWz3SD@#Gs345ZH$%JKxcA233vf

Display Shared Key: ●

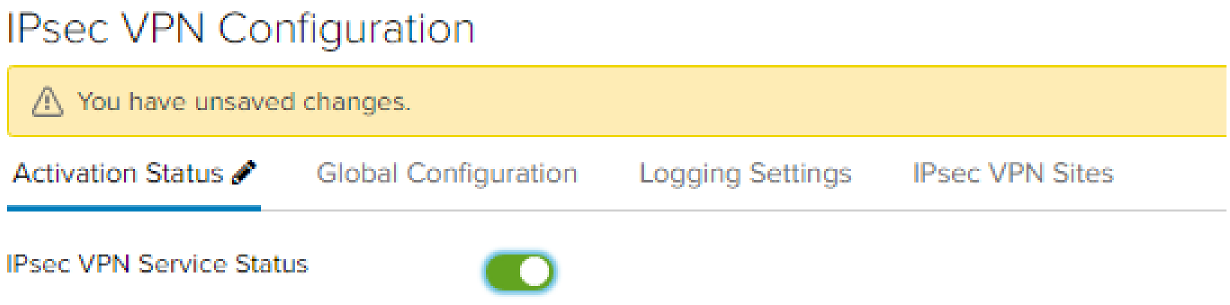
The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.

Diffie-Hellman Group: DH5

Extension:

Note: the parameters: encryption protocol, key exchange method and preshare key must be configure as same as on both sides that has been set up the VPN connection. With IKE use version 1 and SHA1 by default.

Step 2: Switch to the **Activation Status tab**, enable the "**IPsec VPN Service Status**" option and click "**Save Changes**":

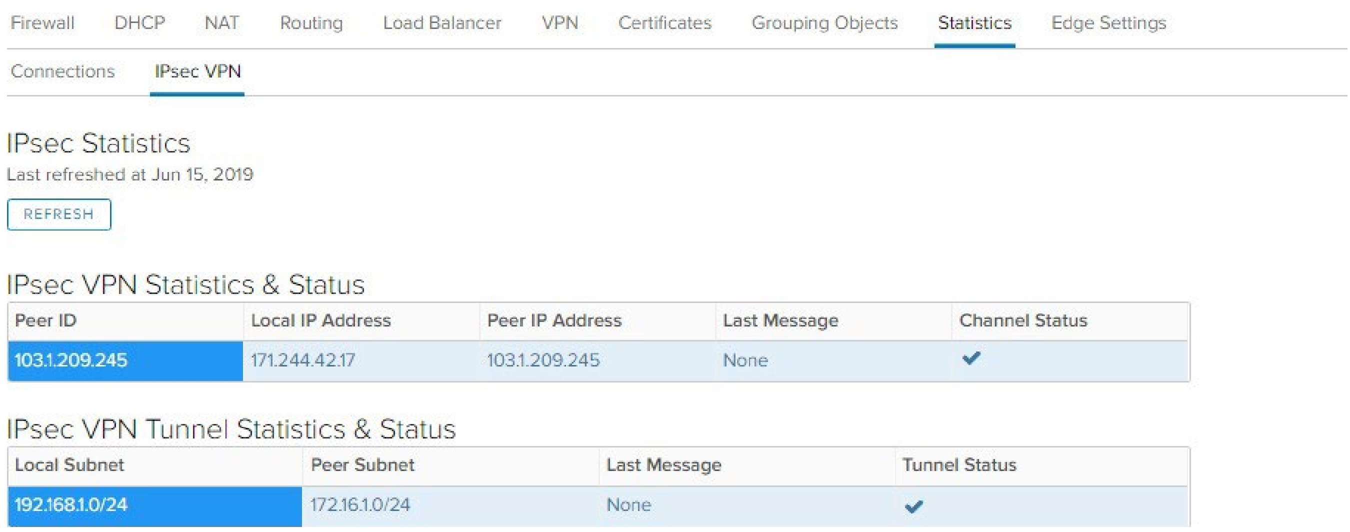


IPsec VPN Configuration

⚠ You have unsaved changes.

IPsec VPN Service Status: ●

✍ **Check the status of the VPN connection**: select the Statistics tab -> IPsec VPN:



IPsec Statistics

Last refreshed at Jun 15, 2019

IPsec VPN Statistics & Status

Peer ID	Local IP Address	Peer IP Address	Last Message	Channel Status
103.1.209.245	171.244.42.17	103.1.209.245	None	✓

IPsec VPN Tunnel Statistics & Status

Local Subnet	Peer Subnet	Last Message	Tunnel Status
192.168.1.0/24	172.16.1.0/24	None	✓

4. Configure SSL VPN Client to Site

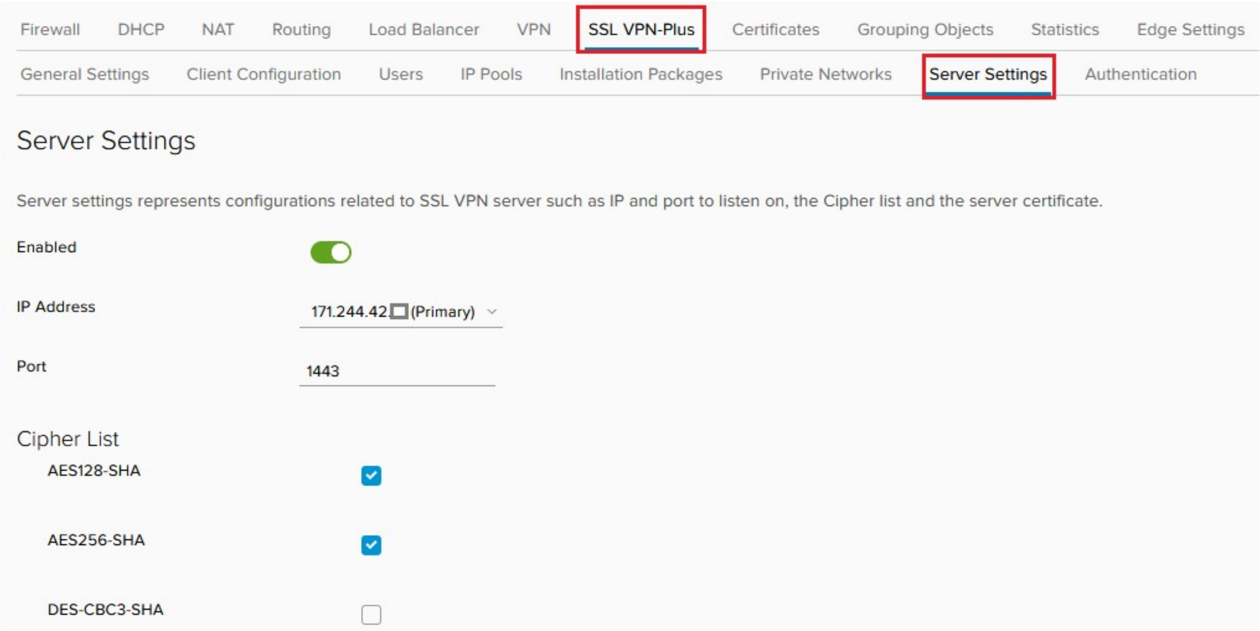
USDC Technology’s Virtual Private Cloud supports VPN Client to Site configuration on vFirewall

Step 1: From main dashboard, choose tab **SSL VPN-Plus -> Server Setting** and choose configuration:

- **Enable Server**
- **IP Address:** Choose IP Public VPN (usually Master IP)
- **Port**: port and access the portal download package installation page for the client.

Note: If you use the vLoad Balancer (vLB) service, you must specify a port other than the port used for vLB (usually ports http: tcp / 80, https: tcp / 443). In the illustration below, I use port 1443.

- **Cipher List:** Choose with minimal configuration of AES256-SHA
- Click **Save Changes**



Server Settings

Server settings represents configurations related to SSL VPN server such as IP and port to listen on, the Cipher list and the server certificate.

Enabled: on

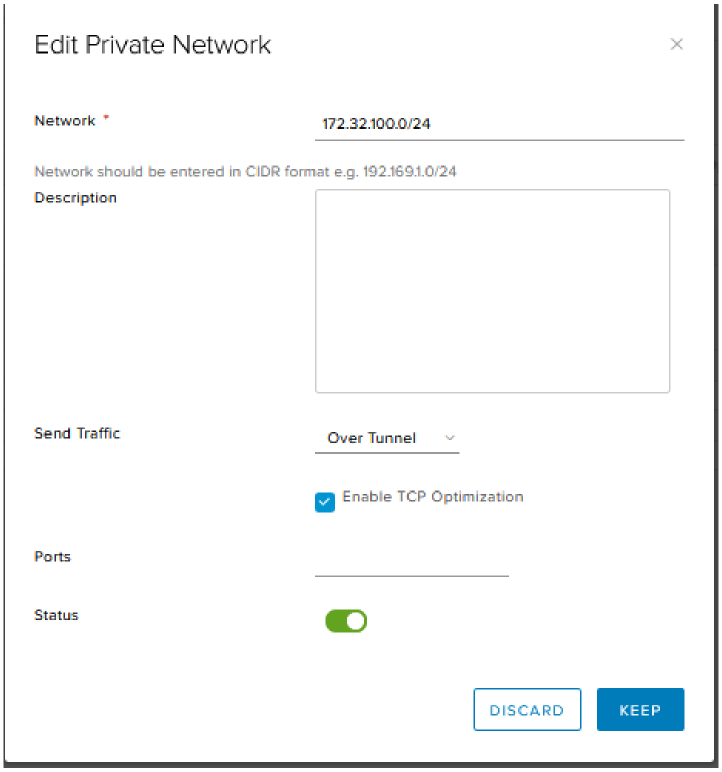
IP Address: 171.244.42□ (Primary)

Port: 1443

Cipher List

- AES128-SHA ☑
- AES256-SHA ☑
- DES-CBC3-SHA ☐

Step 2: In tab **Private Network.** Choose + to declare private network range on Cloud. This range should be declared similar to the private network ranges that the VM is using.


Edit Private Network

Network *: 172.32.100.0/24

Network should be entered in CIDR format e.g. 192.169.1.0/24

Description:

Send Traffic: Over Tunnel

☑ Enable TCP Optimization

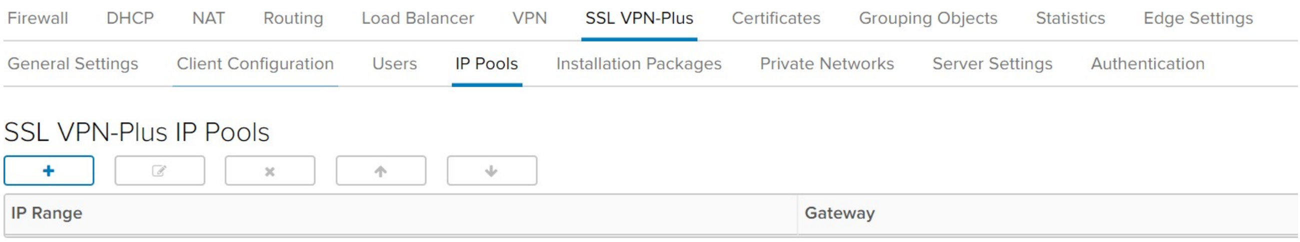
Ports:

Status: on

Choose **Keep** to save the changes.

Click **Save Changes**

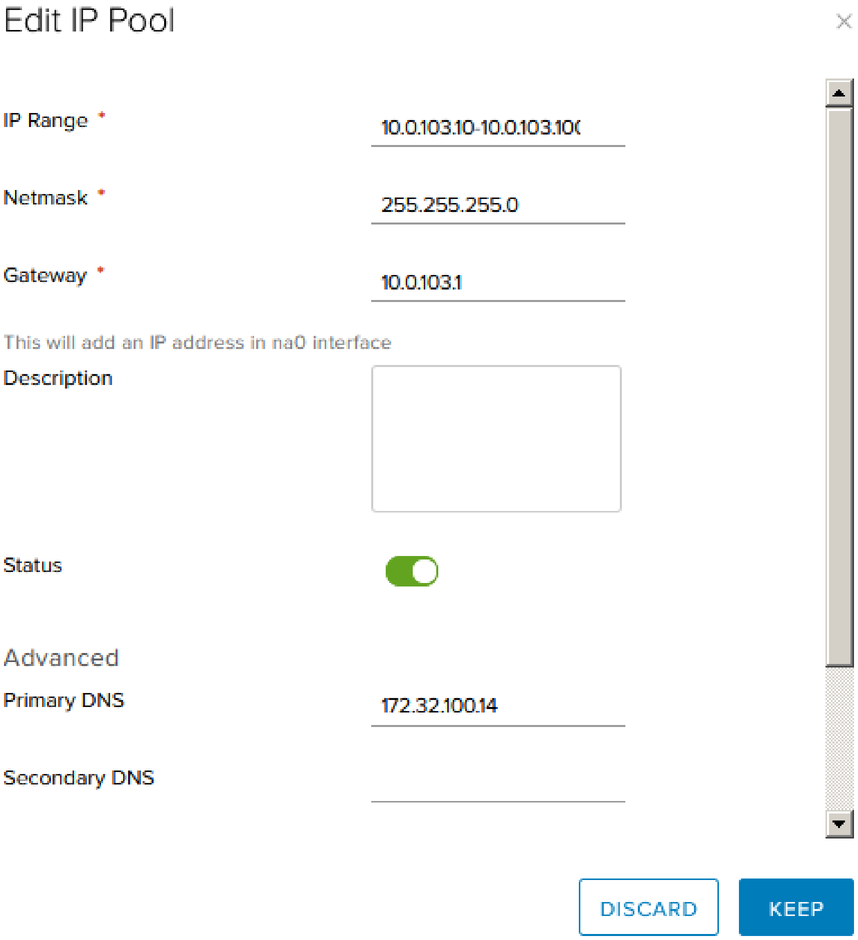
Step 3: Tab **IP Pool** is used to create network range used for users (clients) when connecting **SSL VPN.** Click + to create range.



SSL VPN-Plus IP Pools

IP Range	Gateway

Fill out the network range information as shown below. Any network range can be used but must not coincide with the internal network band used for VMs.



Edit IP Pool

IP Range * 10.0.103.10-10.0.103.10(

Netmask * 255.255.255.0

Gateway * 10.0.103.1

This will add an IP address in na0 interface

Description

Status

Advanced

Primary DNS 172.32.100.14

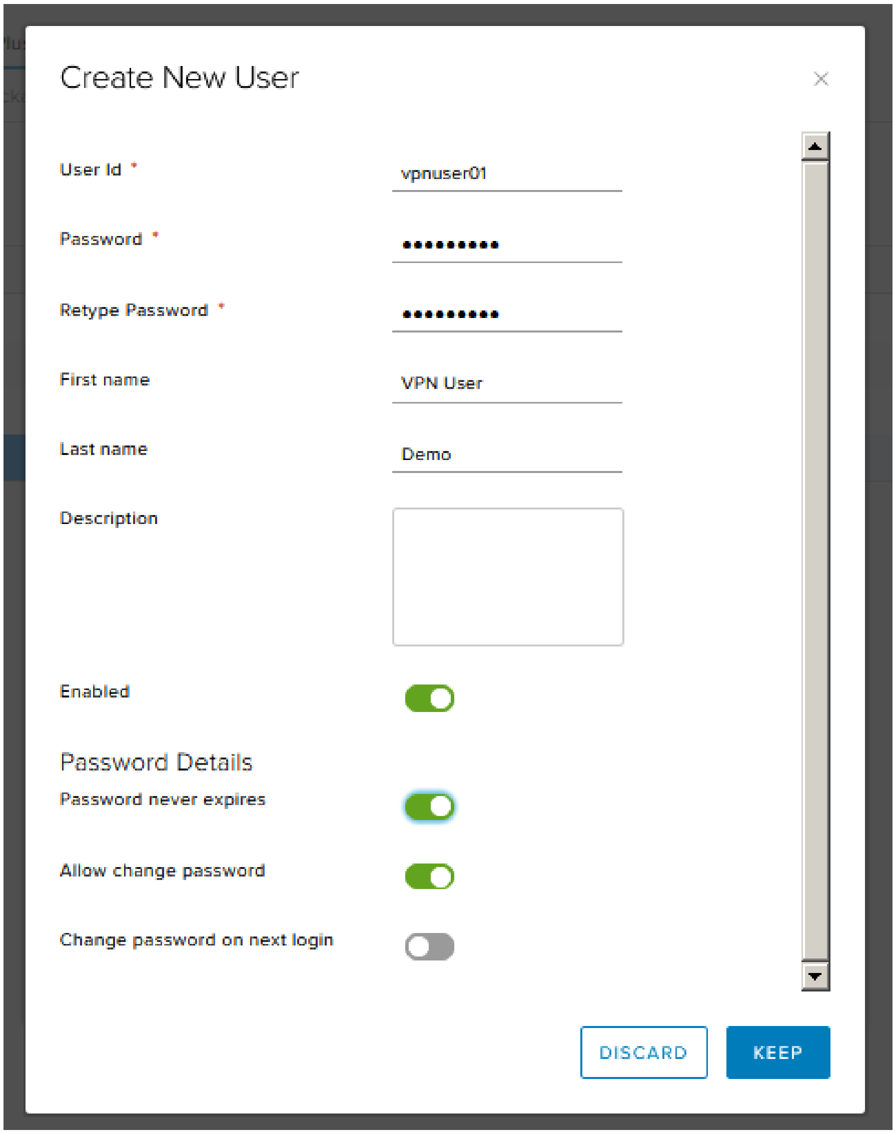
Secondary DNS

Choose **Keep** to save changes.

Click **Save Changes**

Step 4: Tab **User** is used to create accounts for users that allow to connect **SSL VPN.**

Click + to create accounts



Create New User

User Id *: vpnuser01

Password *: ••••••••••

Retype Password *: ••••••••••

First name: VPN User

Last name: Demo

Description:

Enabled: ●

Password Details

Password never expires: ●

Allow change password: ●

Change password on next login: ○

Then fill in and choose configuration below:

- **User ID**: Account name SSL VPN

- **Password**: Password SSL VPN

- **Retype Password**: Retype password

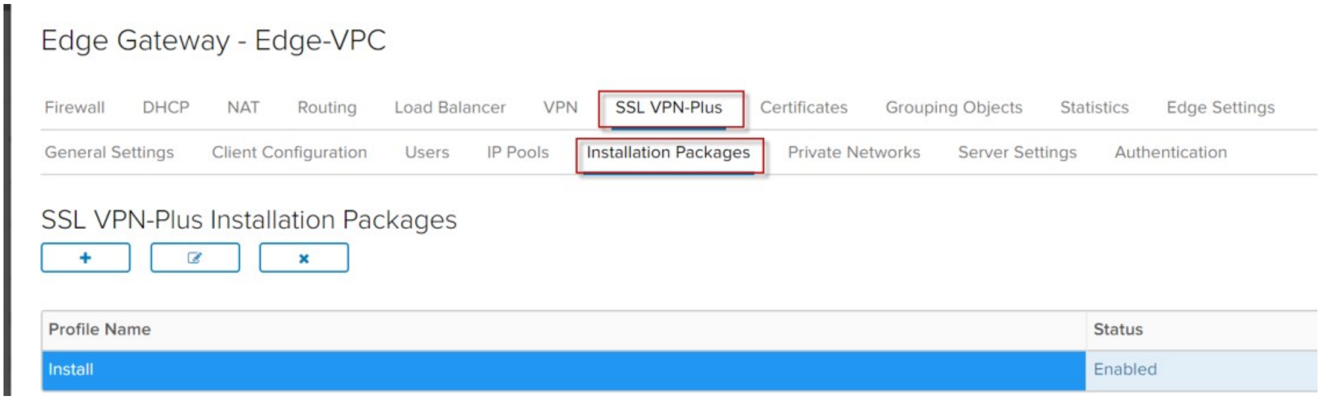
- **Password never expries** (optional): Unlimited exprired password

- **Allow change password** (optional): Allow users to change passwords (via SSL VPN portal page)

- **Change password on next login (optional)**: Force users to change the password on the first login.

Choose Keep to save changes

Step 5: In tab **Installation Packets.** Click + to create an installation package from the web interface for the client.



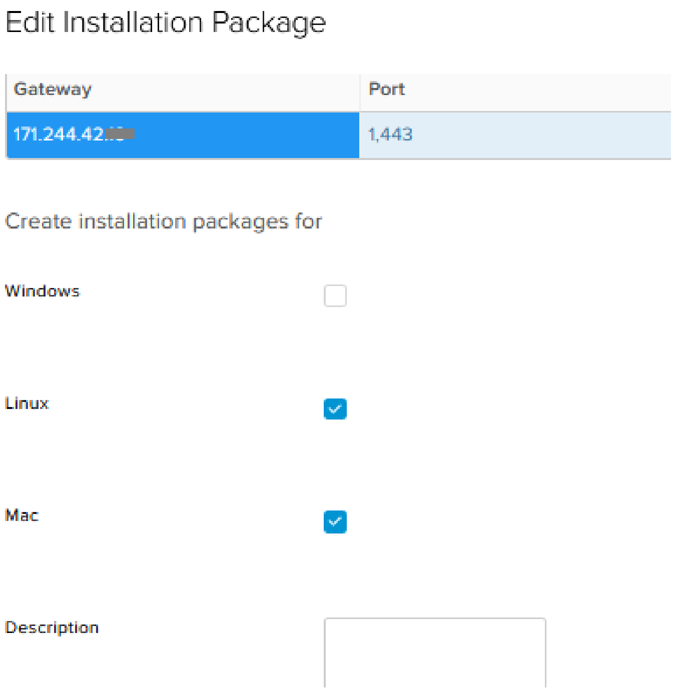
Edge Gateway - Edge-VPC

SSL VPN-Plus Installation Packages

Profile Name	Status
Install	Enabled

Then fill in configuration below:

- **Profile Name**: Package name
- Fill in **IP address and port** that configured in **Step 1**.
- Tick in OS that will create installation package for users.
- Check **Create destop icon**.
- **Don't Tick "Hide SSL client network adapter"** (if not, you will face with error "Driver installation failed for reason E000024B" on some clients).



Edit Installation Package

Gateway	Port
171.244.42.[redacted]	1,443

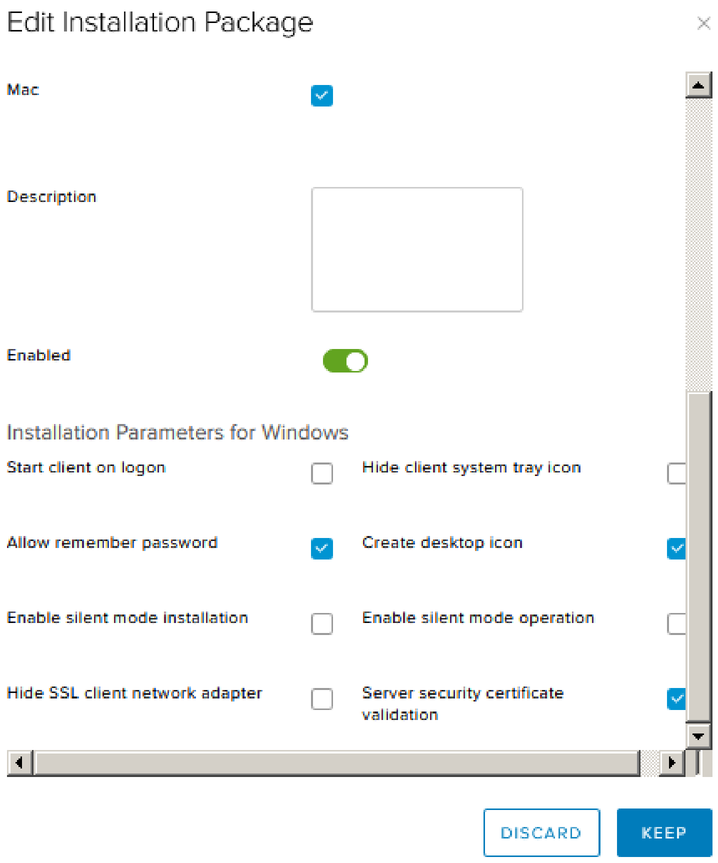
Create installation packages for

Windows ☐

Linux ☑

Mac ☑

Description



Edit Installation Package

Mac ☑

Description

Enabled

Installation Parameters for Windows

Start client on logon ☐ Hide client system tray icon ☐

Allow remember password ☑ Create desktop icon ☑

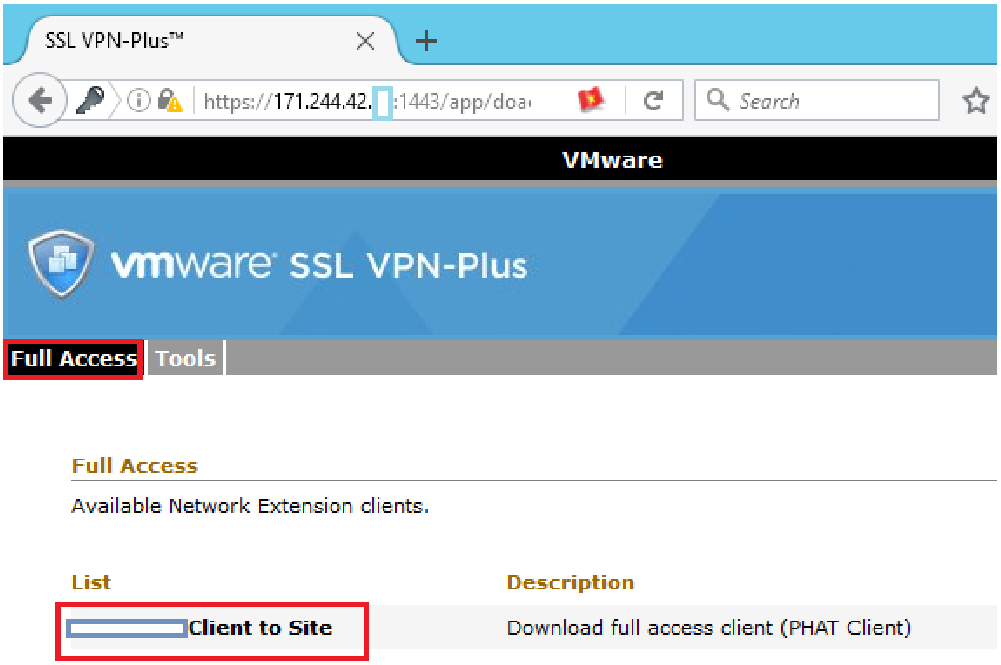
Enable silent mode installation ☐ Enable silent mode operation ☐

Hide SSL client network adapter ☐ Server security certificate validation ☑

At this point, the installation of the SSL VPN client to site SSL service has been completed. Users can use and connect VPN to virtual server cluster on Cloud as follows:

How to establish an SSL VPN Client to Site connection on the user's computer

Step 1: Access **https://IP-SSL_VPN_Server:Port** with the account created in the above steps. Click on the installation package name in the list and download the soft client:

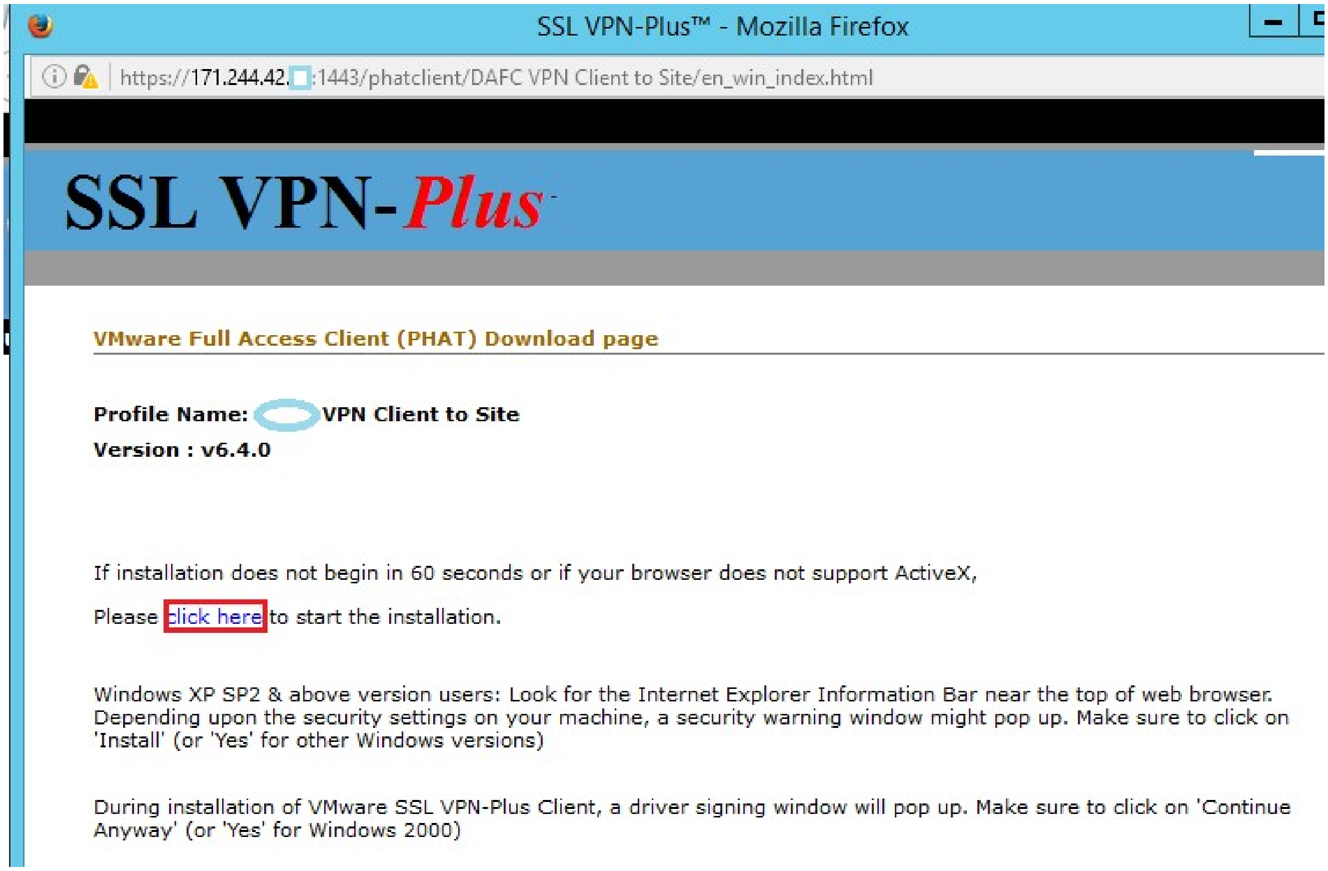


https://171.244.42.[redacted]:1443/app/doa

Full Access

Available Network Extension clients.

List	Description
[redacted]Client to Site	Download full access client (PHAT Client)



https://171.244.42.[redacted]:1443/phatclient/DAFC VPN Client to Site/en_win_index.html

VMware Full Access Client (PHAT) Download page

Profile Name: [redacted]VPN Client to Site

Version : v6.4.0

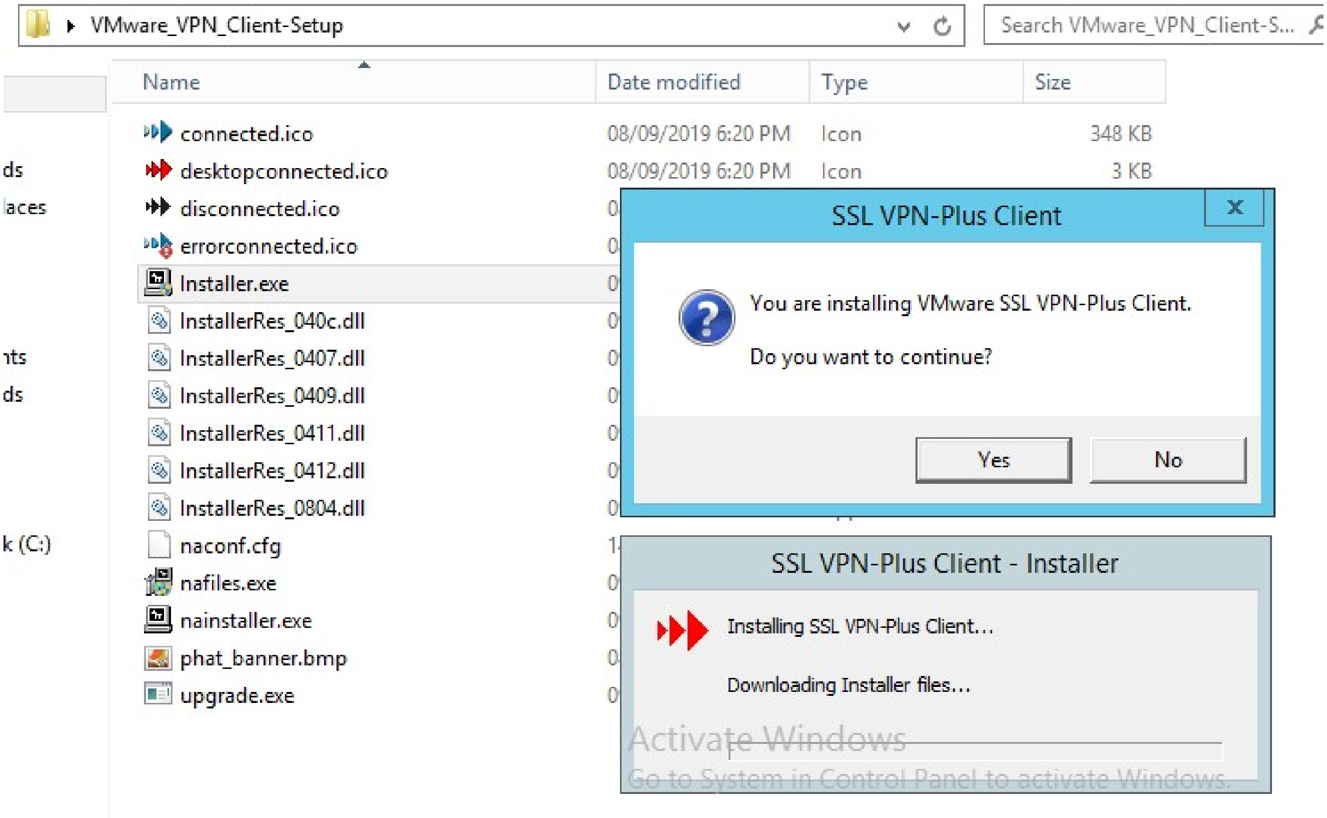
If installation does not begin in 60 seconds or if your browser does not support ActiveX,

Please click here to start the installation.

Windows XP SP2 & above version users: Look for the Internet Explorer Information Bar near the top of web browser. Depending upon the security settings on your machine, a security warning window might pop up. Make sure to click on 'Install' (or 'Yes' for other Windows versions)

During installation of VMware SSL VPN-Plus Client, a driver signing window will pop up. Make sure to click on 'Continue Anyway' (or 'Yes' for Windows 2000)

Step 2: Extract compressed file and Run installation with Installer.exe


VMware_VPN_Client-Setup
Search VMware_VPN_Client-S...
ds
laces
nts
ds
k (C:)
Yes
No
Activate Windows
Go to System in Control Panel to activate Windows.

Name	Date modified	Type	Size
connected.ico	08/09/2019 6:20 PM	Icon	348 KB
desktopconnected.ico	08/09/2019 6:20 PM	Icon	3 KB
disconnected.ico	0		
errorconnected.ico	0		
Installer.exe	0		
InstallerRes_040c.dll	0		
InstallerRes_0407.dll	0		
InstallerRes_0409.dll	0		
InstallerRes_0411.dll	0		
InstallerRes_0412.dll	0		
InstallerRes_0804.dll	0		
naconf.cfg	1		
nafiles.exe	0		
nainstaller.exe	0		
phat_banner.bmp	0		
upgrade.exe	0		

SSL VPN-Plus Client

You are installing VMware SSL VPN-Plus Client.

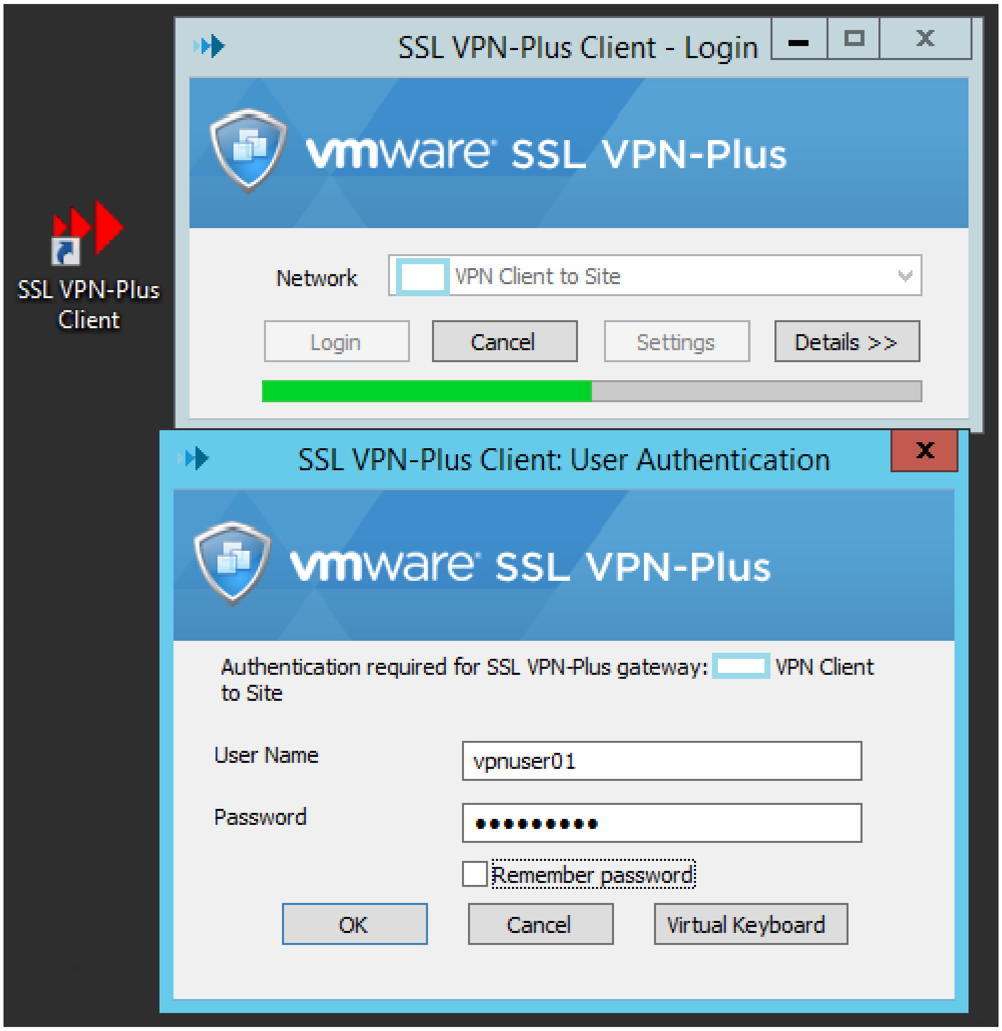
Do you want to continue?

SSL VPN-Plus Client - Installer

Installing SSL VPN-Plus Client...

Downloading Installer files...

Step 3: Implement the SSL VPN-Plus Client application on the Desktop. Click the login button on the interface and enter the VPN account created in the above steps.



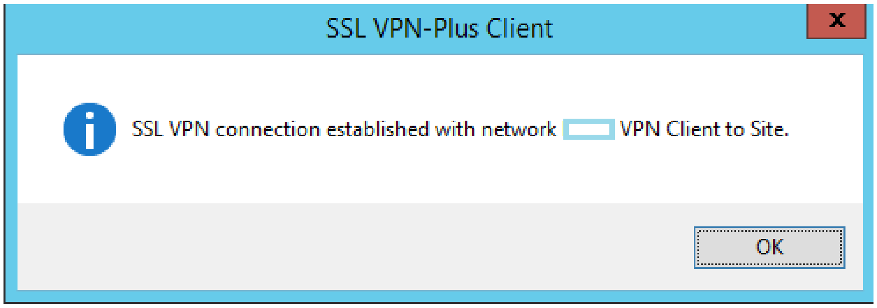
Network [redacted] VPN Client to Site

Authentication required for SSL VPN-Plus gateway: [redacted] VPN Client to Site

User Name vpnuser01

Password ●●●●●●●●●●

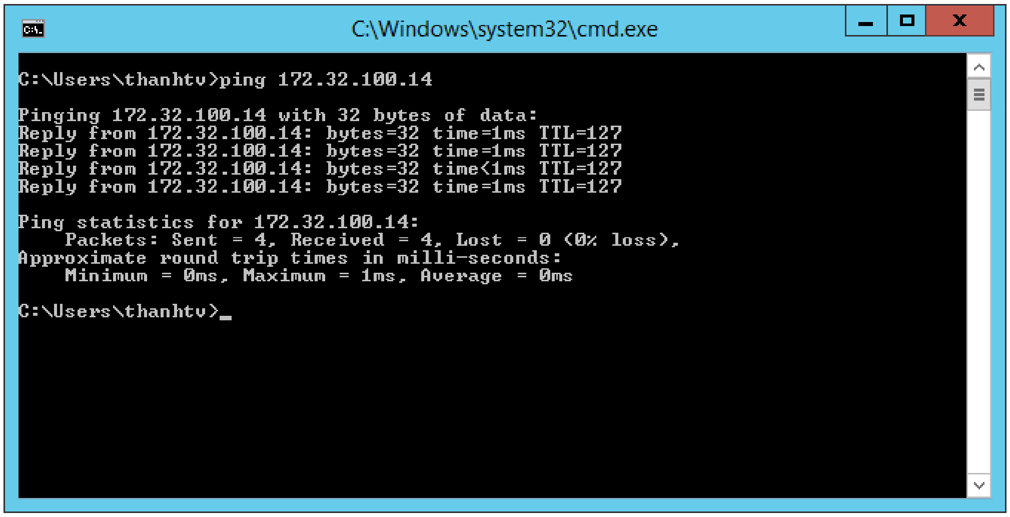
□ Remember password



SSL VPN connection established with network [redacted] VPN Client to Site.

Successful connection!

Tested by successfully pinging the server's local ip on the Virtual Private Cloud system of USDC Technology.



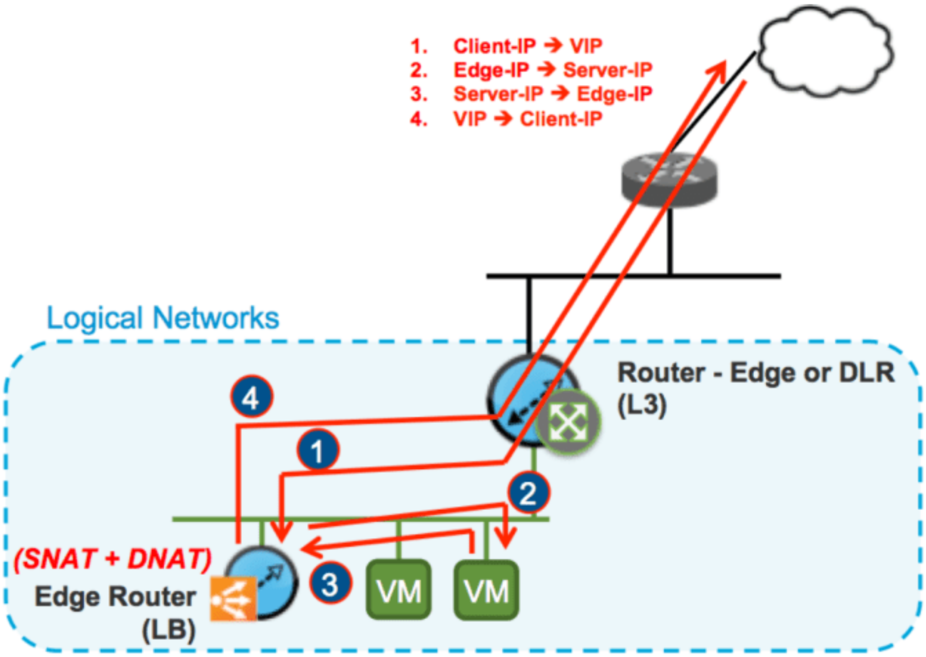
```
C:\Users\thanhtv>ping 172.32.100.14

Pinging 172.32.100.14 with 32 bytes of data:
Reply from 172.32.100.14: bytes=32 time=1ms TTL=127
Reply from 172.32.100.14: bytes=32 time=1ms TTL=127
Reply from 172.32.100.14: bytes=32 time<1ms TTL=127
Reply from 172.32.100.14: bytes=32 time=1ms TTL=127

Ping statistics for 172.32.100.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\thanhtv>_
```

Note: Each account can only be logged in and used on one device, to create accounts for users refer to the above installation steps.

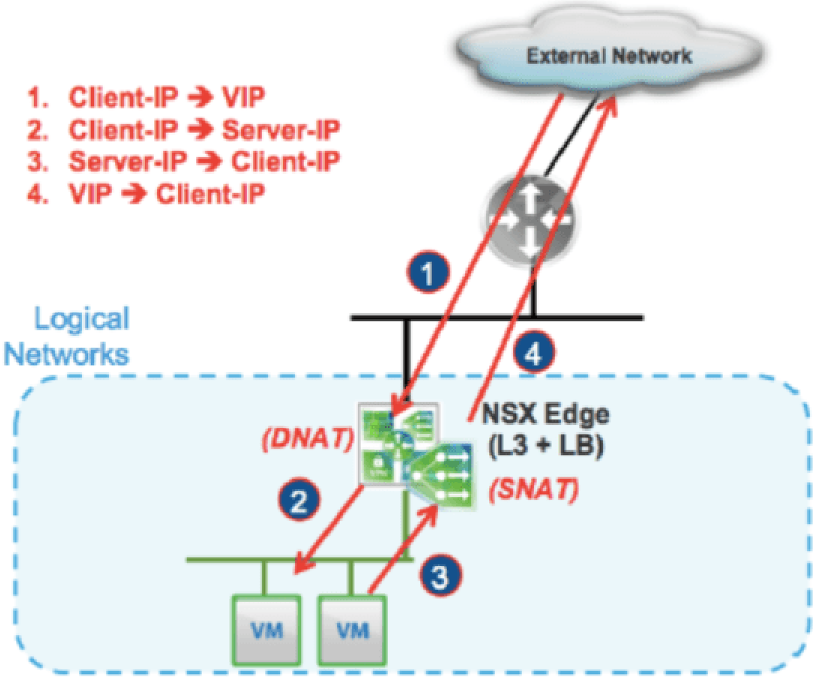
III. vLoad Balancer service

Customer can deploy in Two mode: *Proxy mode and transparent mode* in vLoadBalancer service.

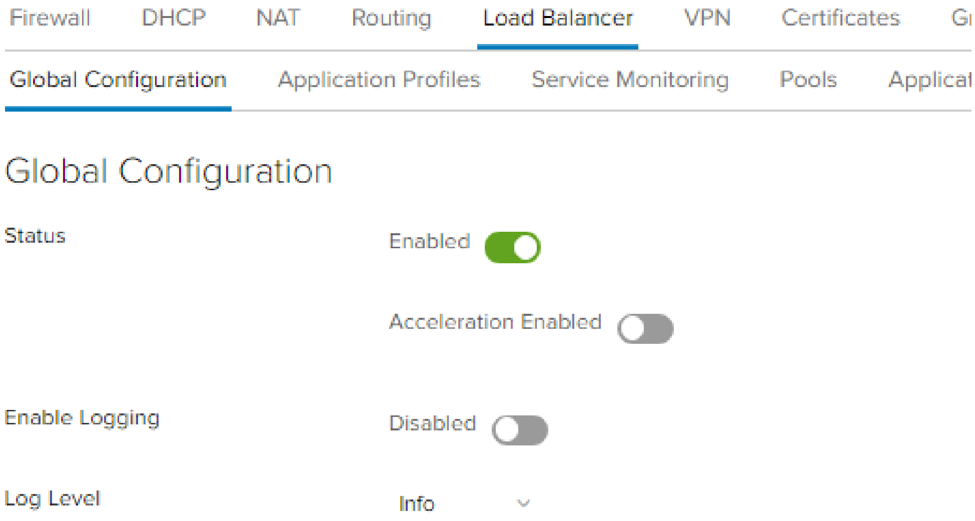
In Proxy mode, vLB acts as a reverse proxy like **nginx**.



As for the transparent mode, vLB plays a transparent role with user:



First, we need to enable vLB service by selecting the **Load Balancer** tab -> **Global Configuration** -> checking the **Enable Status** -> click "**Save Changes**"



Global Configuration

Status: Enabled

Acceleration Enabled

Enable Logging: Disabled

Log Level: Info

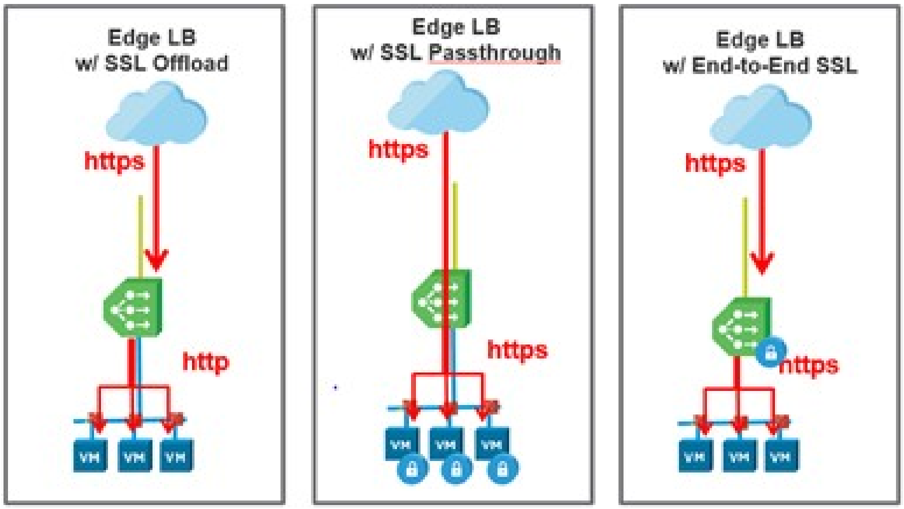
The process of initializing and configuring vLB through the following steps:

1. **Import certificate**

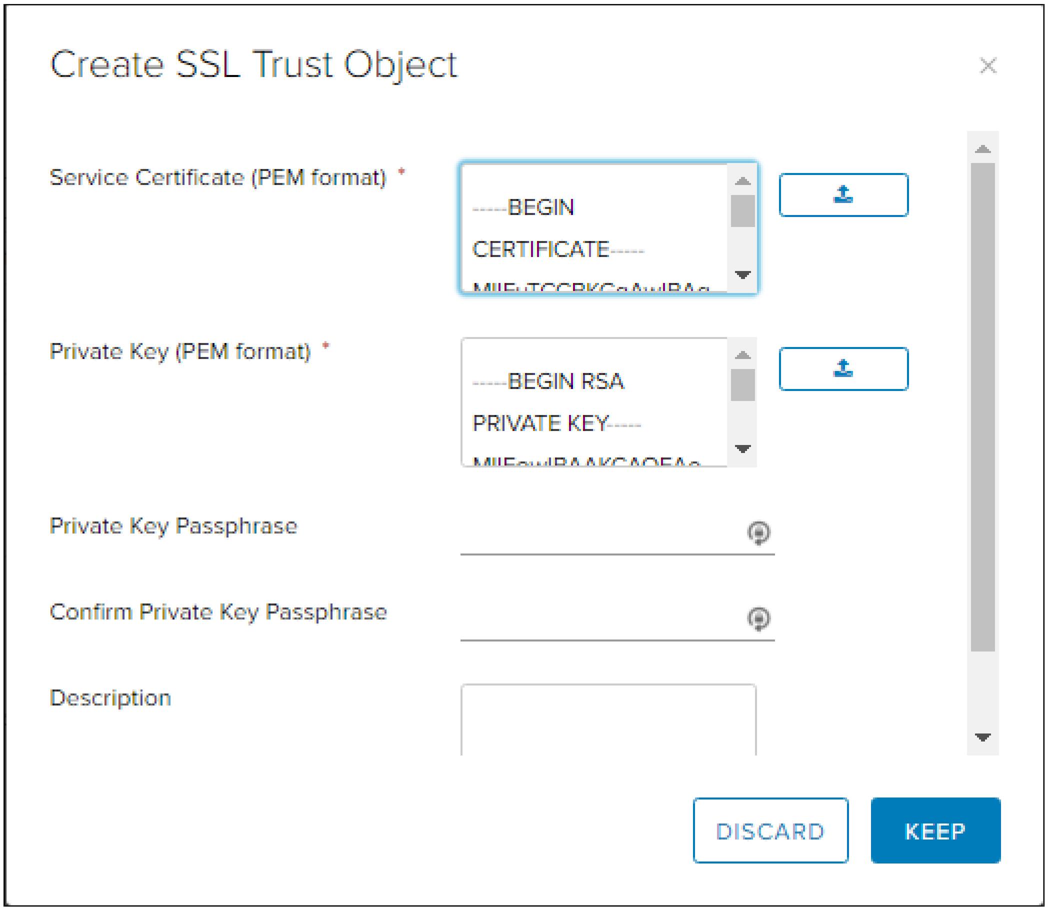
Note: *In the case you want to deploy the Website HTTPS, with a valid certification and run compatible with vLB, you need to perform this step. If not (running the regular HTTP protocol or the SSL Passthrough model), this step is not required.*

HTTPS running SSL, vLB is compatible with all three deployment models: SSL Offload, SSL

Passthrough and End-to-End SSL.



To import an existing certification, select the **Certificates tab** -> click **+ SERVICE CERTIFICATE** Select **"Create SSL Trust Object"** -> click the **upload** button, and choose the path to the **.crt** and **.pri** files corresponding to the **Service Certificate** and **Private Key**. Then press **Keep** saving the configuration.



Create SSL Trust Object

Service Certificate (PEM format) *: -----BEGIN CERTIFICATE-----

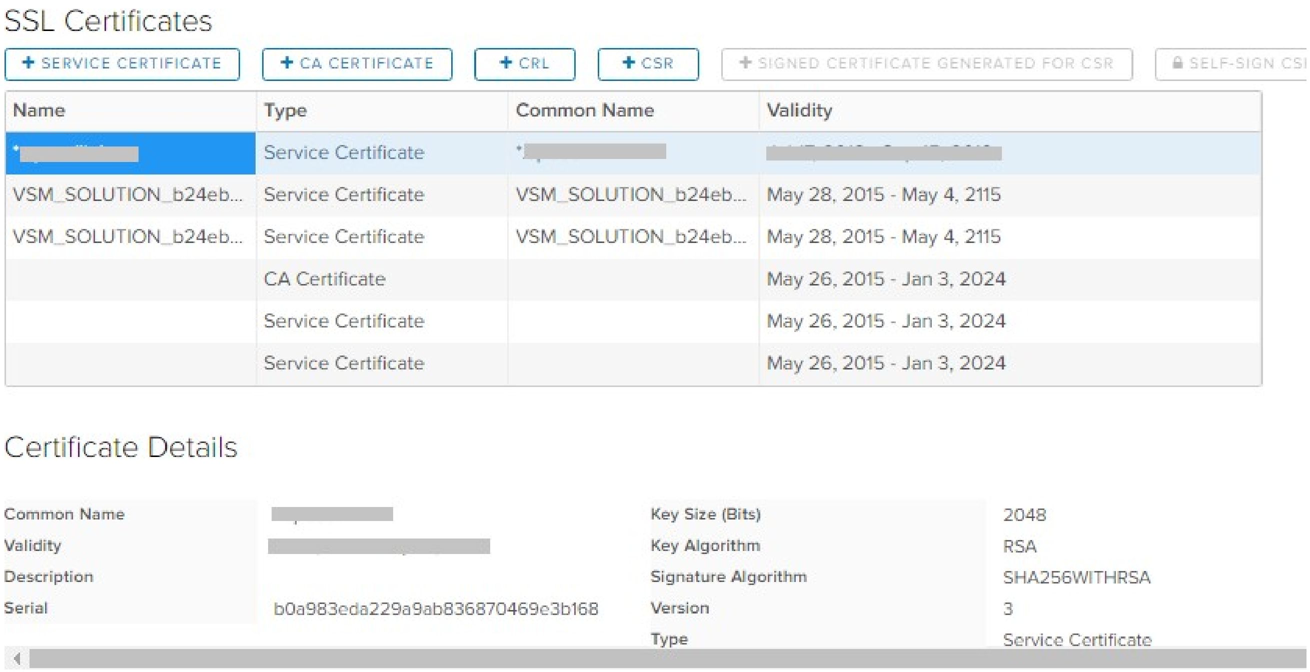
Private Key (PEM format) *: -----BEGIN RSA PRIVATE KEY-----

Private Key Passphrase

Confirm Private Key Passphrase

Description

The newly imported certificate will appear in the list:



SSL Certificates

Name	Type	Common Name	Validity
*[redacted]	Service Certificate	*[redacted]	[redacted]
VSM_SOLUTION_b24eb...	Service Certificate	VSM_SOLUTION_b24eb...	May 28, 2015 - May 4, 2115
VSM_SOLUTION_b24eb...	Service Certificate	VSM_SOLUTION_b24eb...	May 28, 2015 - May 4, 2115
	CA Certificate		May 26, 2015 - Jan 3, 2024
	Service Certificate		May 26, 2015 - Jan 3, 2024
	Service Certificate		May 26, 2015 - Jan 3, 2024

Certificate Details

Common Name	[redacted]	Key Size (Bits)	2048
Validity	[redacted]	Key Algorithm	RSA
Description		Signature Algorithm	SHA256WITHRSA
Serial	b0a983eda229a9ab836870469e3b168	Version	3
		Type	Service Certificate

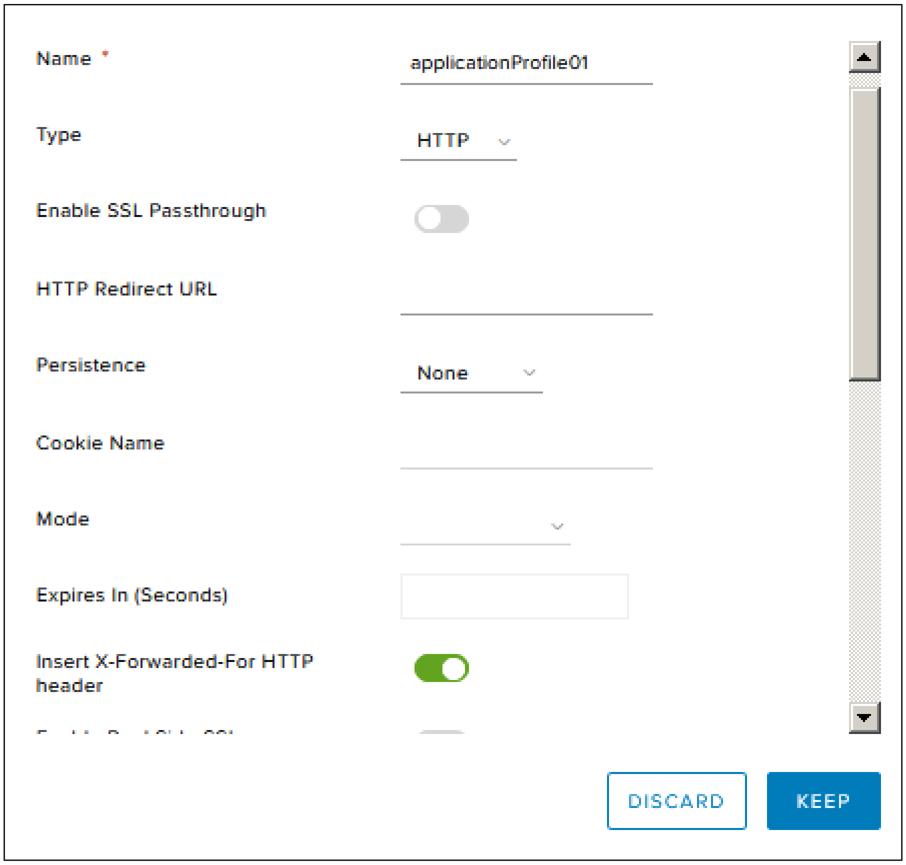
2. Application Profiles

To create an Application Profile, select the **Load Balancer** tab -> **Application Profiles**, click the button +

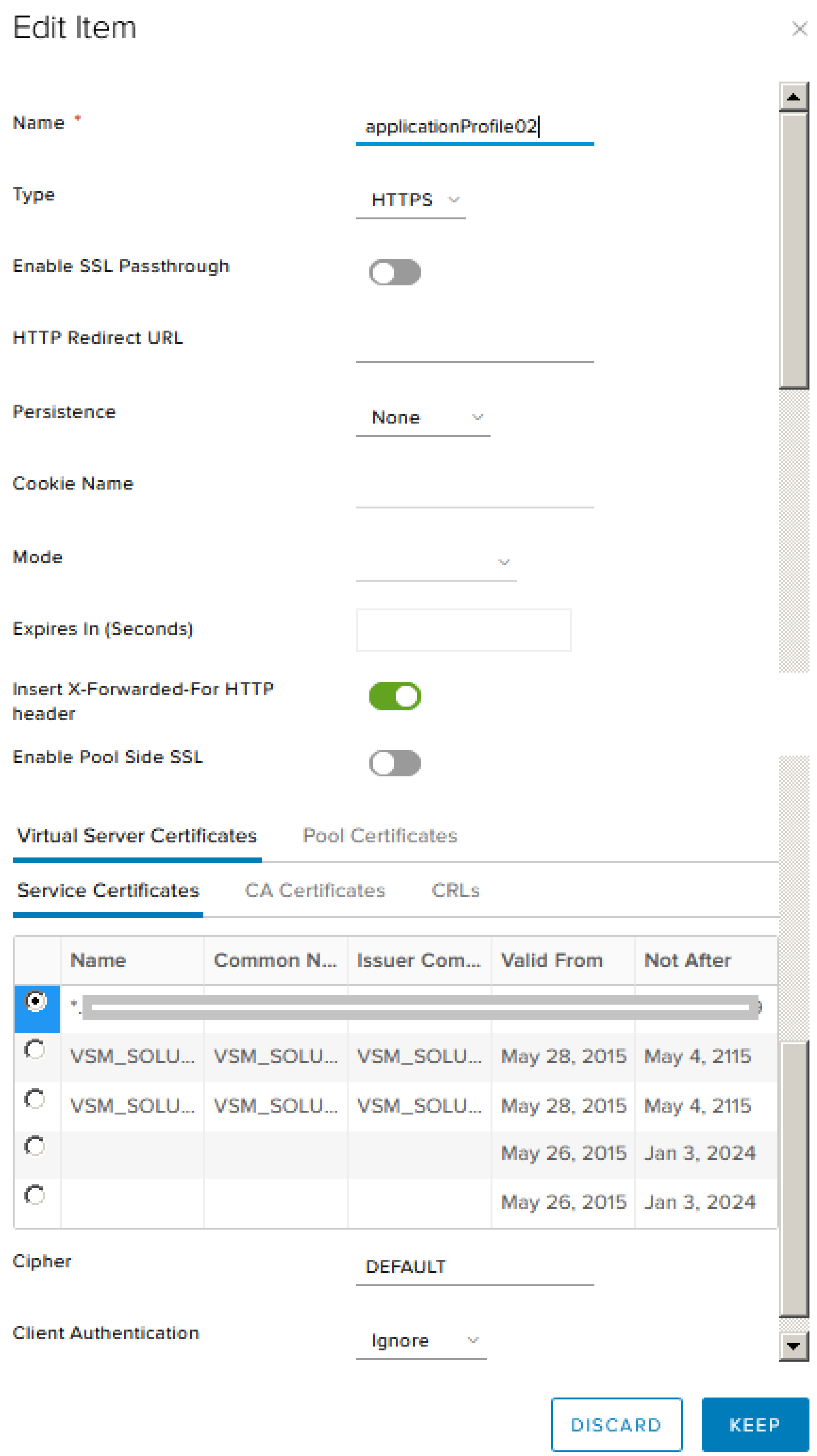
Parameters:

- **Name**: give name to Profile
- **Type**: protocol type, support HTTP, HTTPS, TCP, UDP
- **Enable SSL Passthrough**: run vLB in SSL Passthrough model
- **Persistence:** support 3 modes: source IP, cookie and none
- **Insert X-Forwarded-For HTTP header**: add X-Forward-For HTTP header (to use in some situations like identificate Client's IP).
- **Virtual Server Certificates**: select the certificate that was imported in step 1. This case can only be used if the **type** selects HTTPS.

The figure below illustrates creating Application Profile for 2 protocols HTTP and HTTPS:



Name *	applicationProfile01
Type	HTTP
Enable SSL Passthrough	○
HTTP Redirect URL	
Persistence	None
Cookie Name	
Mode	
Expires In (Seconds)	
Insert X-Forwarded-For HTTP header	●



Edit Item

Name * applicationProfile02

Type HTTPS

Enable SSL Passthrough

HTTP Redirect URL

Persistence None

Cookie Name

Mode

Expires In (Seconds)

Insert X-Forwarded-For HTTP header

Enable Pool Side SSL

	Name	Common N...	Issuer Com...	Valid From	Not After
●	*. [redacted]				
○	VSM_SOLU...	VSM_SOLU...	VSM_SOLU...	May 28, 2015	May 4, 2115
○	VSM_SOLU...	VSM_SOLU...	VSM_SOLU...	May 28, 2015	May 4, 2115
○				May 26, 2015	Jan 3, 2024
○				May 26, 2015	Jan 3, 2024

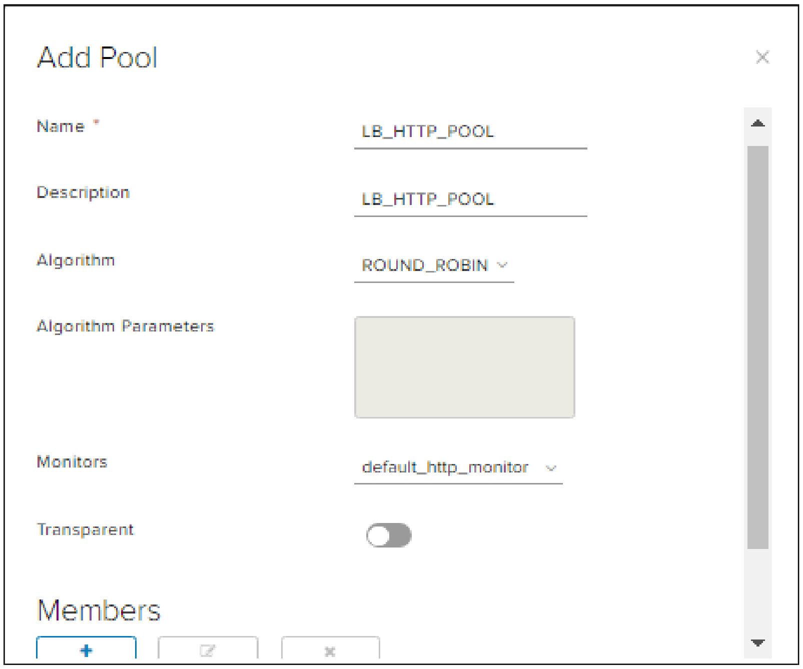
Cipher DEFAULT

Client Authentication Ignore

3. Server Pool

Select the **Load Balancer** tab -> **Pools**, click the **Add** icon, enter the following parameters:

- **Name and Description**: enter a name and description for the Pool
- **Algorithm:** use the following 2 algorithms to control traffic down to the underlying servers: *Round Robin* or *Least connected* (choose a server with less connections).
- **Monitors:** select **Service monitor**, the default system has default_http_monitor, default_https_monitor and default_tcp_monitor corresponding to 3 protocols HTTP, HTTPS and TCP. With HTTP and HTTPS protocols, this monitor uses the default method **GET** to the original URL ("/"). You can define these monitors at the **Service Monitor tab**.
- **Transparent:** enable this if you want to run *Transparent model*.



Add Pool

Name * LB_HTTP_POOL

Description LB_HTTP_POOL

Algorithm ROUND_ROBIN

Algorithm Parameters

Monitors default_http_monitor

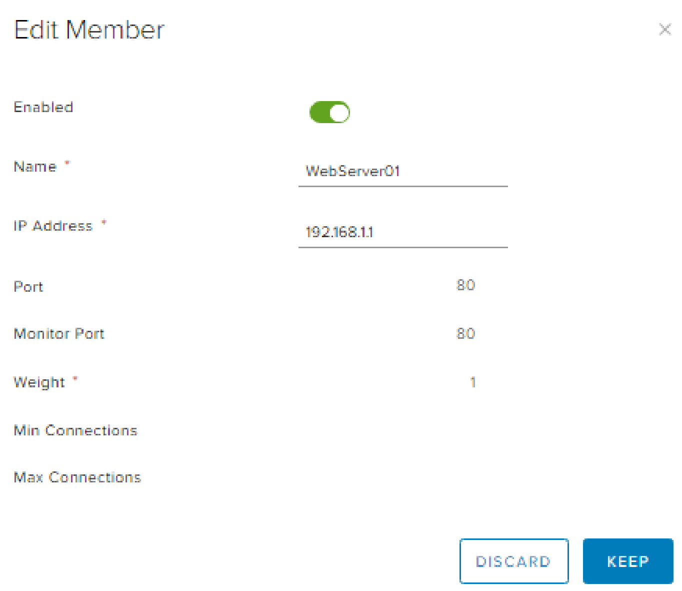
Transparent

Members

In the Member section, select **Add** and configure the underlying Web Servers in turn:

- **Name**: Example: WebServer01
- **IP Address**: the private IP address of the server
- **Port**: corresponding service port, eg: 80, 443
- **Monitor Port:** monitoring port (to detect the up / down status of server)
- **Weight**: priority weight.

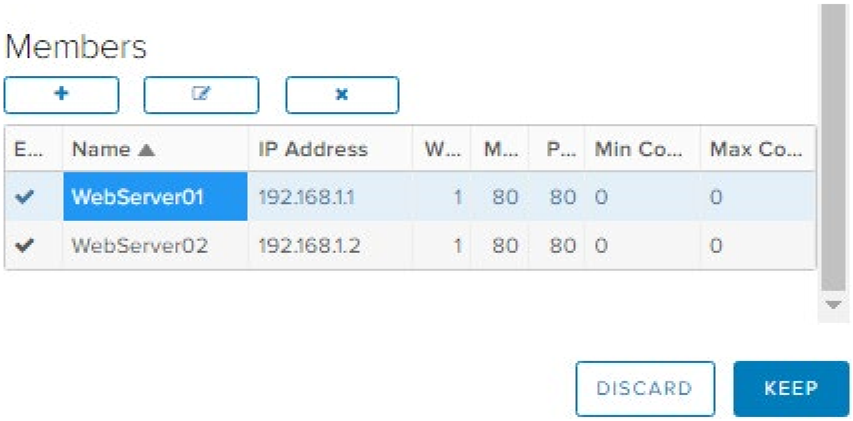
Click **Keep** after entering the parameters.



Edit Member

Enabled	●
Name *	WebServer01
IP Address *	192.168.1.1
Port	80
Monitor Port	80
Weight *	1
Min Connections	
Max Connections	

2 members have created into pool LB_HTTP_POOL:

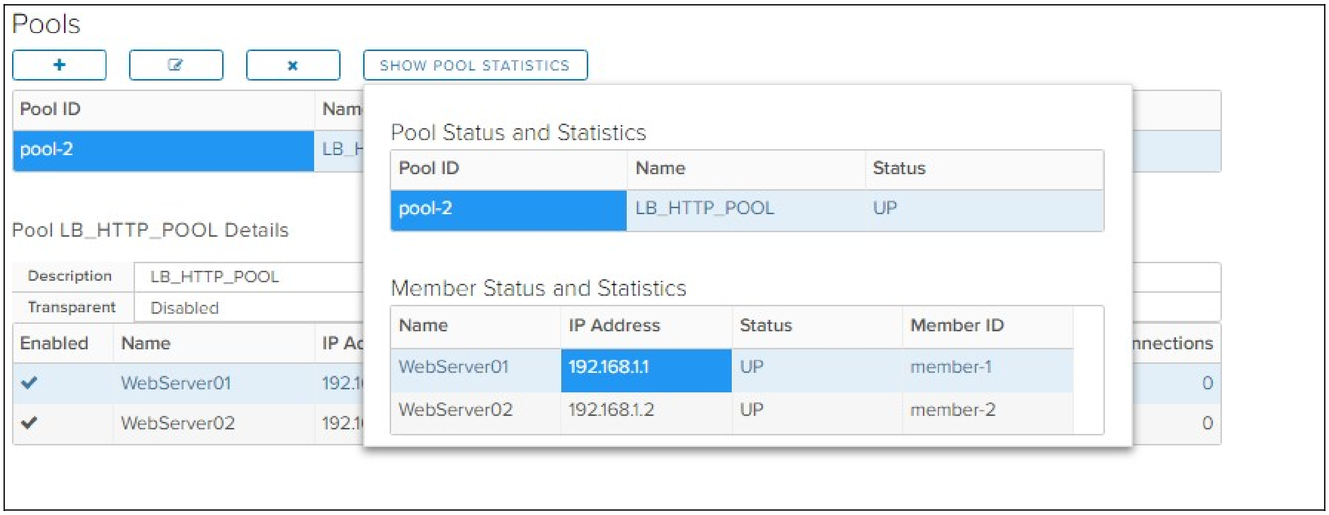


Members

E...	Name ▲	IP Address	W...	M...	P...	Min Co...	Max Co...
✓	WebServer01	192.168.1.1	1	80	80	0	0
✓	WebServer02	192.168.1.2	1	80	80	0	0

Click **Keep** to create server pool.

After the initialization completed, we can check the status of the Pool and the servers in the Pool by clicking **Show Pool Statistics**:



Pools

Pool ID	Nam
pool-2	LB_H

Pool LB_HTTP_POOL Details

Description	LB_HTTP_POOL
Transparent	Disabled

Enabled	Name	IP Ac	nnections
✓	WebServer01	192.1	0
✓	WebServer02	192.1	0

Pool Status and Statistics

Pool ID	Name	Status
pool-2	LB_HTTP_POOL	UP

Member Status and Statistics

Name	IP Address	Status	Member ID
WebServer01	192.168.1.1	UP	member-1
WebServer02	192.168.1.2	UP	member-2

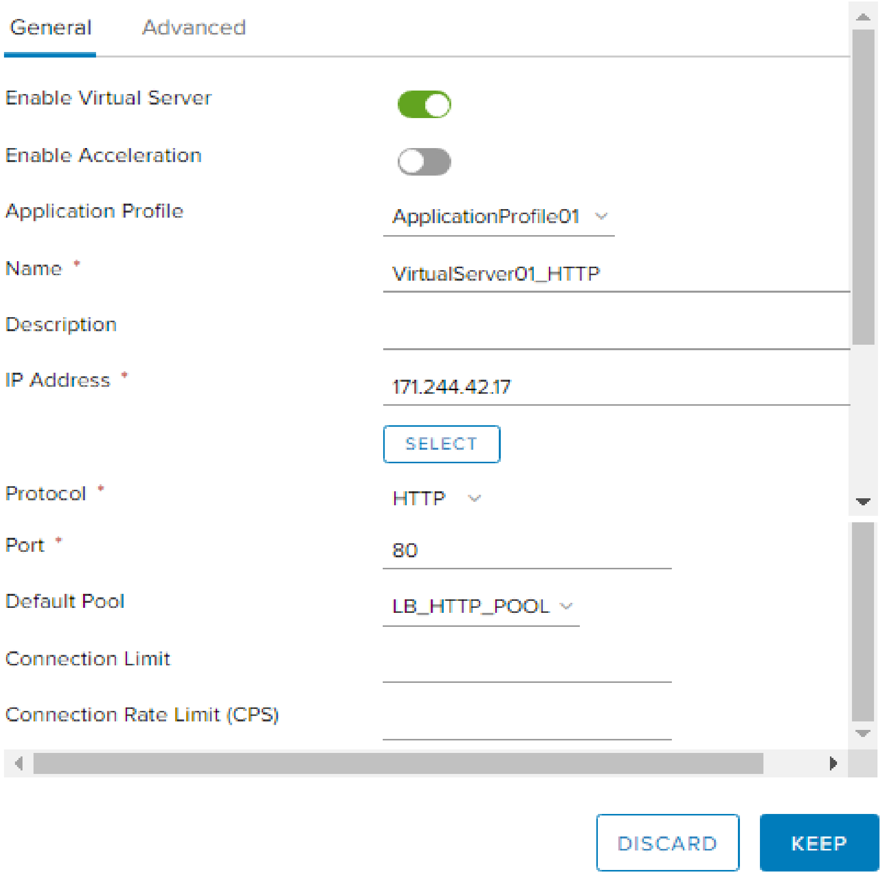
4. Virtual Server

This is the final step to set up vLoad Balancer. Select the **Virtual Servers** tab then click **ADD** icon + .

The parameters need to be set:

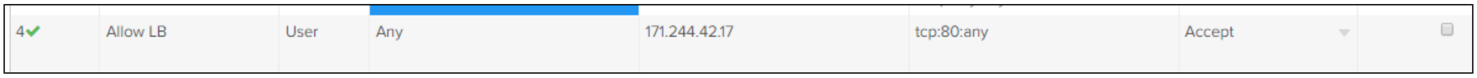
- **Enable Virtual Server:** Enables to execute Virtual Server
- **Application Profile**: select the corresponding Application Profile created in Step 2. Notice that choosing protocol (HTTP, HTTPS) correctly.
- **Name**: give a name
- **IP Address**: click Select and select Public Master IP obtained in Section II of this document.
- **Protocol and Port**: select the protocol and port for the client connection
- **Default Pool**: select the Pool created in Step 3.

Click **Keep** to save and apply new configuration.



Enable Virtual Server	● (on)
Enable Acceleration	○ (off)
Application Profile	ApplicationProfile01
Name *	VirtualServer01_HTTP
Description	
IP Address *	171.244.42.17
Protocol *	HTTP
Port *	80
Default Pool	LB_HTTP_POOL
Connection Limit	
Connection Rate Limit (CPS)	

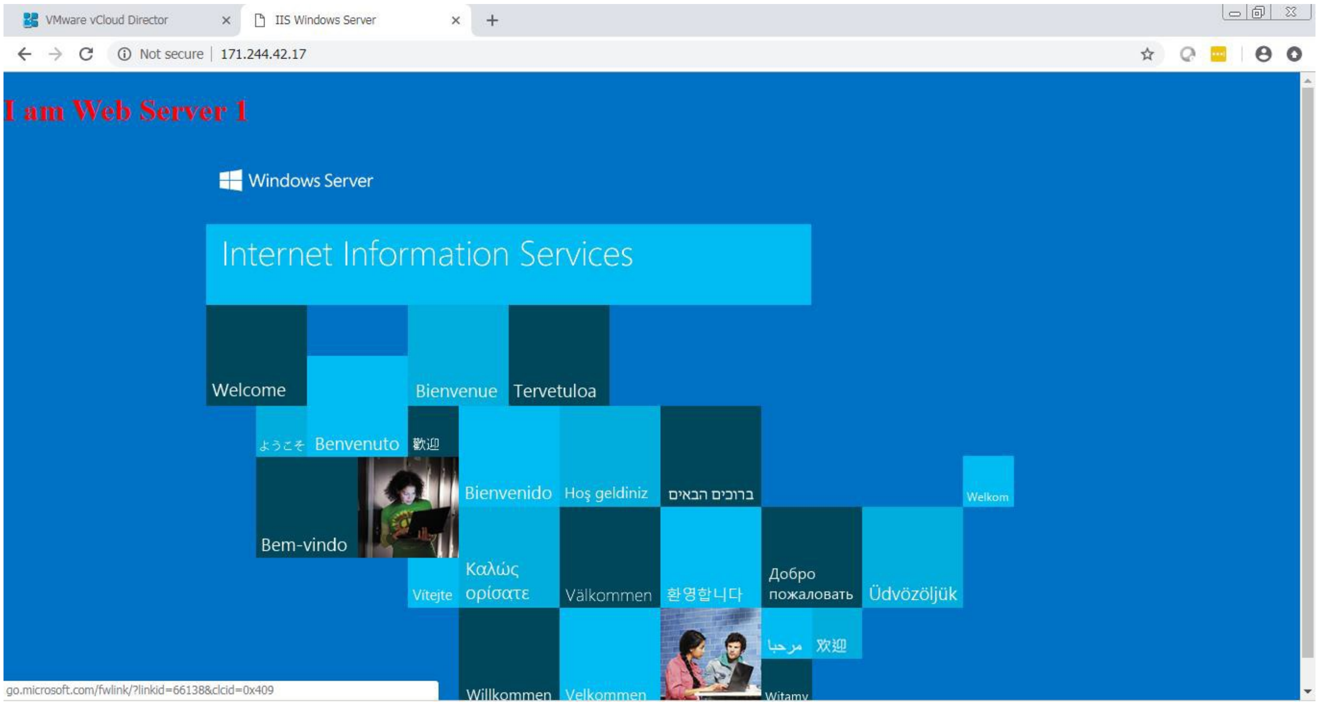
Note: vLB configuration process is completed, you might need to create a Firewall Rule to allow users to access the Virtual Server Public IP created above:



4✓	Allow LB	User	Any	171.244.42.17	tcp:80:any	Accept	□

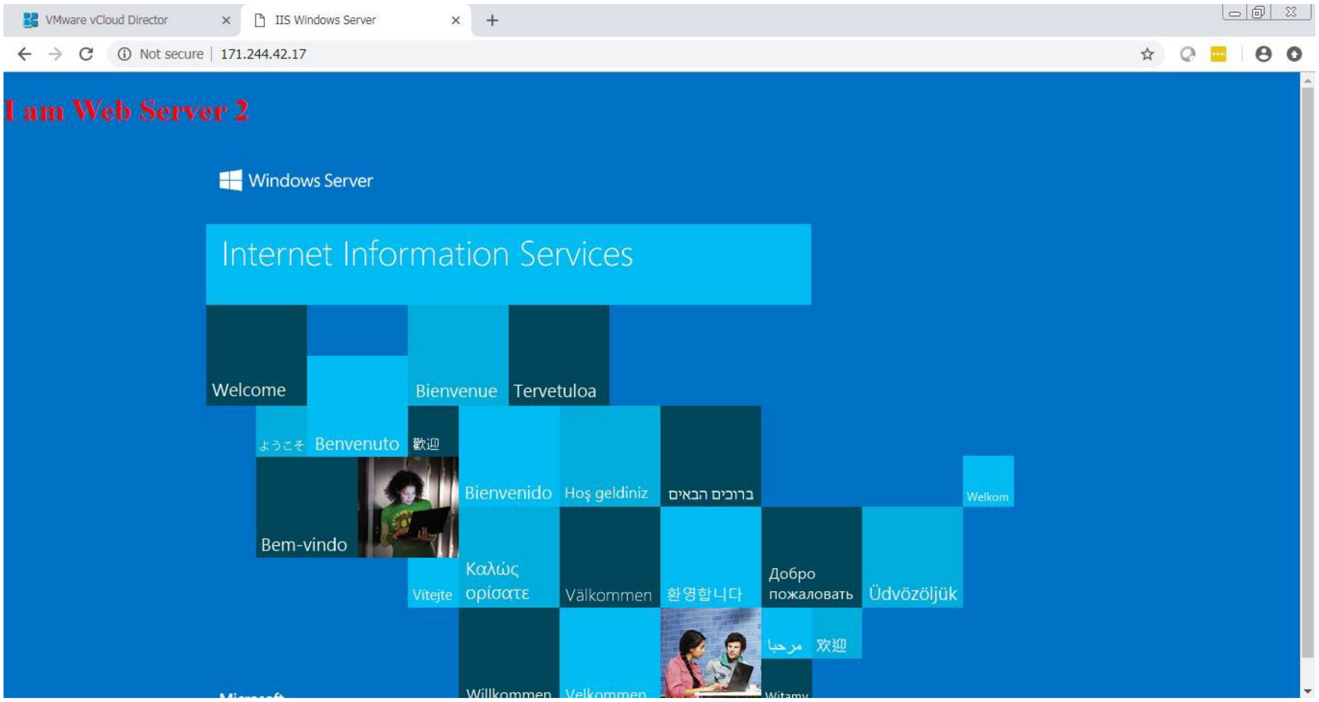
5. Test the service

Access to vLB's VIP above with mode Round Robin: First time access:



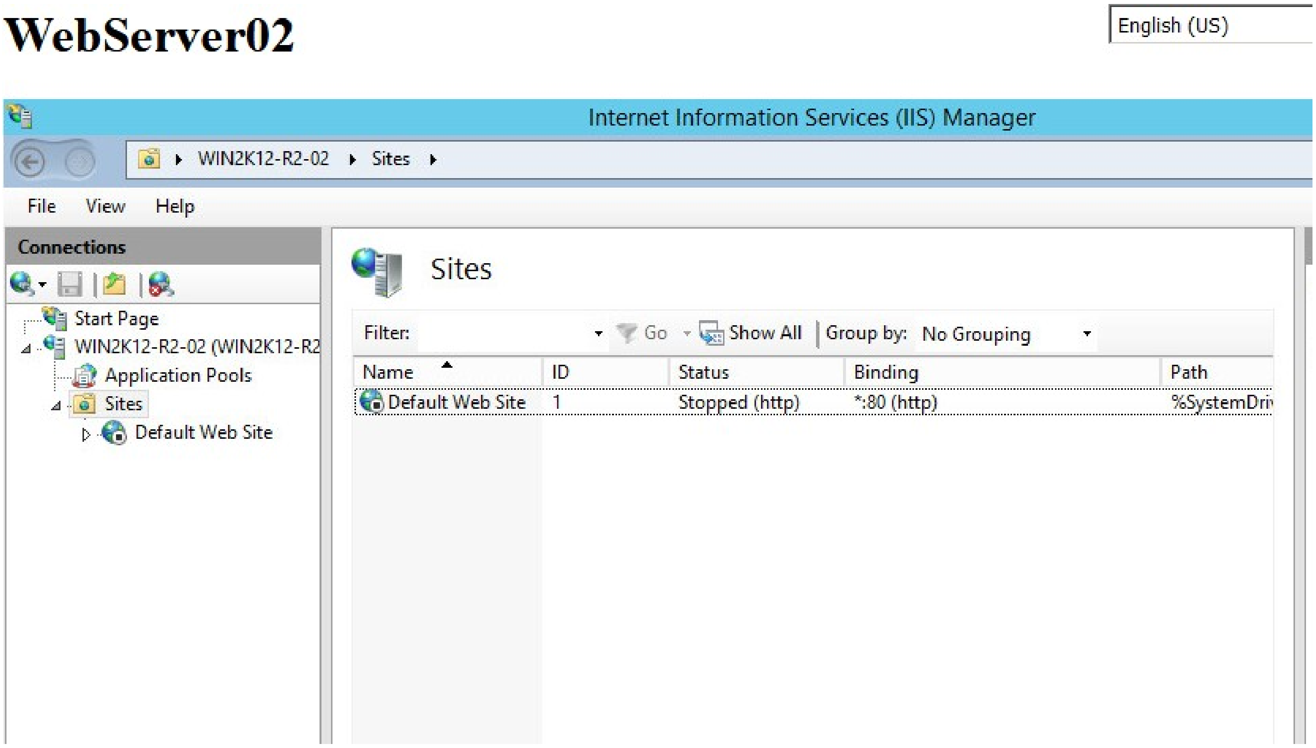
I am Web Server 1

Second time: The Web Server 2 will serve traffic:



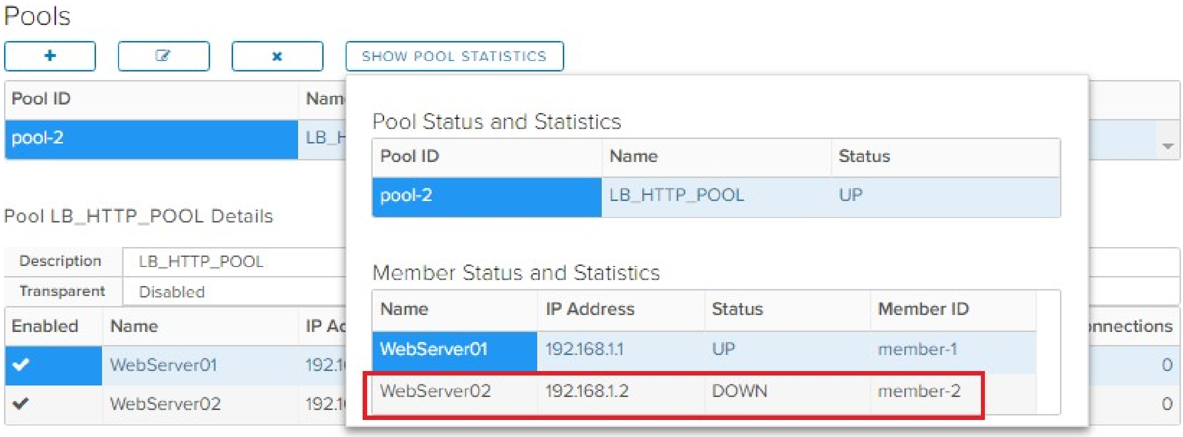
I am Web Server 2

Turn off service IIS on Web Server 02:



Name	ID	Status	Binding	Path
Default Web Site	1	Stopped (http)	*:80 (http)	%SystemDri

vLB recognizes immediately and changes the status of WebServer 02 in the pool to down:



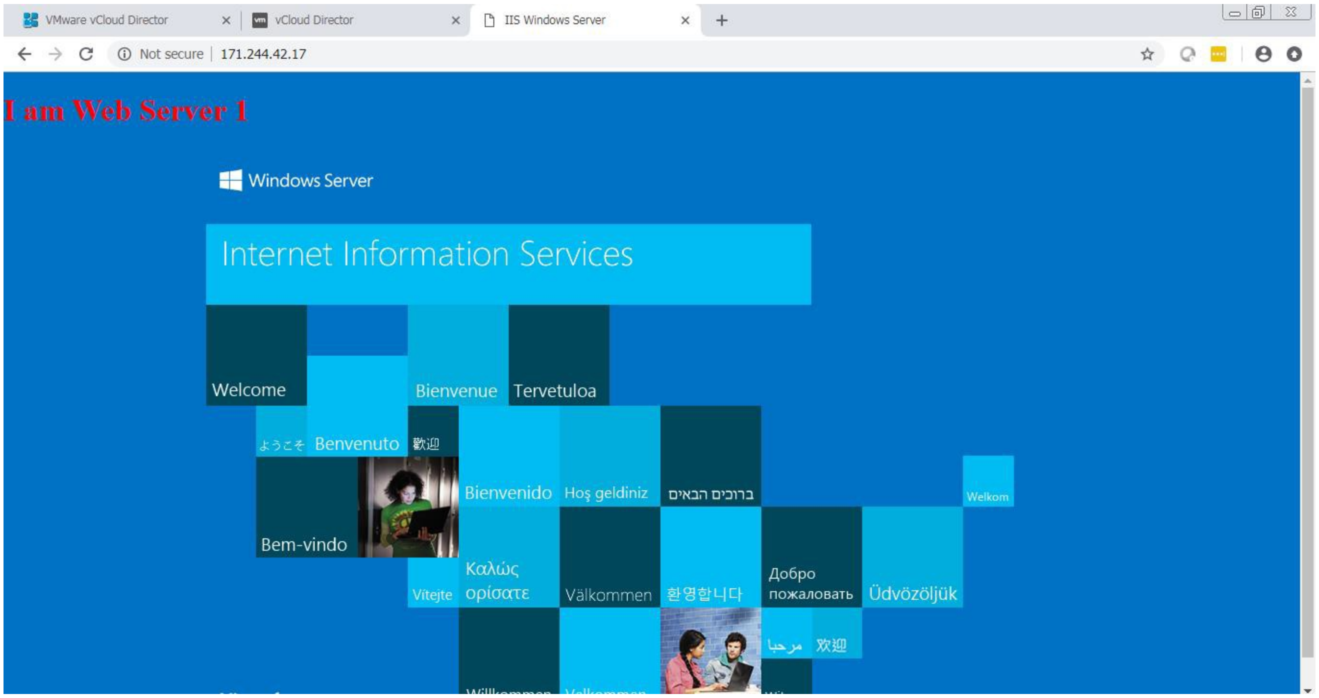
Pool Status and Statistics

Pool ID	Name	Status
pool-2	LB_HTTP_POOL	UP

Member Status and Statistics

Name	IP Address	Status	Member ID
WebServer01	192.168.1.1	UP	member-1
WebServer02	192.168.1.2	DOWN	member-2

At the moment, Web Server 01 acts as the only server responses for user’s traffic:



I am Web Server 1

Through this User guide, Customer have knowledge to use the vCloud Director Portal for manage vFirewall and vLoad Balancer services of USDC Technology.

For any questions regarding the service, please contact the hotline **(028) 7308 0708** or support ticket page at *https://portal.usdc.vn* or email *support@usdc.vn*

Sincerely.

-THE END-