USDC TECHNOLOGY
Smart Data Center

HƯỚNG DẪN SỬ DỤNG DỊCH VỤ VFIREWALL VÀ VLOAD BALANCER

MỤC LỤC

I. Giới thiệu 2
II. Cấu hình dịch vụ vFirewall 3
1. Cấu hình Network Address Translation (NAT) 7
2. Khai báo Firewall Rules 9
3. Cấu hình IPsec VPN Site to Site 12
4. Cấu hình SSL VPN Client to Site 13
III. Dịch vụ vLoad Balancer 22
1. Import chứng chỉ (certificate) 23
2. Application Profiles 25
3. Server Pool 28
4. Virtual Server 30
5. Test – Kiểm tra dịch vụ 31

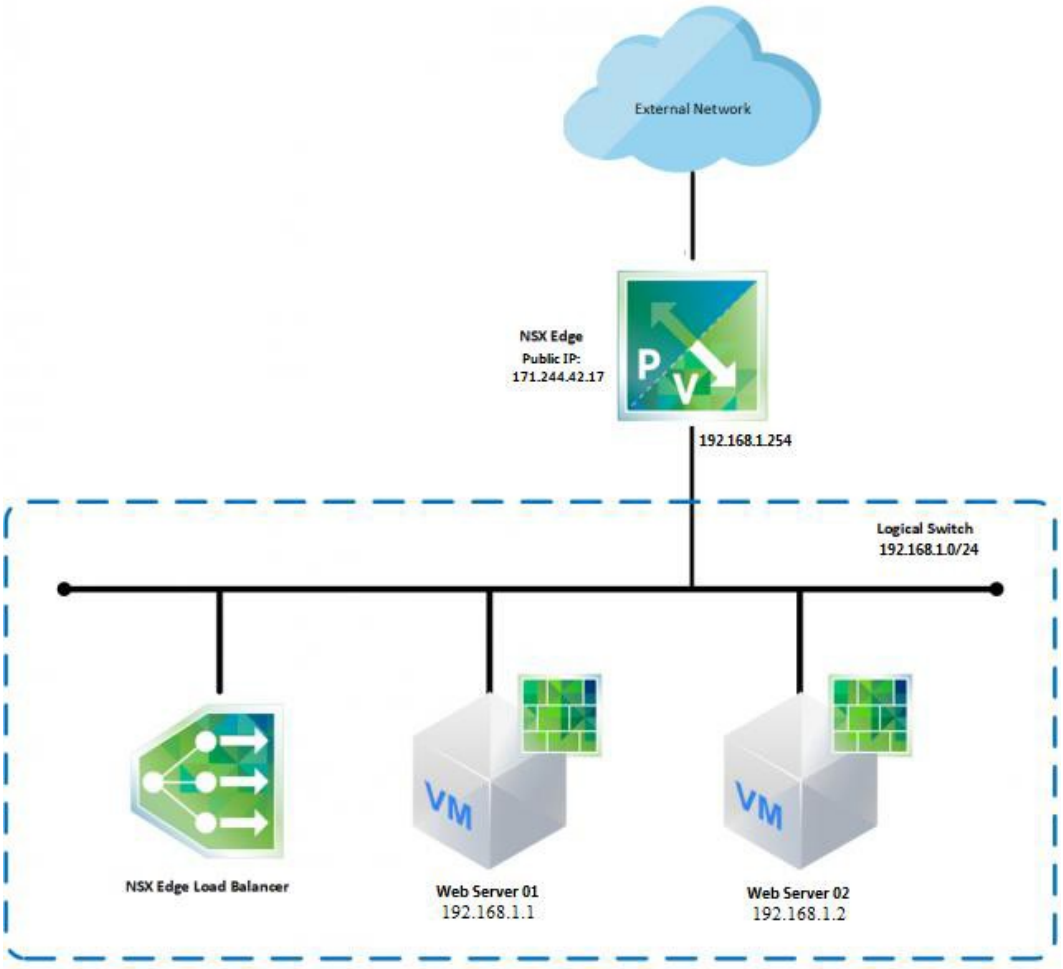
I. Giới thiệu

vFirewall và vLoad Balancer là 2 dịch vụ gia tăng (addon) dựa trên giải pháp VMWare NSX cung cấp trên nền tảng dịch vụ Virtual Private Cloud USDC Technology.

Quý khách vui lòng đăng nhập vào vCloud Director Portal với đường dẫn và tài khoản đã được cung cấp.

Cú pháp đường dẫn đăng nhập: https://vpc.vcpp.vn/tenant/YOUR_ID với YOUR_ID là Mã khách hàng

Giả sử chúng ta cần thiết lập mô hình mạng mức cơ bản như sơ đồ dưới:



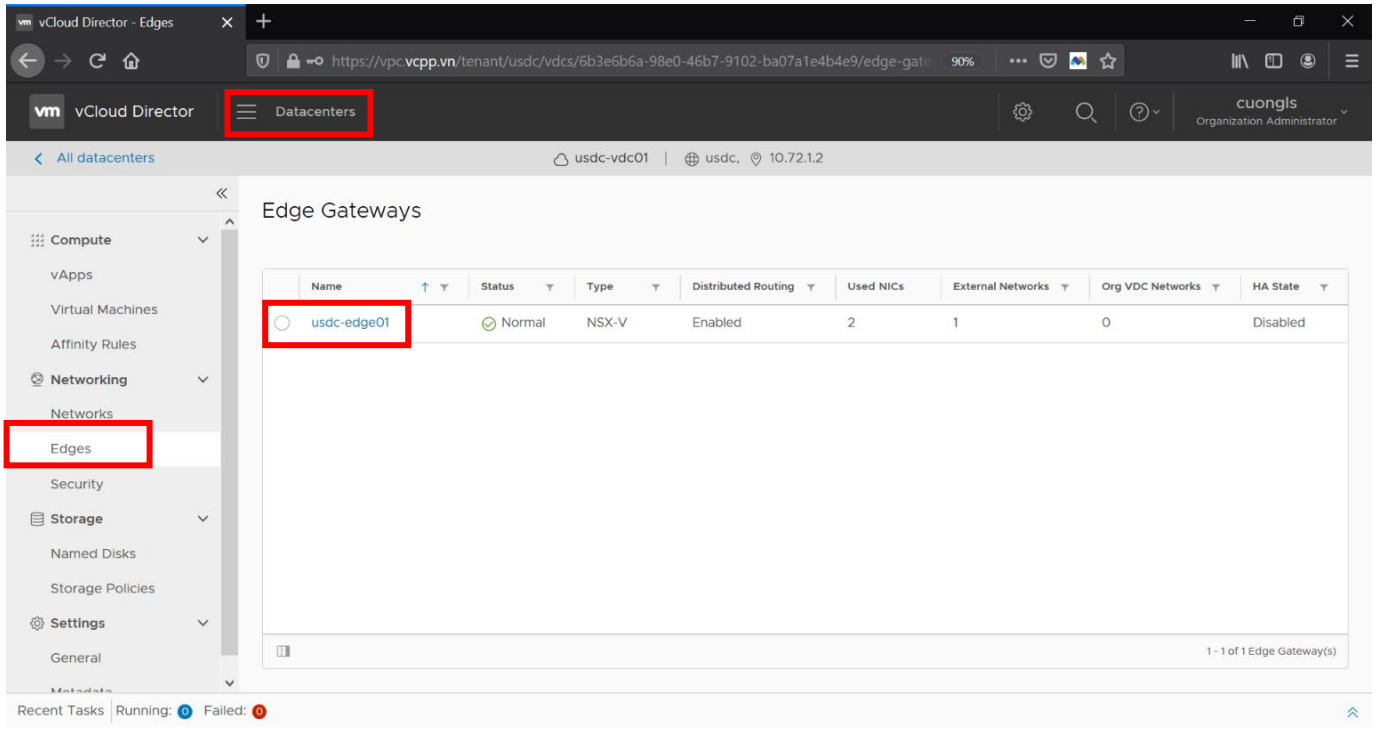
	Private Zone	Public Zone	Mode
NSX Edge (vFirewall)	192.168.1.254	171.244.42.17	Có interface trực tiếp với internet
NSX Edge Load Balancer	1 cluster gồm 2 member Web Server ở dưới	171.244.42.17	VIP đại diện cho cluster
Web Server 01	192.168.1.1	171.244.42.111	NAT qua vFirewall
Web Server 02	192.168.1.2	171.244.42.112	NAT qua vFirewall

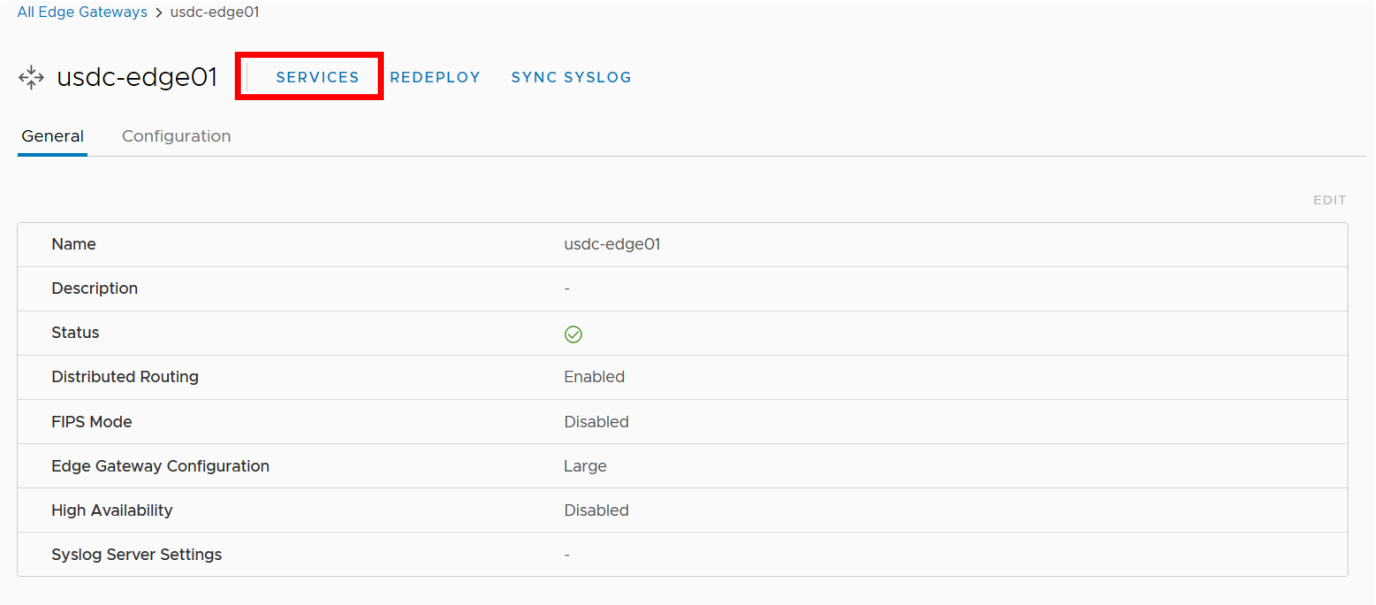
Trong mô hình này có ta thấy có 2 loại Public IP: 1 là IP sử dụng đại diện cho NSX Edge (vFirewall), làm virtual IP cho vLoad Balancer (tạm gọi là Master IP); 2 là các IP public dùng để NAT 1:1 cho các Cloud Server/VM (tạm gọi là các NAT IP).

II. Cấu hình dịch vụ vFirewall

Sau khi đăng nhập vCloud Director Portal thành công, từ giao diện chính, chọn **Datacenters -> Networking -> Edge Gateway.**

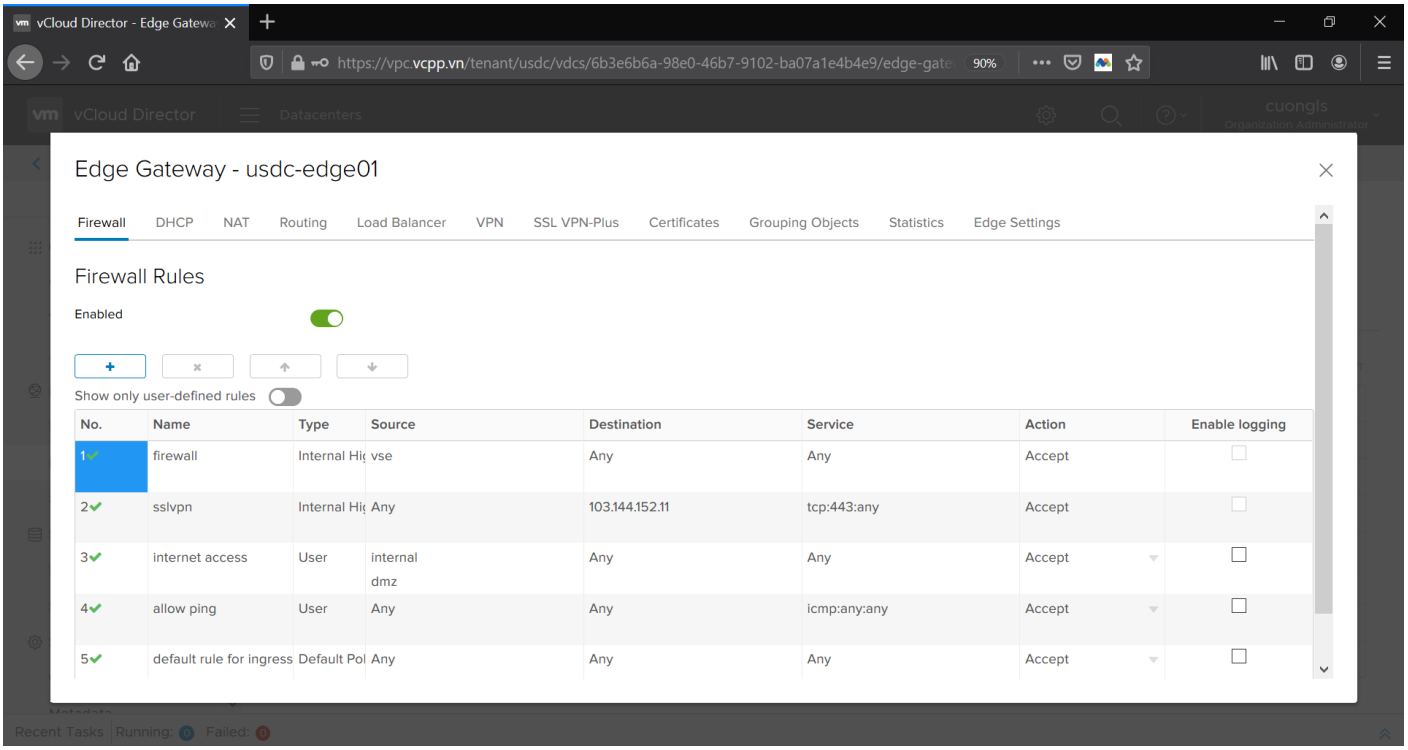
Thông số của vFirewall sẽ được thể hiện khi quý khách click vào tên của Edge.





✍ *Để xem được thông tin về cấu hình và dịch vụ của Edge (Firewall, DHCP, VPN, SSL, v.v.):* nhấn chọn Edge Gateway tại mục **Networking -> Edge -> Services** ở trên.

Lưu ý: NSX Edge sẽ thể hiện thông số cấu hình, chọn **Enable** để kích hoạt cấu hình của Tường lửa



1. Cấu hình Network Address Translation (NAT)

Qúy khách phải Enable tại tab Firewall

Chuyển sang tab **NAT**, trong này sẽ hiển thị danh sách tất cả các Rule NAT đã cấu hình. Giải pháp vFirewall của USDC Technology hỗ trợ 2 loại NAT chính: NAT theo nguồn (SNAT) và NAT theo đích (DNAT) cho cả IPv4 và IPv6. Hướng dẫn này tập trung vào IPv4.

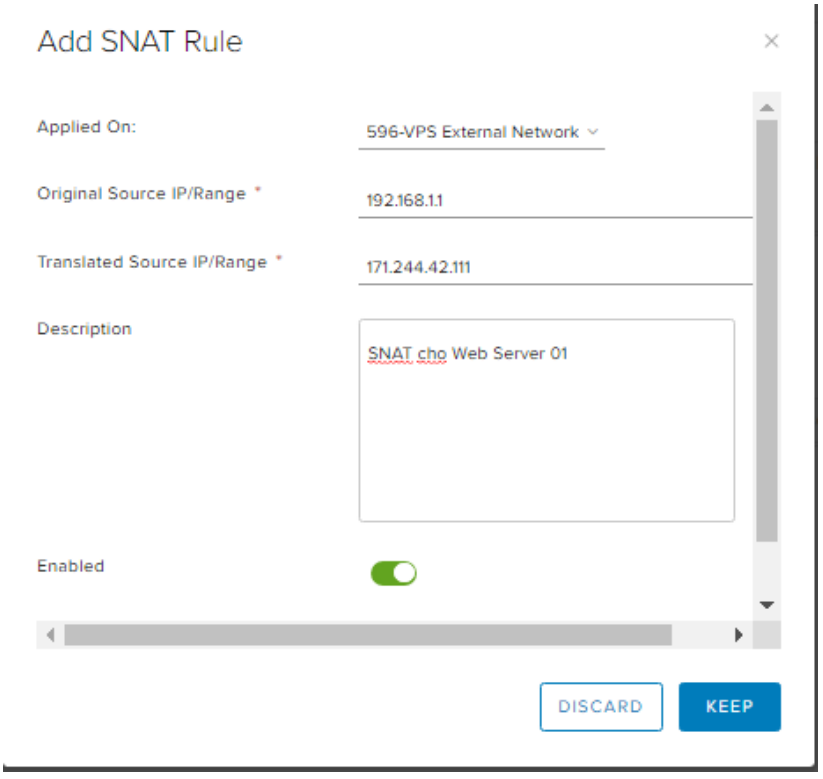
Để tạo rule NAT mới, chọn biểu tượng

☑ SNAT

(từ IP local định tuyến ra ngoài IP public)

- **Applied On**: Chọn vùng mạng thực thi, mặc định là lớp mạng ngoài (External).
- **Original Source IP/Range**: nhập IP gốc (IP private của server)
- **Translated Source IP/Range**: IP được chuyển đổi sau NAT (chính là các Public NAT IP đã lấy được ở trên)
- **Description**: nhập mô tả
- **Enable:** chọn mục này để rule có hiệu lực

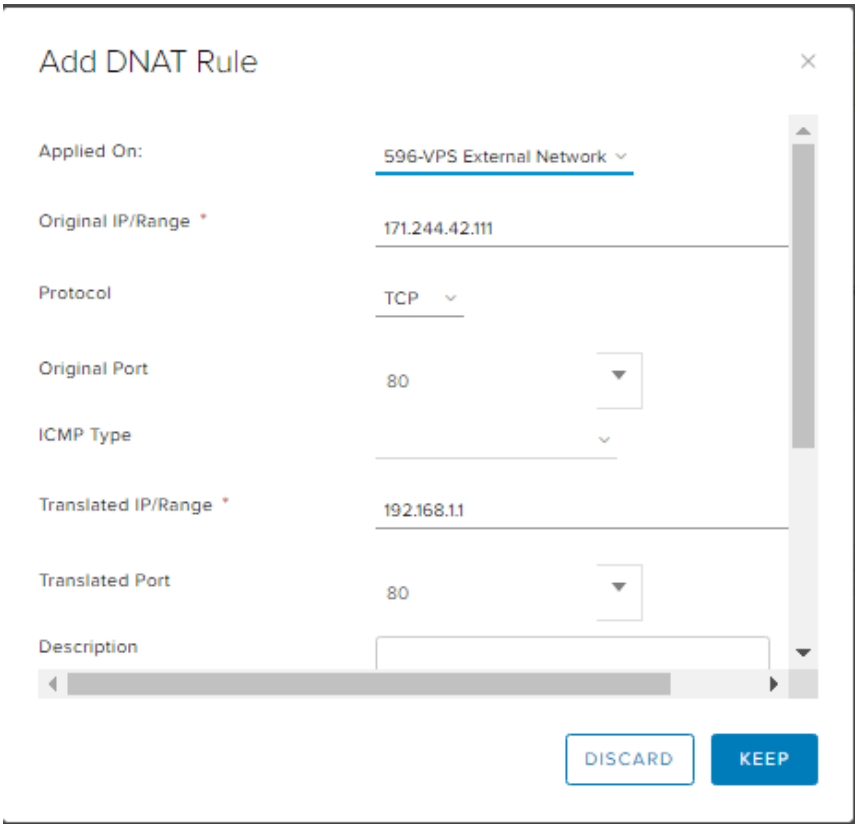
Nhấn **Keep** sau khi điền xong thông số.



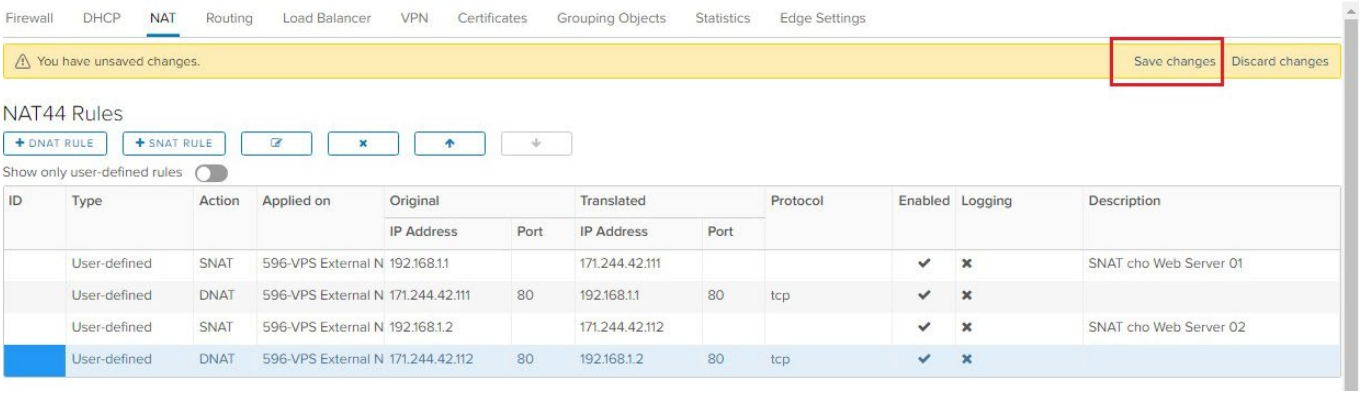
☑ **DNAT** + DNAT RULE **(từ IP public trỏ về IP local)**

- **Applied On**: Chọn vùng mạng thực thi, mặc định là lớp mạng ngoài (External).
- **Original IP/Range:** nhập IP gốc (IP Public, chính là các Public NAT IP đã lấy được ở trên)
- **Protocol:** chọn loại giao thức (TCP, UDP, ICMP, Any)
- **Original Port:** port gốc do client gửi tới
- **Description**: nhập mô tả
- **Translated IP/Range:** IP Private của server được chuyển đổi sau NAT
- **Translated Port:** Port chuyển đổi, chuyển đến server sau khi NAT
- **Enable:** chọn mục này để rule có hiệu lực

Nhấn **Keep** sau khi điền xong thông số



Thực hiện tương tự cho Web Server 02. Sau khi hoàn thành nhấn nút "**Save Changes**" để lưu lại và thực thi cấu hình mới:



✍ Để thực hiện điều chỉnh NAT rule đã khai báo, chọn NAT rule tương ứng và nhấn nút [✎]. Tương tự để xóa rule chọn nút [×]. Chọn "Save Changes" để áp dụng các thay đổi mới.

2. Khai báo Firewall Rules

Chuyển sang tab Firewall, đảm bảo Firewall phải đang được **Enable** và tùy chọn "**Show only user-defined rules**" được bật

[+]: Tạo rule mới

[×]: Xóa rule đang chọn

[↑]: Chuyển thứ tự ưu tiên của rule lên trên 1 bậc

[↓]: Hạ thứ tự của rule xuống 1 bậc

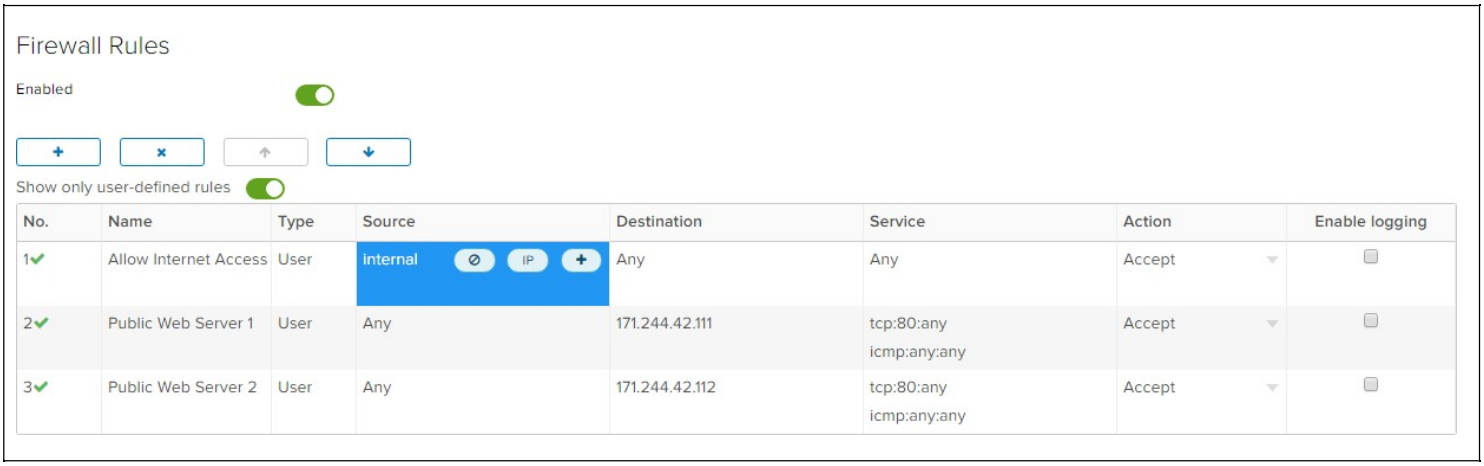
Sau khi nhấn chọn tạo rule mới, cửa sổ quản trị sẽ tạo ra 1 dòng mới với các ô thông tin mặc định (any, any, accept), nhấn chuột vào ô tương ứng để sửa thông tin cần:

- **No**: Thứ tự ưu tiên của rule
- **Name**: tên của rule
- **Type**: kiểu (do hệ thống hay user tạo ra)

- **Source**: địa chỉ IP nguồn, có thể nhấn IP để nhập IP hoặc + để chọn đối tượng (internal, external, all..)
- **Destination**: địa chỉ IP đích.
- **Service**: chọn giao thức (TCP, UDP, ICMP, Any) và cổng (80, 443, 21..) cho nguồn và đích.
- **Action:** chọn loại hành động: **Accept** – cho phép hay **Deny** – chặn

Sau khi hoàn thành các rule như mong muốn, nhấn nút "**Save Changes**" để lưu lại và thực thi cấu hình mới.

🕮 **Ví dụ minh họa cho mô hình hệ thống giả lập ban đầu ở Mục I:**



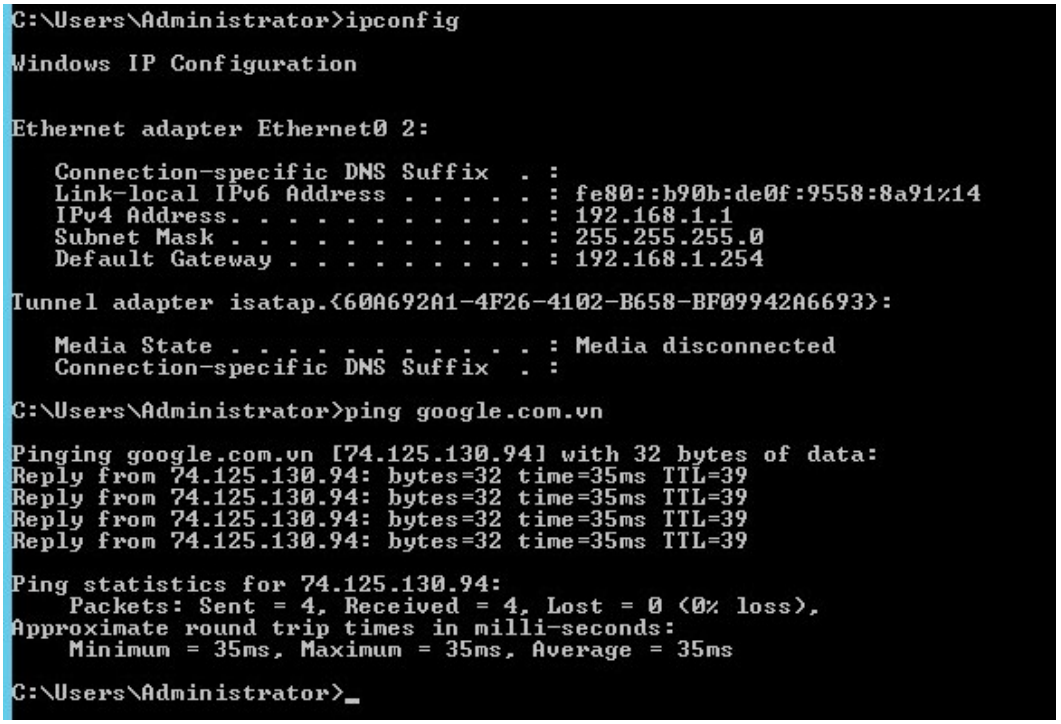
Ý nghĩa:

- Rule số 1: cho phép traffic từ mạng internal (192.168.1.x) đến tất cả các hướng (gồm cả mạng external). Mạng internal lúc này sẽ theo rule NAT đã khai báo ở trên để ra internet.
- Rule số 2 và 3: cho phép client có thể ping (ICMP) và truy cập đến dịch vụ web (http-tcp port 80) của 2 public IP 171.244.42.111 và 171.244.42.112. Đây chính là NAT IP của 2 Web server 192.168.1.1 và 192.168.1.2. Kết hợp với rule NAT ở trên, client từ mạng external (internet) có thể truy cập web đến 2 server này.

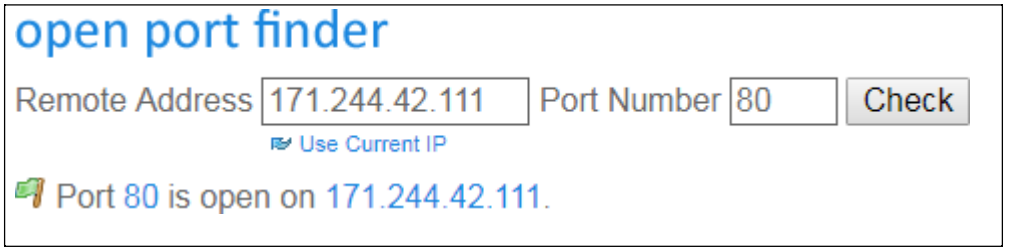
Các traffic không khớp với 3 rule trên mặc định bị chặn (deny).

✍ Kiểm tra kết quả:

Từ Web Server 1, ping ra internet:

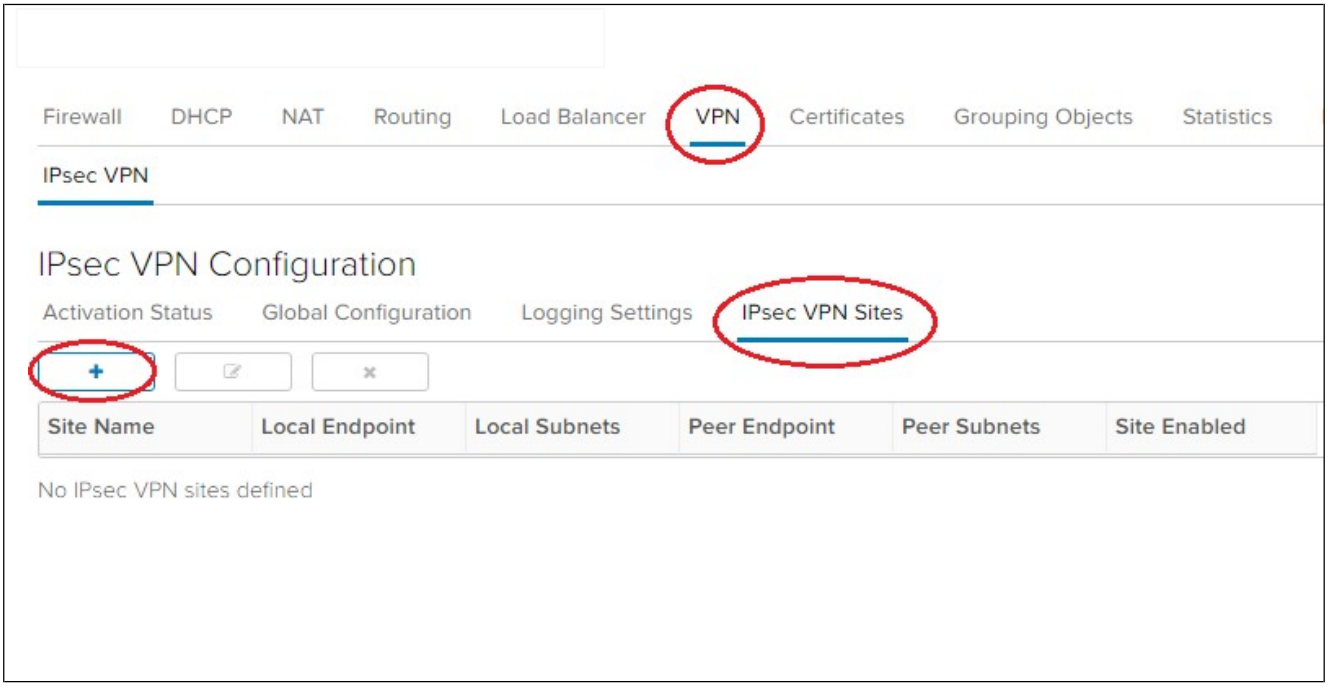


Check trạng thái dịch vụ:



3. Cấu hình IPsec VPN Site to Site

Trong gói dịch vụ vFirewall của USDC Technology có hỗ trợ tính năng khai báo kết nối VPN Site to Site. Từ giao diện quản trị chính, chọn tab **VPN -> IPsec VPN -> IPsec VPN Sites**. Nhấn chọn để tạo kết nối VPN mới.



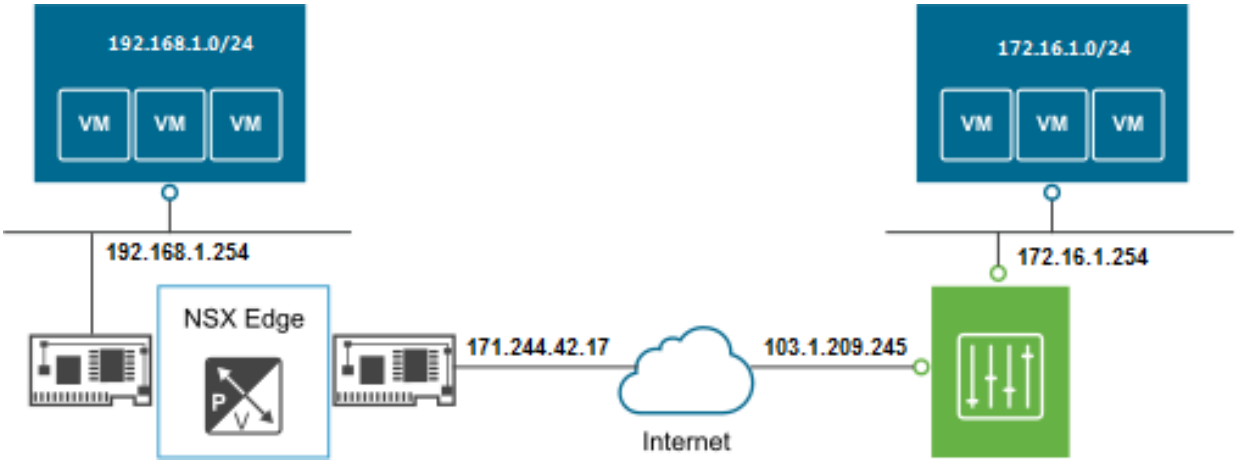
Sau đó điền các thông số để thiết lập phiên VPN như dưới. Lưu ý các thông số này phải khớp với cấu hình trên router/firewall đầu xa.

- **Enabled:** cho phép hoặc vô hiệu thực thi phiên VPN.
- **Enable perfect forward secrecy (PFS):** cho phép chạy mode PFS để tăng tính bảo mật (khuyến nghị nên dùng).
- **Name**: tên phiên kết nối VPN
- **Local Id và Local Endpoint**: điền địa chỉ Public Master IP của vFirewall đã lấy ở mục II.1. Trường hợp mô hình giả lập là 171.244.42.17
- **Local Subnets**: dải mạng private của đầu local, trường hợp này là 192.168.1.0/24
- **Peer Id và Peer Endpoint**: IP Public của router đầu xa.
- **Peer Subnets**: dải mạng private của đầu xa.
- **Encryption Algorithm**: thuật toán mã hóa, hỗ trợ các thuật toán: AES, AES256 và 3DES
- **Authentication**: hình thức chứng thực, thông thường dùng preshare key (PSK)
- **Pre-Shared Key**: nhập preshare key
- **Diffie-Hellman Group**: chọn phương thức trao đổi khóa, hỗ trợ các phương thức: DH2,

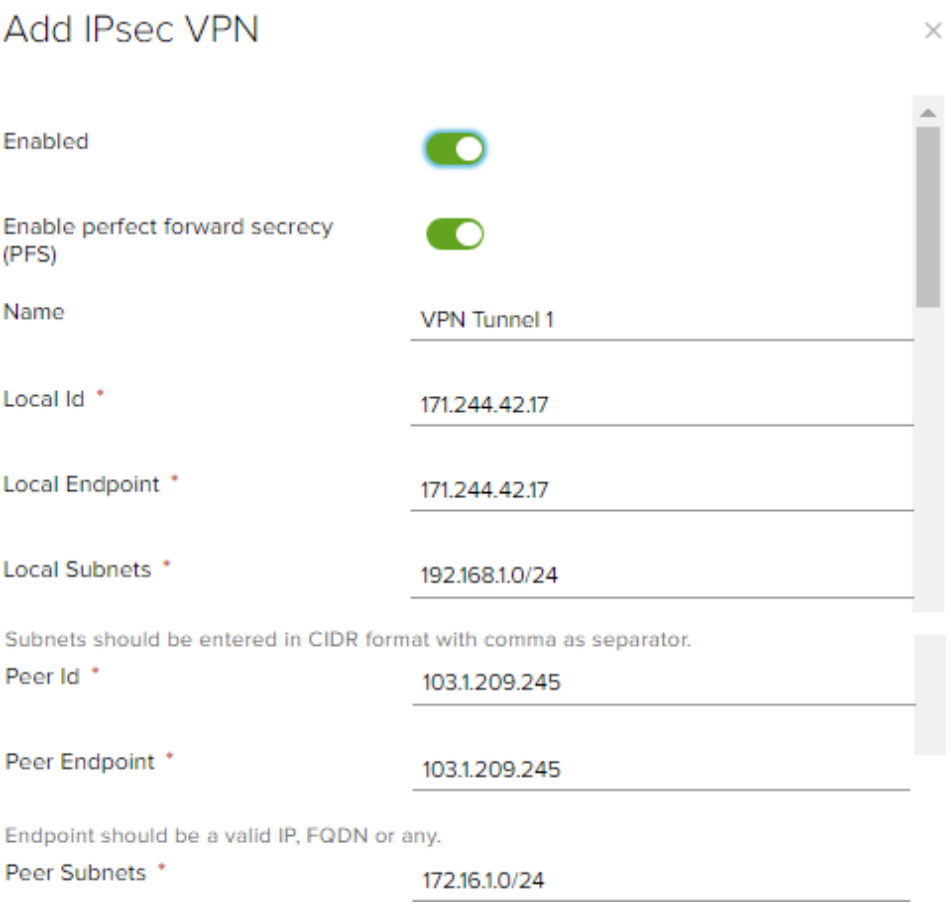
DH5, DH14, DH15, DH16

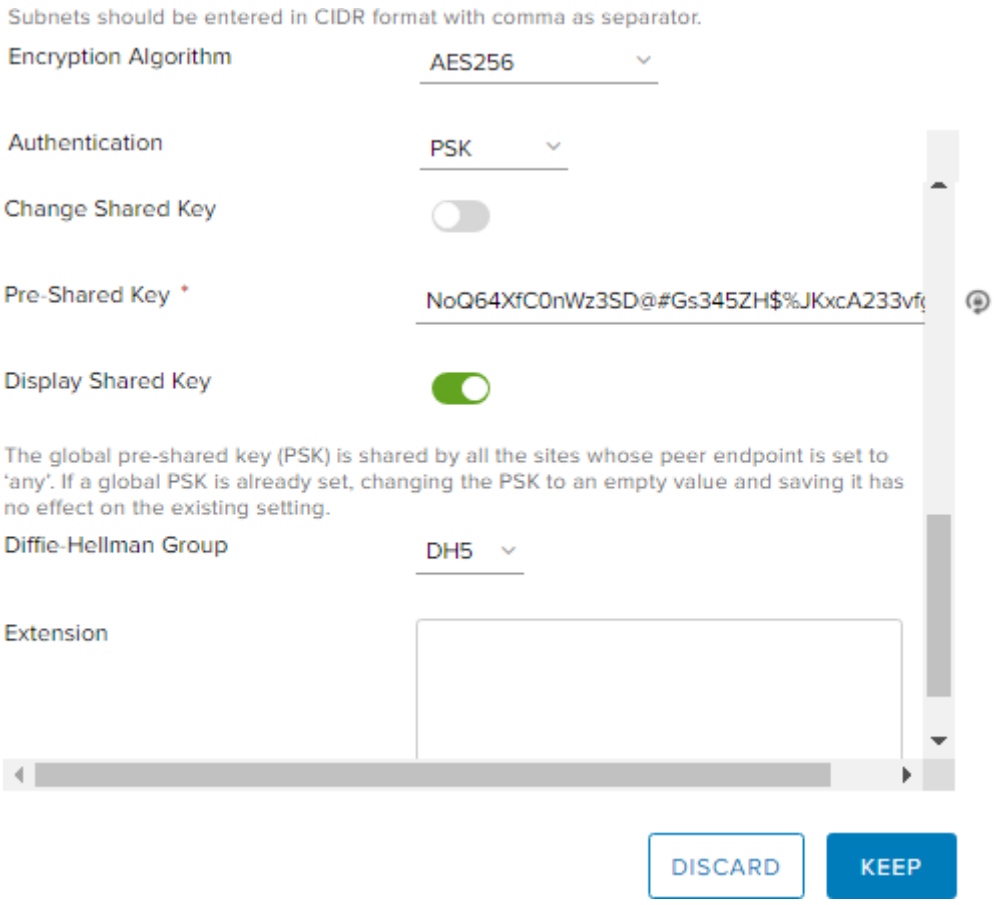
Nhấn **Keep** sau khi điền xong thông số. Cuối cùng chọn "**Save Changes**" để áp dụng các thay đổi mới.

🕮 **Giả sử chúng ta cần thiết lập kênh kết nối VPN theo mô hình sau**:



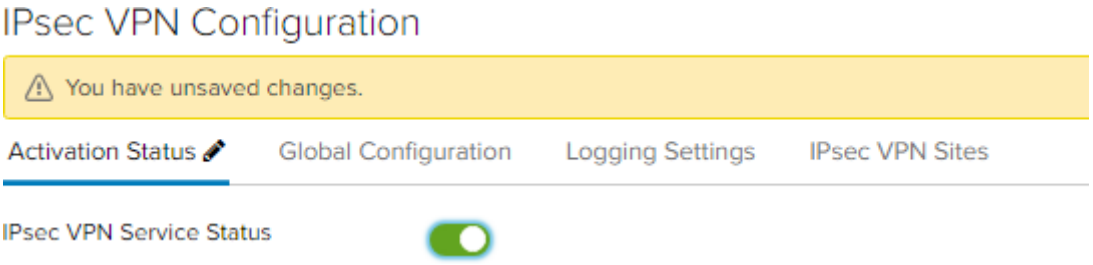
Bước 1: Cấu hình đầu phía Cloud của USDC Technology như sau:



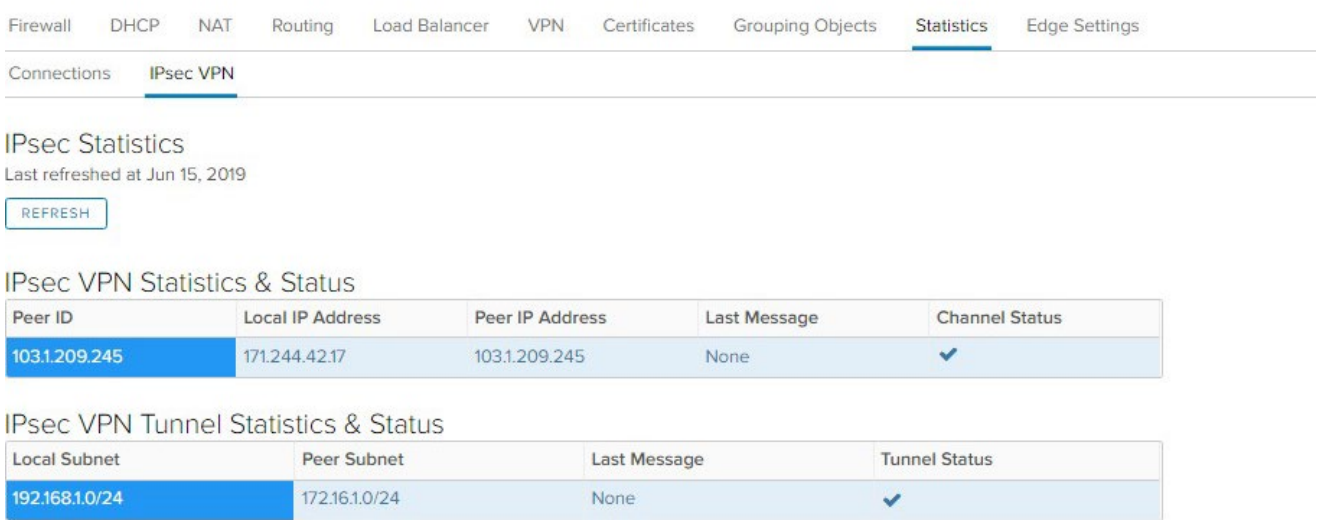


Lưu ý: Các thông số bao gồm: giao thức mã hóa, phương thức trao đổi khóa và preshare key phải được thiết lập giống nhau giữa 2 đầu thiết bị thiết lập kênh VPN. *Với IKE mặc định sử dụng version 1*.

Bước 2: Chuyển sang tab **Activation Status,** bật tùy chọn "**IPsec VPN Service Status**" và nhấn "**Save Changes**":



✍ **Kiểm tra trạng thái kênh VPN**: chọn tab **Statistics -> IPsec VPN**:



Đến đây chúng ta đã sử dụng được các tính năng cơ bản: NAT, Firewall rule và VPN Site to Site trên vFirewall của USDC Technology.

4. Cấu hình SSL VPN Client to Site

Trong gói dịch vụ Virtual Private Cloud và Dedicated Private Cloud của USDC Technology có hỗ trợ tính năng khai báo kết nối VPN Client to Site trên vFirewall (với dịch vụ vCloud Server hiện chưa cung cấp tùy chọn này).

Bước 1: Từ giao diện quản trị chính, chọn tab **SSL VPN-Plus -> Server Setting** và chọn các thông số:

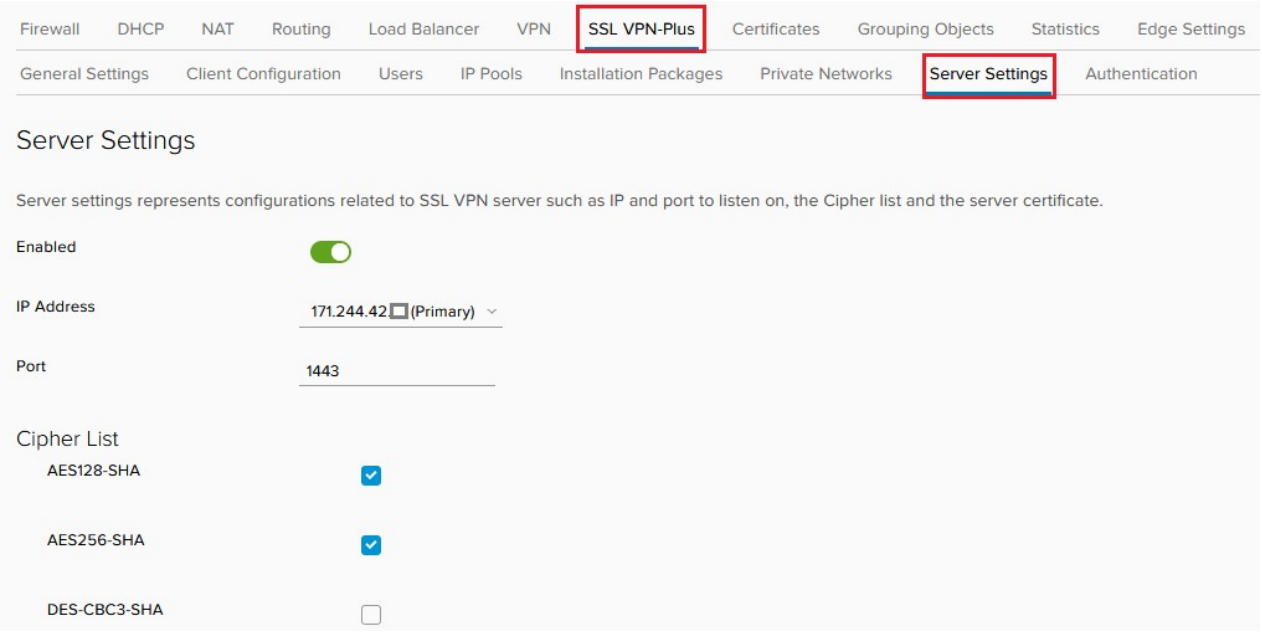
- Enable Server

- IP Address: Chọn IP Public VPN (thường là Master IP)

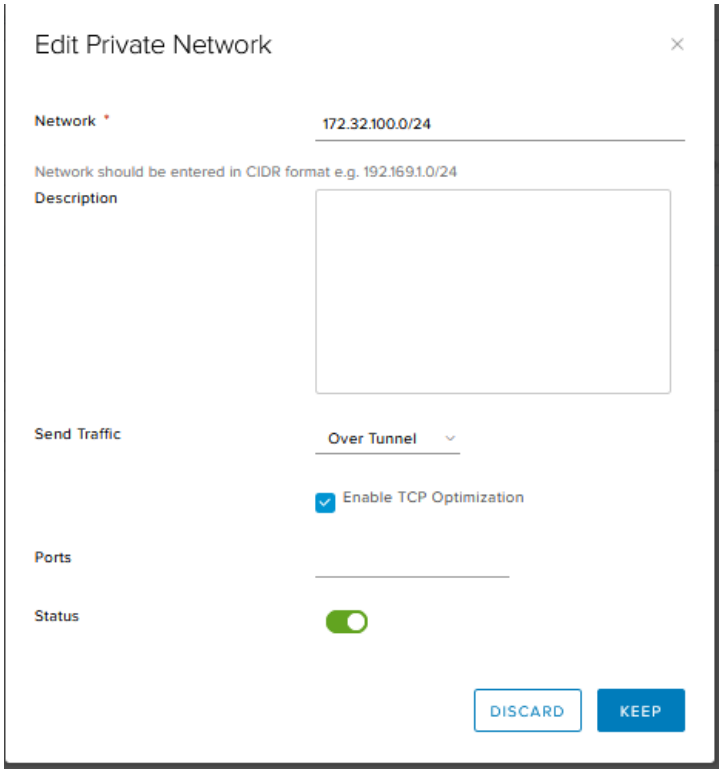
- Port: cổng kết nối và truy cập trang portal download packge cài đặt cho client. *Lưu ý: nếu bạn có sử dụng dịch vụ vLoad Balancer(vLB) thì phải chỉ định port khác với port sử dụng cho vLB* (thường là các port http:tcp/80, https: tcp/443). Trong hình minh họa dưới sử dụng port 1443.

- Cipher List: Chọn tối thiểu AES256-SHA

Nhấn **Save Changes:** Lưu lại các thay đổi



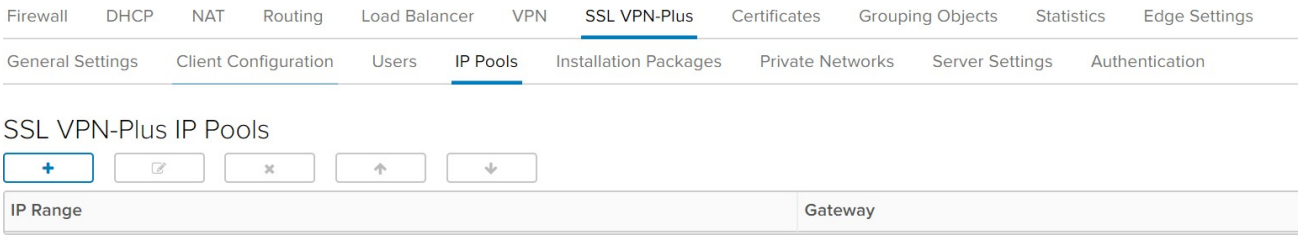
Bước 2: Vào tab **Private Network.** Nhấn chọn + để khai báo dải mạng private trên Cloud. Dải này cần khai báo giống với các dải mạng private mà VM đang dùng.



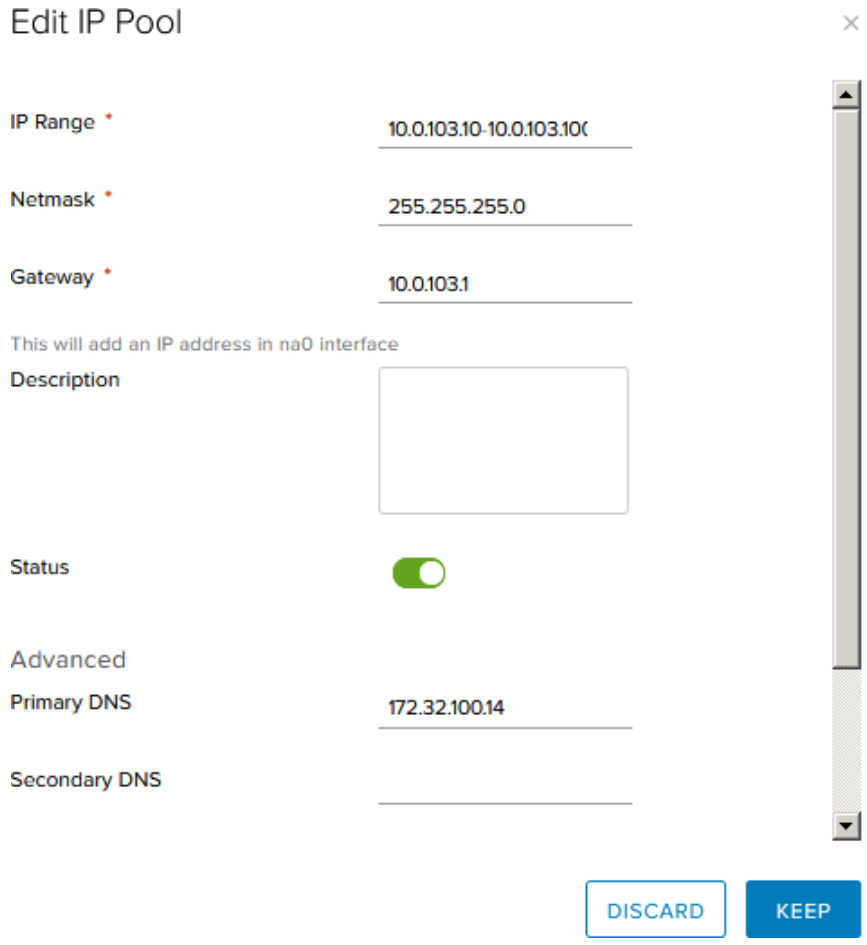
Chọn **Keep** để giữ lại các thay đổi.

Chọn **Save Changes:** Lưu lại các thay đổi

Bước 3: Vào tab **IP Pool** để tạo dải mạng sử dụng cho người dùng (client) khi kết nối **SSL VPN.** Nhấn chọn để tạo dải mạng.



Điền các thông tin dải mạng như hình dưới. Có thể dùng dải mạng bất kỳ nhưng không được trùng với dải mạng nội bộ đang dùng cho các VM.

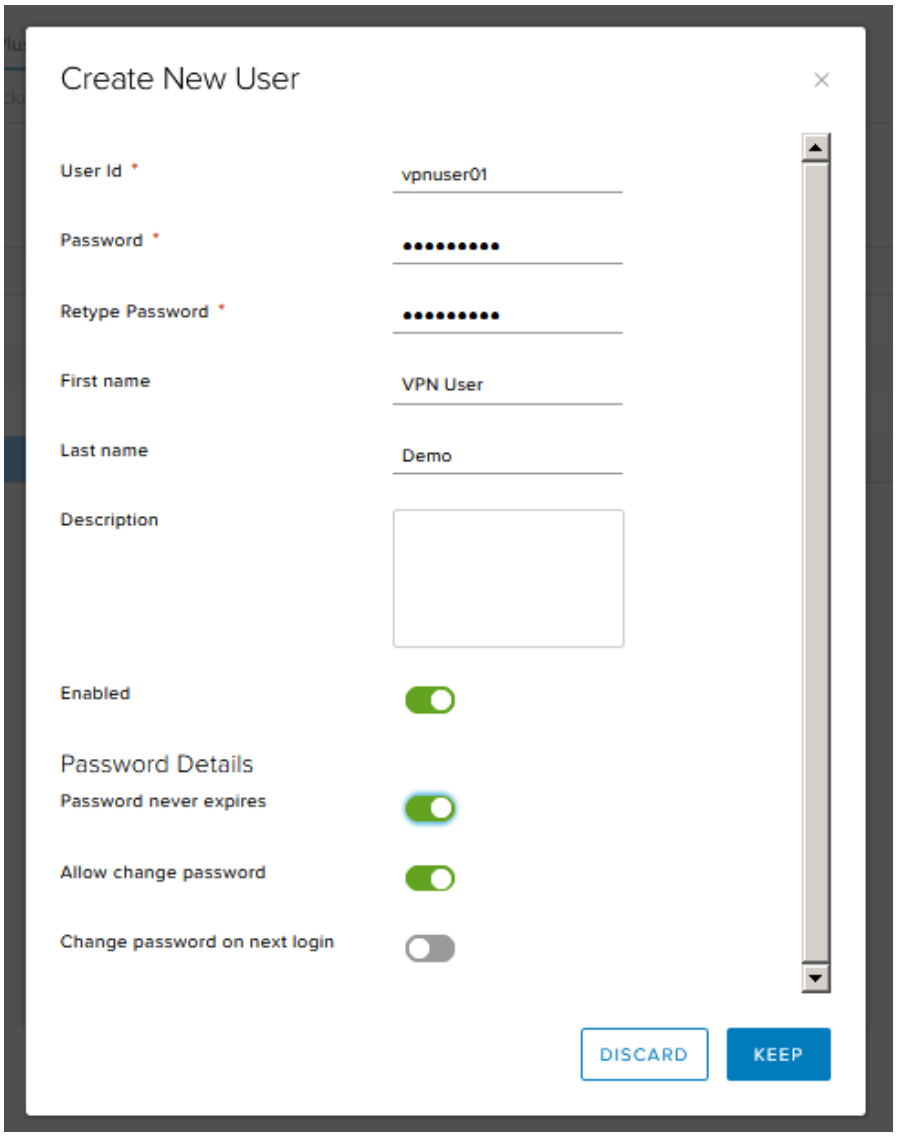


Chọn **Keep** để giữ lại các thay đổi.

Chọn **Save Changes:** Lưu lại các thay đổi

Bước 4: Vào tab **User** để tạo người dùng cho phép kết nối **SSL VPN.**

Nhấn chọn để tạo tài khoản



Sau đó điền và chọn các thông số:

- **User ID**: tên tài khoản kết nối SSL VPN

- **Password**: Mật khẩu kết nối SSL VPN

- **Retype Password**: Gõ lại mật khẩu

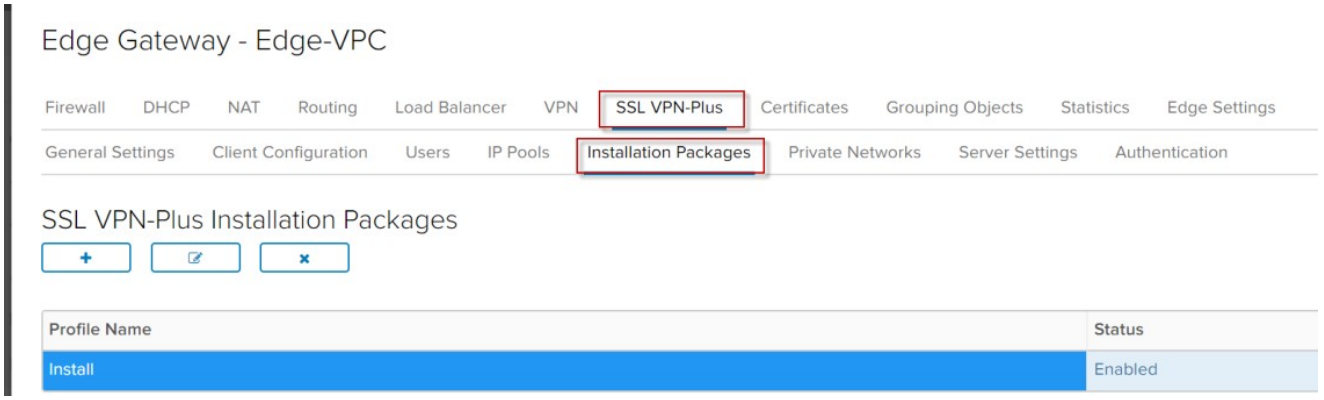
- **Password never expries** (tùy chọn): mật khẩu không thời hạn

- **Allow change password** (tùy chọn): cho phép người dùng đổi mật khẩu (thông qua trang portal SSL VPN)

- **Change password on next login (tùy chọn)**: bắt buộc người dùng đổi mật khẩu trong lần đăng nhập đầu.

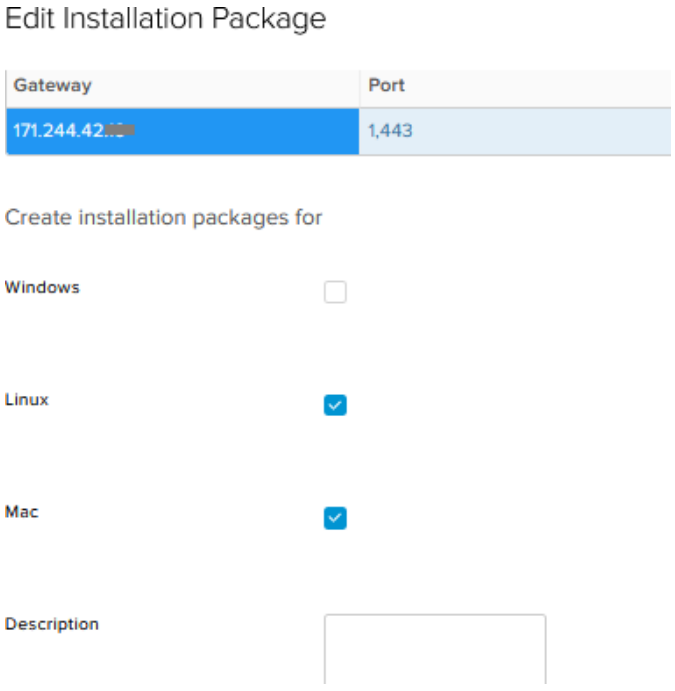
Chọn **Keep** để giữ lại các thay đổi

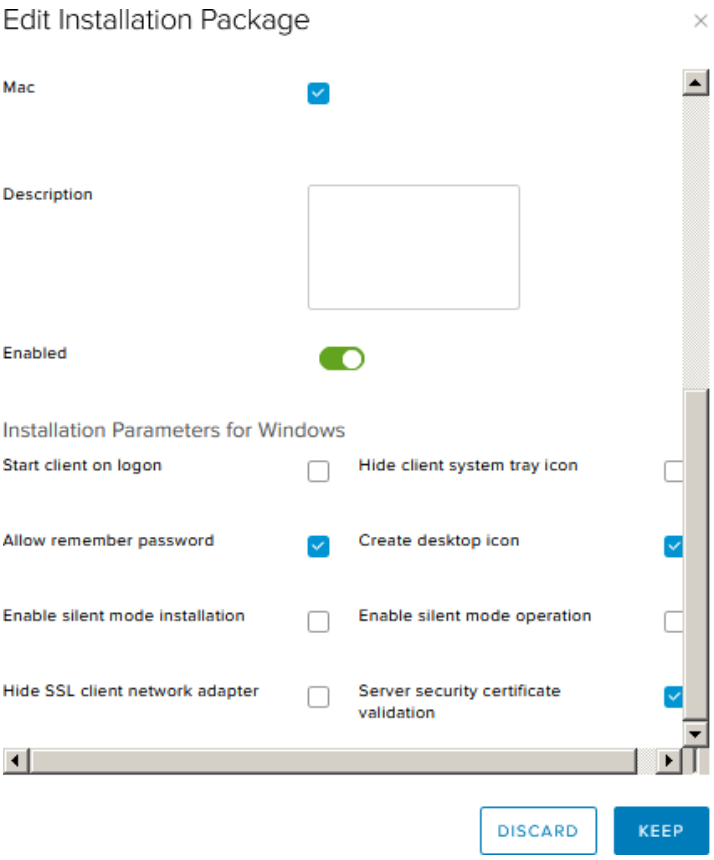
Bước 5: Vào tab **Installation Packets.** Nhấn chọn [+] để tạo gói cài đặt từ giao diện web cho client.



Sau đó điền các thông số sau:

- **Profile Name**: Tên gói cài đặt.
- Điền thông tin **địa chỉ IP và port** kết nối đến đã cấu hình ở **Bước 1**.
- Tích chọn vào hệ điều hành sẽ tạo gói cài đặt cho người dùng
- Check chọn **Create destop icon**.
- **Không tích chọn Hide SSL client network adapter** (nếu không sẽ gặp lỗi "Driver installation failed for reason E000024B" trên một số máy).

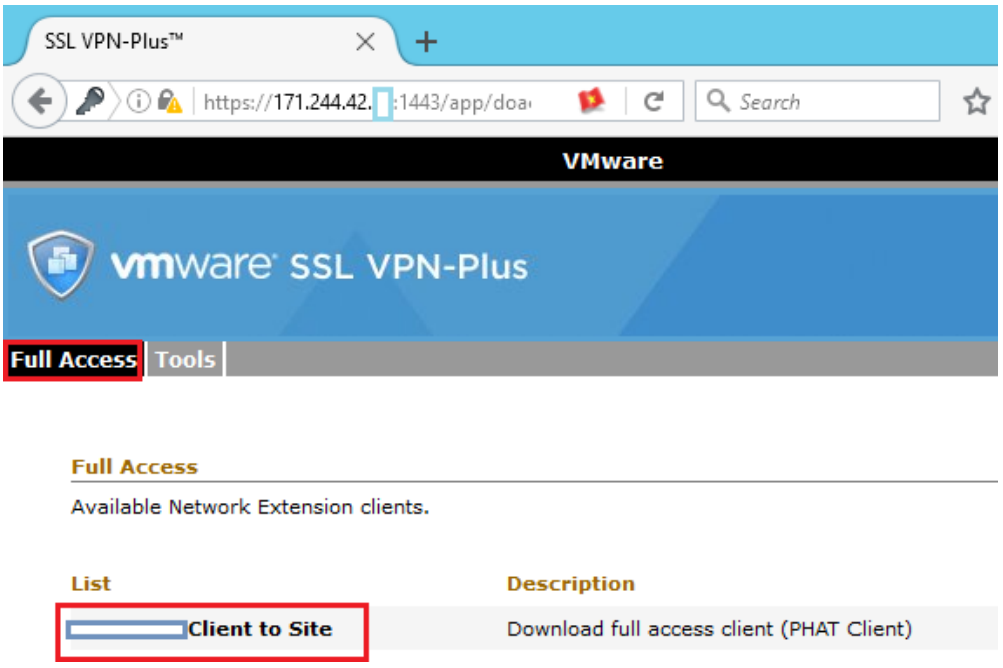


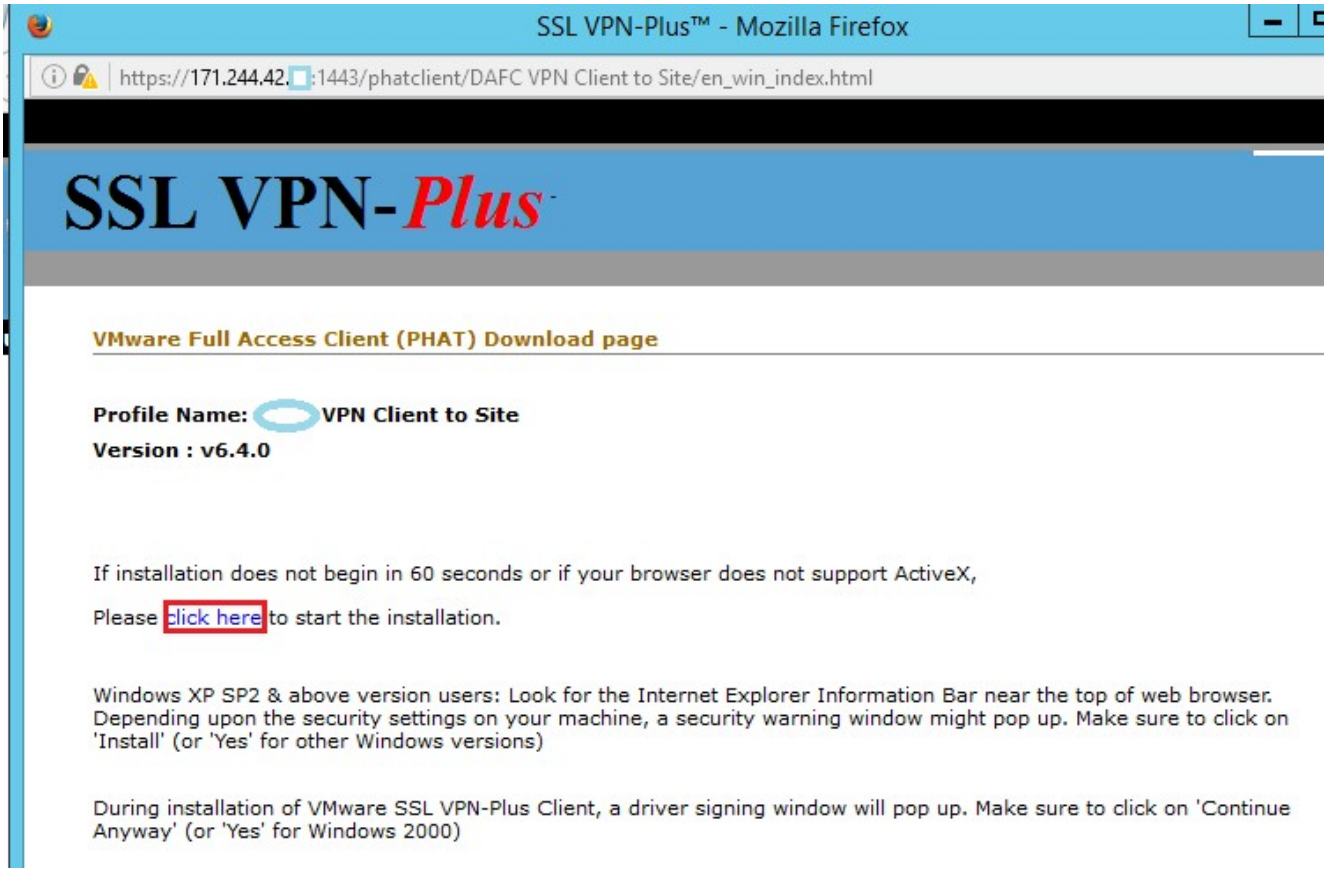


Đến đây quá trình cài đặt, cấu hình dịch vụ SSL VPN client to site đã hoàn thành. Người dùng có thể sử dụng và kết nối VPN đến cụm máy chủ ảo trên Cloud như sau:

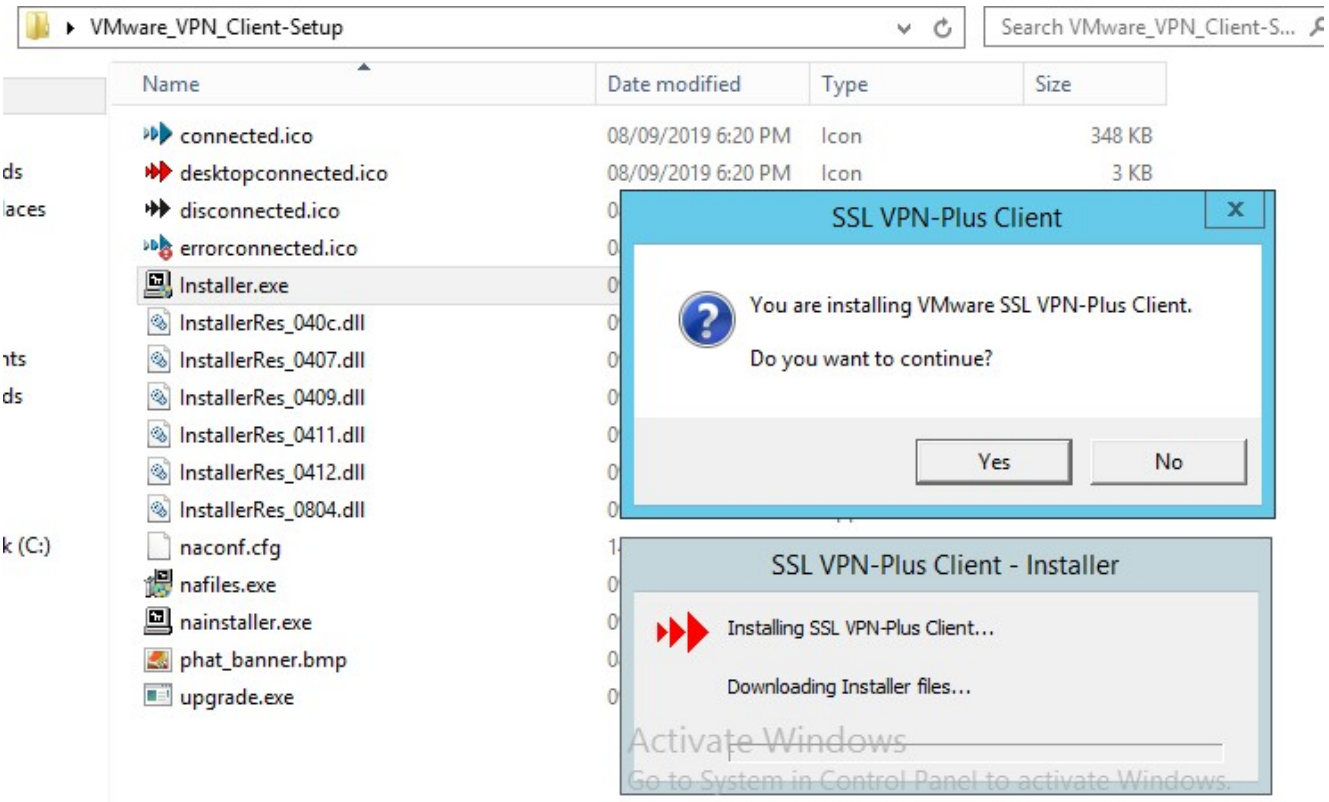
🕮 Hướng dẫn thiết lập kết nối SSL VPN Client to Site trên máy người dùng

Bước 1: Truy cập https://IP-SSL_VPN_Server:Port với tài khoản đã được tạo ở các bước trên. Click chọn vào tên gói cài đặt trong list và tải về soft client:

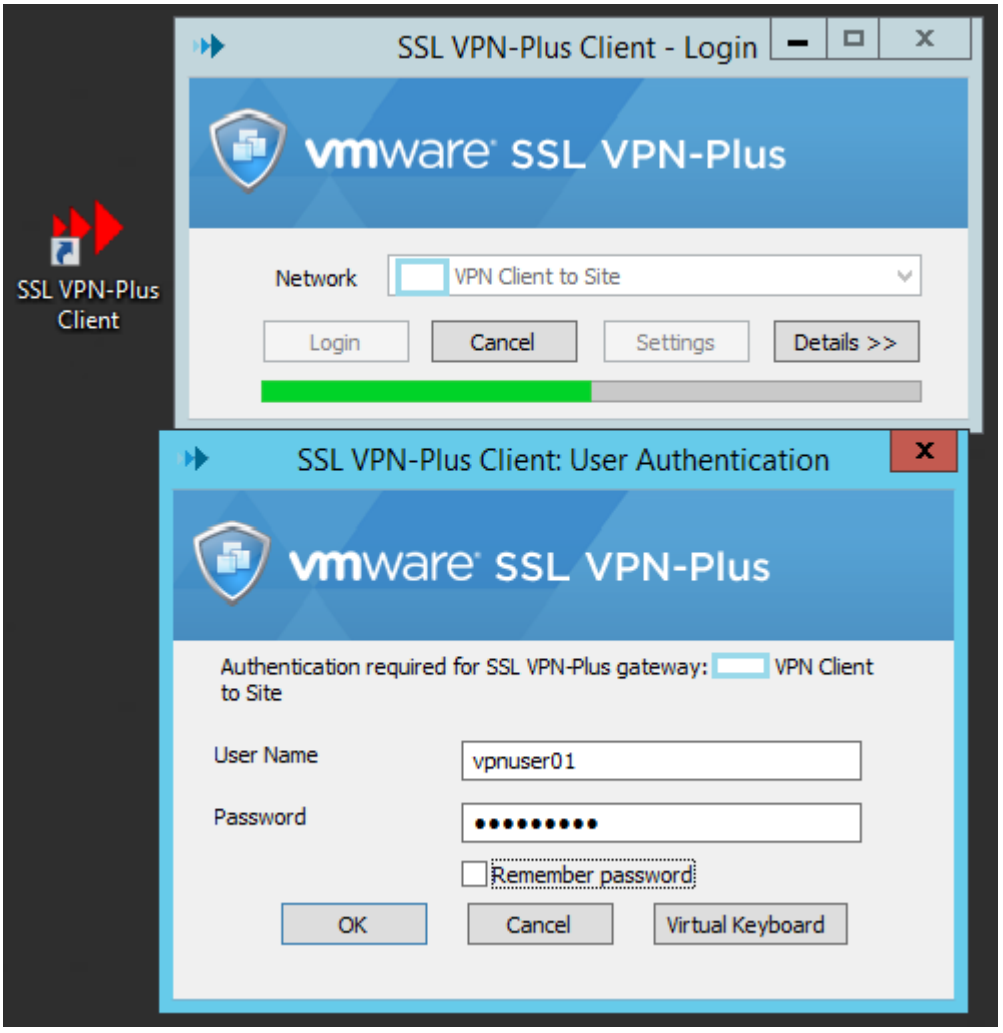

SSL VPN-Plus™
https://171.244.42.:1443/app/doa
Search
VMware
vmware SSL VPN-Plus
Full Access
Tools
Full Access
Available Network Extension clients.
List
Description
Client to Site
Download full access client (PHAT Client)

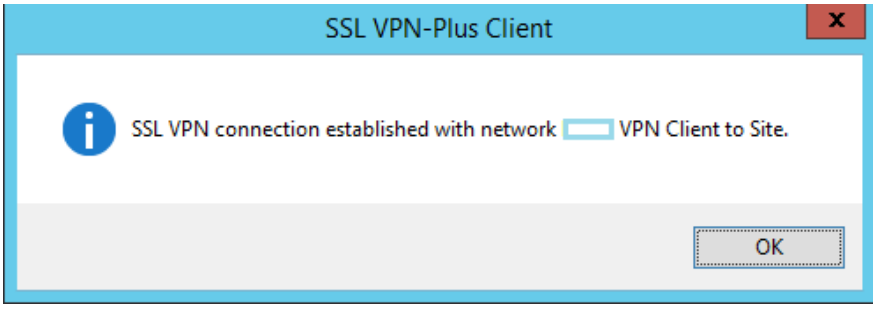

SSL VPN-Plus™ - Mozilla Firefox
https://171.244.42.:1443/phatclient/DAFC VPN Client to Site/en_win_index.html
SSL VPN-Plus
VMware Full Access Client (PHAT) Download page
Profile Name: VPN Client to Site
Version : v6.4.0
If installation does not begin in 60 seconds or if your browser does not support 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)

Bước 2: Xả file nén và chạy file cài đặt Installer.exe đã tải về.



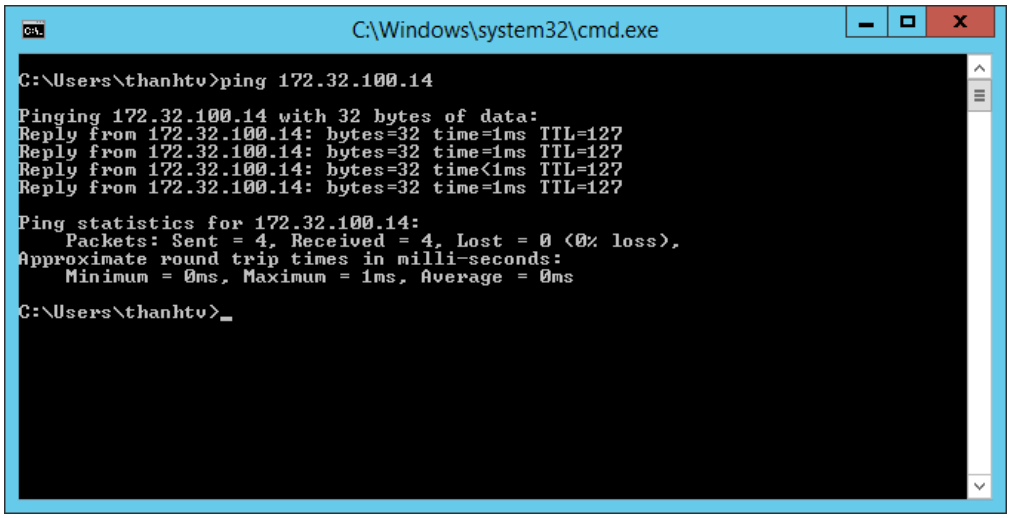
Bước 3: Thực thi ứng dụng SSL VPN-Plus Client trên màn hình Desktop. Nhấn nút login trên giao diện và nhập tài khoản VPN đã tạo ở các bước trên.





Kết nối thành công:

Kiểm tra bằng cách ping thành công đến ip local của máy chủ trên hệ thống Cloud của USDC Technology.

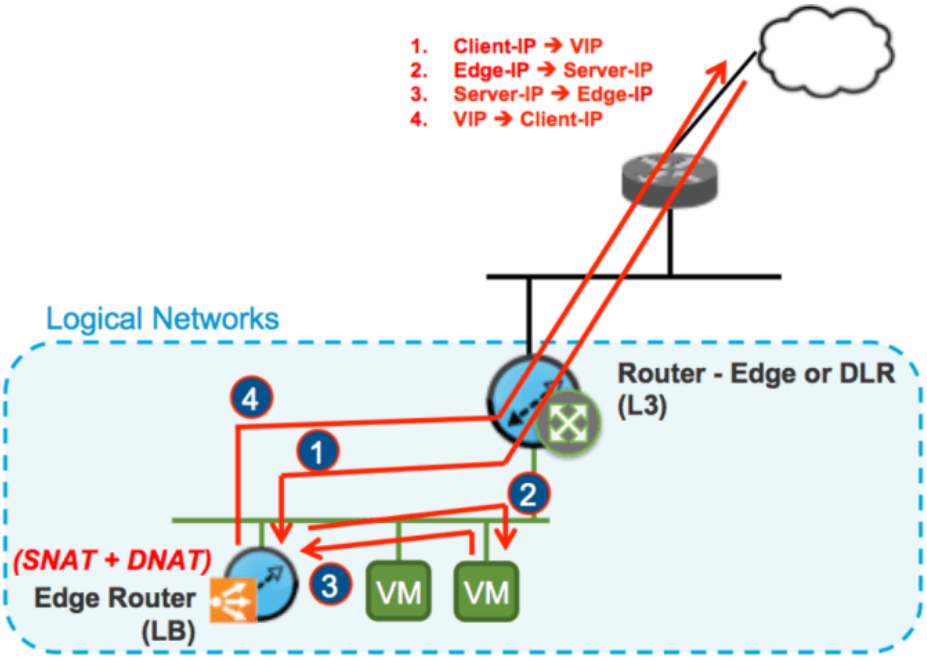


Lưu ý: mỗi tài khoản chỉ được đăng nhập sử dụng trên 1 máy, để tạo tài khoản cho người dùng tham khảo các bước cài đặt ở trên.

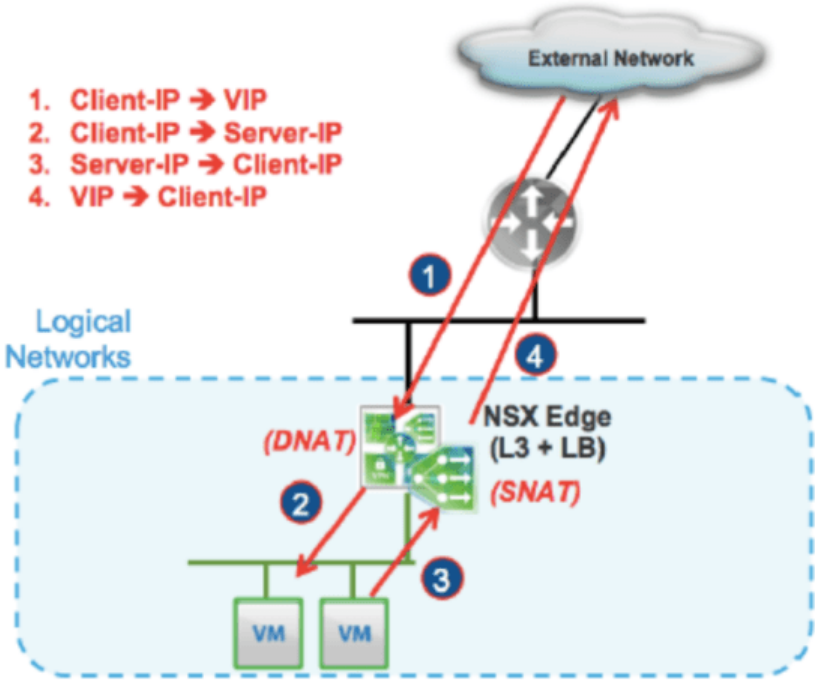
III. Dịch vụ vLoad Balancer

Với dịch vụ vLoad Balancer(vLB) của USDC Technology, Quý khách có thể triển khai theo cả 2 mô hình: *Proxy mode* và *transparent mode*.

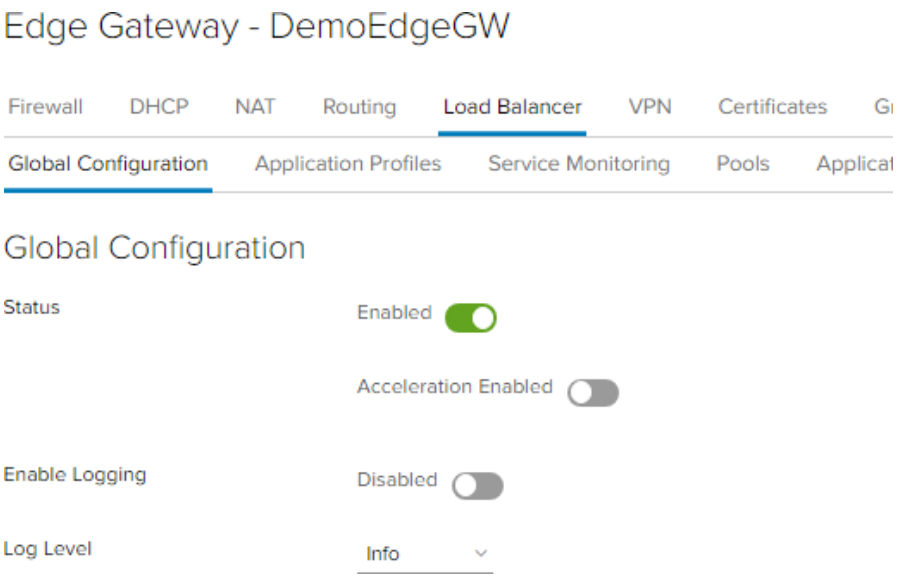
Trong mô hình Proxy mode, vLB đóng vai trò làm reverse proxy tương tự nginx.



Còn với mô hình transparent mode, vLB đóng vai trò trong suốt với traffic của người dùng:



Trước hết chúng ta cần enable dịch vụ vLB lên bằng cách chọn tab **Load Balancer -> Global Configuration** -> check chọn vào mục **Enable Status** -> nhấn **"Save Changes"**



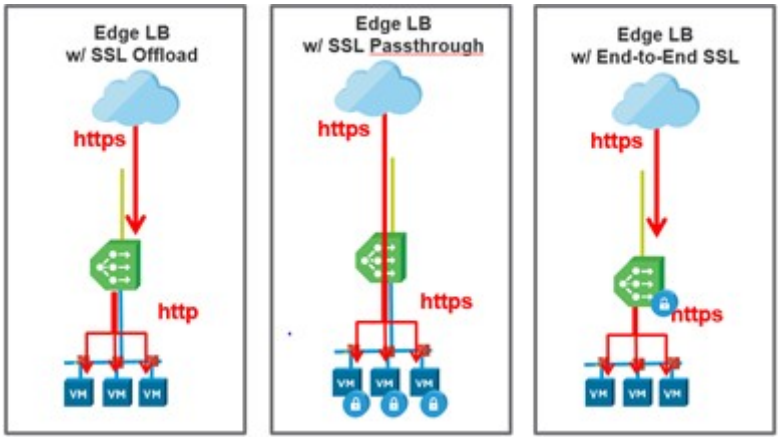
Quá trình khởi tạo, cấu hình vLB được thực hiện qua các bước như sau:

1. **Import chứng chỉ (certificate)**

***Ghi chú**: Trường hợp bạn muốn triển khai Website với giao thức HTTPS có Certificate hợp lệ và muốn chạy tương thích với vLB thì cần thực hiện bước này. Ngược lại (chạy giao thức*

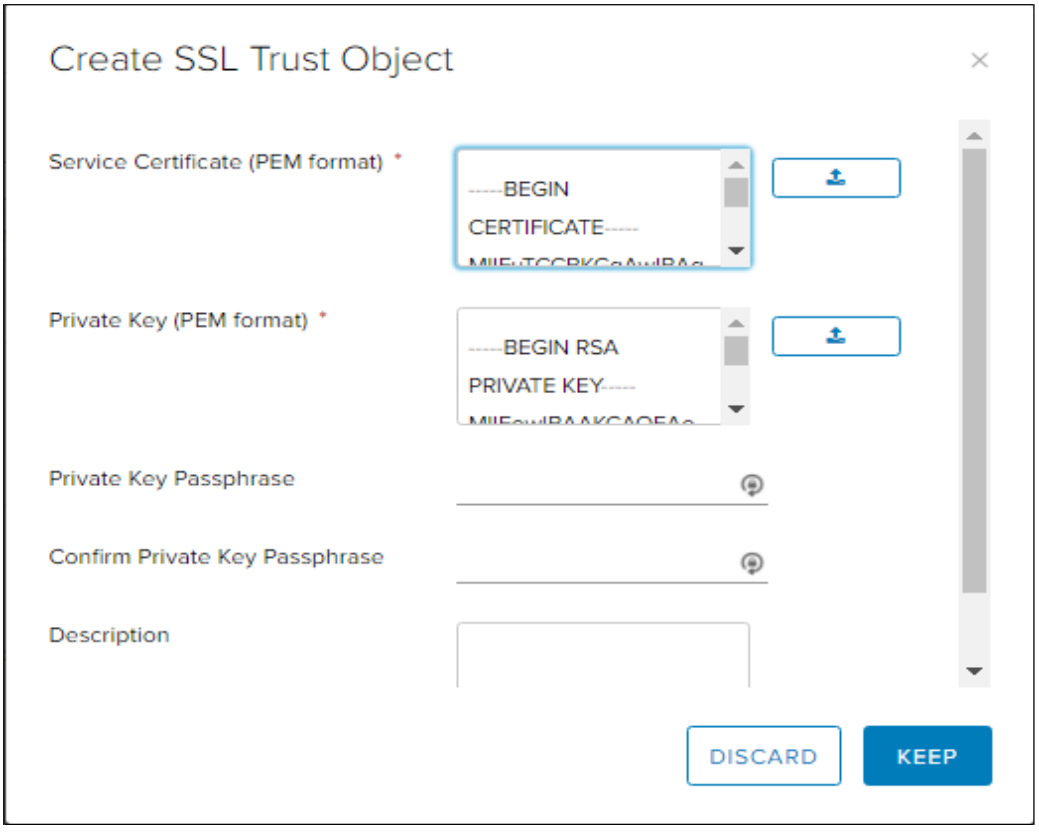
HTTP thông thường hoặc mô hình SSL Passthrough) thì không cần thực hiện bước này.

Với HTTPS chạy SSL, vLB tương thích với cả 3 mô hình triển khai: SSL Offload, SSL Passthrough và End-to-End SSL.

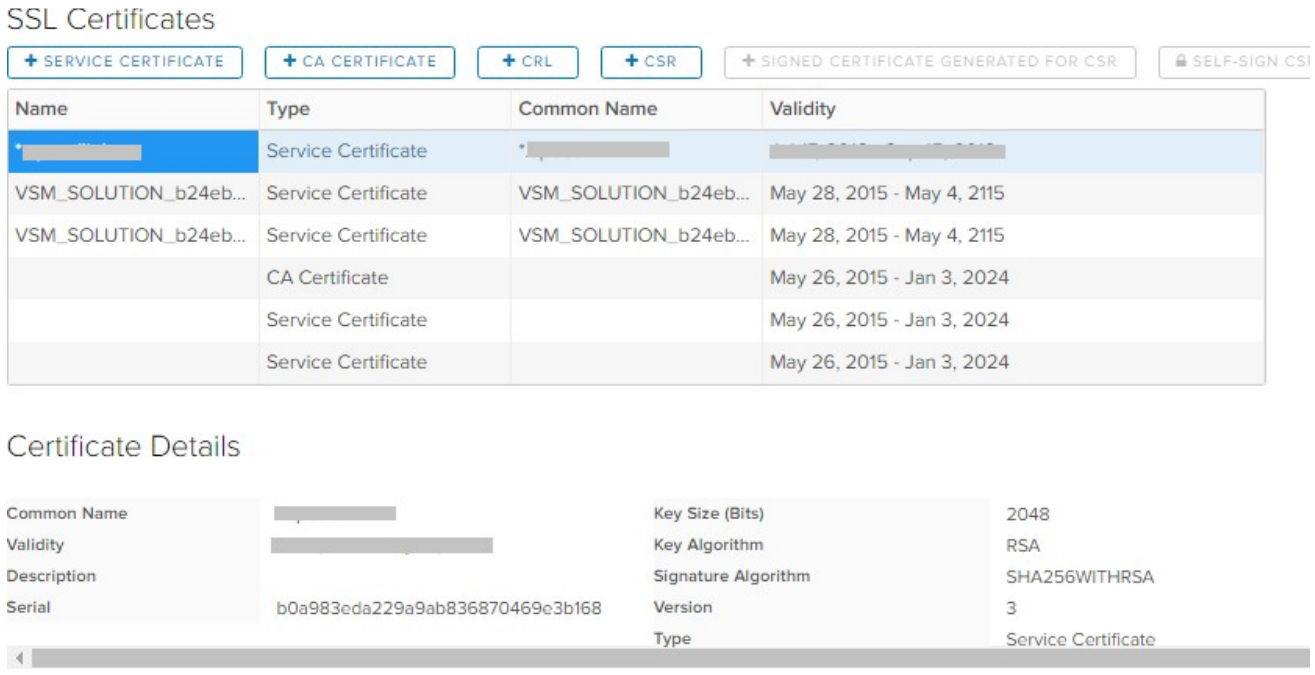


Để import certificate sẵn có, chọn tab **Certificates** -> nhấn chọn nút + SERVICE CERTIFICATE

Cửa sổ Create SSL Trust Object hiện ra, nhấn chọn nút upload và trỏ đường dẫn đến các file .crt và .pri tương ứng với mục Service Certificate và Private Key. Sau đó nhấn **Keep** để lưu lại cấu hình.



Certificate mới được import sẽ hiện ra trong danh sách:



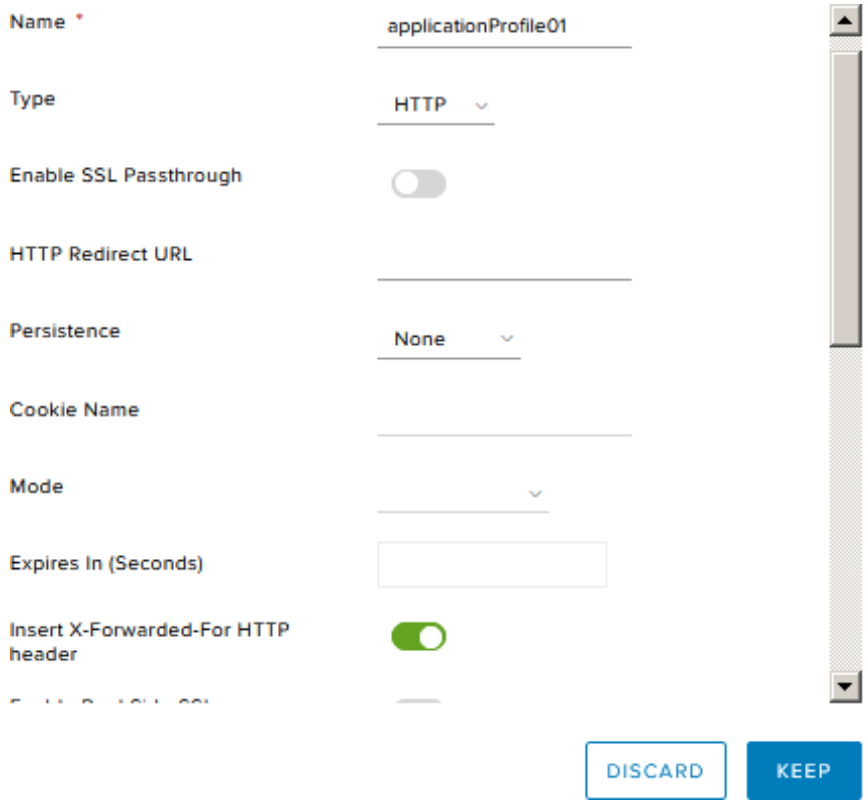
2. Application Profiles

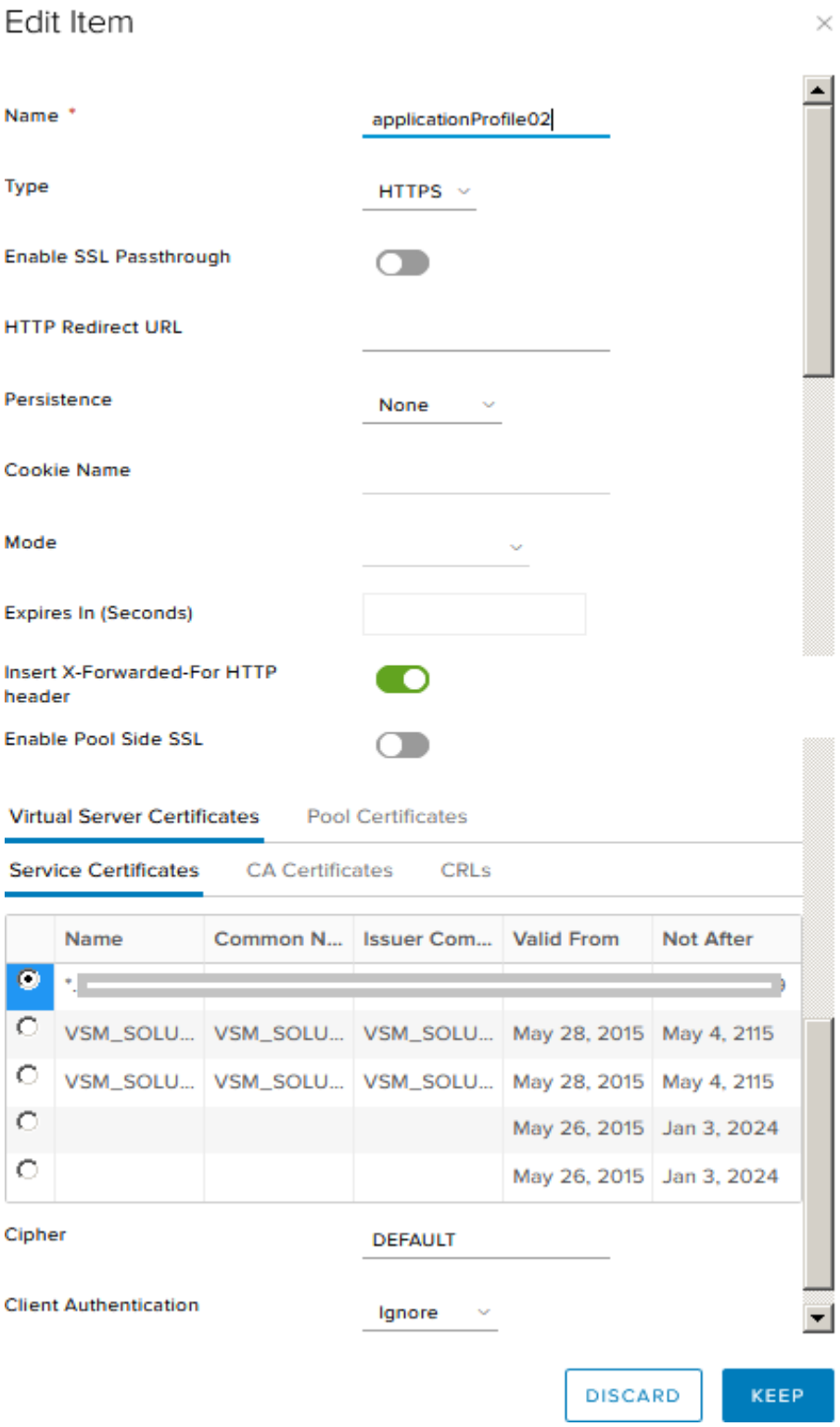
Để tạo Application Profile chọn tab **Load Balancer -> Application Profiles**, nhấn chọn nút

. Các thông số lưu ý:

- **Name**: đặt tên cho Profile
- **Type**: kiểu giao thức, hỗ trợ HTTP, HTTPS, TCP, UDP
- **Enable SSL Passthrough**: chạy vLB ở mô hình SSL Passthrough
- **Persistence:** hỗ trợ 3 mode: source IP, cookie và none
- **Insert X-Forwarded-For HTTP header**: thêm header X-Forward-For HTTP (để dùng trong 1 số tình huống như nhận diện IP thực của client).
- **Virtual Server Certificates**: chọn certificate đã import ở bước 1. Trường hợp này chỉ dùng được nếu trường type ở trên chọn HTTPS.

Hình dưới minh họa tạo Application Profile cho 2 giao thức HTTP và HTTPS:

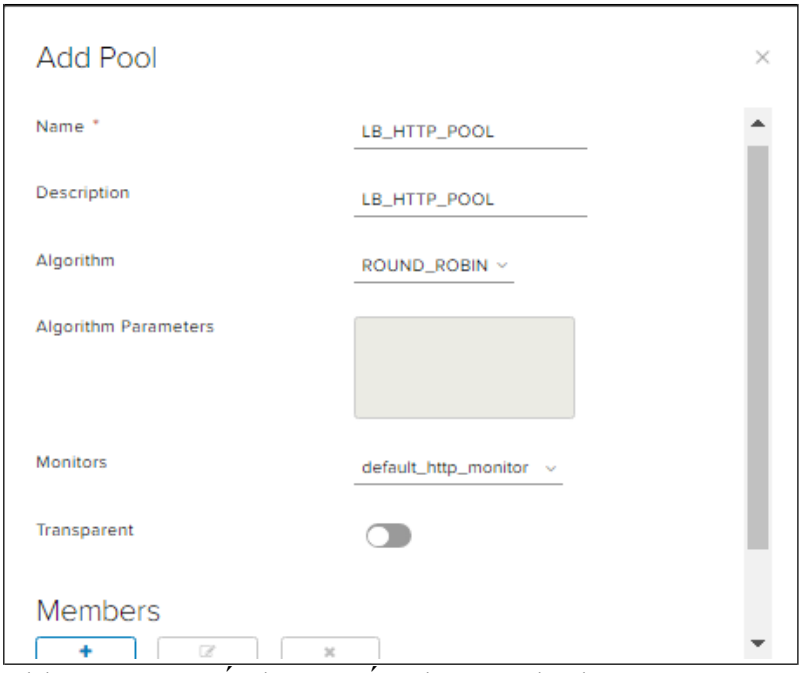



Edit Item
Name *
applicationProfile02
Type
HTTPS
Enable SSL Passthrough
HTTP Redirect URL
Persistence
None
Cookie Name
Mode
Expires In (Seconds)
Insert X-Forwarded-For HTTP header
Enable Pool Side SSL
Virtual Server Certificates
Pool Certificates
Service Certificates
CA Certificates
CRLs
Name
Common N...
Issuer Com...
Valid From
Not After
VSM_SOLU...
May 28, 2015
May 4, 2115
May 26, 2015
Jan 3, 2024
Cipher
DEFAULT
Client Authentication
Ignore
DISCARD
KEEP

3. Server Pool

Chọn tab **Load Balancer -> Pools**, nhấn vào biểu tượng Add, nhập các thông số sau:

- **Name và Description**: nhập tên và mô tả cho Pool
- **Algorithm:** thường sử dụng 2 thuật toán sau để điều phối traffic xuống các server lớp dưới: *Round Robin* (xoay vòng) hoặc *Least connected* (chọn server ít kết nối đến hơn).
- **Monitors:** chọn Service monitor, mặc định hệ thống sẵn có default_http_monitor, default_https_monitor và default_tcp_monitor tương ứng với 3 giao thức HTTP, HTTPS và TCP. Với giao thức HTTP và HTTPS, mặc định monitor này sử dụng phương thức GET đến URL gốc ("/"). Bạn có thể định nghĩa các monitor này tại tab Service Monitor.

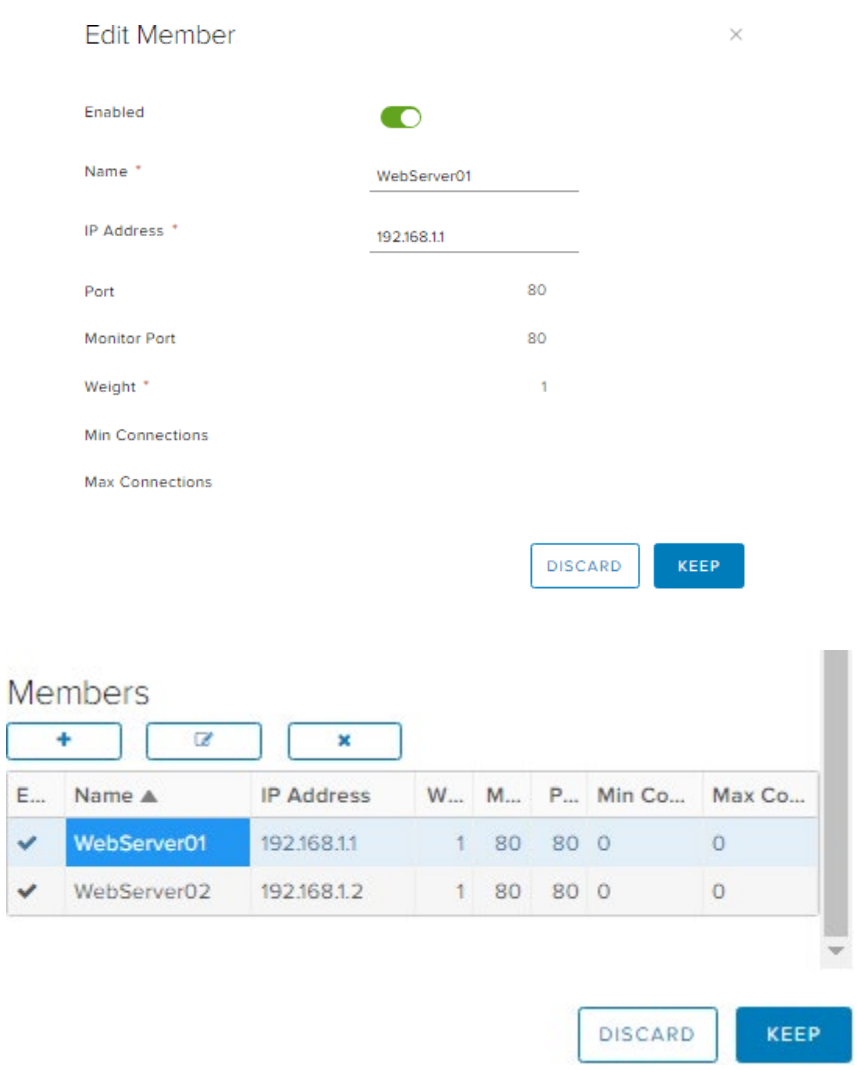


- **Transparent:** enable mục này nếu bạn muốn chạy mô hình *Transparent mode*.

Tại mục Member, chọn biểu tượng Add và cấu hình lần lượt các Web Server lớp dưới:

- **Name**: Tên, VD: WebServer01
- **IP Address**: địa chỉ IP private của server
- **Port**: cổng dịch vụ tương ứng, VD: 80, 443
- **Monitor Port:** cổng giám sát (để phát hiện trạng thái up/down của server)
- **Weight**: trọng số ưu tiên.

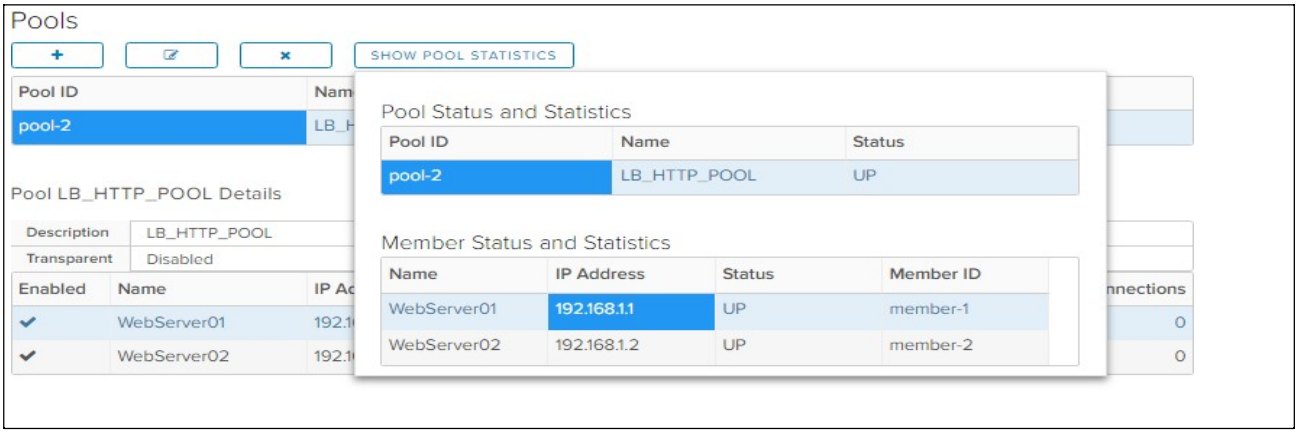
Nhấn **Keep** sau khi nhập xong thông số.



2 member được tạo nằm trong pool LB_HTTP_POOL:

Nhấn **Keep** để khởi tạo server pool.

Sau khi khởi tạo xong, chúng ta có thể kiểm tra trạng thái của Pool và các server trong Pool bằng cách nhấn chọn **Show Pool Statistics**:

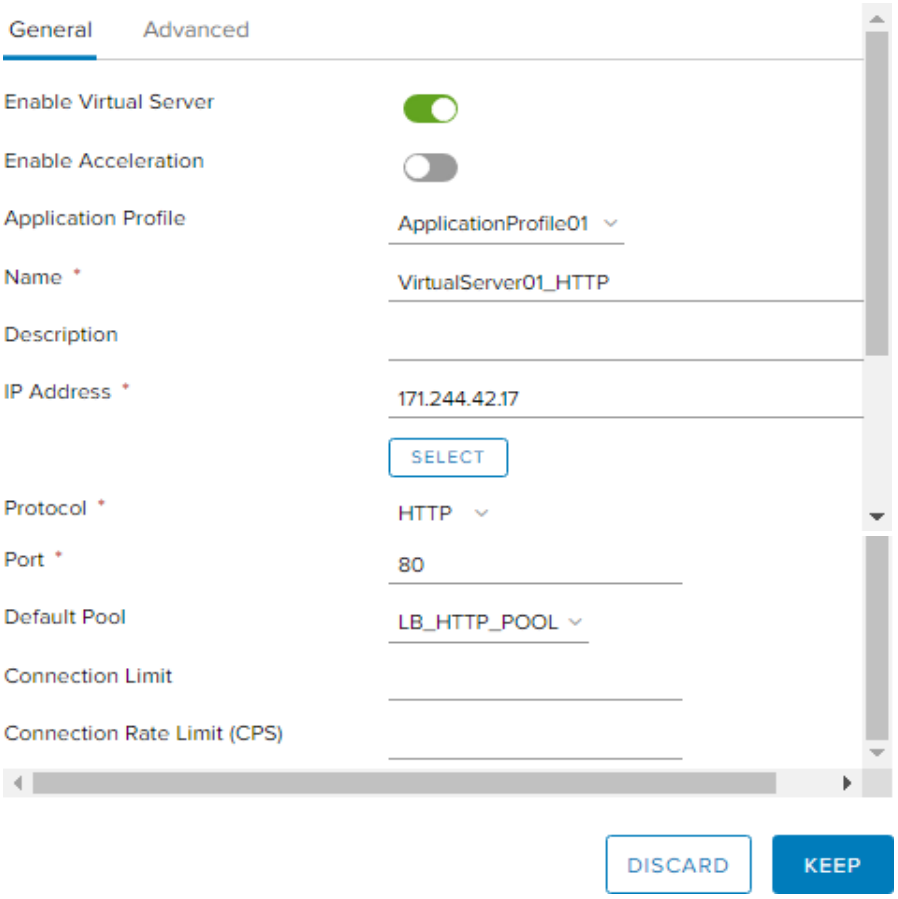


4. Virtual Server

Đây là bước cuối cùng để thiết lập vLoad Balancer. Chọn tab Virtual Servers sau đó nhấn biểu tượng thêm mới [+]. Các thông số cần thiết lập như sau:

- **Enable Virtual Server:** cho phép thực thi Virtual Server
- **Application Profile**: chọn Application Profile tương ứng đã tạo ở Bước 2. Lưu ý chọn đúng với giao thức (HTTP, HTTPS..) mong muốn.
- **Name**: đặt tên
- **IP Address**: nhấn tiếp Select và chọn Public Master IP đã lấy được ở Mục II trong tài liệu này.
- **Protocol và Port**: chọn giao thức và port lắng nghe kết nối của client
- **Default Pool**: chọn Pool đã tạo ở Bước 3.

Nhấn **Keep** để lưu lại cấu hình thông số.

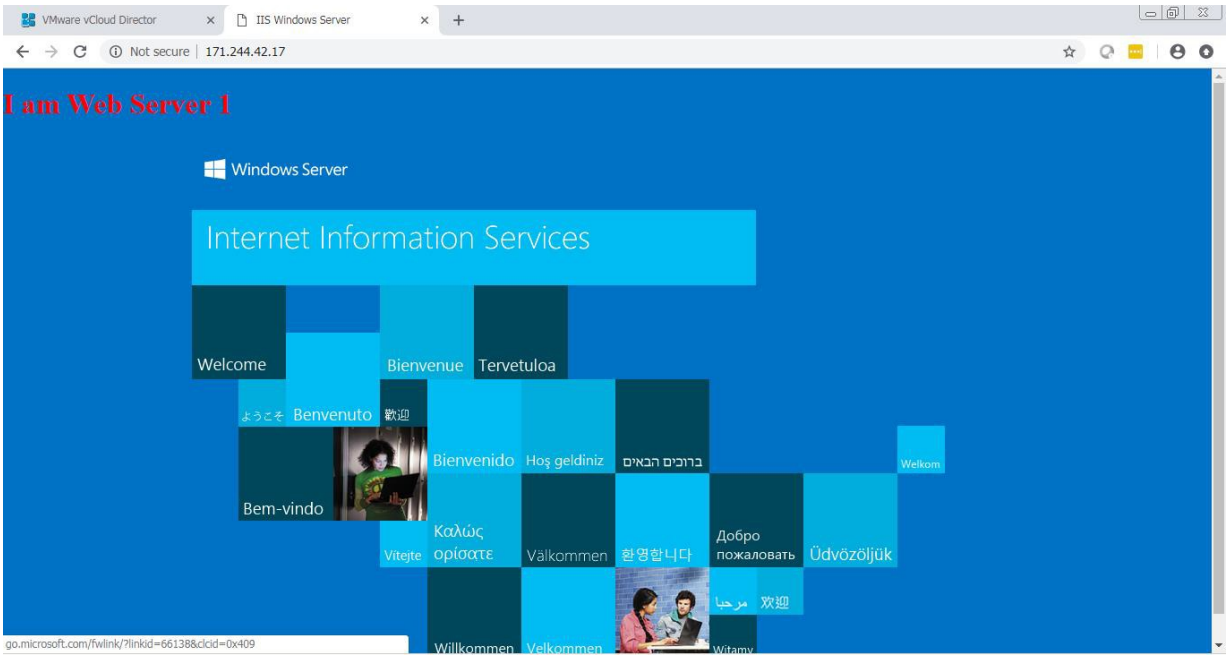


Lưu ý: tới đây quá trình cấu hình vLB cơ bản đã xong, bạn có thể cần phải tạo Firewall Rule để cho phép người dùng truy cập đến Public IP của Virtual Server đã tạo ở trên.

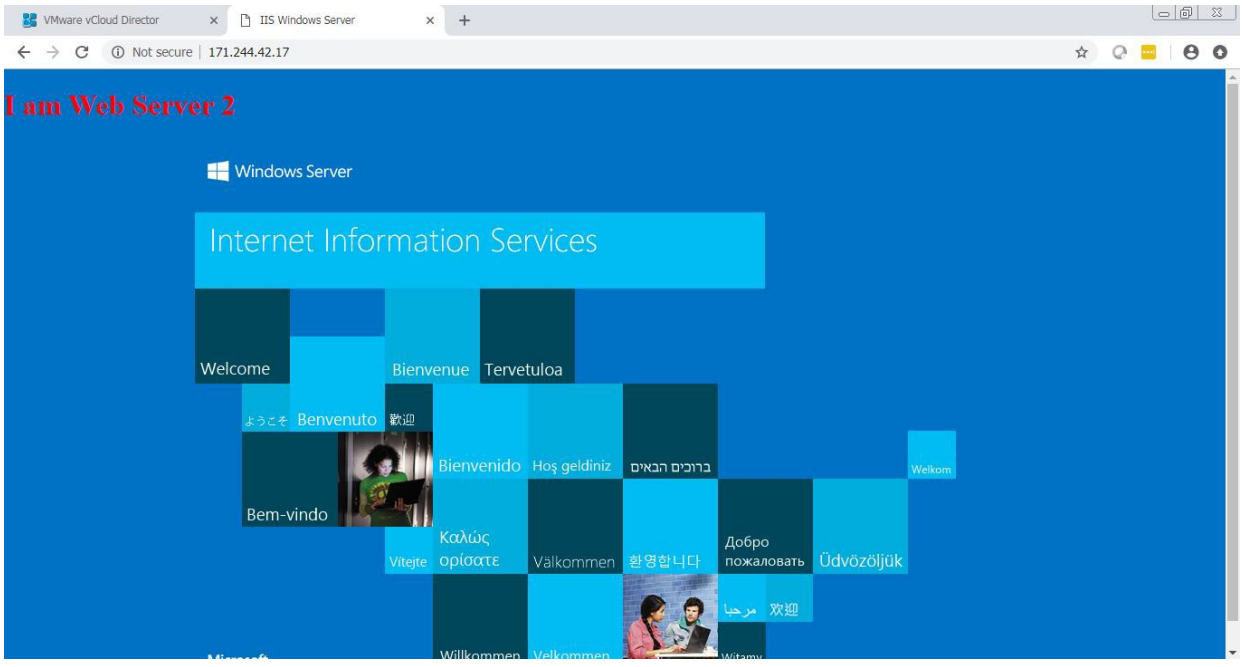
5. Test – Kiểm tra dịch vụ

Truy cập đếnVIP của vLB ở trên với mode Round Robin:

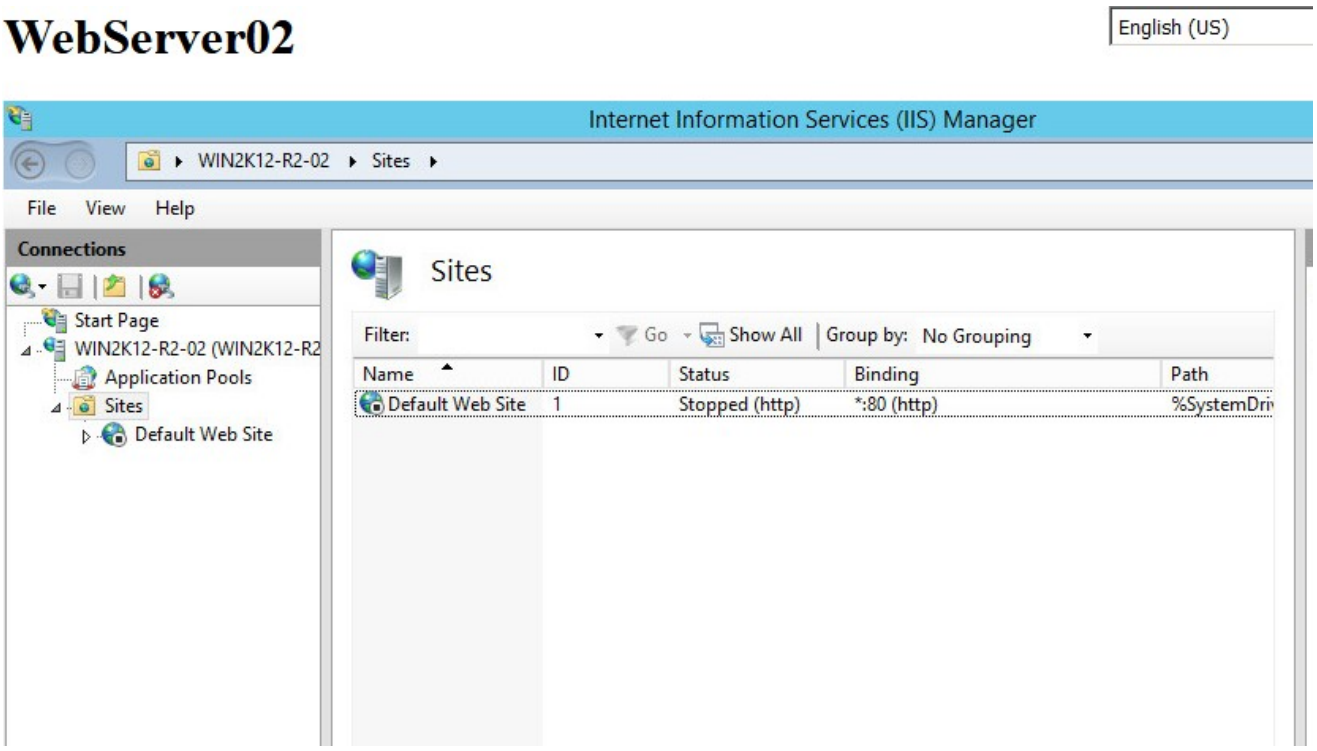
Truy cập lần thứ 1:



Truy cập lần thứ 2: Web Server thứ 2 sẽ phục vụ traffic:

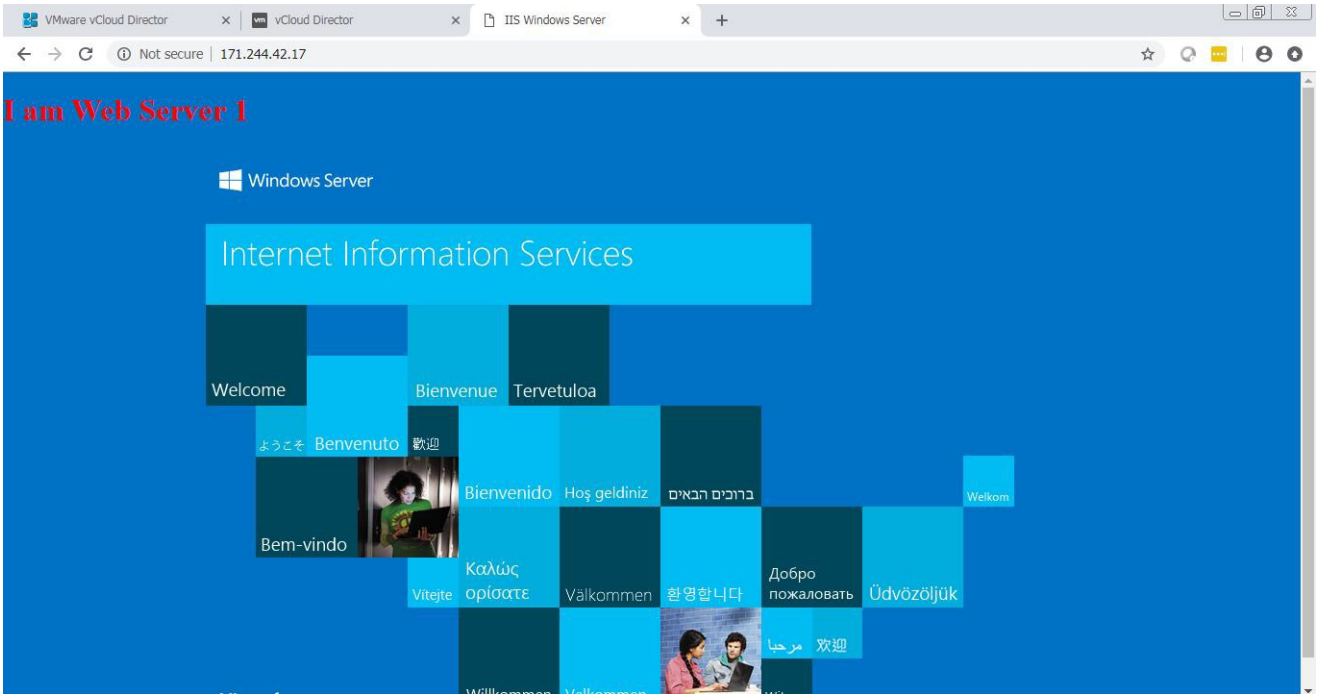


Tiến hành giả lập tắt service IIS trên Web Server 02:



Ngay lập tức vLB nhận diện và chuyển trạng thái WebServer 02 trong pool sang down:

Web Server 01 lúc này đóng vai trò đáp ứng traffic duy nhất cho người dùng:



Qua hướng dẫn vừa rồi, Quý khách đã được trải nghiệm các bước khởi tạo và cấu hình dịch vụ vFirewall và vLoad Balancer của USDC Technology.

Mọi thắc mắc liên quan đến dịch vụ Quý Khách vui lòng liên hệ số hotline **(028) 7308 0708** hoặc trang support ticket tại https://portal.usdcvn hoặc gửi email đến địa chỉ **support@usdc.vn**

Trân trọng cảm ơn.

-HẾT-