

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VCLLOUD SERVER	Lần ban hành: 1

1. MỤC ĐÍCH

Mục đích của tài liệu là hướng dẫn khách hàng sử dụng dịch vụ vCloud Server - một trong những dịch vụ chính của Viettel IDC nhằm đảm bảo chất lượng, sự hài lòng tốt nhất của khách hàng.

2. PHẠM VI

Tài liệu này được áp dụng cho dịch vụ vCloud Server và dùng cho khách hàng sử dụng dịch vụ.

3. HƯỚNG DẪN SỬ DỤNG PORTAL VCLLOUD SERVER

3.1 Đăng nhập vào hệ thống

vCloud Portal là cổng giao diện dùng để quản trị dịch vụ vCloud Server của Viettel IDC, giúp thực hiện các thao tác cơ bản như Power off, suspend, reset, tạo snapshot, kiểm tra thông số cấu hình (CPU, Memory, Disk, Network...), biểu đồ hiệu suất sử dụng tương ứng của máy chủ ảo cũng như các tác vụ liên quan đến quản lý user, cấu hình vFirewall, vLoad Balancer... Giao diện Tenant Portal dùng HTML5 với nhiều tính năng mới và thân thiện với người dùng.

Để truy cập vào trang quản lý dịch vụ, Khách hàng đăng nhập vào đường dẫn và tài khoản đã được cung cấp.

Cú pháp đường dẫn link đăng nhập:

Cụm Miền Bắc (TTDL Hòa Lạc)

- Dịch vụ vCloud Server:

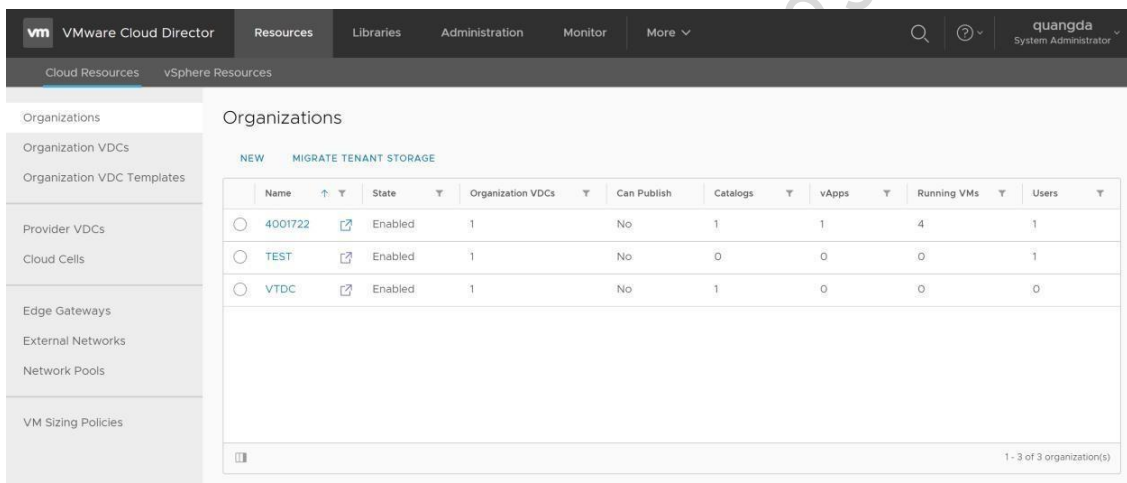
[https://cloud.viettelidc.com.vn/tenant/\[Organization name\]](https://cloud.viettelidc.com.vn/tenant/[Organization name]) Cụm Miền Nam (TTDL Bình Dương)

- Dịch vụ vCloud Server:

[https://cloud2.viettelidc.com.vn/tenant/\[Organization name\]](https://cloud2.viettelidc.com.vn/tenant/[Organization name]) Với [Organization name] là Tên mã của Khách hàng trên hệ thống

Theo giải pháp điện toán đám mây của Viettel IDC, mỗi Khách hàng sẽ được phân tách thành các chủ thể riêng biệt thường được gọi là Organization hoặc Tenant. Tài nguyên được tổ chức thành các Trung tâm dữ liệu ảo (Virtual DataCenter) riêng biệt cho từng Khách hàng với đủ các thành phần: Compute (tính toán), Storage(lưu trữ) và Network (mạng) được gắn vào các Máy chủ ảo (VM).

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VCLLOUD SERVER	Lần ban hành: 1

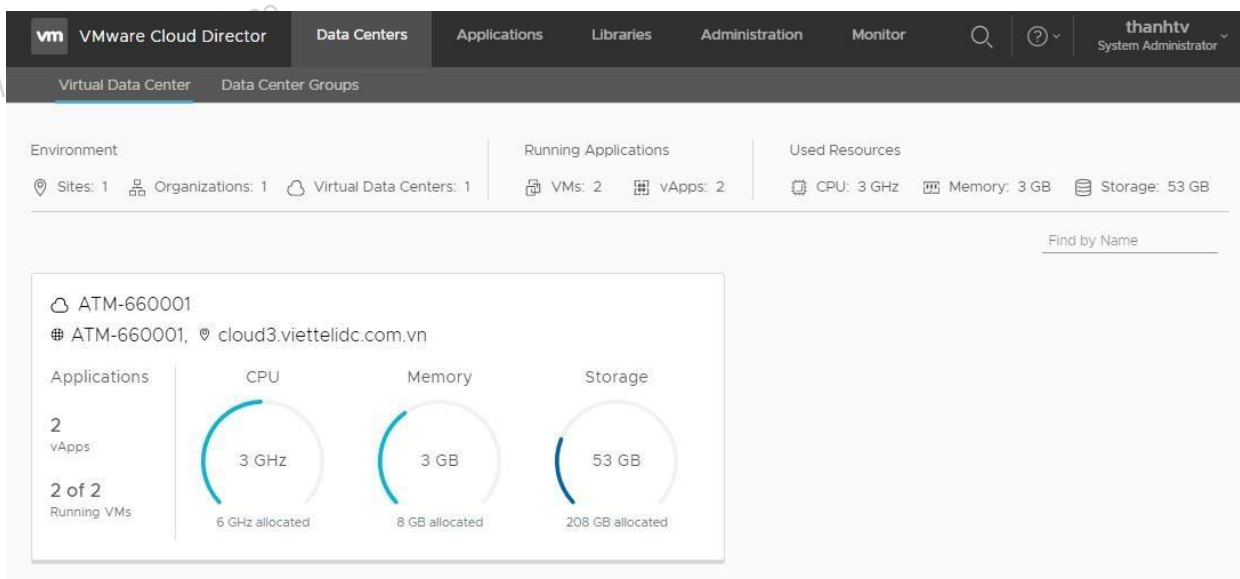


The screenshot shows the VMware Cloud Director interface. The top navigation bar includes 'Resources', 'Libraries', 'Administration', 'Monitor', and 'More'. The left sidebar lists various resource types like Organizations, Organization VDCs, and Provider VDCs. The main content area displays a table of Organizations.

Name	State	Organization VDCs	Can Publish	Catalogs	vApps	Running VMs	Users
4001722	Enabled	1	No	1	1	4	1
TEST	Enabled	1	No	0	0	0	1
VTDC	Enabled	1	No	1	0	0	0

3.2 Kiểm tra thông tin trạng thái

Sau khi đăng nhập thành công, từ màn hình quản trị chính Khách hàng có thể xem được các thông số tổng quát trong Datacenter ảo: Site, vApp, VM, tài nguyên cấp phát, tài nguyên đã dùng...



The screenshot shows the VMware Cloud Director interface for a specific Data Center. The top navigation bar includes 'Data Centers', 'Applications', 'Libraries', 'Administration', and 'Monitor'. The left sidebar lists various resource types like Environment, Running Applications, and Used Resources. The main content area displays a summary of the Data Center's resources and usage.

Environment	Running Applications	Used Resources
Sites: 1 Organizations: 1 Virtual Data Centers: 1	VMs: 2 vApps: 2	CPU: 3 GHz Memory: 3 GB Storage: 53 GB

Find by Name

ATM-660001
cloud3.viettelidc.com.vn

Applications	CPU	Memory	Storage
2 vApps 2 of 2 Running VMs	3 GHz 6 GHz allocated	3 GB 8 GB allocated	53 GB 208 GB allocated

Nhấn vào Datacenter của Khách hàng và để xem thông tin về các máy chủ ảo đang có. Có thể chọn biểu tượng tìm kiếm và nhập tên máy để tìm nhanh Server.

- Để xem thông tin chi tiết của VM: Tên, HĐH đang sử dụng, trạng thái của server, thông tin về phần cứng RAM, CPU (Compute), HDD, network... nhấn vào VM tương ứng:
- Để xem thông tin và danh sách vApp, chọn vApp trong menu Compute bên trái:

Kiểm tra danh sách và trạng thái các network:

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

Kiểm tra trạng thái Edge Gateway (trong trường hợp Khách khách có thuê dịch vụ vFirewall, vLoad Balancer):

3.3 Thao tác trên máy chủ ảo

Tại màn hình chính, chọn menu Virtual Machines, chọn VM cần thao tác và nhấn nút Actions.

Gồm các thao tác chính sau:

- Power on: mở lại máy chủ (đang ở trạng thái power off trước đó).
- Power on and Force Recustomization: mở máy và thực thi tự động các thuộc tính Guest Customize cho Hệ điều hành (computer name, change SID, mật khẩu admin,...). Thông số này được cấu hình trong phần Guest OS Customization của VM (chọn nút Details).
- Power off: tắt máy chủ.
- Shutdown Guest OS: gọi lệnh shutdown hệ điều hành (cần có Vmware tools).
- Reset: reset cứng lại máy chủ ảo.
- Suspend: tạm dừng máy chủ (tương tự trạng thái sleep trên Windows)
- Copy To: Clone (nhân bản) VM. VM phải ở trạng thái Power off và không chứa bản snapshot. Move To: chuyển VM sang vApp khác
- Change Owner: chuyển quyền sở hữu cho User khác trong Org của Khách hàng.
- Launch Web console: console vào VM bằng trình duyệt web
- Create Snapshot: tạo bản snapshot (chỉ lưu 1 bản duy nhất). Khách hàng

cần mua bổ sung dung lượng lưu trữ (tổng bằng dung lượng HDD + dung lượng RAM-để lưu swap file). Lưu ý: khuyến nghị không nên lưu snapshot quá lâu(>3 ngày). Nếu có nhu cầu bản dự phòng thời gian dài có thể sử dụng dịch vụ Backup Cloud server.

- Revert to Snapshot: phục hồi bản snapshot đã tạo trước đó.
- Remove Snapshot: Xóa bản snapshot đã tạo trước đó.
- Insert media: chèn các file ISO cài đặt Hệ điều hành, đĩa khởi động.
- Eject media: nhả file ISO đã insert trước đó.
- Install Vmware Tools: khởi động chế độ cài đặt Vmware tool. Hệ thống sẽ tự động chèn file cài đặt vào thành các ổ media bên trong Hệ điều hành. Khách hàng cần console vào và làm theo các bước hướng dẫn.

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ V-CLOUD SERVER	Lần ban hành: 1

Viettel IDC có sẵn thư viện file ISO nguồn cài đặt các Hệ điều hành và các ứng dụng/appliance (SQL Server, Pfsense, Sophos...), tiện ích(Hiren Boot, Gparted CD...) phổ biến. Quý khách có thể lọc theo trường Name để tìm kiếm nhanh hơn và vui lòng tham khảo “Hướng dẫn tự cài đặt lại Hệ điều hành cho Máy chủ từ vCloud Portal”.

Lưu ý: Trong trường hợp Quý khách tự cài mới lại Hệ điều hành cho Máy chủ ảo, vui lòng cài đặt thêm ứng dụng Vmware Tool hoặc Open-VM-Tools để đảm bảo tính tương thích, hiệu suất và các tính năng trên hệ thống được hoạt động ổn định.

3.4 Console

Khách hàng có thể console trực tiếp vào màn hình của máy chủ ảo thông qua trình duyệt Web hoặc VM Remote Console (cần cài ứng dụng VMware Remote Console- VMRC trên máy client).

- Launch Web Console: console vào màn hình máy chủ qua giao diện Web Console.
- Launch VM Remote Console: Truy cập Server bằng VM Remote Console.
- Download VMRC: Tải tiện ích VMware Remote Console.

3.5 Snapshot

Trong trường hợp có thuê dung lượng lưu trữ cho Snapshot, Khách hàng có thể sử dụng chức năng này để tạo ảnh chụp cho máy chủ. Lưu ý: hệ thống chủ lưu 1 bản snapshot duy nhất, việc tạo mới sẽ ghi đè lên bản snapshot cũ.

- Create Snapshot: tạo bản Snapshot
- Revert to Snapshot: Phục hồi lại bản Snapshot đã tạo trước đó.
- Remove Snapshot: Xóa Snapshot.

3.6 Hướng dẫn quản lý User

Để thêm/xóa/sửa user đăng nhập sử dụng vCloud Portal của Quý Khách, từ giao diện quản trị chọn menu Administration -> Users

Để tạo mới User, chọn nút New:

- Nhập tên và mật khẩu vào ô Username, Password và các thông tin cá nhân trong mục Contact Info.
- Chọn quyền trong mục Role. Thông thường chọn quyền cao nhất là: Organization Administrator.
- Chọn Unlimited trong phần Quotas

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

Cuối cùng nhấn Save để lưu lại thay đổi.

Để chỉnh sửa chọn nút Edit và xóa chọn Disable-Delete tương ứng.

3.7 Hướng dẫn khởi động lại máy chủ

Chức năng reset trên trang quản trị Cloud Server còn là chức năng reset server khi server treo hoặc gặp sự cố. Ngoài cách thông thường truy cập vào server và thực hiện reset, ta còn thể reset bằng cách truy cập vào trang quản trị Cloud Server và thực hiện reset server.

Vào Datacenter - Compute, phần Virtual Machines.

Click vào biểu tượng VM cần Reset. Chọn Reset

3.8 Hướng dẫn tắt máy chủ

Ngoài việc thực hiện Power Off (hay còn gọi là Shutdown server) trong hệ điều hành. Còn có thể sử dụng chức năng Power Off để thực hiện Shutdown server.

Vào Datacenter - Compute, phần Virtual Machines.

Click vào biểu tượng VM cần tắt. Chọn Power Off.

Lưu ý: Ngoài việc shutdown server bằng Power Off, ta vẫn có thể sử dụng Shut Down Guest OS.

3.9 Hướng dẫn tạm dừng máy chủ

Suspend là chức năng để tạm dừng dịch vụ. Có thể so sánh chức năng này giống như Sleep trong windows. Khi Resume lại VM thì trạng thái trước khi suspend sẽ được giữ trạng thái trước khi tạm dừng.

Vào Datacenter - Compute, phần Virtual Machine.

Click vào biểu tượng tại VM cần tạm dừng. Chọn Suspend.

Lưu ý: Sau khi tiến hành Suspend, muốn resume lại server ta làm như sau: Vào Datacenter - Compute, phần Virtual Machine.

Click vào biểu tượng tại VM cần resume. Chọn Power On.

3.10 Hướng dẫn reset mật khẩu admin của Hệ điều hành

Để thực hiện thao tác này, Hệ điều hành của Máy chủ ảo cần được cài đặt ứng dụng Vmware tools trên Windows hoặc gói Open-vm-tools trong các hệ điều hành Linux. Đồng thời chỉ các Hệ điều hành phổ biến sau tương thích với tính năng Guest customization này:

- Windows Server 2008 R2, 2012 R2, 2016, 2019
- CentOS/ Red Hat Enterprise Linux 6.x -> 8.x
- Ubuntu 14.04, 16.04, 18.04

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

Bước 1: từ màn hình quản trị VM, chọn tab Guest OS Customization -> Edit để thực hiện Reset password cho user Administrator/Root

Bước 2:

- Enable guest customization: Cho phép thay đổi thông số bên trong Hệ điều hành, cần chọn để các tính năng phía dưới có hiệu lực.
- Allow local administrator password: Thay đổi password đăng nhập của user administrator.
- Chọn Require Administrator to change password on first login nếu muốn thay đổi password admin lần đăng nhập đầu tiên.
- Nhập mật khẩu mới vào ô Specify password

Các thao tác bên dưới sẽ hiệu lực trong lần đầu Máy chủ được mở hoặc khi quản trị viên nhấn chọn Power on and force recustomization. Để thực thi các thay đổi, cần power off VM và dùng lệnh Power on and force recustomization. Hoặc cách đơn giản Khách hàng có thể thực hiện tự động thông qua tính năng “Đổi mật khẩu” trên giao diện Cổng thông tin dịch vụ tự động (Automation).

3.11 Biểu đồ hiệu suất tài nguyên của VM

vCloud Portal cung cấp sẵn tính năng xem biểu đồ hiệu suất tài nguyên (CPU, memory, Disk, network) cơ bản cho toàn bộ VM. Từ giao diện quản trị truy cập menu Datacenters -> Virtual Machines, click chọn VM cần xem biểu đồ hiệu suất tài nguyên và tìm đến mục Monitoring Chart:

Sau đó chọn chỉ số (metric) và chu kỳ (Period) cần theo dõi. Hiện gói hỗ trợ các chu kỳ ½ Hour, Hour, Day, Week.

Tổng cộng có 12 chỉ số Khách hàng có thể theo dõi:

Chỉ số	Mô tả
cpu.usage.average	CPU usage (average) as a percentage during the interval
cpu.usage.maximum	CPU usage(maximum) as a percentage during the interval
cpu.usagemhz.average	CPU usage in megahertz during the interval
disk.provisioned.latest	Amount of storage set aside for use by a datastore or a virtual machine
disk.read.average	Average number of kilobytes read from the disk each second during the collection interval
disk.used.latest	Amount of space actually used by the virtual machine or the datastore

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ V-CLOUD SERVER	Lần ban hành: 1

disk.write.average	Average number of kilobytes written to disk each second during the collection interval
mem.usage.average	Memory usage as percentage of total configured or available memory
net.bytesRx.average	Average amount of data received per second
net.bytesTx.average	Average amount of data transmitted per second
disk.numberReadAveraged.average	Average number of read commands (IOPS) issued per second to the virtual disk during the collection interval

Lưu ý: Các biểu đồ hiệu suất này được giám sát ở lớp hạ tầng, các chỉ số giám sát chi tiết hơn cho lớp hệ điều hành và ứng dụng, Khách hàng có thể sử dụng các công cụ giám sát chuyên dụng được cài đặt bên trong Hệ điều hành.

3.12 Kiểm tra sự kiện tác động trên hệ thống

Sử dụng khi khách hàng cần kiểm tra các vấn đề, sự kiện và các thông tin tác động trực tiếp vào hệ thống máy chủ.

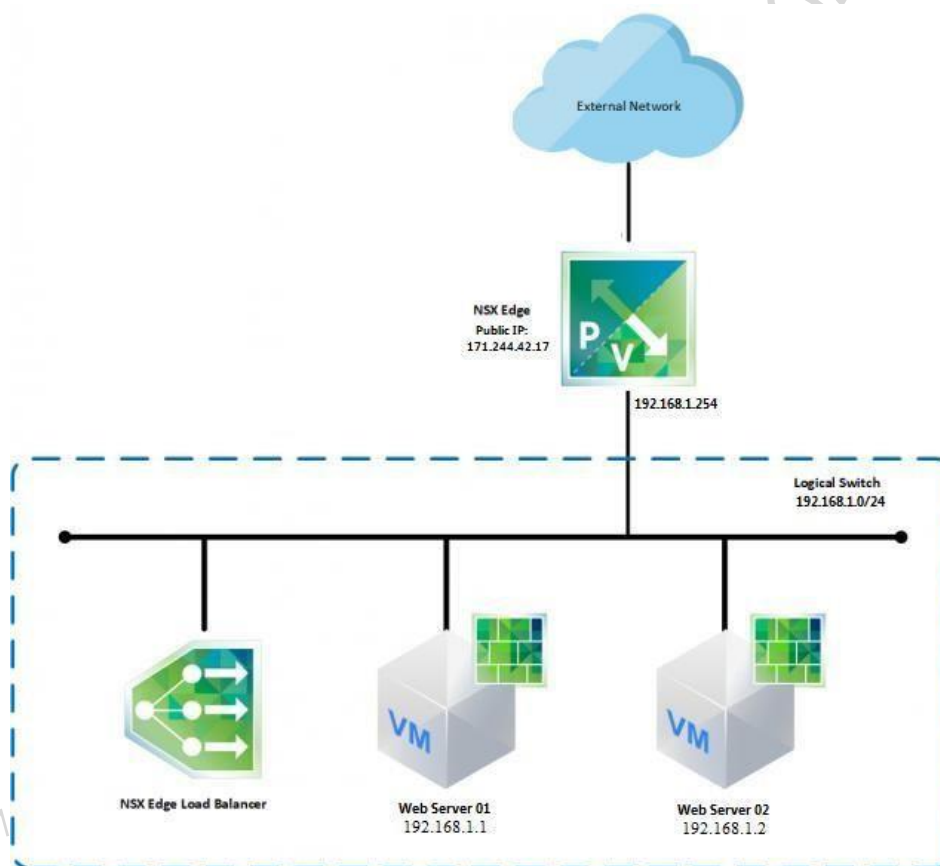
Vào Tab Monitor Task và Events

4. Hướng dẫn cấu hình dịch vụ vFirewall, vLoad Balancer

vFirewall và vLoad Balancer là 2 dịch vụ gia tăng (addon) dựa trên giải pháp của VMWare cung cấp trên nền tảng dịch vụ vCloud Server của Viettel IDC.

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

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1



		Private Zone	Public Zone	Mode
NSX Edge	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	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).

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

☐ Để xem được thông tin Master IP và NAT IP theo mô hình cần thực hiện ở Mục I, chúng ta thực hiện như sau:

Từ giao diện quản trị Org VDC của Khách hàng, nhấn chọn Edge Gateway tại mục Data Center -> Networking -> Edges

IP tại mục IP Setting là Master IP:

Tại mục IP Allocations là NAT IP cho VM:

4.1 Cấu hình Network Address Translation (NAT)

Từ màn hình quản trị trong Org VDC Khách hàng, bấm Data Center -> Networking -> Edges. Check chọn vFirewall và nhấn Services

Màn hình cấu hình Edge Gateway hiện ra, chọn 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 Viettel IDC 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 tương ứng với hình thức NAT mà bạn muốn tạo:

☐ SNAT

- 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

- 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)

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VCLOUD SERVER	Lần ban hành: 1

- 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.

4.2 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 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:

Ý nghĩa:

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ V-CLOUD SERVER	Lần ban hành: 1

- 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:

4.3 Cấu hình IPsec VPN Site to Site

Trong gói dịch vụ vFirewall của Viettel IDC 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.

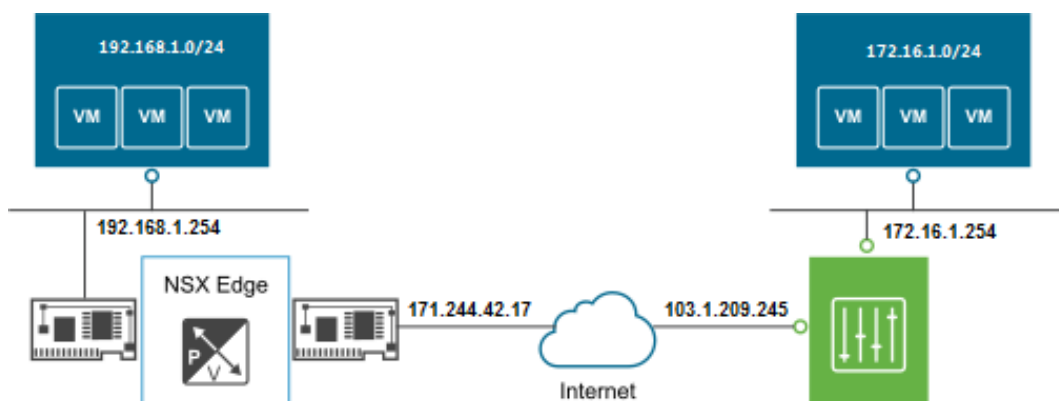
- Enabled: cho phép hoặc vô hiệu thực thi phiên VPN.
- Enable perfect forward secrecy (PFS): cho phép chạy mode PFS để tăng tính bảo mật (khuyến nghị nên dùng).
- Name: tên phiên kết nối VPN
- Local Id và Local Endpoint: điền địa chỉ Public Master IP của vFirewall. Trường hợp mô hình giả lập là 171.244.42.17
- 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

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VCLOUD SERVER	Lần ban hành: 1

- 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 Viettel IDC như sau:

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

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

Lưu ý: các thông số: 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 Viettel IDC.

4.4 Dịch vụ vLoad Balancer

Với dịch vụ vLoad Balancer(vLB) của Viettel IDC, 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:

4.4.1 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  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:

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

4.4.2 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.

4.4.3 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.

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

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:

4.4.4 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 các hướng dẫn trên.
- 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:

4.4.5 Test – Kiểm tra dịch vụ

Truy cập đến VIP 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:

5. An toàn thông tin

Các máy chủ Viettel IDC cung cấp cho khách hàng đã được đảm bảo các chính sách an toàn thông tin và được cập nhật bản vá lỗi hồng định kỳ:

- Cài đặt hệ điều hành mới nhất và cập nhật bản vá. Với mỗi phiên bản hệ điều hành Windows Server, yêu cầu nâng cấp lên bản Service Pack mới nhất. (Chỉ cài đặt các bản vá security).
- Đối với các hệ thống mới sử dụng hệ điều hành Windows Server, yêu cầu cài đặt phiên bản Windows Server 2008 R2 Service Pack 2 trở lên.
- Thiết lập chính sách tài khoản.
- Xóa hoặc disable tất cả các tài khoản không sử dụng trên hệ thống.

	VINA AI RACE	Public 619
	TÀI LIỆU HƯỚNG DẪN KHÁCH HÀNG DỊCH VỤ VPCLOUD SERVER	Lần ban hành: 1

- Thiết lập chính sách mật khẩu mạnh. (8 ký tự, có chữ thường, chữ hoa, ký tự đặc biệt).
- Enable tường lửa mềm.
- Thiết lập các phân vùng được định dạng NTFS.
- Thiết lập đồng bộ thời gian cho hệ điều hành.
- Cấu hình time Zone (UTC+7:00 Bangkok, HaNoi, Jakarta)
- Cấu hình NTP Server (Default là times.windows.com)
- Enable Remote Desktop, SSH.

6. Mã hóa dữ liệu

Dữ liệu của khách hàng được lưu tại hệ thống lưu trữ của Viettel IDC. Các dữ liệu của khách hàng chưa được mã hóa do vậy khách hàng cần tự xử lý và cấu hình trên máy chủ của khách hàng. (Tham chiếu tài liệu Hướng dẫn mã hóa dữ liệu hệ điều hành Windows và Hướng dẫn mã hóa dữ liệu hệ điều hành Linux).

7. Máy chủ đồng bộ thời gian

Các máy chủ Viettel IDC cung cấp cho khách hàng đã cấu hình timezone, NTP default:

- Cấu hình time Zone (UTC+7:00 Bangkok, HaNoi, Jakarta).
- Cấu hình NTP Server (Default là times.windows.com).

Ngoài ra Viettel IDC cung cấp cho các khách hàng máy chủ NTP như sau:

- NTP Server 01: 115.84.177.8

8. Vi phạm bản quyền phần mềm

Bản quyền phần mềm được quy định trong hợp đồng ký kết với khách hàng. Khi khách hàng có yêu cầu, thắc mắc về bản quyền xin vui lòng liên hệ theo hotline: 18008000 hoặc gửi email tới địa chỉ support@viettelidc.com.vn.