

Managed Private Cloud - User Guide

4

Version 1.0, July 2024

Contents

Μ	anaged	Private Cloud - User Guide1
1.	Intro	duction3
2.	Con	cepts4
	2.1	Equinix Customer Portal and Managed Solutions Portal
	2.2	Operational Console4
	2.3	Organization4
	2.4	Organization Virtual Datacenter (OVDC)5
	2.5	Tenant Roles5
	2.5.1	Tenant Admin5
	2.5.2	Tenant User5
	2.5.3	Tenant Viewer6
3.	Onb	oarding7
4.	Use	Management and SSO8
	4.1	User Management8
	4.2	Login To The Operational Console
	4.3	Using a Different Identity Source9
	4.4	API Access 10
	4.4.1	Terraform Automation10
	4.4.2	API Tokens10
	4.4.3	Service Accounts12
	4.4.4	API Explorer 14
5.	Use	of the Operational Console15
	5.1	VAPP15
	5.1.1	Create a new vApp15
	5.2	Virtual Machines16
	5.2.1	Creating a virtual machine16
	5.2.2	Link installation media from catalog to a VM 18
	5.2.3	VM Console
	5.2.4	Shapshots
	5.3	
	5.3.1	Creating a catalog
	533	Create a vAnn Template 23
	5.3.4	Shared Catalogs
	5.4	Connectivity
	5.5	Networks
	5.5 1	MPC Gateway Firewall Architecture 25
	5.5.2	How to create an isolated OVDC network
	5.5.3	How to create a touted OVDC network







5.5.4	How to create Gateway Firewall Rules	
5.5.5	How to create NAT rules	41
5.5.6	How to configure IPsec VPN	
5.5.7	How to create OVDC Distributed Firewall	Rules50
Other docu	mentations	56
Where to f	ind Service Description?	56
Where to f	ind EMS policy?	56
Where to f	ind official VMware documentation?	56
How to ask	for help	





1. Introduction

Welcome to Managed Private Cloud (MPC), the Infrastructure as a Service platform of Equinix Managed Solutions. MPC is using the Operational Console to control and manage your resources like vApps, virtual machines and networks.

This quick start guide explains how to access the MPC Operational Console and manage your organization user accounts. Next to that it will give you guidelines and best practices for controling your IT environment with the functions available.

Please refer to MPC Service Description for a full list of features and information.



Figure 1 Overview MPC





2. Concepts

To gain a good understanding of the names and terms used later on in in this document, they will be explained first.

2.1 Equinix Customer Portal and Managed Solutions Portal

The Equinix Customer Portal (ECP) is the portal where the user management for the users who need access to the Operational console is performed. Part of the ECP is the Managed Solutions Portal (MSP) where you can raise tickets, services requests and get insights in the usage of the MPC service. On the ECP you will find the Product page where you can access the Operational Console.

2.2 Operational Console

The Operational Console is the portal where all the tasks for managing your MPC environment can be performed. The Operational Console gives you access to MPC in a certain region, MPC has four Regions, e.g. South America, North America, Europe and Asia. If you have an MPC in a specific region, the Operational Console will be accessable via one of the four buttons on the page.

MANAGED SOLUT	IONS PORTAL	Orange Services Ltd.	• 4 3 00
😵 🏘 Services 🛩 Orders & Tickets	✓ Administration ✓ Trial ✓ Docume	ints	
My Environment / Services / Manage Your Services / N	Kanaged Private Cloud		
🚖 Managed Private Cloud			
North America	South America	Europe Asia	
Operational Console 😢	Operational Console 😢	Operational Console	
Equinix Managed Private Clou Solw-your cloud challenges with our fielding MF is an information and a solution of the solution	sd isolable and secure Managed Private Cloud (MPC) servic atomn offering compute, storage and networking resou	а. 19	
managed through the MPC console.			
0.2	023 Equinix, Inc. All rights reserved. Equinix Customer	Portal Terms of Use Privacy Statement Contact Us	

2.3 Organization

An Organization (Org) defines the customer within the Operational Console. The Org can be viewed as a container that groups together all MPC resources like virtual datacenters (compute, storage, networking) users and libraries located in a MPC region.

The name of the Org is needed when logging into the MPC Operational Console. Use the Org name when this quick start guide mentions "<organization name>".





2.4 Organization Virtual Datacenter (OVDC)

Customer compute, storage and networking resources are grouped in a Organizational Virtual Datacenter (OVDC). A customer can have multiple OVDC's with different characteristics such as the geographic location of an Equinix IBX (Amsterdam, London or Ashburn) or with different compute performance. If the existing capacity is not sufficient, you can contact your Service Delivery Manager or Account Manager.

2.5 Tenant Roles

In the Operational Console, three pre-defined roles have been defined that can be assigned to users

- Tenant Admin
- Tenant User
- Tenant Viewer

When Equinix performs the initial deployment for a new MPC customer, the first user that is configured is the customer administrator account. This account is created by Equinix during the onboarding process and is based on the name and email provided by the customer.

The first customer administrator account added is automatically added to the "Tenant Admin" group. Being a member of this group assigns the account all the permissions in the Operational Console.

2.5.1 Tenant Admin

Permissions:

- Access VM Console
- Create and delete Snapshots
- Create and delete personal API Tokens
- Create, change and delete Organization wide Service Accounts
- Create, change and delete VMs in tenant scope
- Create, change and delete vApp's in tenant scope
- Create, change and delete Networks in tenant scope
- Create, change and delete Content Libraries and Content in tenant scope
- Configure Edge Gateways in tenant scope
- Set Affinity Rules
- View Tasks and Event Logs in tenant scope

2.5.2 Tenant User

The Tenant User rol permissions:

- Access VM Console
- Create and Delete Snapshots
- Create and delete personal API Tokens
- Start / Stop VM in tenant scope
- Start / Stop vApp in tenant scope
- Update VM Tools in tenant scope
- View Tasks and Event Logs in tenant scope





2.5.3 Tenant Viewer

The Tenant Viewer rol permissions:

- View everything the Tenant-User can, except for:
 - No VM and vApp Create / Change / Update / Delete (CRUD) permissions
 - No Console Access





3. Onboarding

During the MPC onboarding process you receive the following information:

- Organization name
- One or more customer accounts with one of the above roles assigned
- The ordered compute, storage and networking resources that are provisioned to one or more Organization Virtual Datacenters (OVDC), according to the design
- Information about the connectivity to Internet, Cloud Service Providers, Colocation and/or WAN providers



Figure 2: Example of MPC environment after onboarding





4. User Management and SSO

4.1 User Management

Users of the Operational Console are managed at the ECP, you can find the documentation on User Management and Password management at the following link.



Once the users have been added to the ECP customer can raise a Service Request to assign a MPC Tenant role to the new user. Use the <u>link</u> to find the userguide for raising a service request in the Managed Solutions Portal.

4.2 Login To The Operational Console

When logged into the ECP you navigate to the product page via the Managed Solutions Portal/ Services/ Managed Private Cloud from here you can login to the Operational Console in the region of your choice.









When you access direct from the URL of the Operational Console and click "Sign In", you will be redirected to ECP where you can enter your ECP credentials.



4.3 Using a Different Identity Source

In the ECP you can configure federation to your own identity provider so you can use your company credentials to login to the Operational Console, you can find the instructions about federation at <u>docs.equinix.com</u>





4.4 API Access

Access to the MPC Operational Console API is mainly needed for programmatic access or automation purposes. Examples of automation tools which can be used are: Terraform, Ansible, Python or just plain XML / JSON based calls.

For authentication to the API, customers need to generate an access tokens within the Operational Console, which supports two access methodes each serving a different purpose.

METHOD	INTENDED USE	
API TOKENS	API access to the Operational Console on behalf of ECP Federated user accounts for personal programmatic access	or
	 Can be configured by all ECP or Federated user accounts 	
SERVICE ACCOUNTS	 API access to the Operational Console based on standald accounts that are intended for Organization wide automation a third-party applications / tools 	ne Ind
	Can only be configured by members of the Tenant-Admin role	
	 Can be assigned one of the supported roles 	
	Only supports API access	

4.4.1 Terraform Automation

Terraform is the preferred infrastructure as code tool that lets you define both cloud and on-prem resources in human-readable configuration files that you can version, reuse, and share. You can then use a consistent workflow to provision and manage all of your infrastructure throughout its lifecycle. Terraform can manage low-level components like compute, storage, and networking resources.

Most of the functions in the Operation Console are available via the API or via Terraform. You can find the Terraform documentation at the Terraform website:

https://www.terraform.io/docs/providers/vcd/index.html

4.4.2 API Tokens

API Tokens can be configured by every ECP or Federated user account in the Operational Console.

To configure the personal API Token:

1: Login to the Operational Console and access the "User preferences" in the top right menu.

Q	?~	Sector Sector
		User preferences Change Password
편 Memory: OMB		Log out





2: Go to the API Token section and click "New"

API Tokens			
Name	↑ Туре	Expires On	
		7	
	No toke	ns found.	
Manage Columns			

3: Give token a suitable name and click "Create"

Create General Token						
Create a general token f	or the current user.					
Client Name *	API Token for XYZ					
	DISCARD	E				

4: The API Token is generated. Make sure to store the token in a safe place. After closing this screen, the token cannot be viewed anymore from the Operational Console and must be re-generated.

Create General Token	\times					
⊘ Your token was generated successfully.						
(1) Make sure to store the refresh token in a safe place where you can access it. Once you close this dialog, you will not be able to retrieve this token again.						
v6wwK9UbgJrU						
ок						

5: When the token is created, it's visible in the Operational Console and can be removed when needed.

Туре	Expires On
General	-
	Type General



4.4.3 Service Accounts

Service Accounts can be created / viewed an deleted by members of the "Tenant-Admin" roles only due to the sensitive nature of these accounts.

Note: The Service Account will be the owner of its created objects in the Operational Console.

To configure a Service Account:

1: Login to the Operational Console and access the "Service Accounts" option in the "Administration" section and click "New".

🌔 Managed Private	Cloud	Data C	enters	Applicat	tions Networking	Content Hul	b Libraries	Administration	Monitor	Q	:
	«	Service	e Acc	ounts							
咨 Access Control	~	NEW	REVIE	W ACCE	SS REQUESTS						
Groups			Name	↑ τ	Role	Status	Software ID			Client UR	9
Service Accounts											
E Certificate Managem Certificates Library	~										

2: Give the Service Account a suitable name, assign a role and use the magic wand to generate unique ID. Click "Next" to continue.

New Service Account	General			
1 General	Name *	SA-Automation-XYZ		-
2 Quotas	Assign Role *	Tenant-Admin Select a role	~]
3 Review and Complete	Software ID *	471a4036		<i>:</i> //•
	Software Version			
	Client URI			-

3: Optional: Assign quota's to the Service Acount one or more types of limits.

Quotas			
ADD	REMOVE		
Nam	e	Quotas	
0	✓ All VMs quota	1	0 Uni
	CPU quota Memory quota		
	Number of Tanzu Kubernetes clu Running VMs quota	usters	1 Quota Resources
	ADD Nam	Quotas ADD REMOVE Name V All VMs quota CPU quota Memory quota Number of Tanzu Kubernetes clu Running VMs quota Storage quota	Quotas ADD REMOVE Vame Quotas Vali VMs quota CPU quota Memory quota Number of Tanzu Kubernetes clusters Running VMs quota Storage quota



New Service Account	Review and Complete	
1 General	General	
2 Quotas	Name	SA-Automation-XYZ
1 dubias	Role	Tenant-Admin
3 Review and Complete	Software ID	471a4036-100 0016c02463e6f
1	Software Version	
	Client URI	
	Quotas	
	No quotas have been assigned.	
		CANCEL PREVIOUS FINISH

5: After the Service Account is created, the API key can always viewed in the "Client ID" field when opening its properties. Most settings of the Service Account can be modified afterwards via the "Edit" option.

🌔 Managed Private	Cloud	Data Ce	nters Applic	ations Net	working	Content Hub	Libraries	Administration	Monitor	Q	:
	~	Service	Accounts	s							
答 Access Control	~	NEW	REVIEW ACC	ESS REQUES	TS	EDIT DELET	E				
Users			Name	^ -							
Groups					SA	-Automation	-XYZ			\times	
Service Accounts		• •	SA-Automatic	on-XYZ <							
Eg Certificate Managem	~				Ge	neral					
Certificates Library						Name	SA	-Automation-XYZ			
	~					Status	Cre	ated			
66 Resources	Ť					Role	Ter	nant-Admin			
Organizations						Software ID	471	a4036-	-Of6c02	463e6f	
Settings	~					Software Version					
General						Soltware version	-				
Email						Client ID	251	71f4f-	-71527087	'a1ba	
Guest Personalization							Ľ	GOPY			
Metadata						Client URI					
Multisite					Qu	iotas					
Policies					N	o quotas have bee	en assigned.				
Quotas											







4.4.4 API Explorer

To graphically view, test and execute API calls the API Explorer is accessible via the Operational Console.

1: Go to "API Explorer " in the top right menu under the "Help" section.

Monitor	Q	? ×	ORG-TEST
	API Explorer		
	Help	3C 1	
	Keyboard Shortcuts	36/	
	About	ж;	

2: The API Explorer provides access to the Swagger based JSON API on behalf of the logged-in user account.

\varTheta sv	wagger	/api-explorer/tenant/ORG-TEST/cloudapi.json	Explore
VMM [Base U /api-explor VMware 0 This ReST as descril	RL: /cloudapi] rer/tenant/ORG-TEST/cloudapi.json Cloud Director OpenAPI is a new fful API borrows some elements o bed below.	API that is defined using the OpenAPI standards. of the legacy VMware Cloud Director API and establishes new patterns for use	
	accessControls		
	GET /1.0.0/entitie	es/{objectId}/accessControls Get the access-control list for the specified vCD entity.	
	Get the access-control list for th	ne specified vCD entity.	
	Parameters	Try it out	
	Name	Description	
	<pre>objectid * required string (path)</pre>		
	page * required	Page to fetch, zero offset.	
	(query)	Default value: 1	
	pageSize • required	Results per page to fetch.	
	(query)	Default value: 25	
	Responses	Response content type application/json;version=38.1 🗸	
	Code Descrip	ption	
	200 <i>ok</i>		
	Example	e Value Model	
	C me rec rec rec rec rec rec rec rec rec re	ewittotal": 0, agcCant": 0, agcSiat": 0, gegSiat": 0, "entitylä" "string", "associationtä": "string") ("de: "string", "teamt": { "maamt": "string",	
	31	"ja"; "string", "grantype: "string", "objectid": "string", "accessievelid": "urn;vcloud:accessievel:xxxxxxxxxxxxxxxxxxxxx"))	





5. Use of the Operational Console

From the Operational console you can execute the actions to create VMs, networks and security rules below you will find topics related to applications, Virtual Machines, Snap shots and networking.

5.1 VAPP

A vApp is a set or group of virtual machines within the virtual data center, for example an application landscape. You can manage the machines as a set, for example taking a snapshot or restarting it. Of course it is also possible to manage the individual virtual machines as vApp. VMs and vApps can get a lease, that is, they are cleaned up automatically after a period of time, the default is set to never expire.

5.1.1 Create a new vApp

A vApp can initially be created with or without virtual machines. Creating a vApp without VMs is for example usefull if you want to create the network within the vApp before creating the virtual machines.

1: Go to the main page under Applications > vApps click on Build New vApp.

III Compute	~	vApps
vApps		
Virtual Machines		Find by: Name ADVANCED FILTERING
Affinity Rules		3 Virtual Applications Expired: No 🛞 Clear all filters
Networking	~	NEW ~
Networks		
Edges		III VAPP3 III VAPP2 III VAPP1
Storage	~	
Named Disks		Powered on Powered on Powered on Runtime lease Never Suspends @ Runtime lease Never Suspends @
Storage Policies		Created On 05/20/2024, 04:27:52 PM Created On 05/20/2024, 04:21:43 PM Created On 05/20/2024, 04:31:40 PM Owner system Owner system Owner system Owner system
Settings	~	VMs Manage VMs Manage VMs Manage 1 VM Consoles 2 VM Consoles 2 VM Consoles
General		
Metadata		CPUs Storage Memory Networks CPUs Storage Memory Networks 2 604 GB_0 4 GB - 4 612 GB_0 12 GB - 6 1.08 TB_0 10 GB -
Sharing		BADGES BADGES BADGES
Kubernetes Policies		ACTIONS Y DETAILS ACTIONS Y DETAILS ACTIONS Y DETAILS

Give a name and description to the vApp and click on build. Wait for the proces to finish.

New vApp				\times
Name *	vApp1			
Description	vApp1			
Power on				
Virtual Machines	os	Compute		
ADD VIRTUAL MACHINE				
			CANCEL	ATE





2: Options in the vApp window

- Click on power to turn on the vApp, shut it down, restart it or pause it. This will only work if there is a virtual machine in the vApp.
- Click on more to add or remove a VM to/from a vApp
- Click on details if you want to find or change additional information.

5.2 Virtual Machines

Virtual machines can be created in two ways, as part of a vApp or as a separate virtual machine. Equinix advices to create a VM always as part of a vApp, a vApp can contain up to 100 VMs. Afterwards a VM can always be moved to another vApp. It is also possible to create a network between two VMs in different vApps.

Advantages of creating a VM as part of a vApp are:

- The ability to group VMs for task, function or backup / archive retention.
- Configure the VM startup and shutdown sequence.
- Better insight into VM network configuration through vApp "Network diagram" function.
- Apply delegated management by granting rights.

The allocated storage resources and the amount of GBRam of a VM counts as used storage for the allocated Storage Policy. When you start a VM, the compute resource are subtracted from the compute quota of the OVDC.

When creating a new VM, the most common OS installation options are:

- 1. A new VM is created, after which an ISO file is chosen from the own private catalog (see 5.3 Catalogs), or from the shared Equinix catalog. When you turn on the VM, it starts from the ISO file and the installation can be started.
- 2. A new VM including vApp is created from an OVF / OVA file that exists at the administrator's workstation as part of the creation procedure.

5.2.1 Creating a virtual machine

1: Go to the main page under Applications > Virtual Machines click on Create VM or click on more at an vApp and choose Add VM.

III Compute	~	Virtual Machines
vApps		
Virtual Machines		Find by: Name Y ADVANCED FILTERING
Affinity Rules		5 Virtual Machines Expired: No 8 Clear all filters
Networking	~	NEW VM
Networks		

- 2: Follow the steps in the dialog and click on OK and wait for the creation of the VM.
 - a. Choose a name and computername and enter.
 - b. Choose New at Type.
 - c. Choose or the VM has to start directly after creation.
 - d. Choose OS family, Guest OS, Boot image
 - e. Boot option, EFI Secure Boot, enter Boot setup
 - f. Trusted Platform Module
 - g. Compute, CPU, cores, Memory
 - h. Storage, storage policy and size

Now VM		_
New VM		
iame •	vm1	
Computer Name *	vml	
Sescription		٦
fype	O New	
	O From Template	
Yower on		
Operating System		
Suest OS family *	Microsoft Windows	~
Avest U.S.	Microsoft Windows Server 2022 (64-64)	-
Soot image	SW_DVD9_Win_Server_STD_CORE_2019_1809.7_6488_English_DC_STD_MLF_X22-38323.iso	v
Poot Options		
Boot Firmware	EPI	~
Ti faarina Baat		
Cry and any block		
Enter Boot Setup		
Cocurity Davisos		
Trusted Platform Module		
	_	
Compute		
CPU	2 ~	-
Cores per socket	2 ~	,
Number of sockets	1	
Memory	8 08 0	-
Storage ADD		
Disk Sto	pe Policy IOPS Reservation Size	
1	HIGHPERFORMANCE-S-1 V Not Applicable '50 0 08 V	
M.	NOT APPROX ATOM	

i. Networking configuration

С	Network	Network Adapter Type		IP Mode		IP Address	IP Type	Primary NIC	
	None ~	VMXNET3	~	None	~	Auto-assigned	-	•	ŵ

3: In the Virtual Machines screen

- 1. Click Power to turn on, turn off, restart, or pause the VM. This is only possible if there are VMs in the vApp.
- 2. Click More to mount installation media, work with snapshots to open the console or to delete.
- 3. Click on View and / or change details or additional matters

Virtual Machines		Find by: Name	~		ADVANCED	FILTERIN	3
Affinity Rules		5 Virtual Machines	Expired: No 🗴 Clear	all filters			
Networking Networks	~	NEW VM					
Edges		VMDebian1		VMU	Jbuntu2		
🖹 Storage	~	Powered on VM Console		Powere VM Cor	d on Isole		
Named Disks		Runtime lease N	Never Suspends	Runtime	e lease N	ever Suspend	S (1)
Storage Policies		Owner s	system	Owner	sy	/stem	4.25:41 PM
Settings	~	Guest OS	/APP3 Debian GNU/Linux 12 (64-bit)	VApp Guest C	s U	APP2 buntu Linux ((64-bit)
General			Mamory Natworks		Storage	TT Memory	(Second second s
Metadata		2 604 GB	4 GB	2	206 GB ()	6 GB	()
Sharing			BADGES				BADGES
Kubernetes Policies		ACTIONS ~	DETAILS	ACTI	ONS ~	DETAIL	.S

5.2.2 Link installation media from catalog to a VM

If a catalog is already present and installation media has been uploaded, it can be linked to the VM.

1. Find the VM and click on More.

CTIONS - DETAILS	
Delete	
Edit Badges	
Сору	
Move	
Upgrade Virtual Hardware Version	
Install VMware Tools	
Media	>
VM Console	>
Snapshot	>
Power	>

2. Choose Insert Media and select the installation file, this is going to be connected as a virtual CD-player.

Insert CD			×
Select the media file to insert in the VM.			
Media available now:			
Name T	Catalog T	Owner T	Created On
Rocky-9.3-x86_64-dvd.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:27:56 P
ubuntu-20.04.6-live-server-amd64.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:33:44 P
SW_DVD9_Win_Server_STD_CORE_2019_1809.7_64Bit_English_DC_STD_MLF_X22-38323.i	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:31:12 PM
AlmaLinux-9.3-x86_64-dvd.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:22:31 PM
SW_DVD9_Win_Server_STD_CORE_2022_2108.11_64Bit_English_DC_STD_MLF_X23-17134.1	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:33:14 PM
debian-12.5.0-amd64-DVD-1.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:23:47 P
Rocky-8-latest-x86_64-dvd.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:26:10 PM
ubuntu-22.04.4-live-server-amd64.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:33:52 P
AlmaLinux-8.9-x86_64-dvd.iso	AM6-FLEX-1-OS-CATALO	system	5/22/2024, 12:16:46 PM
<			1-9 of 9 media
			1- 5 01 5 11 (010
Selected media:			
			CANCEL

3. As soon as the job is finished it is adviced to decouple the installation file via Eject Media

5.2.3 VM Console

A virtual machine can be managed via the Operational Console at any time. There are 2 different VM consoles:

- the Web Console which works from your browser.
- the VM Remote Console which requires installing a plug-in.

Using (installation) media (ISO) directly from your device to boot or install a VM is not possible. The media should first be uploaded to the catalog.

The VM Remote Console plug-in for Windows devices is available in the shared catalog. For MacOS and Linux (incl. Windows), VMRC functionality is respectively part of VMware Fusion Pro and Workstation Pro when the. Both are available in two licensing models, which are commercial (licensed) and personal use (free) and are not part of MPC nor are provided by Equinix.

- 1. Find the VM from the vApp or the Virtual Machines overview.
- 2. Click on More and choose the console type you want to use, the web console where no plugin is needed or the VM Remote Console where this is necessary.

Power	>	ACTIONS - DETAILS
Snapshot	>	
VM Console	>	Launch Web Console
Media	>	Launch Remote Console
Install VMware Tools		Download VM Remote Console
Upgrade Virtual Hardware	Version	
Move		
Сору		
Edit Badges		
Delete		

5.2.4 Snapshots

A snapshot is a mechanism for taking a snapshot of the complete VM or vApp before an action. Operational Console provides the ability to take only one snapshot with or without the active memory state. The snapshot mechanism will double the storage usage of the VM or vApp.

Snapshots can impact the performance of the VM. It is recommended to save a Snapshot for a maximum of 2 or 3 days, after a week the Snapshot will be automatically removed. If the state of the VM needs to be saved longer, create a clone or make a backup of the VM or vApp.

1. Find the VM or vApp and click on Actions, Snapshot and choose Create Snapshot and confirm.

- 2. To go back to the stored status of the VM in the snapshot, choose Revert to Snapshot and confirm.
- 3. To remove the snapshot choose Remove Snapshot and confirm

Notes

- When a new Snapshot is created from a VM with an existing Snapshot the old Snapshot will be removed.
- To have access to all the Snapshot options, the VMware tools needs to be installed in the VM.

5.3 Catalogs

The catalog in Operational Console is where vApps, virtual machines and other media files (ISOs, for example) are stored. Equinix provides a shared Catalog with a number of ISOs to get you started. The shared catalog is tied to the OVDC or, more precisely, metro of your environment. You can also create your own private catalog to store installation media or templates, you can upload files yourself or save them as a template based on previously created virtual machines or vApps. The files stored in the private catalog are part of the storage quota of your OVDC. All software uploaded needs to be licensed according to the vendors and Equinix policies, next to that the catalog may only be used for ISO's and OVF's.

5.3.1 Creating a catalog

1. In order to store the installation media or templates, a catalog must first be created Go on the home screen to the three horizontal stripes (see diagram below).

(Managed Private Cloud	Data Centers	Applications	Networking	Content Hub 1	Libraries Administ	ration Monitor
~						
🆧 Welcome to Content Hub	Catalogs					
III Content	NEW 3					
E Catalogs 2						
	Name	\uparrow	version	Status	Shared	External

- 2. In the Content Hub screen go to Catalogs and choose New.
- 3. Give a name and description to the catalog. You can store the catalog on the available storage profiles. By default the fastest profile is chosen. To choose a profile, turn on the Pre-provision on specific storage policy select the ORGOVDC and choose the specific storage policy.

Create Catalog		\times					
Name this Catalog							
You can use a catalog for sharing vApp templates and media with other users in your organization. You can also have a private catalog for vApp templates and media that you frequently use.							
Name *	NEW_CATALOG						
Description	Description	li					
Pre-provision on specific storage policy							
Org VDC	OVDC-TEST	~					
Storage Policy	MPC-HIGHPERFORMANCE-S-1	~					
	CANCEL	ок					

5.3.2 Adding installation media

When the catalog is available, you can upload installation media to it.

1. Go to Content Libraries > Media & Other en choose Add.

All Catalogs > NEW_CATALOG > App	lication Image	S				
Rew_Catalog	SHARE	PUBLISH S	ETTINGS	SYNC	ALL A	CTIONS ~
General						
Application Images	ADD					
vApp Templates	Name	т т	Application	Name	Τ	Application Version
Helm Charts						
Media						
Metadata						

2. Select the catalog in the new opened screen and click on the icon with the arrow upwards to start the dialog to the file browser. Select the installation file and click on ok.

Upload Media		×
Catalog •	NEW_CATALOG	~
Name	ubuntu-20.04.6-live-server-amd64	
Description		
		h.
Select media to upload		
Selected File: • ubuntu-20.04.6-live-s	erver-amd64.iso	
	DISCARD	ок

3. Edit the name if necessary and choose OK, the upload proces will now start.

l		-								
		Name 🐨	Application Name	Application Version	Status	Owner	VDC	Created On	Storage Policy	Storage used
	:	ubuntu-20.04.6-live-serv	ubuntu-20.04.6-live-serv	vcd-ch-app-ver:1.0.0:H1c	⊘ Resolved	system	OVDC-TE	05/31/2024, 12:08:41 P	MPC-HIGHPERFORMANCE	1.39 GB

In the overview screen of Media & Other there will be a rotating circle at status as long as the upload is in progress. When the upload is complete there will be a green check mark. The file is now ready to use.

4. If you click on the three dots in front of the name, you can choose to delete the file or download it back to the workplace.

5.3.3 Create a vApp Template

AD

A vApp template can be created based on an upload from a local workstation or based on a already existing vApp. If a template must be created for a single VM based on vApp, it is only possible if it is the only VM in the vApp.

1. Find the vApp what the template should be made of and click on More en choose Add to Catalog.

Choose the catalog where the template should land and enter a name. You can choose to make a exact copy but you can also choose to have VM settings adjusted. This only works if VMWare tools are installed before the template is created.

Add to Catalog: vA	APP1	\times
Add this vApp to catalog:	NEW CATALOG	^
Catalog.	NEW_CATALOG	
(1) This catalog is local to yo	pur organization.]
Name *	VAPP1	
Description		
When using this template:	O Make identical copy	
	Customize VM settings	
	This setting applies when creating a vApp based on this template. It is ignored when building a vApp using individual VMs from this template.	>
	CANCEL	

2. To access the vApp template gto to Content Hub > Catalogs > open the catalog.

R NEW_CATALOG	SHARE PU	BLISH SETTINGS	SYNC	ALL ACTIONS ~					
General									
Application Images	ADD								
vApp Templates									
tripp templates	Name			↑ ()	Version	Catalog	Status	Туре	Sourc
Helm Charts	: 🕾 VAP	P1			vcd-ch-app-ver:1.0.0:pMUJt	NEW_CATALOG	⊘ Ready	VM App	
Media	- 3,								

Once available, the template can be used to roll out new machines. See the work instruction "Working with vApps and VMs".

5.3.4 Shared Catalogs

Equinix offers a catalog (* OS-CATALOG-1) per MPC metro containing a number of OS variants. Choose the catalog with the location where the Virtual Machine will reside.

The shared catalog is associated with your PMC variant (FLEX, ST) per metro, so if a customer is using MPC FLEX and MPC ST in one Metro customer will see two catalogs for that Metro.

		Name	↑ т Ver	rsion	Status	Shared	External	τ	Owner	т	Created On	vApp Templates	Media & Other
-	:	CH3-FLEX-1-OS-CATALOG-1	15		Ready	8			system		04/25/2024, 02:28:48 AM	0	10
-	:	DC10-FLEX-1-OS-CATALOG-1	10		Ready	啓			system		04/11/2024, 05:10:41 AM	0	9

5.4 Connectivity

The Operational Console offers a number of ways in which you can connect and access your services

with your organization or the rest of the world. Depending on your choice an OVDC is created with Bridging (MPC Connectivity Customer Routed in your order) or Routing (MPC Connectivity Routed in your order).

5.5 Networks

Depending on your choice for Customer Routed or Routed the network functions in your Console will differ.

In the operational Console 2 types of networks can be created in Self Service, isolated and routed:

- An isolated (internally connected) network is a network that only exists for VMs within the OVDC. Creation of isolated networks is described in How to create an isolated OVDC network.
- A routed network (externally connected) provides access to networks outside the OVDC via the edge gateway. Creation of routed networks is decribed in How to create a routed OVDC network.

MPC CONNECTIVITY TYPE	ISOLATED	ROUTED
BRIDGING	Yes	No
ROUTING	Yes	Yes

From here you can start building your VMs or change the configuration.

In the next sections we give a brief introduction about commonly used network task in the MPC Operational Console:

- MPC Firewall Architecture
- How to create an isolated OVDC network
- How to create a routed OVDC network
- How to create firewall rules
- How to create NAT rules
- How to configure IPsec VPN
- How to create Distributed Firewall Rules (we need Datacenter Group here)

5.5.1 MPC Gateway Firewall Architecture

The MPC Firewall design includes two types or layers of firewalls, Gateway Firewalls and the Distributed Firewall.

Gateway Firewalls are North-South Firewalls that are designed to protect the MPC's perimeters or boundaries, whereas Distributed Firewalls are East-West Firewalls that protect workloads at the vNIC level.

5.5.2 How to create an isolated OVDC network

Overview

An organization virtual data center network enables its virtual machines (VMs) to communicate with each other or to provide access to external networks. A single OVDC can have multiple networks.

Figure 3 Isolated Network

Creating an isolated network..

- 1. In the Operational Console Virtual Datacenters dashboard, select the OVDC in which you want to create the network.
- 2. In the left navigation panel, select Networks.

3. Click New

4. Scope, we select the current OVDC for current isolated network

New Organization VDC Network	Scope
	Ourrent Organization Virtual Data Center
1 Scope	Provides connectivity for VMs in the current VDC only
2 Network Type	
3 General	
4 Static IP Pools	
5 DNS	
6 Ready to Complete	
	CANCEL NEXT

5. In the Network Type page of the New Organization VDC Network dialog box, select Isolated then click Next.

New Organization VDC	Network Type
Network	Select the type of network that you are about to create
1 Scope	Routed This type of network provides controlled access to machines and networks outside of the VDC or VDC Group through an edge gateway.
2 Network Type	Isolated
3 General	This type of network provides a fully isolated environment, which is accessible only by this organization VDC or VDC Group.
4 Static IP Pools	
5 DNS	
6 Ready to Complete	
	CANCEL PREVIOUS NEXT

- 6. In the *General* page, enter a **Name** and **Description** for the network
- 7. In the **Gateway CIDR** field, select the ip-space for the network from the drop down list. The list of gateways is pre-populated by Equinix based on customer input during deployment.
- 8. Dual Stack can be switched on when IPv6 is used
- 9. Guest VLAN Allowed can be switched on multiple VLAN's within connected VMs

New Organization VDC Network	General	
1 Scope	Name * Description	NET-ISOLATE
2 Network Type 3 General		
4 Static IP Pools		
5 DNS	Dual-Stack Mode	
6 Segment Profile Template	Gateway CIDR *	192.168.11/24
7 Ready to Complete	Guest VLAN Allowed	
		CANCEL PREVIOUS NEXT

- 10. Click Next.
- 11. Optional: In the **Static IP Pools** field, enter a range of addresses to be consumed by the VMs connecting to the network, then click Add. In this way the Operational Console will automaticly select a IP-address when creating a VM, otherwise you need to add the IP-address manually during VM creation.

As an example, if you give the gateway address as 192.168.1.1/24, you may then want to create a **Static IP Pool** of 192.168.1.10-192.168.1.100. This will give you a pool of 91 IP addresses to assign to machines within your network. You can always increase this later if needed.

You can add multiple IP pools.

New Organization VDC Network	Static IP Pools	
	Gateway CIDR 192.168.1.1/24 (j)	
1 Scope	Static IP Pools	
2 Network Type	Enter an IP range (format: 192.168.1.2 - 192.168.1.100)	
3 General		ADD
	Allocated IP Ranges List	MODIFY
4 Static IP Pools	192.168.1.10 - 192.168.1.100	REMOVE
5 DNS		
6 Segment Profile Template		
7 Ready to Complete	Total IP addresses: 91	

- 12. When you're done, clieck Next.
- 13. Optional: In the DNS page, enter the DNS information then click Next. In this way the Operational Console will configure the DNS settings when creating a VM, otherwise you need to add the DNS information manually during VM creation.

		<u> </u>			
New Organization VDC Network	DNS				
	Primary DNS				
1 Scope					
1 50000	Secondary DNS				
2 Network Type					
	DNS suffix				
3 General					
4 Static IP Pools					
5 DNS					
C. Comment Desfile Template					
6 Segment Profile Template					
7. Ready to Complete					
, neady to complete					
			CANCEL	PREVIOUS	NEXT

14. On the Ready to C	omplete page, review you	ir selections then click Fir	nish.		
New Organization VDC Network	Ready to Complete				
1.0000	Scope				
1 Scope	Site	© EUROPE-ML6			
2 Network Type	Scope	○ OVDC-TEST			
3 General	General				
4 Static IP Pools	Name	NET-ISOLATE			
	Description				
5 DNS	Network Type	Isolated			
6 Ready to Complete	Guest VLAN Allowed	No			
	Gateway CIDR				
	Dual-Stack Mode	No			
	Gateway CIDR	192.168.1.1/24			
	Static IP Pools				
	Static IP Pools	• 192.168.1.10 - 192.168.1.20			
	DNS				
			CANCEL	PREVIOUS	FINISH

5.5.3 How to create a touted OVDC network

Overview

A routed OVDC network enables its virtual machines (VMs) to communicate with each other or to provide routed (L3) connectivity to external networks. A single OVDC can have multiple routed networks. The process is different based on the use of Distributed Firewall functionality for the network yes or no.

Note:

Figure 4 Routed Network

Creating a routed network

- 1. In the Operational Console Virtual Datacenters dashboard, select the OVDC in which you want to create the network.
- 2. In the left navigation panel, select Networks/New

< All Virtual data centers	Site:	EUROPE-ML6	Organization: ORG-TEST	Data center: OVDC-TEST
	~	Networks		
## Compute	~			
vApps		NEW		
Virtual Machines		Name	↑ ⊤ Status	Gateway CID
Affinity Rules				
Setworking	~			
Networks				
Edges				

3. Scope, we select "Current Organization Virtual Data Center" if we are not going to use DFW

Ne Ne	ev et	v Organization VDC work	Scope	
			Current Organization Virtual Data Center	
	1	Scope	Provides connectivity for VMs in the current VDC only	
	2	Network Type		
	3	Edge Connection		
	4	General		
	5	Static IP Pools		
	6	DNS		
	7	Ready to Complete		
			CANCE	LNEXT

4. In the Network Type page of the New OVDC Network dialog box, select **Routed** then click **Next**.

lew Organization VDC letwork	Network Type
	Select the type of network that you are about to create
1 Scope	Routed This type of network provides controlled access to machines and networks outside of the VDC or VDC Group through an edge gateway.
2 Network Type	
3 Edge Connection	This type of network provides a fully isolated environment, which is accessible only by this organization VDC or VDC Group.
General	
Static IP Pools	
DNS	
7 Ready to Complete	
	CANCEL PREVIOUS NEX

5. Edge connection, we have to select Edge gateway which you want to connect the routed segment.

New Organization VDC Network	Edge Connection				
1 Scope	Name	↑ ⊤ External Networks	Org VDC Networks		
1 Stope	T1-test	1	0		
2 Network Type					
3 Edge Connection					
4 General					
5 Static IP Pools					
6 DNS					
7 Segment Profile Template					
8 Ready to Complete					
			1 - 1 of 1 Edge Gateway(s)		
	Distributed Routing				
			CANCEL PREVIOUS NEXT		

- 6. In the General page, enter a **Name** and **Description** for the network.
- 7. In the **Gateway CIDR** field, select the ip-space for the network from the drop down list. The list of gateways is pre-populated by Equinix based on customer input during deployment.
- 8. Dual Stack can be switched on when IPv6 is used

- 9. Guest VLAN Allowed can be switched on multiple VLAN's within connected VMs

Note: If Distributed Routing is switched on, Gateway firewalling on this routed network is not possible, in that case Distributed Firewall can be used and North South Firewalling is still possible. When switched off, only Gateway firewalling is possible on this routed network.

New Organization VDC Network	General	
1 Scope 2 Network Type 3 Edge Connection	Name * Description	NET-ROUTED
4 General		
5 Static IP Pools	Dual-Stack Mode	
6 DNS	Gateway CIDR *	<u>192168.</u> ↓1/24 ✓ ①
7 Segment Profile Template	Shared	
8 Ready to Complete	Guest VLAN Allowed	
		CANCEL PREVIOUS NEXT

10. Click Next.

New Organization VDC Network	Static IP Pools			
	Gateway CIDR 192.168.1.1/24 (j)			
1 Scope	Static IP Pools			
2 Network Type	Enter an IP range (format: 192.168.1.2 - 192.168.1.100)			
3 Edge Connection			ADD	
	Allocated IP Ranges List		MODIFY	
4 General	192.168.1.10 - 192.168.1.20		REMOVE	
5 Static IP Pools				
6 DNS				
7 Segment Profile Template	Total IP addresses: 11			
8 Ready to Complete				
		CANCEL	PREVIOUS	NEXT

Optional: In the DNS page, enter the DNS information then click Next. In this way the Operational Console will configure the DNS settings when creating a VM, otherwise you need to add the DNS

information manually during VM creation.

New Organization VDC Network	Ready to Complete		
1.0000	Scope		
1 Scope	Site	© EUROPE-ML6	
2 Network Type	Scope	○ OVDC-TEST	
3 Edge Connection	General		
4 General	Name	NET-ROUTED	
	Description	-	
5 Static IP Pools	Network Type	Routed	
6 DNS	Connection	•** T1-test	
	Distributed Routing	Active	
7 Ready to Complete	Guest VLAN Allowed	No	
	Gateway CIDR		
	Dual-Stack Mode	No	
	Gateway CIDR	192.168.1.1/24	
	Static IP Pools		
	Static IP Pools	• 192.168.1.10 - 192.168.1.20	

Note: When using the Distributed type of routed network, firewalling network traffic between Distributed networks is only possible by using Distributed Firewalling since traffic does not passes the Edge Gateway. Traffic to and from Internal or External network will pass the Edge Gateway and can (also) be firewalled there.

Using the Distributed Firewalling requires the "MPC Service Option for "Distributed Firewall", this option can be ordered as part of your MPC contract.

Guest VLAN Allowed

Enabling this option allows you to configure TAGs on the network interfaces of the VMs and allows you to have several VLANs on same network.

Edit network: 'NE	T-ROUTED'		×
General Connection			
Name *	NET-ROUTED		
Description			11.
Dual-Stack Mode			
Gateway CIDR	192.168.1.1/24		
Shared			
Guest VLAN Allowed			
		DISCARD	SAVE

12. On the Ready to Complete page, review your selections then click Finish.

Now you've created your network to connect your OVDC with the outside world, you may want to configure your edge gateway to control what traffic is allowed into and out of your OVDC.

5.5.4 How to create Gateway Firewall Rules

Overview

The Operational Console provides a fully featured layer 4 firewall to control transit from inside to outside security boundaries, and within the various OVDC networks you create.

When you specify networks or IP addresses, you can use:

- An individual IP address
- IP ranges separated by a dash (-)
- A CIDR, for example, 192.168.2.0/24
- The keywords internal, external or any

Creating firewall rules

- 1. In the Operational Console Virtual Datacenters dashboard, select the OVDC that contains the edge gateway in which you can create the firewall rules.
- 2. In the left navigation panel, click **Edges**, and on the right you could see the Edge gateway

All Virtual data centers	Si	te: EUROPE-ML6 Organization: ORG-TEST Data center: OVDC-TES
	~	Edge Gateways
III Compute	~	
vApps		
Virtual Machines		Name 个 T Status T Scope
Affinity Rules		○ T1-test ○ Normal ○ OVDC-T
Networking	\sim	
Networks		
Edges 1		
Storage	\sim	

3. Select the edge that you want to configure and select firewall tab.

All Org VDC Edge Gateways > T1-te	st	
↔ → T1-test		
Configuration	General	
Rate Limiting	Name	T1-test
Services	Status	⊘ Normal
Firewall	Description	-
IPSec VPN	Allow Non-Distributed Routing	No
Load Balancer	Connected	Yes
General Settings	Provider Gateway	sl6-tst-nsxgw-01-t0-test
Routing Static Routes	Come	
Security	scope	
Static Groups	Organization Virtual Data Center	OVDC-TEST
IP Sets Application Port Profiles	Organization	B ORG-TEST
Network Context Profiles		
IP Management		

4. In the **Firewall** tab, you can create firewall rules.

All Org VDC Edge Gateways > TI-	test																					-
↔ ≁→ T1-test																						
Configuration General Rate Limiting	^	NE	w	EDIT RU	JLES	EDIT	DELETE	MOVE TO	REARRANGE													
Services				Name		т	Categor	, т	State	τ	Application	s T	Context	т	Source	1	Destinat	ion	τ	Action		r
Firewall			8	default	t_rule		Default		Active						Any		Any			Drop		
IPSec VPN																						
Load Balancer General Settings																						
Routing Static Routes																						
Security Static Groups																						
IP Sets																						
Network Context Profiles																						
IP Management	~	Mar	nage	Columns																1	1 of 1 rule(s)

5. Click the NEW option to add a new rule

<hr/> <hr/> <hr/> <hr/> T1-test									
Configuration General Rate Limiting	NEW	EDIT RULES	EDIT DELETE	MOVE TO REARRANGE					
Services	1	Name	T Category	T State	T Applications	T Context	T Source	T Destination	T Action
Firewall		A default rule	Default	Active			Any	Any	Drop
NAT									
IPSec VPN									

- 6. For the New Rule, specify:
- Name
- Applications
- Context
- Source (IP address, IP sets, Static Groups)
- Destination (IP address, IP sets, Static Groups)
- Action (Allow, Drop, Reject)
- Protocol (IPv4, IPv6 or both)
- Login
- Comments

New Rule		×
Name	Rule-name	
Category	User defined	
State		
Applications	HTTP	0
Context		0
Source	192.168.1.5-192.168.1.10	0
Destination	10.20.30.10	0
Action	Allow	~
IP Protocol	IPv4	~
Applied To	<u>.</u>	~
Logging		
Comments	Comments	0
	DISCARD	SAVE

- 7. In the **Source** and **Destination** fields, specify the source and destination addresses for the firewall rule.
- To specify an IP address or range, click **IP** and enter the appropriate **Value**. When you're done, click **Keep**.

Select Source Firewa	ll Groups	×
Any Source		
Firewall Groups Firewall IP A	ddresses	
		Show selected
□ Name ↑ ▼	Туре	T Description
IP-Set-test	IP Set	-
Static-Group-test	Static Group	-
		1 - 2 of 2 firewall group(s)
		DISCARD KEEP

If you're likely to reuse a group of the same source or destination IP addresses in multiple rules, select the **Grouping Objects** tab and click + to create an IP set. You can then select this IP set in the Select objects dialog box.

← T1-test			
Configuration General Rate Limiting	NEW EDIT DELETE		
Services	Name	↑ τ Status	τD
NAT IPSec VPN	IP-Set-test	⊘ Normal	-
Load Balancer General Settings			
Routing Static Routes			
Security Static Groups IP Sets Application Port Profiles Network Context Profiles			
Edit IP Set			×
Name *	IP-Set-test		
Description			11.
IP Addresses	Enter an IPv4 or IPv6 addre	ess, range or CIDR (j)	
		ADD	
	192.168.1.12	MODIFY	
		REMOVE	
		S UNDO	
		DISCARD	SAVE

8. In the **Application** field, click + and, in the Add Service dialog box, specify the Protocol, **Source Port** and **Destination Port** for the rule or you can define a custom port protocol. When you're done, click **Keep.**

plic	e a specific ation				Show	selec
	Name 1	Description	Туре	T Pro Por	tocol & Destination ts	٣
	AD Server	AD Server	Default	тс	P: 1024	
	Active Directory Server	Active Directory Server	Default	тс	P: 464	
	Active Directory Server	Active Directory Server	Default	UD	P: 464	
	CIM-HTTP	CIM-HTTP	Default	тс	P: 5988	
	CIM-HTTPS	CIM-HTTPS	Default	тс	P: 5989	
	DCM Java Object Cache	DCM Java Object Cache	Default	тс	P: 7100	
	DHCP, MADCAP	DHCP, MADCAP	Default	UD	P: 2535	
	DHCP-Client	DHCP-Client	Default	UD	P: 68	
				1 - 15 of 412 Application(s)	K < 1/28	>

Applicatio	ons and Raw Po	ort-Protocols		X
Applications	Raw Port-Protocols			
Ports and Port	Ranges should be com	ma separated. Up to 15 su	pported.	
Туре		Source Ports	Destination Port	s
		No Raw Port-Prot	ocols found	
				DISCARD

You can create Custom applications in advance and apply in the firewall rule.

	Custom Applications (1)				
eneral ate Limiting	NEW				
vices	Name	↑ T Status	T Description	Protocol and Destination Ports	
AT Sec VPN					
d Balancer neral Settings			No Custom Application Port Profiles		
ing	Default Applications ()				
tic Routes	Name	1 τ Status	T Description	Protocol and Destination Ports	
rity	AD Server	Normal	AD Server	TCP : 1024	
tic Groups	Active Directory Server	O Normal	Active Directory Server	TCP: 464	
ets	Active Directory Server ODP	() Normal	Active Directory Server ODP	0DP: 464	
Dication Port Profiles	CIM-HTTPS	Normal	CIM-HTTPS	TCP : 5955	
twork context Profiles	DCM Java Object Cache part	() Normal	DCM Isus Object Carbo part	TCD : 2000	
anagement ,	~			1 - 10 of 412 Application Port Profile(s)	/ 42 >
Name •	Application1				
Name • Description	Application1				
Name •	Application1	ĥ			
Name - Description					
Name • Description ADD PORT PROFILE	Application1				
ame * Description ADD PORT PROFILE Protocol TCP ~	Application1				
escription DD PORT PROFILE rotocol TCP ~	Application1				
ame • escription DD PORT PROFILE rotocol ICP ~	Application1				
ame • escription DD PORT PROFILE rotocol rCP ~	Application1 Ports 666 Ports separated by comma				
ame • escription DD PORT PROFILE rotocol ICP ~	Application1				
ame • escription DD PORT PROFILE rotocol TCP ~	Application1				
ame • escription DD PORT PROFILE rotocol TCP ~	Application1				
ame • escription DD PORT PROFILE rotocol rCP ~	Application1				
ame • escription DD PORT PROFILE 'otocol 'CP ~	Application1				
ame • escription DD PORT PROFILE rotocol rCP ~	Application1				

- 9. Select whether the rule is an **Accept** or **Deny** rule.
- 10. If you have a syslog server configured, select the Enable logging check box.
- 11. Click Save changes.

Example

A common use case for a firewall rule is to allow HTTPS through from the internet. The following example uses allocated public IP addresses.

In the example below, the source is any (any IP address within the OVDC). The source port is also any. The destination is a private IP address and the destination port is 443 for HTTPS.

New Rule			\times
Name	HTTP inbound		
Category	User defined		
State			
Applications	HTTPS		0
Context	-		0
Source	Any		0
Destination	192.168.1.10		0
Action	Allow		~
IP Protocol	IPv4		~
Applied To	-		~
Logging			
Comments	-		0
			_
		DISCARD	SAVE

For this to work you need an DNAT configuration. See the next section "How to create NAT rules".

5.5.5 How to create NAT rules

Overview

Network Address Translation (NAT) allows the source or destination IP address to be changed to enable traffic to transition through a router or gateway.

This guide explains the most common types of NAT within your edge gateway:

- Destination NAT (DNAT) changes the destination IP of the packet.
- Source NAT (SNAT) changes the source IP of the packet.

Other options are:

- NO DNAT
- NO SNAT
- REFLEXIVE

For a virtual machine (VM) to access an external network resource from its OVDC, the IP address of its network can need NAT in certain use cases, in that case use:

- The public internet IP addresses provided by Equinix.
- The private networks via MPC Connect.

Note

- This functionality is mostly applicable if the Edge Gateway is configured with Public IP's while the VMs are using Private IP's.
- NAT rules only work if the firewall is enabled. For security reasons, you should ensure that the firewall is always enabled.

Creating a DNAT rule

DNAT changes the destination IP address of a packet and performs the reverse function for any replies. You can use DNAT to publish a service located in a private network on a public IP address.

To create a DNAT rule:

- 1. In the Operational Console Virtual Datacenters dashboard, select the OVDC that contains the edge gateway in which you to create the DNAT rule.
- 2. In the left navigation panel, click Edges.

All Virtual data centers	S	ite: EUROPE-ML6 Organization: ORG-TEST Data center: OVDC-TES
	~	Edge Gateways
III Compute	~	. ,
vApps		
Virtual Machines		Name 🔿 🔻 Status 💌 Scope
Affinity Rules		
Ø Networking	~	
Networks		
Edges 1		
🛢 Storage	\sim	

Select Nat tab and add a NEW NAT rule

All Org VDC Edge Gateways > Ti-te ←↓→ T1-test	st															
Configuration General Rate Limiting	NEW															
Services Firewall NAT IPSec VPN Load Balancer	Name	T Cate	gory T	State	т	NAT Action	T	External IP	T	Internal IP	Ŧ	Application	T	External Port	τ I)e

Г

3. In the NAT section, click + DNAT Rule.

Name *	DNAT-rule	^
Description		
NAT Ashien		
NAT Action *	SNAT ~	
External IP *	10.30.40.95 ~	
	Translated IP or CIDR	
Internal IP	192.168.1.10	
	Source IP or CIDR	
Destination IP		
V log Advanced Setting	ngs	
State		
Logging		
Priority	0	
	If an address has multiple NAT rules, the rule with the highest priority is applied. A lower value means a higher precedence for this rule.	
Firewall Match	Match Internal Address 🗸 🧃	
	Determines how the firewall matches the address during NATing if firewall stage is not skipped.	
Applied To	- ~	
	Applies this NAT rule only for the selected Org Vdc network. Only networks with distributed routing disabled can be used	~
	DISCARD	

4. In the NAT Action select the type of NAT rule

Add NAT Rule		×
Name *	DNAT-rule	
Description		
		h.
NAT Action	DNAT	~
External IP *	DNAT SNAT	
External Port	NO DNAT NO SNAT	
Internal IP *	REFLEXIVE	

- 5. Enter an External IP. For example 10.30.40.95
- 6. Enter an External Port. For example 443
- 7. Enter Internal IP. For example 192.168.1.10
- 8. Application
- 9. Advance Setting
- State: it is to enable the rule or disable
- Logging: To log the rule

- Priority: A lower value means a higher priority. 0 is the default Value
- Firewall Match:
 - Match Internal Address
 - o Match External Address
 - o Bypass
- Applied To, leave blank
- 10. If you have a syslog server configured, select the Enable logging option.
- 11. When you're done, click Keep then Save changes.

For more information also see the VMware Product documentation

Creating an SNAT Rule

SNAT changes the source IP address of a packet and performs the reverse function for any replies. When connecting to an external network, such as the internet, to access services (for example, DNS), you need to define an SNAT rule to translate your internal address into something available on the external network.

To create an SNAT rule:

- 1. In the Operational Console Virtual Datacenters dashboard, select the OVDC that contains the edge gateway in which you to create the SNAT rule.
- 2. In the left navigation panel, click Edges.

All Virtual data centers	Si	te: EUROPE-ML6 Organization: ORG-TEST Data center: OVDC-TES
	~	Edge Gateways
III Compute	~	
vApps		
Virtual Machines		Name 🔨 🛪 Status 🛪 Scope
Affinity Rules		
Ø Networking	~	2 © Normal 2000C-1
Networks		
Edges 1		
🗎 Storage	\sim	

Select Nat tab and add a NEW NAT rule

All Org VDC Edge Gateways > T1-test ←↓→ T1-test	t														
Configuration General Rate Limiting	NEW														
Firewall NAT IPSec VPN Load Balancer	Name	T Cat	legory	T State	Ţ	NAT Action	т	External IP	T	Internal IP	т	Application	T	External Port	T Di

3. In the	NAT Section,	click +SNAT	Rule
-----------	--------------	-------------	------

Add NAT Rule		\times
Name *	SNAT-rule	^
Description		l
NAT Action *	SNAT ~	
External IP *	10.30.40.99 🗸	
	Translated IP or CIDR	
Internal IP	192.168.1.0/24	
	Source IP or CIDR	
Destination IP		
 Ø Advanced Settii State Logging 	ngs	
Priority	F an address has multiple NAT rules, the rule with the highest priority is applied. A lower value means a higher precedence for this rule.	
Firewall Match	Match Internal Address 🗸 😮 🚺	
	Determines how the firewall matches the address during NATing if firewall stage is not skipped.	
Applied To	- ~	
	Applies this NAT rule only for the selected Org Vdc network. Only networks with distributed routing disabled can be used.	~
	DISCARD	E

4. In the NAT Action select the type of nat rule, in this case SNAT

NAT Action *	SNAT	~
	DNAT	
External IP *	SNAT	
	NO DNAT	
Internal IP	NO SNAT	
	REFLEXIVE	
Destination IP	L	

- 5. External IP, this will be the external network (usually named *VCD_CUSTOMER_WAN).
- 6. Internal IP, this will be the network or Ip which it is nated to the internet.
- 7. Advance Setting
- State: it is to enable the rule or disable
- Login: To log the rule
- Priority: A lower value means a higher priority. 0 is the default Value
- Firewall Match:
 - o Match Internal Address
 - o Match External Address
 - o Bypass
- Applied To, leave blank
- 8. When you're done, click Keep then Save changes.

For more information on SNAT see the VMware Product documentation

Creating an NO SNAT Rule

No-SNAT rules exist to negate existing SNAT rules. So we can create a NO SNAT rule when we want to avoid a SNAT rule for a specific Destination IP. To do that, we will configure a Priority in Advanced setting for this NO SNAT that should be lower than the SNAT rule. The default priority is 0 and this will be the highest priority.

To create an No SNAT rule:

- 1. In the Operational Console Virtual Datacenters dashboard, select theOVDC that contains the edge gateway in which you to create the No SNAT rule.
- 2. In the left navigation panel, click Edges.

All Virtual data centers	S	ite: EUROPE-ML6 Organization: ORG-TEST Data center: OVDC-TE
	~	Edge Gateways
## Compute	~	Lage outenays
vApps		
Virtual Machines		Name 🔨 Y Status Y Scope
Affinity Rules	~	○ Ti-test 2 ⊘ Normal △ OVDC
Networks		
Edges 1		
Storage	\sim	

Select Nat tab and add a NEW NAT rule

All Org VDC Edge Gateways > T1-t	test																
← T1-test																	
Configuration General Rate Limiting	NEW																
Services Firewall	Name	т 1	Category	т	State	т	NAT Action	т	External IP	Ŧ	Internal IP	т	Application	т	External Port	۲	D
IPSec VPN Load Balancer																	

3. In the NAT section, click + No SNAT Rule

Name •	NO-SNAT-rule
Description	
	l
NAT Action *	NO SNAT Y
Internal ID	102 169 1 10
nterna in	Source IP or CIDR
Destination IP	192 168 5 20
	tings
 Ø Advanced Set State Logging 	tings
 Advanced Set State Logging Priority 	tings
 Ø Advanced Set State Logging Priority 	tings
 ② Advanced Set State Logging Priority Firewall Match 	tings
 Ø Advanced Set State Logging Priority Firewall Match 	titing d d Maddense has multiple MAT des, the rule with the model of the second
 State Logging Priority Firewall Match Applied To 	titing

5.5.6 How to configure IPsec VPN

Overview

Operational Console supports the following types of site-to-site VPN:

- Another edge gateway in the same organization
- An edge gateway in another organisation (Equinix or another vCloud service provider)
- A remote network offering IPsec VPN endpoint capability like Cloud Service providers or your Colocation environment

Depending on the type of connection required, you'll need to complete IP addressing for both ends, together with a shared secret, and indicate which OVDC networks are allowed to connect to the VPN link.

Before you begin

Before you start configuring IPsec VPN settings, you'll need to make a note of the IP address of your edge gateway to use as your tunnel endpoint address:

- 1. In the Operational Console Virtual Datacenters dashboard, select theOVDC that contains the edge gateway you want to configure.
- 2. In the left navigation panel, click **Edges**.
- 3. On the Edges page, select the edge that you want to configure.
- 4. Within the Services tab we can see the IPSec VPN option, and to create a new IPSec VPN, we have to select "NEW"

All Org VDC Edge Gateways > T1-tes	t
←∱→ T1-test	
Configuration General Rate Limiting	NEW
Services Firewall NAT	Name T State
IPSec VPN	

Configuring edge gateway IPsec VPN settings

1. We need to configure a name, enable the Login if you want to check the logs and we leave the rest of the options by default

Add IPSec VPN Tunnel	General Settings		
1 General Settings	Name *	IPSEC-TEST	
2 Peer Authentication Mode	Description		_
	Security Profile	Default	~
4 Ready to Complete		> IKE Profiles	
		> Tunnel Configuration	
		V DPD Configuration	
		Probe Interval (seconds) 60	
	Status		
	Logging		
		CANCEL	NE)

- 2. Peer Authentication Mode
- Pre-Shared Key: The shared secret used to authenticate and encrypt the connection. It must be an alphanumeric string between 32 and 128 characters that includes at least one uppercase letter, one lowercase letter and one number. This must be the same on both sites.

Add IPSec VPN Tunnel	Peer Authentication Mode		
1 General Settings	Authentication Mode	Pre-Shared Key	
2 Peer Authentication Mode		○ Certificate	
3 Endpoint Configuration 4 Ready to Complete	Pre-Shared Key *	Enter pre-shared Key	0

• Certificate: To use a certificate, you will have to upload the certificate and the CA certificate.

А	dd IPSec VPN Tunn	el Peer Authentic	ation Mode		
ľ	1 General Settings	Authentication Mode	O Pre-Shared Key		
	2 Peer Authentication Mode	2	O Certificate		
	3 Endpoint Configuration	Server Certificate •	SELECT		
	4 Ready to Complete	CA Certificate *	SELECT		

3. Endpoint Configuration

Add IPSec VPN Tunnel	Endpoint Configur	ation	\times
1 General Settings	Local Endpoint		
2. Deep Authentientien Mede	IP Address *	Enter Local IP Address 🗸 🗸	
2 Peer Authentication Mode	Networks *		
3 Endpoint Configuration			
4 Ready to Complete		Comma separated CIDRs (i.e. 192.168.10.0/24, 212.138.0.0/16)	
	Remote Endpoint		
	IP Address *		
	Networks *		
		Comma separated CIDRs (i.e. 192.168.10.0/24, 212.138.0.0/16)	
	Remote ID	0	

Local Endpoint

- IP Address: The external IP of your edge gateway (refer to the first steps of this procedure for more information).
- Networks: Enter the organisation networks that can access the VPN (separate multiple local subnets with commas).

Remote Endpoint

- IP Address: The external IP of your remote site or on-premises firewall or edge where VPN is being set up.
- Networks: This is the subnet on your on-premises network that you want to make accessible from your OVDC. For example, if your on-premises networks sit inside the 172.20.0.0/16 range, you could enter 172.20.0.0/16 here or limit your entry to a smaller subnet of that, for example 172.20.0.0/25.
- Remote ID:
- This remote ID uniquely identifies the peer site and depends on the authentication mode for the tunnel. If you do not set it, the remote ID defaults to the remote IP address.
- Pre-shared Key The pre-shared key depends on whether NAT is configured. If you configure
 NAT on the remote ID, enter the private IP address of the remote site. Otherwise, use the public
 IP address of the remote device terminating the VPN tunnel.
- Certificate The remote ID must match the certificate SAN (Subject Alternative Name), if available, or the distinguished name of the certificate used to secure the remote endpoint.

NOTE

The remote ID must match the SAN (Subject Alternative Name) of the remote endpoint certificate, if available. If the remote certificate does not contain a SAN, the remote ID must match the distinguished name of the certificate that is used to secure the remote endpoint, for example, C=US, ST=Massachusetts, O=VMware,OU=VCD, CN=Edge1.

4. When you're done, click Keep to create the edge end of the VPN tunnel then click Save changes.

Creating the second VPN gateway

You now need to create the endpoint of the VPN tunnel. If this is a differentOVDC, go through the steps described above again to create the tunnel. When you've done that, you can change your firewall settings and validate the connection (see below).

If you're connecting to an external data center, you'll need to set up the tunnel on that premises.

Creating an external data center VPN gateway

Although we can't provide specific instructions on setting up an external data centre gateway to connect to the edge gateway, we've provided information about some configuration requirements below.

IKE Phase 1 and Phase 2

IKE is a standard method for arranging secure, authenticated communications.

Phase 1 parameters

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys. The supported Phase 1 parameters are:

- Main mode
- AES/AES256/AES-GCM (user configurable)
- Diffie-Hellman Group
- Pre-shared secret (user configurable)
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying
- ISAKMP aggressive mode disabled

Phase 2 parameters

IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSec tunnel to use (either by using the IKE phase 1 keys as a base or by performing a new key exchange). The supported IKE Phase 2 parameters are:

- AES/AES256/AES-GCM (Will match the Phase 1 setting)
- ESP tunnel mode
- Diffie-Hellman Group
- Perfect forward secrecy for rekeying (only if it was turned on in both endpoints)
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

Configuring the edge gateway firewall for VPN

When the VPN tunnel is up and running, you'll need to create firewall rules on the edge gateway for any traffic passing over the tunnel. For how to do this, see How to create firewall rules. Key points to note:

- You need to create a firewall rule for both directions, that is, from data center toOVDC and fromOVDC to data center.
- For data center to OVDC, set:
 - Source as the source IP range for your external OVDC/data center network
 - o Destination as the destination IP range for your OVDC network
- ForOVDC to data center, set:
 - Source as the source IP range for your OVDC network
 - Destination as the destination IP range for your data center/VDC network

Validating the tunnel

When you've configured both ends of the IPSec tunnel, the connection should start without any issues. To verify the tunnel status in Operational Console:

- 1. On the Edges page, select the edge that you want to configure and click Configure Services.
- 2. Select the Statistics tab and then the IPsec VPN tab.
- 3. For each configured tunnel, if you can see a tick, the tunnel is up and running and operational. If any other status is shown, you'll need to review your configuration and any firewall rules.
- 4. You should now be able to send traffic via the VPN.

NOTE

It can take up to two minutes after the tunnel is established to show that the VPN connection is active.

5.5.7 How to create OVDC Distributed Firewall Rules

Overview

On the OrgOVDC level it is possible to use the OrgOVDC distributed firewall to make use of the Micro Segmentation capabilities in Operational Console.

NOTE

Using Distributed Firewalling requires the MPC Service Option "Distributed Firewall" to be contracted.

Before you begin

- IP set, as a source or destination in a rule, Create an IP Set for Use in Firewall Rules and DHCP Relay Configuration. IP Sets are often used to group resources outside of the VCD Organization, like the Internet of comapny WAN. In that case IP addresses or subnets are the only way to group them.
- Static Group, When using a static groups, a group is created to which one or more networks are added. When using the static group in a DFW rule, the rule applies to all VMs that are attached to the networks in the group.
- **Dynamic Groups** are used to group VM based on VM Name, Security Tag or both. When creating a Dynamic Group, by default it has single criteria and rule. When needed it can be extended up to 3 criteria, with 4 rules each.

Creating distributed firewall rules

- 1. In the Operational ConsoleOperational Console Virtual Datacenters dashboard, select theOVDC that contains the distributed you want to configure.
- 2. In the left navigation panel, click Networking/Datacenter Groups/Distributed Firewall.

🎒 Managed Private Cloue	d Data Centers Applications	Networking 1 Content Hu	ub Libraries Adr	ninistration Monitor
Networks Edge Gateways	Data Center Groups 2 Security Tags			
All Data Center Groups > DCG-name				
DCG-name SYNC	DELETE			
General	Default Policy Status		Enabled	
Participating VDCs				
Edge Gateway	NEW EDIT RULES EDIT DELET	E MOVE TO REARRANGE		
Distributed Firewall 3	# Name	T State	T Applications	T Context
Security	0 1 Default_VdcGroup_DCG-name	Active		-
Static Groups				
Dynamic Groups				

3. Click the + button to add a new row to the firewall rules table.

Default	Policy Status			Enabled									DISABLE
NEW	EDIT RULES EDIT DELETE MOVE	TO REARRANGE											
	Name	T State	т	Applications	т	Context	т	Source	т	Destination	т	Action	
0 1	Default_VdcGroup_DCG-name	Active						Internal		Internal		Allow	

4. For the New Rule, specify a Name.

New Rule		×
Name	Name-FW-rule	
State		
Applications		0
Context		0
Source		0 /
Destination	-	0 /
Action	Allow	~
IP Protocol	IPv4	Ŷ
Logging		
Comments	-	0
	[DISCARD

- 5. In the Source and Destination fields, specify the source and destination addresses for the firewall rule.
- Firewall groups
 Select Source Firewall Groups
 Any Source
 Firewall Groups
 Firewall Groups
 Firewall IP Addresses
 There aren't any groups available yet, you can create or manage IP Sets.
 Dynamic Groups or Static Groups

• IP sets, select NEW.

All Data Center Groups > DCG-name				
CG-name syn	NC DELETE			
General				
Participating VDCs	NEW			
Edge Gateway	Name			
Distributed Firewall				
Security				
Static Groups				
IP Sets				
Dynamic Groups				
Application Port Profiles				
Network Context Profiles				

Name, description, IP range or CIDR

New IP Set		
Name *	IPSet-name	
Description		
IP Addresses	Enter an IPv4 or IPv6 address, range or CIDR ()	ADD
		MODIFY
		REMOVE
		+> UNDO
		DISCARD

• Static Groups, select NEW.

All Data Center Groups > DCG-	-name
CG-name	SYNC DELETE
General	
Participating VDCs	NEW
Edge Gateway	Name
Distributed Firewall	
Security	
Static Groups	
IP Sets	
Dynamic Groups	
Application Port Profiles	
Network Context Profiles	

We add a name, and Save

New Static Group		\times
Name *	Static-group-name	
Description		
	DISCARD	E

Select Manage members to add new member

DCG-name SYN	C DELETE	
General Participating VDCs	NEW EDIT MANAGE MEMBERS ASSOCIATED VMS DELETE	
Edge Gateway	Name	↑ ⊤ Status
Distributed Firewall	Static-group-name	⊘ Normal
Security		

Select a network to add to the static group

In Associated VM, you will be able to see which VMs are connected to the networks attached

Associated VMs of group "Static-group-name"				
Virtual Machine	T Virtual Application	т		
VMUbuntu1	vAPP1			

	-,
All Data Center Groups > DCG	3-name
CG-name	SYNC DELETE
General	
Participating VDCs	NEW
Edge Gateway	Name
Distributed Firewall	
Security	
Static Groups	
IP Sets	
Dynamic Groups	
Application Port Profiles	
Network Context Profiles	\$

• Dinamic Groups, select NEW.

Give a name to the Dynamic group, and select the type of criteria you want to use.

New Dynamic Gi	roup					2
Name *	Dinam	icGroup-Name				
Description						11.
VM Criteria						
You can add up to 3 criter + ADD CRITERION	ria, containi	ng up to 4 rule	es.			
VM Tag Type	<u> </u>	Equals Operator	× Q	t is required	 III REMOVE	^
V OR Criterion 2					TREMOVE	
+ ADD RULE						
VM Nar Type	ne 🗸	Contains Operator	~	Enter value Value	 🗓 REMOVE	
V OR Criterion 3					💼 REMOVE	
+ ADD RULE						
OS Nan Type	ne v	Equals Operator	~	Enter value Value	II REMOVE	
						~

• Firewall IP Addresses, you can add an IP, CIDR or Range and select Keep

Select Source Firewall Groups $\qquad \qquad \qquad$	New Rule		\times
Any Source	Name	Name-FWrule	
	State		
Firewall Groups Firewall IP Addresses	Applications	HTTPS	0
ADD	Context		0
IP Address	Source	Static-group-name	0
Enter IP Address, CIDR or Range	Destination	10.10.20.20	0
	Action	Allow	~
	IP Protocol	IPv4	~
	Logging		
	Comments		0
DISCARD KEEP		DISCARD	AVE

- 1. Select Action (Allow/Drop/Reject
- 2. **Ip Protocol** (IPV4, IPv6 or both)
- 3. Loggin
- 4. Select Save

Other documentations

Where to find Service Description?

You will find the most up to date service description on <u>docs.equinix.com</u> website.

Where to find EMS policy?

You will find it on our website.

Where to find official VMware documentation?

You will find it on https://docs.vmware.com

How to ask for help

Please make sure to open a ticket every time you need help. This is your guarantee that the right team has received your request and will work on that under the expected SLAs.