

Enterprise Cloud Services

How To Set-Up Networking?

Experience the power of the future with Cyfuture Enterprise Cloud - The ultimate cloud solution for your business needs. Our cloud portal offers a wide range of cutting-edge features such as containers, object storage, data protection, advanced networking, load balancing, and more, all in one place. Our Enterprise Cloud solution provides everything you need to scale your business and take it to the next level. So why wait? Try Enterprise Cloud today and transform your business with the power of the cloud.

<u>Step-1</u> : Let's begin with network setup within our enterprise cloud console.

In order to begin, click on the Networking tab from the left or either from the top bar at the console page.

Next, when you click on Networks you can find the internal network.

	«	Networks								
III Compute	~									
vApps		NEW								
Virtual Machines		Name 🕆 T	Status	Gateway CIDR	Y Network Type	Connected To	IP Pool Consumed	Shared T	Route Advertised	τ
Affinity Rules		O Internal Network	Normal	192.168.0.1/24	Routed	++++	115	No	No	
Scale Groups	_									
O Networking	~									
Networks										
Edges										
🗐 Storage	~									
Named Disks										
Storage Policies										
Settings	~									
General										
Metadata										
Sharing										
Kubernetes Policies										
		Manage Columna							1-1 of 1 networ	3(8(8)
ecent Tasks Running	Failed									

In internal networks tab, it **highlights the various networking components** such as in the General tab- Gateway CIDR value (for ex. here- 192.168.0.0/24), Network type, Backing type, Backing ID, etc.

In the IP Management it showcases the static IP pools allocations, IP Usage, etc.

Networks Edge Gi	iteways Provider Gateways Data Center Groups Security Ta	34	
Mi Networks > Internal Netwo	à		
🔠 Internal Net	NOTK OPEN IN VDC CONTEXT		
Seneral	General		
P Management	Name.	Internal Network	
Static IP Pools DHCP	Description	1.22	
Plusage	Gateway CIDR	192.168.0.1/24	
acurity Groups	Network Type	Routed	
ecurity orougis	Backing Type	Segment	
	Backing Id	d929d966-a66a-4022-a32c-6119fee172c2	
	Connected To	-Q+ Wattherius Finewall	
	Distributed Routing	Active	
	Guest VLAN Allowed	No	
	Route Advertisement	Inactive	
	Scope		
	Organization Virtual Data Center		
	Organization		
	Networking Tenancy	Inactive	

<u>Step-2</u>: Now we need to set up the SNAT AND DNAT rules for the virtual machine to enable access to outside networks and vice-versa.

Thus click on Networks, then click on Edge Gateways.

Then click on the name of your firewall.

Within this tab click on NAT under services and create new NAT service.

By default for every virtual machine both SNAT and DNAT is required to be setup.

cynthure Cloud	Data Centers Applicatio	ons Networking Content I	lub Libraries Administ	ration Monitor Mo	не~	Q	Ø-
							EXPORT EDGE GATEWA
ame	† τ Status	Y Scope	T Distributed Routing	τ Used NICs	External Networks	T Org VDC Networks	τ HA State
Erewall	@ Normal		Enabled	2	¥.	1	Not Applicable
e Columna							1.1 of 1 Educe Galaxie
- Addressed							1 - 1 ar 1 maple content

Cyfuture Cloud	Data Centers	Applications	Networking	Content Hub	Libraries	Administration	Monitor	More			Q @-
Networks Edge Gatew	ays Data Center	Groups Security	Tags								
All Edge Gateways > Watherlub Fir	ewall										
<∱→ WaffleHub Fire	Wall OPEN IN V	DC CONTEXT	ICREASE SCOPE								
Configuration General Rate Limiting	NEW	1-									
Services	Name	T Ca	legory Y	State T	NAT Action	Y External IP	τ Int	iernai iP 🛛 🔻	Application 1	r External Port T	Destination IP
NAT IPSec VPN											
Load Balancer General Settings											
Routing Static Routes							8				
Security							1				
Static Groups IP Sets						No N	IAT Rules Fo	bund			
Application Port Profiles Network Context Profiles											
IP Management IP Allocations											
DNS DHCP Ennwarding	4										
oncer to marking	Manage Column	.]									
Recent Tasks Running: 1 Faile	ed: 🔘										

Step-3: Now in order to **create an SNAT rule**, begin with entering the name (usually we prefer to write the NAT rule name along with the private IP Address: SNAT-192.168.0.2 in both the

name and description to identify).

Then choose the NAT action, here SNAT.

Then choose the External IP address from the right 'i' button and write your private IP as well. Now your basic necessary configuration is done and finally click on save to finish. Similarly create the same rule for DNAT.

Firewalk owners context increase score							
	Add NAT Rule		1	×			
NEW	Name *	SNAT-192.168.0.2	-	_			
(1) may be been as a line	Description	SNAT-192.168.0.2		1			
O married balls the needed with	NAT Action *	SNAT		Y			
	External IP *	-		Ø			
	Internal IP	192.168.0.2					
	Destination IP						
	> @ Advanced Setti	ngs					
			DISCARD	SAVE			

Rate Limiting	NEW E	DIT DELET	Ē																
Services Eirmund	Name		Category	.v State	τ.	NAT Action		External IP	π.	internal IP	Ψ.	Application	т	External Port	π.	Destination IP	٣	Logging	
NAT	O DNAT-1	R2.168.0.2	User defined	Active		DNAT				192.168.0.2		55		Any				No	
IPSec VPN	SNAT-1	2.168.0.2	User defined	Active		SNAT				192.168.0.2		÷2		Any		2		No	
oad Balancer General Settings							_		_		_		_		_		_		_
outing Static Routes																			
scurity Static Orouns																			
P Sets Application Port Profiles Vetwork Context Profiles																			
P Sets Application Port Profiles Vetwork Context Profiles Management P Allocations																			
P Sets Application Port Profiles Network Context Profiles Management IP Allocations ONS DHCP Forwarding	¢																		

Further, you can edit the rules as per your requirement.

Also in order to check the set of available public IP's allocated to you in your enterprise portal, in IP Management on left tab, click on the **IP Allocations** to check the same.

Configuration	Allocated IPs	
Rate Limiting	IP Range T IP Block	т
-	40.00.00	(24)
Services		_
NAT		
IPSec VPN		
Load Balancer		
General Settings		
Routing		1 - 1 of t IP ranges
Static Routes		
Security	IPs Used	
Static Groups	IP Used 🕆 Y Usage	Υ
IP Sets	DNAT	
Network Context Profiles	SNAT	
IP Management		
DNS		
DHCP Forwarding		
		1 - 2 of 2 IP usages

Step-4: Now after **connecting to the external or internal networks**, is is essential to setup the firewall rules.

In order to enable access from to the internet and various networking services like SSH, RDP, DNS, ICMPv4 enablement, etc. we need to configure the firewall rules.

Click on Firewall under the services tab on left. By default the firewall is dropped to ensure security and prevent unauthorized access.

ervices			Name	τ.	Category	τ	State	τ	Applications	τ	Context	π.	Source	τ	Destination	т	Action	
ewall	0	1	Internet_Access		User defined		Active		HTTP, DNS-TCP, DNS-UDP.				Any		Any		Allow	
to VPN		۵	default_rule		Default		Active		•		140		Any		Any		Drop	
c Routes ty c Groups ts ication Port Profiles vork Context Profiles																		

<u>Step-5</u>: We begin with **creating the flrewall rule** for Internet Access and few mandatory services like RDP (Remote Desktop connection Port-9007) for Windows machine and SSH (Port-22 or 2232), DNS- TCP & UDP, ICMPv4 and HTTP as well as HTTPS rule.

Since the RDP on port 9007 is not created by default, we have to create the port by clicking on Application Port profile on the left under the security tab.

In custom application click on new and create an RDP port rule, select the protocol as TCP and write the port for the same and finally click on save.

Cyluture Coud	Data Contast Applications (Net	Aning Control take Advance	Administration American	Balance of	Q. Ø ^{. 1}
		Edit Applicatio	on Port Profile	×	
		Name *	RDP-9007		
		Description		le	
		Protocol TCP *	Ports 9007 Ports separated by comma		
		+- +-			
			DISC	ARD	
		Course .	00x 2mm (2mm	I Gove por	

<u>Step-6</u>: Now coming back to firewall rules setup, for Internet access rule, click on new rule. Now enter the name as **Internet_Access** or anything of your choice.

Now click on Applications to select the applications to enable on firewall on their allocated ports.

For example, here for basic use bare minimum you must allow these below mentioned applications by choosing the specific ones and then click on save.

<pre>de Gateways > WattleHub Fir</pre>	ewall														
WaffleHub Fire	wall op	EN IN VDC CONTEXT	INCREASE SCOPE												
guration eral	NEW	EDIT RULES EDIT	DELETE MOVE TO	REAR	INGE										
e Limiting															
ces		Name	T Category	т	State	т	Applications	т	Context	Τ.	Source	 Destination	Ŧ	Action	12
vall	0 8	default_rule	Default		Active				8		Any	Any		Drop	
VPN															
alanses															
ral Settings															
v : Routes															
w.															
Groups															
15															
ication Port Profiles															
ork Context Profiles															
agement															
ocations															
P Forwarding															
The second se															

Recent Tasks Running: () Failed ()

		New Pule				
		New Rule		0.1		
		Name	internet_Access			
		Category	User defined			
		State		t		
		Applications	DNS-TCP, DNS-UDP, RDP-9	007.HTT_ Ø 🖉		
		Context	2	0		
		Source	Any	~ ~		
		Destination	Any			
		Action	Allow			
		IP Protocol	IPv4			
		Applied To	<u>.</u>	~		
		Logging				
		Comments	*	0		
			DI	SCARD SAVE		
Ancest Taxa Survey @ Frees						

	Арр	lications and Ra	w Port-Protocol	5		×
DC CONTEXT INCR	Applio Choose applica	cations Raw Port-Pro			Show	v selected
· · · · ·	- 1	Name	Description	Туре	Protocol & Destination Ports	
ilt_nule	×	ICMP ALL	ICMP ALL	Default	ICMPv6 ICMPv4	
	×	DNS-TCP	DNS-TCP	Default	TCP : 53	
	×	DNS-UDP	DNS-UDP	Default	UDP : 53	
	×	НТТР	HTTP	Default	TCP : 80	
	×	HTTPS	HTTPS	Default	TCP : 443	
	×	RDP-9007	-	Custom	TCP : 9007	
						6 items
					DISCARD	SAVE
				_		

<u>Step-7</u>: Select the source and the destination by specifying the access on the flrewall from which source to which destination you want to allow.

For example, in the below snippet you can find the source setup- you can either mention the source virtual machine IP Address or the select Any to allow any virtual machine.

Similarly you set up the same for the Destination. Here, we have for the ease chosen Source-Any and Destination- Any.

Then **select the Action to Allow and select the IP Protocol** (by default IPv4). Finally click on save to save the firewall rule and now the access for the specific applications over firewall is setup.

New Rule		
Select Source Firewall Groups	×	
Any Source		
Firewall Groups Firewall IP Addresses		
ADD		
IP Address		
in Position		
Enter IP Address, CIDR or Range		
DISCARD	KEEP	

Data Centers Applications					
Data Center Groups Security	New Rule		×		
all цовении урокомтехт, ни	Name	Internet_Access			
	Category	User defined			
NEW EDITAULES	State				
A Number of	Applications	DNS-TCP, DNS-UDP, RDP-9007, HTT_	00	T Source	
and contract, size	Context		0	Aine	
	Source	Any	0		
	Destination	Any	0		
	Action	Allow	~		
	IP Protocol	IPv4	~		
	Applied To	5 <mark></mark>	~		
	Logging				
	Comments	340	0		
		DISCARD	SAVE		
[Manape Dillamon]					

Configuration General Rate Limiting	N	EW	EDIT RULES EDIT	061	ETE MOVE TO	erana)	40E									
Services			Name	π	Category	τ	State	τ	Applications	т	Context T	s	ource T	Destination T	Act	ion 1
Firewall	0	1	internet_Access		User defined		Active		HTTP, DNS-TCP, DNS-UDP.,		10	A	lny	Any	AB	pw
IPSec VPN		Ð	default_rule		Default		Active		17			A	uny	Any	Dre	op.
Load Balancer General Settings																
Routing Static Routes																
Security Static Groups																
IP Sets Application Port Profiles Network Context Profiles																

<u>Step-8</u>: Further as a part of networking, if you want an **IP set or group**, you can do the same by clicking on **IP Sets** under security tab and specify the set of IP's you want to be grouped together for ease during selection of source and destination as well as other networking setup.

Alteri Greeka Villenaa	line							
		incluin an ann an						
		New IP Set		1		×		
		Name *	Y			- 1		
		Description						
		IP Addresses	Enter an IPv4 or IPv6 address, range or CIDR ()					
					ADC			
				E	MODULA MODULA			
						1		
					DISCARD	LAVE		
		7						
Origin Commandia								

Thus, **finally your basic necessary configurations setup for networking is achieved** and you can explore as well as access the enterprise cloud portal and various networking services as per your organization's need and requirement.

https://cyfuture.cloud/