НТМL5 ПОРТАЛ – УПРАВУВАЊЕ СО БЕЗБЕДНОСТ И МРЕЖА

Прирачник за користење на новиот HTML5 портал за neoCloud услугата vDC, управување со периметарска заштита, рутирање и мрежни параметри.





3a neoCloud

neoCloud е бренд од портфолиото на професионални ИКТ услуги на Неоком во соработка со телекомуникацискиот оператор Неотел.

neoCloud е првата македонска "cloud computing" платформа базирана на виртуелизација од VMware со комплетна автоматизација и управување од производителите VMware и HP.

Целта на neoCloud е да овозможи комплетна услуга во делот на ИКТ на сите потенцијални клиенти, без разлика на нивната големина и без инвестициски трошоци на принципот на месечно изнајмување ресурси и услуги. Со користење на нашите услуги, овозможуваме поголема агилност на клиентите и нивен фокус во примарната дејност на нивниот бизнис

neoCloud е заштитена трговска марка во сопственост на Неоком А.Д. Скопје.

За Неоком

Неоком АД е лидер на македонскиот ИКТ пазар во поглед на виртуелизациски решенија, автоматизација и управување на бизнис процесите. Во поглед на "cloud computing" технологијата, Неоком е единствениот сертифициран провајдер според VSPP програмата од страна на VMware на територијата на Р. Македонија. Посветеноста кон високо технолошки решенија и стручната експертиза е потврдена од страна на HP со највисоката партнерска титула HP Platinum Partner.

За Неотел

Неотел ДОО е телекомуникациски оператор основан во 2004 година со македонски капитал обезбеден од страна на Неоком. На пазарот нуди широк спектар на услуги од областа на широкопојасен интернет пристап, телефонија, изнајмени линии, хостирање и колокација на опрема. Започнува со нудење на услуги на бизнис-корисници со капацитет не поголем од неколку мегабити во секунда (Mbps), денес НЕОТЕЛ е компанија која нуди услуги на бизнис и домашни корисници преку WiMAX безжична технологија и сопствена оптичка мрежа со гигабитен (Gbps) капацитет.



Содржина

Org VDC Networks
Управување со постоечки мрежи
Создавање на нова мрежа4
Edge Gateways
Firewall7
DHCP12
NAT13
Routing14
Load Balancer
VPN
Certificates19
Grouping Objects
Statistics
Security



Org VDC Networks

Управување со постоечки мрежи

Покрај делот за управување со виртуелните машини (Applications), во новиот портал е додаден и делот за управување со организациската мрежа и Edge gateway рутерот (Network). Веднаш по најавата на новиот портал https://vdc.neocloud.mk/tenant/(име_на_вашата_компанија)/, откако ќе го одберете виртуелен дата-центар, во зависност за која мрежна конфигурација е потребна промена се позиционирате во една од поткатегориите на Network (Слика 1).

👼 🖛 vCloud Director 🛛 🗙						
← → C 🔒 Secure https://vde						
Virtual Data Center					⑦	
÷		Orion Demo	Orion @vdc.neocloud.mk			
«						
ett ann linnaisen.	+ ADD × DELETE					
III Applications 🔹	Status Name	↑ ⊤ Gateway address	y Routing	Connected To	IP Pool Consumed	
Virtual Machines	Orion Demo LAN	192.168.0.1/24	Routed	Orion Demo	14%	
Network						
Network						
Edges						
Edges						
Security					1 - 1 of 1 items	

Слика 1

За почеток во Network табелата се претставени сите организациски мрежи, кои се создадени во Вашиот виртуелен дата центар. Со одбирање на посакуваната мрежа, под табелата се прикажуваат сите конфигурациски параметри за истата. Дополнително може да се избрише или додаде нова мрежа со помош на Add и Delete.

Во конфигурациските параметри за одбраната мрежа, покрај името и краткиот опис, се читаат и останатите вредностите: Gateway, Subnet (Network Mask), јавните DNS сервери како и статичкиот IP Pool од кој се доделуваат последователни адреси за сите нови членови на мрежата. Во долниот дел е прикажана табела на сите доделени IP адреси кои се асоцирани со одредена виртуелна машина и vApp (Слика 2).





v vCloud Director	× _								- 6
									orion admir
Feellous Virtual Data Ce	enter	Datacenters						(?)~	Organization Administ
←			Orion Demo O	rion 🛛 vdc.neoclou	id.mk				
	~	Edit Org VDC Network							
# Applications	~	Name *	Orion Demo LAN		Interface type	Internal			
Virtual Machines		Description			Guest VLAN Allowed	No			
Network	~								
Network			Share this network with other VDCs in this organization						
Edges Security		Address and DNS							
		Gateway address *	192.168.0.1		Static IP Pool Enter an IP range (format: 192.168.1.2 - 192.168	8.1.100)			
		Network mask *	255.255.255.0						
			Use Gateway DNS		192.168.0.50 - 192.168.0.100		MODIFY		
		Primary DNS	95.180.141.194						
		Secondary DNS	95.180.141.195						
		DNS suffix							
					Total IP adresses in pool: 51				
		Allocated IP addresses							
		IP Address	Deployed	VM		vApp			
		192.168.0.1	Yes	NSX Edge					
		192.168.0.50	No	MS Win Srv 20	16	2016Test			
		192.168.0.51	Yes	OdooAP		Odoo Test			
								1 - 8 of 8 items	
		SAVE DISCARD							

Слика 2

Создавање на нова мрежа

Доколку е потребно да се додаде нова мрежа, со одбирање на опцијата Add се прикажува нов преглед, каде потребно е да се внесат параметри за новата мрежа *(Слика 3)*.

👼 🖙 vCloud Director 🛛 🗙						- 0 ×
← → C 🔒 Secure https://vd						
Feelaw Virtual Data Center	Datacenters					orion.admin Organization Administrator
←		Orion Demo	Orion 🛛 vdc.neocloud.mk			
*						î
# Applications	+ ADD × DELETE					
vApps	Status Name	↑ 🔻 Gateway address	⊤ Routing	Connected To	IP Pool Consumed	
Virtual Machines	Orion Demo LAN	192.168.0.1/24	Routed	Orion Demo		14%
© Network ∽						
Network						
Edges						
Security						
						1 - 1 of 1 items
	Edit Org VDC Network					
	Name *	Orion Demo LAN	Interface type	Internal		
	Description		Guest VLAN Allowed	No		
			é			
		Share this network with other VDCs in this organization				
	Address and DNS					
	Gateway address *	192.168.0.1	Static IP Pool Enter an IP range (format: 192.165	312 - 1921681100)		
	Network mask *	255.255.255.0			ADD	
		Use Gateway DNS	192.168.0.50 - 192.168.0.100		MODIFY	
	Primary DNS	95.180.141.194	-			
	Secondary DNS	95.180.141.195	_			
	DNS suffix		Total IP adresses in pool: 51			





Покрај стандардните параметри потребно е да се одбере и каков тип ќе биде новата мрежа, дали ќе функционира како изолирана внатрешна мрежа, без пристап до Edge Gateway или рутирана мрежа. Во примерот е прикажано создавање на нова мрежа од типот **Routed network connecting to an existing edge gateway**, а од табелата е одбран единствениот постоечкиот Edge gateway за демо организацијата Orion. Важно е да се напомене дека доколку корисникот има повеќе од една претплата на vDC во neoCloud, од менито во полето Org VDC треба да се одбере соодветниот виртуелен дата центар. Во продолжение се внесуваат стандардните параметри: Gateway, Network mask, DNS сервери и статички IP Pool, каде потребно е да се внесе ранг на IP адреси (пр. 10.100.10.10 – 10.100.10.100) и со притиснување на Add во табелата ќе се додаде тој запис. За крај потребно е да се притисне Save за да се зачува конфигурацијата *(Слика 4)*.

👼 🐂 vCloud Director	×										- 0 ×
\leftarrow \rightarrow \mathbf{C} \square Secure ht											☆ :
rectour Virtual Data Ce	enter	Datacenters							Ì	@~	orion.admin Organization Administrator
←				Orion Demo Ori	ion @ vdc.neocloud.m	k					
	~	Org VDC *	Orion Demo	× .							^
ttt. Annelline Alema		Name *	Orion HTML5								
::: Applications	~	Description	Demo Org <u>vDC</u> Network								
vApps											
Virtual Machines											
O Network	~		Share this network with oth	ner VDCs in this organization							
Network		Type *	Isolated network within this	s Virtual Data Center							
Edges			 Routed network connecting 	g to an existing edge gateway							
Security											
		Edge Gateway *	Name	↑ ⊤ # External Networks	Ŧ	# Org VDC Networks	Ŧ	# Available Networks		Ŧ	
			Orion Demo	1		1		8			
										1 - 1 of 1 items	
			Allow Guest VLAN								
			Create as subinterface								
		Addross and DNS									
		Gateway address	10 100 10 1		st	atic IP Pool					- I
		Notwork mark	255 255 255 0		En	ater an IP range (format: 192.168.1.2 - 192	2.168.1.100)		100		
		Network mask			L	0.100.10.10-10.100.10.100			ADD		
			Ose Gateway DNS								
		Drimony DNS	05 190 141 104								
		Primary DNS	95.180.141.194								
		Secondary DNS	95.180.141.195								*
				Сли	ика 4						



Edge Gateways

Во новата верзија на vCloud Director управувањето со сите функционалности и сервиси на Edge Gateway уредите е исклучително преку HTML5 порталот. Сите уреди се надградени на последна верзија, со што сите промени кои треба да бидат направени на некој од сервисите преку Flash порталот, ќе бидете пренасочени кон HTML5 порталот *(Слика 5)*. Во оваа верзија тоа е единствениот сегмент кој е комплетно изработен во HTML5.

👼 🖉 wCloud Director	× V 🛃 VMware vCloud Dire	ector ×						- 0 ×
\leftrightarrow \Rightarrow ${f C}$ $\ $ Secure $ $ https:								
Orion Company						orion.a	dmin (Organization Administrator)	Preferences Help - Logout
🚮 Home 🖾 My Cloud 📋 Ca	talogs 🖧 Administration							
Administration	强 Orion Demo							
Cloud Resources	vApps vApp Template	s Media & Other Storage Policies Edge G	ateways Org VDC Networks Affinity Rul	95				
Recent Items	@-						All	C 0
A Orion Demo	Name	1 A Status	Multi-Interface Mode	# Used NICs	Distributed Routi	# External Networks	# Organization VDC Networks	HA Status
Members	🥺 Orion Demo	Original Dama	✓	2	-	- <u>ka</u> 1	<u> 4</u> 1	Disabled
S Groups		Edge Gateway Services						
A Lost & Found		External IP Allocations						
✓ Settings		Re-Deploy Synchronize Syslog Server Settings						
@ Email		Properties						
Policies								
Guest Personalization								
A Metadata								
				-				
0 Running 🛇 0 Failed				ReoCloud Virtual Data Center				Powered by VmWare

Слика 5

Доколку сте најавени директно преку HTML5 порталот, од менито во Network се одбира табот Edges *(Слика 6)*. Во долниот дел се прикажани информации поврзани со одбраниот Edge gateway од табелата, од каде што можете да ја прочитате и јавната IP адреса за самиот уред.



	c.neocloud.mk/ter	nant/orion/vdcs/	92ccc077-2h37-4965-a84c-29	cb819e4a33/eo	doe-oateways									-	8 ×
Fieldour Virtual Data Center	⊟ Da	atacenters												orion.adm Organization Admin	nin nistrator
÷					Orion Demo	Orion @vdc.neoclou	id.mk								
Applications	& CONFIGUR	RESERVICES	CONVERT TO ADVANCED												
vApps	Status	Name	↑ ▼	Used NICs		# External Networks			т <u>4</u>	f Org VDC Netwo	orks	Ψ	HA Status		Ŧ
Virtual Machines	\odot	Orion Demo		2		1			1				Disabled		
Network															
Edges															
Security														1-10	f 1 items
	Edge Cate	unu Catting													
	Edge Gale	way setting	5												
	General		Orion Demo				Edge Gateway	/ Configu	uration		Compact				
	Description						High Availabili	ty			No				
	ID														
	Addresses						Default Gate	way							
	External Netw	vorks	Subnets		IP Addresses		External Netw	orks			SiteB laaS Public 01				
	SiteB laaS Pu	ublic 01	95.180.141.0/25		95.180.141.29		Delaut Gatew	dy			95.100.141.120				
	Sub-allocated	I IP Addresses					Rate Limits								
	External Netw	rork	Sub-a	illocated IP Pool			Enabled	Exterr	nal Netw	orks	Incoming Rate Limit	Out	tgoing Rate Limit		
	SiteB laaS Pu	ublic 01					No	SiteB	3 IaaS Pu	iblic 01	10	10			

Слика б

Со одбирање на постоечкиот Edge gateway од табелата и притиснување на **Configure Services**, се отвара нов прозорец во кој се сместени сите дополнителни сервиси како што се: Firewall правила, DHCP, NAT, Routing, Load Balancer, VPN, Certificates, Statistics и др.

Firewall

Прв сервис кај Edge gateway се firewall правилата. Над главната табела постојат четири опции: додавање на ново правило, бришење на постоечки правила и промена на позиција (горе/долу). При додавање на ново правило *(Слика 7)*, веднаш се појавува нов запис во табелата каде секое поле е интерактивно и може да се менува доколку се позиционира курсорот.

		-				 Organization 	Ad
Edge Ga	iteway - Orion HTML5	Test					
Firewall [DHCP NAT Routing Load B	Balancer VPN (Certificates Grouping Objects Statistics Edge	Settings			
Firowall E	lulos						
newdli P	uies						
nabled							
+	X • •						
how only use	er-defined rules						
No.	Name	Type	Source	Destination	Service	Action	
140.							
140.							
1	Outbound Traffic	User	Any	Any	Any	Accept	
/	Outbound Traffic	User	Any	Any	Any	Accept	
×	Outbound Traffic	User	Any	Any	Any	Accept	
1~	Outbound Traffic	User	Any	Any	Any	Accept	
14	Outbound Traffic	User	Any	Any	Any	Accept	
1	Outbound Traffic	User	Any	Any	Any	Accept	
1~	Outbound Traffic	User	Any	Any	Any	Accept	
1~	Outbound Traffic	User	Any	Any	Any	Accept	
1 ∕	Outbound Traffic	User	Any	Any	Any	Accept	
1~	Outbound Traffic	User	Any	Any	Any	Accept	
1~	Outbound Traffic	User	Any	Any	Any	Accept	
14	Outbound Traffic	User	Any	Any	Any	Accept	



Правата колона е редниот број на правилото во табелата. Со притиснување на самата бројка можете да ја менувате состојбата на правилото, односно дали ќе биде во функција Уили не 🧭. Во втората колона со притиснување на полето за името може да се промени името на правилото. Кога сте позиционирани над полињата Source и Destination се појавуваат две нови опции, додавање на IP ℙ или објект 🕂 *(Слика 8)*.

🐉 🗎 Secure https://vdc.neocloud.mk/tenan				
rirtual Data Center				C Organization Ac
Edge Gateway - Orion HTML	5 Test			
Firewall DHCP NAT Routing Lo	ad Balancer VPN Certificates Grouping Object	s Statistics Edge Settings		
irewall Rules				
nabled				
ihow only user-defined rules	<u>,</u>			
No. Name	Type Source	Destination	Service	Action
1 Outbound Traffic	User Any	IP 🛨 Any	Any	Accept

Слика 8

Доколку се одбере опцијата IP, потребно е да се внесе IP адреса, опсег или опцијата any *(Слика 9)*. Со новата верзија на порталот може во едно правило да се внесуваат поединечни IP адреси од виртуелни машини за кои е потребно да важи одредено правило. Откако ќе биде додадена IP адресата, со повторно притиснување на опцијата IP може да се додаде дополнителна адреса.

Source IP Address	×
Value:	10.100.10.10
Valid values can be IP address, CIDR	IP range or the keyword any.
	DISCARD

Слика 9



Во главната табела со притиснување на Х се отстранува записот од правилото (Слика 10).

👼 🖉 ym vCloud Director 🛛 🗙 💽					- 0	×
← → C Becure https://vdc.neocloud.mk/tenant/orion/r						
Virtual Data Center					C · orion.admin Organization Administr	itor
Edge Gateway - Orion HTML5 Tes	st				×	
Firewall DHCP NAT Routing Load Balar	ncer VPN Certificates	Grouping Objects Statistics Edge	Settings			
Firewall Rules						
A This rule set has unsaved changes. Save to start depl	loying.				Save changes Discard changes	
Enabled						
+ × + V						
No. Name	Type Source		Destination	Service	Action	
1✔ Outbound Traffic	User 10.100.10.10	× 0 P +	Any	Any	Accept v	ns .

Слика 10

Опцијата за додавање објекти 🔹 е нова и нуди многу повеќе опции. Може да се одбира помеѓу интерфејс, виртуелна машина, организациска мрежа, сет на IP адреси и безбедносни групи. За безбедносни групи и сет на адреси е опфатено во делот за *Grouping Objects* подолу во прирачникот. Доколку се одбира gateway интерфејс *(Слика 11)*, покрај јавната адреса на самиот уред и организациската мрежа постојат и познатите опции: Internal, External и ALL (Any).

GATEWAY INTERFACES > Filter SiteB IaaS Public 01 Orion HTML5 Test LAN Internal External Current page: 1	Gateway Interfaces VirtualMachines OrgVdcNetworks Ip Sets Security Groups	ter
--	---	-----

Слика 11



Во примерот го одбираме интерфејсот Internal и го додаваме во листата со помош на стрелката (Слика 12). На овој начин сите внатрешни мрежи ќе добијат пристап кон надвор, односно кон интернет.

Browse objects of type: GATEWAY INTERFACES •	Gateway Interfaces	~
Filter		Filter
 SiteB laaS Public 01 Orion HTML5 Test LAN 	▲ ←	[⊗] Internal
🗸 🖗 Internal		
	-	
Current page: 1		
		DISCARD



Во колоната Service од табелата на правила, се дефинира протоколот и портата за правилото. Со притиснување на 🔹 во полето за сервис се појавува нов прозор каде што е потребно да се одбере типот на протокол и порта за Source и Destination *(Слика 13)*.

Add Service	×
Protocol	Any ~
Source Port	
Leaving this field empty will make this r	Any ule apply to any port
Destination Port	any
Leaving this field empty will make this n	ule apply to any port
	DISCARD
	Слика 13

Последната колона, Actions, од табелата на правилата се однесува на акцијата за firewall правилото, дали сообраќајот ќе се дозволува или ќе се забранува, односно Allow/Deny *(Слика 14)*.





Action	
Accept	
Accept	T
Accept	
Deny	

Откако ќе се постават сите firewall правила во последниот чекор потребно е да се зачува новата конфигурација на Edge gateway рутерот. Истото се прави со притиснување на *Save Changes* во жолтата статусна лента, која е позиционирана во горниот дел *(Слика 15)*.

vm vCloud Director	×						- 0	
C 🔒 Secure h								
Virtual Data Ce	enter					ý 0° ,	orion.admin Irganization Administr	
Edge Gate	way - Orion HTML5 Tes	st					×	
Firewall DHC	P NAT Routing Load Bala	incer VPN	Certificates Grouping Objects Statistics Edg	e Settinas				
Firmuell Dular								
Firewall Rule	es							
▲ This rule set	has unsaved changes. Save to start dep	oloying.				Save changes E	iscard changes	
Enabled								
	× • •							
Show only user-de	efined rules							
No.	Name	Туре	Source	Destination	Service	Action		
1🛩	firewall	Internal High	vse	Any	Any	Accept	v	
2✔	Outbound Traffic	User	internal	Any	any:any	Accept	∇	
3•	default rule for ingress traffic	Default Policy	Any	Any	Any	Accept	∇	
sid(0)								
				Слика 15				





DHCP

Опцијата за динамичко доделување на IP адреси е повторно дел од Edge gateway уредот. На самиот почеток потребно е да се овозможи сервисот во полето *DHCP Service Status (Слика 16)*. Во првиот дел (Pools), се поставуваат параметри за адресниот простор за кој е потребен DHCP, како и пропратните параметри потребни за конфигурација на истиот (Domain, DNS, Gateway, Mask и Lease)

Virtual Data Center Edge Gateway - Orion HTML5 Test Firewall DHCP NAT Routing Load Balancer Pools Bindings Relay	VPN Contificates Grounion Objects	nureonureu		🖄 🕐 - 🛛 orion.ac
Edge Gateway - Orion HTML5 Test Firewall DHCP NAT Routing Load Balancer Pools Bindings Relay	VPN Certificates Grouping Objects			C Organization Ac
Firewall DHCP NAT Routing Load Balancer Pools Bindings Relay	VPN Certificates Grouping Objects			
Firewall DHCP NAT Routing Load Balancer Pools Bindings Relay	VPN Certificates Grouping Objects			
	The octaneous of opping objects	Statistics Edge Settings		
DHCP Pools				
Unice status				
+ 3 ×	N C	Auto Configure DNC	D-f-lk O-t-	Lana Time (Generale)
IP Range Prime	imary Name Server	Auto Configure DNS	Default Gateway	Lease Time (Seconds)

Слика 16

Како дополнителни сервиси во новата верзија се Bindings и Relay. Во делот за Bindings се поставуваат резервации на IP адреси од DHCP за одредена виртуелна машина, односно MAC адреси. Делот за Relay служи за пренасочување кон друг DHCP сервер.



NAT

r

Услугата NAT функционира со иста логика како и кај Flash порталот. Се одбира помеѓу двата стандардни типови SNAT (Source NAT) и DNAT (Destination NAT) и се поставуваат вредности за посакуваните транслациски правила *(Слика 17)*.

C Scare https://vdc.needodud.mk/innamt/orion/network/odge-gateways/2bi3252-ald0-4d36-bi35b-32bb7ebd378b Virtual Data Center O Edge Gateway - Orion HTML5 Test Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings NAT Rules	orion.admin rezeiton Administr X
Vritual Data Center	orion.admin anzation Administr X
Edge Gateway - Orion HTML5 Test Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings NAT Rules tomar Bulle Type Action Applied on Original Translated Port PAddress Port PAddress Port	×
Frewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings NAT Rule ************************************	
NAT Rules NAT Rule x + ID Type Action Applied on Original Translated IP Address Port IP Address Port	
ID Type Action Applied on Original Translated Protocol Enabled Logging Description IP Address Port IP Address Port Port Enabled Logging Description	
ID Type Action Applied on Original Translated Protocol Enabled Logging Description	
Problems Pulk Problems Pulk	

Слика 17

Во прирачникот даден е пример за создавање SNAT за пропуштање на целиот сообраќај кон интернет за локалната мрежа и DNAT за FTP сообраќај кон еден од серверите *(Слика 18)*.

Add SNAT Rule	>	<	Add DNAT Rule	×
Applied On:	SiteB laaS Public 01		Applied On:	SiteB IaaS Public 01
Original Source IP/Range *	10.100.10.0/24		Original IP/Range *	95.180.141.42
Translated Source IP/Range *	95.180.141.42		Protocol	TCP v
Description	Outbound NAT		Original Port	21 💌
			ІСМР Туре	Any ~
			Translated IP/Range *	10.100.10.10
Enabled			Translated Port	21 💌
Enable logging			Description	FTP for server
	DISCARD			•
]		DISCARD





Како и досега потребно е да се зачува промената во главниот предлог (Слика 19).

÷	vCloud Director	× V 🛃 VMware v	Cloud Director	×		01171417				_				- 0
		e nttps://vac.neocioua.m												
	Virtual Dat	a Center										Ŀ		Organization Administrat
£	Edge Gateway - Orion HTML5 Test											\times		
0	Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings													
Ę	NAT Dulas													
NAT Rules									Discard chapter					
		s tours our s											Jave changes	Discard changes
	Show only us	er-defined rules	2	×	¥									
	ID	Туре	Action	Applied on	Original		Translated		Protocol	Enabled	Logging	Description		
					IP Address	Port	IP Address	Port						
		User-defined	SNAT	SiteB laaS Public 01	10.100.10.0/24		95.180.141.42			~	×	Outbound NAT		
		User-defined	DNAT	SiteB laaS Public 01	95.180.141.42	21	10.100.10.10	21	tcp	×	×	FTP for server		
		User-defined	DNAT	SiteB laaS Public 01	95.180.141.42	21	10.100.10.10	21	tcp	*	×	FTP for server		
							Слик	a 19						

Routing

Како и во претходната верзија постои можност за рутирање на сообраќајот, доколку е потребно. Во новата верзија покрај статичкото рутирање, постои можност за динамичко рутирање со помош на OSPF и BGP протоколите *(Слика 20)*.

#	vm vCloud Director X		- 0	×
← -	C Secure https://vdc.neocle			
Test	Virtual Data Center		Orion.admin Organization Administration	tor
6	Edge Gateway - Oric	on HTML5 Test	×	
ę	Firewall DHCP NAT R	Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings		
ş	Routing Configuration Static F	Routes		
	Routing Configuration			
	ECMP			
	STATIC ROUTING DEFAULT GATE	EWAY		
	Applied On	SiteB lasS Public 01 🔹 🚯		
	Gateway IP *	95180.141126		15
	MTU .	1,500		
	Description			
	DYNAMIC ROUTING CONFIGURA	ATION		
	Router ID	◆		
	Enable Logging	Disabled		
	Log Level	Info v		
	OSPE	⊘ Disabled	•	

Слика 20



Load Balancer

Load Balancer е следниот сервис кој е вклучен во Edge Gateway уредот. Во почетниот дел потребно е да се овозможи користење на сервисот. Вториот чекор е наменет за поставување на апликациските профили, односно начинот на кој ќе се одржување сесија во зависност од типот на протокол (TCP, HTTP, HTTPS и UDP) методот во зависност од протоколот (Source IP, MSRDP и Cookie). Дополнително може да се користат и сертификати кои се поставени во Certificates. Делот за Service Monitoring се поставени три записи за следење на TCP, HTTP и HTTPS *(Слика 21)*.

 orion admin Organization Admin
×
Max Retries
Max Retries
3
3
3

Слика 21

Четвриот чекор е делот за Pools или дефинирање на сервери кои ќе бидат дел од Load Balance групата. Покрај стандардните параметри при додавање на нов Pool потребно е да се одбере алгоритамот со кој ќе се извршува балансирањето *(Слика 22)*.

Во делот за одбирање на метод постојат шест избора: *Round Robin, IP Hash, Least Connected, URI, HTTP Header* и *URL*.

- Round Robin претставува алгоритам каде пренасочувањето на сообраќајот се одлучува по пат на одбирање на следната дестинација од листата на членови.
- IP Hash е тип на алгоритам, во кој се извршува математичко пресметување на секој пакет од IP адресата на изворот и на тој начин се одлучува кој од двата учесника ќе биде искористен.
- Least Connected алгоритамот поседува евиденција на активни конекции за секој од членовите и испраќа нова конекција до серверот со најмал број на активни конекции.
- URI (Uniform Resource Identifier) е низа од карактери кои се користат за да се идентификува името на ресурсот. Ваквиот тип на идентификација овозможува интеракција преку мрежа користејќи специфични протоколи. Овој тип на алгоритам е достапен само кај НТТР сервисот.
- HTTP Header претставува тип на алгоритам каде што во секое барање (HTTP request) потребно е да биде содржана информацијата која е предефинирана во Algorithm Parameters.
- URL е проверка на специфичен аргумент во секој query string на HTTP GET барање испратен до Load Balancer.



Add Pool		×
Name *	LB Pool	^
Description	Test	
Algorithm	ROUND_ROBIN ~	
Algorithm Parameters	ROUND_ROBIN IP_HASH LEASTCONN URI HTTPHEADER	
Monitors	URL default_https_monitor ~	
Transparent		
Members		Į.
En Name IP Address	We Mo Port Min Conn Max Conn	•
	DISCARD	

Слика 22

Во табелата за *Members* потребно е да се додадат најмалку два члена кои ќе ја сочинуваат Load Balance групата, каде што дефинираме IP адреса, тежинска вредност и портата на која ќе се мониторира *(Слика 23)*.

Add Pool			×
Add Member			×
Enabled			
Name *	Server	_	
IP Address *	10.100.10.10	_	
Port	443		
Monitor Port	443		
Weight *	1		
Max Connections	null		
Min Connections	null		
	D	ISCARD	КЕЕР
	D	ISCARD	KEEP





Bo Application Rules, можат да се поставуваат скрипти како апликациски правила. Во последниот чекор, Virtual Server, се дефинира виртуелниот сервер кој ќе биде задолжен за таа група, како и примена на апликациските правила (во делот Advanced) кои се поставени *(Слика 23)*.

General Advanced		
Enable Virtual Server		
Enable Acceleration		
Application Profile	~	
Name *	Test VirSer LB	
Description	Test	
IP Address *	95.180.141.42	SELECT
Protocol *	HTTPS ~	
Port *	443	
Default Pool	~	_
Connection Limit		
Connection Rate Limit (CPS)		_
		·
	ſ	

Доколку Ви е потребна техничка помош околу поставување на сервисот Load Balancer, тимот на neoCloud Ви стои на располагање.

VPN

За користење на услугата VPN најнапред треба да биде овозможи во првиот чекор (Activation Status). Доколку се користи услугата VPN и во организацијата има IPSec тунели, овој чекор не е потребен *(Слика 25)*.

idge Gateway - Orion HTML5 Test	×
irewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings	
Sec VPN	
Psec VPN Configuration	Save changes Discard changes
ctivation Status 🖋 Global Configuration Logging Settings IPsec VPN Sites	
sec VPN Service Status	
Critico 25	



Во следниот чекор, Global Configuration (Слика 26), се поставува глобален pre-shared клуч кој може да се користи при создавање на IPsec VPN каде што партнерската страна не поседува фиксна јавна IP адреса (при создавање на таков VPN во полето за Peer се внесува вредноста Any, наместо IP адреса). Дополнително може да се постави и сертификат, доколку се користат за автентикација при воспоставување на тунел. За користење на сертификати претходно е потребна конфигурација на сервисот Certificates, кој е опишан подолу во прирачникот.

	🖛 vCloud Director 💦 🕹 VMware vCloud Director 🗴 💽	- 0	×
	🖓 🦉 兽 Secure https://vdc.neodoud.mk/tenant/orion/network/edge_gateways/2bv9292e-afd09-4656-b15b-a9bb7eb4478b		
Sec.10	Virtual Data Center	⊘ ~ orion.admin Organization Administr	stor Č
C	Edge Gateway - Orion HTML5 Test	×	
ę	Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings		
Ę	IPsec VPN		
	IPsec VPN Configuration		
	A You have unsaved changes.	Save changes Discard changes	
	Activation Status Global Configuration Logging Settings IPsec VPN Sites		
	Change Shared Key		
	Pre-Shared Key *		
	The global pre-shared key (PSR) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting. 7displayPsk		ns
	Enable Certificate Authentication		
	Certificate authentication will only be enabled if a service certificate is set.		
	Service Certificates CA Certificates CRLs		
	Name Common Name (CN) Issuer Common Name Valid From Not After		
	I contraction of the second		

Слика 26

Logging Settings е делот во кој може да се читаат логови од различни категории поврзани со VPN тунелите, доколку се поставени параметри за syslog сервер. Во последниот чекор, IPSec VPN Sites, се поставуваат конфигурациите за IPsec VPN. На иконата + се започнува конфигурацијата. Како и претходно потребно е да се внесат параметри за локалниот дел, параметри за партнерската страна со која ќе се поврзуваме, типот на енкрипциски алгоритам, типот на автентикација PSK или со сертификати, клуч и Diffie-Hellman Group *(Слика 27)*. Дополнително има опција и за продолжување на опсегот.



Add IPsec VPN		×
Enabled		^
Enable perfect forward secrecy (PFS)		
Name	Test VPN	
Local Id *	95.180.141.42	
Local Endpoint *	95.180.141.42	
Local Subnets *	10.100.10.0/24	
Subnets should be entered in CIDR form	nat with comma as separator.	
Peer Id *	95.180.140.100	
Peer Endpoint *	95.180.140.100	
Endpoint should be a valid IP, FQDN or	any.	
Peer Subnets *	192.168.2.0/24	
Subnate chould be entered in CIDD form	nat with comma as constator	*
	DIS	CARD KEEP



Новитет во оваа верзија е менувањето на постоечки VPN конфигурации доколку постои промена во некој од параметрите.

Certificates

Како една од дополнителните опции во новата верзија е секако и можноста за користење на сертификати, за сервисите Load Balancer или VPN. Потребно е да се додадат потребните параметри и да се прикачат постоечки сертификати или пак да се генерира CSR *(Слика 28)*. Доколку има потреба од користење на сертификати во виртуелен дата центар, тимот на neoCloud Ви стои на располагање за техничка помош.

Initial Data Center Image: Center Control of Control of Center Control		
Edge Gateway - Orion HTML5 Test irevall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings iSL Certificates service certificate + care + care + some certificate generate from csr # set.r-sion csr #	irtual Data Center	ଟି ି ୍ orion.adn Organization Admit
irewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings SL Certificates +service CERTIFICATE + CAL + CRL + SIGNED CERTIFICATE GENERATED FOR CSR # SELF-SIGN CSR #	idge Gateway - Orion HTML5 Test	×
	irewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects Statistics Edge Settings	
+ SERVICE CERTIFICATE + CAL CERTIFICATE + CRL + CRL + SIGNED CERTIFICATE GENERATED FOR CSR & SELF-SIGN CSR x	SL Certificates	
Inne Dine Commen Name Validity	+ SERVICE CERTIFICATE + CA CERTIFICATE + CRL + CR + SIGNED CERTIFICATE GENERATED FOR CSR & SELF-SIGN CSR x	
rame type Common Name Valious	Jame Type Common Name Validity	



Grouping Objects

Grouping Objects е новитет преку кој го поедноставува процесот на создавање на безбедносни правила. Grouping Objects се објекти кои се дефинираат (IP Sets и MAC Sets) или се претходно дефинирани (Services и Service Groups) и понатаму може да се употребуваат при додавање на firewall правила *(Слика 29)*. Во IP Sets и MAC Sets потребно е да се додадат објектите со соодветните поединечни адреси или опсег на адреси. Во делот Services постојат голем број на претходно дефинирани објекти за разни типови на сервиси кои се идентификуваат по протокол и порта, додека во Service Groups се објектите кои ги групираат сервисите за да идентификуваат целосна апликација (пр. Exchange, Oracle, SAP, Active Directory итн.)

vCloud Director ×			-	c
C Secure https://vdc.neocloud.mk/tenant/orion/netw				
Virtual Data Center			⑦ ← orion.a Organization #	dmii Iminir
Edge Gateway - Orion HTML5 Test Firewall DHCP NAT Routing Load Balancer IP Sets MAC Sets Services <u>Service Groups</u>	VPN Certificates Grouping Objects Statistics Edge Settings			×
Application Groups				l
Name	Description	Scope	Inheritance	-
MS Exchange 2010 Client Access Servers	MS Unflied Messaging server, IMAP, POP3, KERBEROS, DNS, IMAP_SSL, HTTP, HTTPS, LDAP Global Catalog, MS_RPC_TCP, KERBEROS-UDP, LDAP, POP3_SSL, DNS-UDP, LDAP-UDP	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	
MS Exchange 2010 Mailbox Servers	MS Customizable, KERBEROS, DNS, LDAP Global Catalog, MS-DS-TCP, MS_RPC_TCP, MS Replication service, KERBEROS- UDP, LDAP, Office communication server, DNS-UDP, LDAP-UDP	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	
MS Exchange 2010 Transport Servers	EdgeSync service, KERBEROS, DNS, HTTPS, LDAP Global Catalog, MS_RPC_TCP, KERBEROS-UDP, LDAP, DNS-UDP, SMTP_TLS, SMTP, LDAP-UDP	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	
MS Exchange 2010 Unified Messaging Server	KERBEROS, DNS, MS Unlifed Messaging server - Client Access, HTTP, HTTPS, LDAP Global Catalog, MS_RPC_TCP, KERBEROS-UDP, LDAP, DNS-UDP, SMTP, MS Unlifed Messaging server-Phone, LDAP-UDP	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	
Microsoft Active Directory	Active Directory Server UDP, Windows-Global-Catalog, NBDG-Broadcast, KERBEROS, SOAP, MS-DS-UDP, NTP Time Server, DNS, Windows-Global-Catalog-over-SSL, DHCP-Server, NBDG-Unicast, NBNS-Unicast, MS-DS-TCP, MS_RPC_TCP, WMS, KERBEROS-UDP, LDAP-over-SSL, WINS-UDP, LDAP, NBNS-Broadcast, DNS-UDP, Active Directory Server, SMTP, LDAP-UDP, NBSS	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	
Microsoft Exchange 2003	NNTP_SSL, Site Replication service, Routing Engine service, IMAP_POP3, For X.400 connections over TCP, IMAP_SSL, HTTP, Exchange ActiveSync, HTTPS, MS_RPC_TCP, LDAP, POP3_SSL, NNTP, SMTP	Orion Demo (92ccc077-2b37-4965-a84c-29cb819e4a33)	~	

Слика 29



Statistics

Уште еден новитет покрај претходно споменатите во оваа верзија на порталот, покрај метриките за секоја вритуелна машина, додадена е и статистика за бројот на конекции на firewall *(Слика 30)*. Доколку се користи Load Balancer, во графикот ќе се појави и статистика за овој сервис.



Слика 30

Security

Security делот ги содржи напредните функционалности од продуктот NSX, односно Distributed Firewall, каде е можна микро-сегментација на сообраќајот во виртуелниот дата центар.

Концептот на микро-сегментација е воведен во модерните безбедносни препораки, и овозможува дефинирање на безбедносни правила на ниво на виртуелна машина, па така виртуелните машини меѓусебно ќе комуницираат (или нема да комуницираат) согласно дефинираните правила, иако се во иста мрежа. Правилата овозможуваат автоматизација на процесите преку динамички дефиниции – според имиња на виртуелни машини, додавање на безбедносни тагови и тип на оперативен систем. Така, на пример при креирање на Windows Server виртуелна машина автоматски ќе се овозможат правилата за Remote Desktop и Ping.

Оваа опција е достапна на барање на корисник, за која се предвидени посебни цени и конфигурации. Доколку сте заинтересирани, контактирајте не́ на <u>support@neocloud.mk</u> за повеќе информации.