

HTML5 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.



За 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.

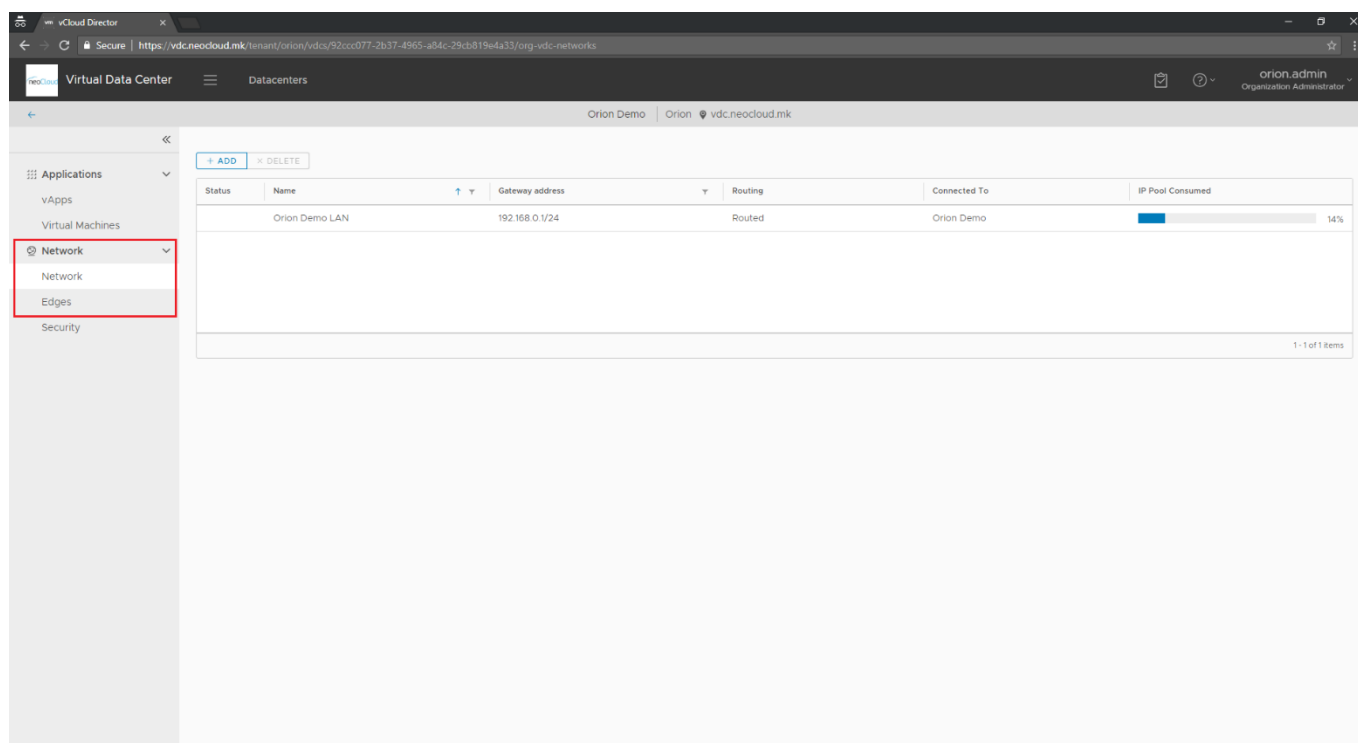
Содржина

Org VDC Networks.....	3
Управување со постоечки мрежи	3
Создавање на нова мрежа	4
Edge Gateways.....	6
Firewall.....	7
DHCP.....	12
NAT	13
Routing.....	14
Load Balancer	15
VPN	17
Certificates.....	19
Grouping Objects.....	20
Statistics	21
Security	21

Org VDC Networks

Управување со постоечки мрежи

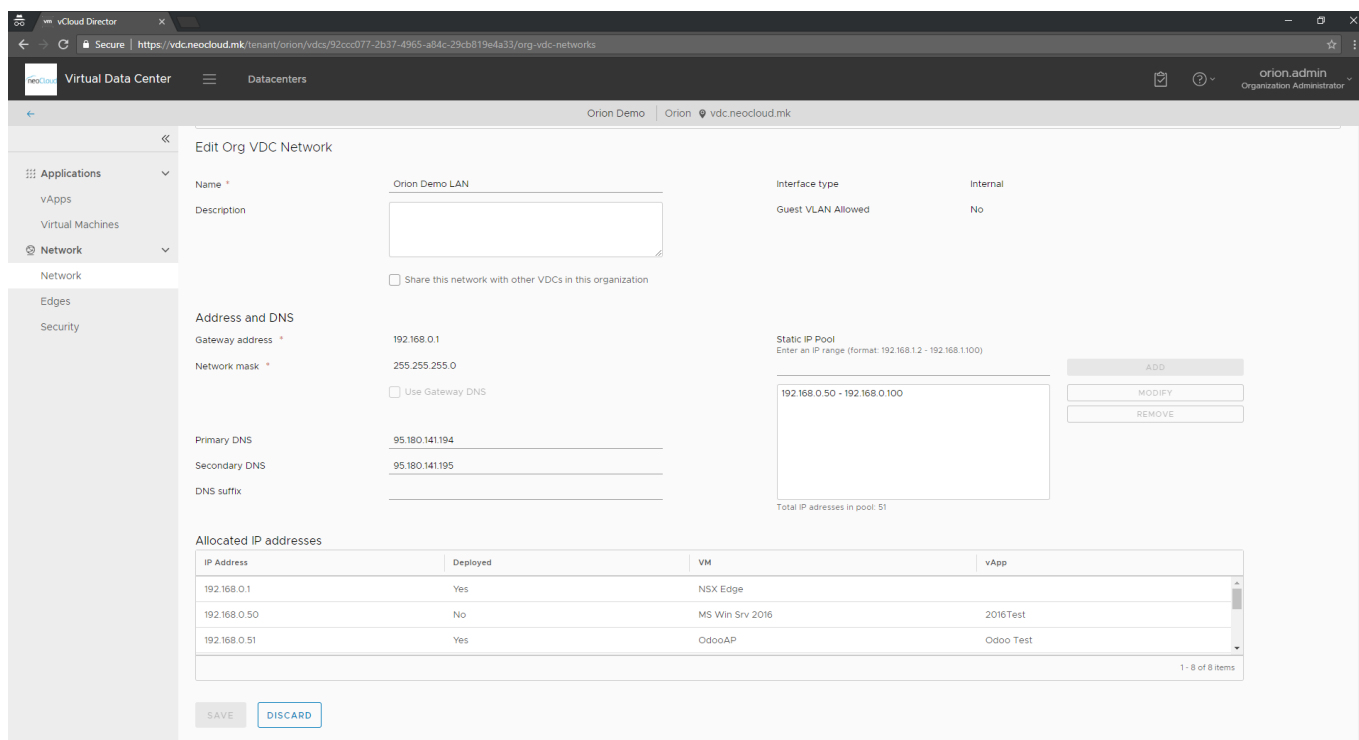
Покрај делот за управување со виртуелните машини (Applications), во новиот портал е додаден и делот за управување со организациската мрежа и Edge gateway рутерот (Network). Веднаш по најавата на новиот портал [https://vdc.neocloud.mk/tenant/\(име_на_вашата_компанија\)/](https://vdc.neocloud.mk/tenant/(име_на_вашата_компанија)/),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



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**.

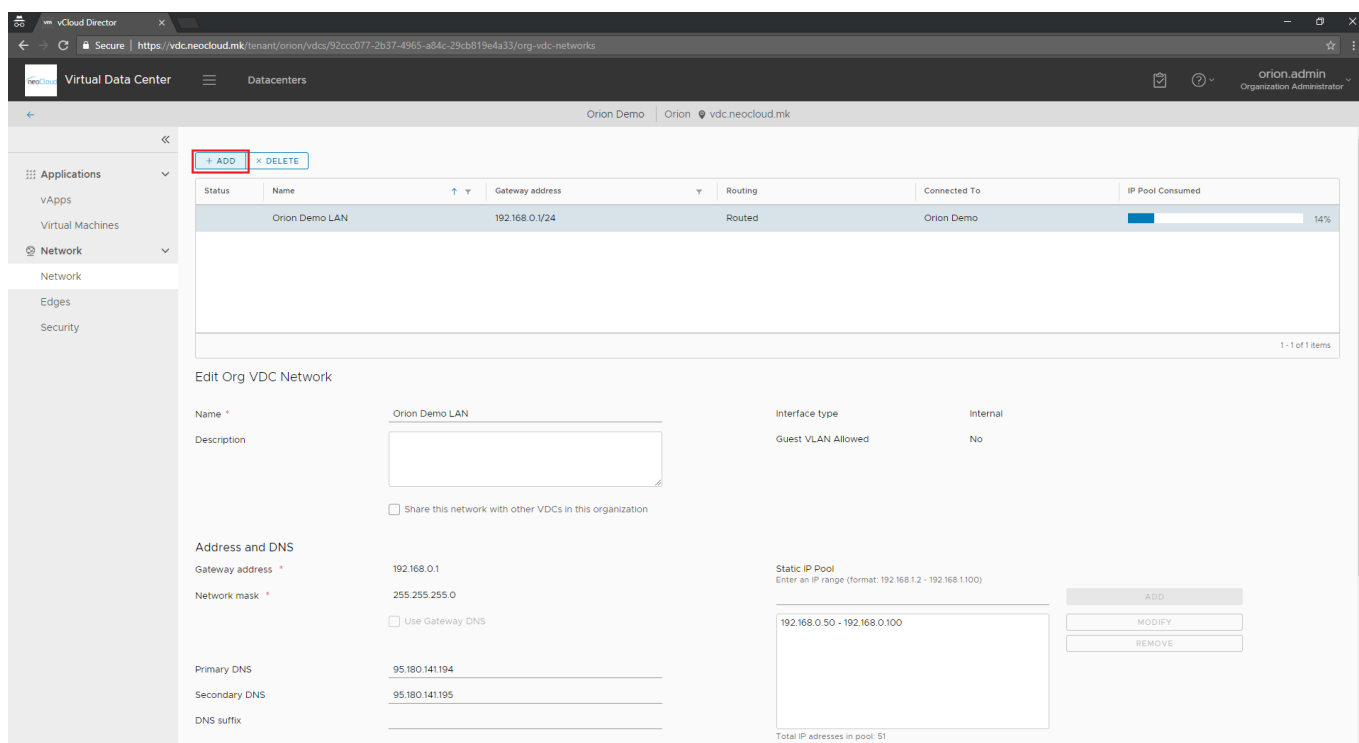
Во конфигурациските параметри за одбраната мрежа, покрај името и краткиот опис, се читаат и останатите вредностите: Gateway, Subnet (Network Mask), јавните DNS сервери како и статичкиот IP Pool од кој се доделуваат последователни адреси за сите нови членови на мрежата. Во долниот дел е прикажана табела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



Слика 2

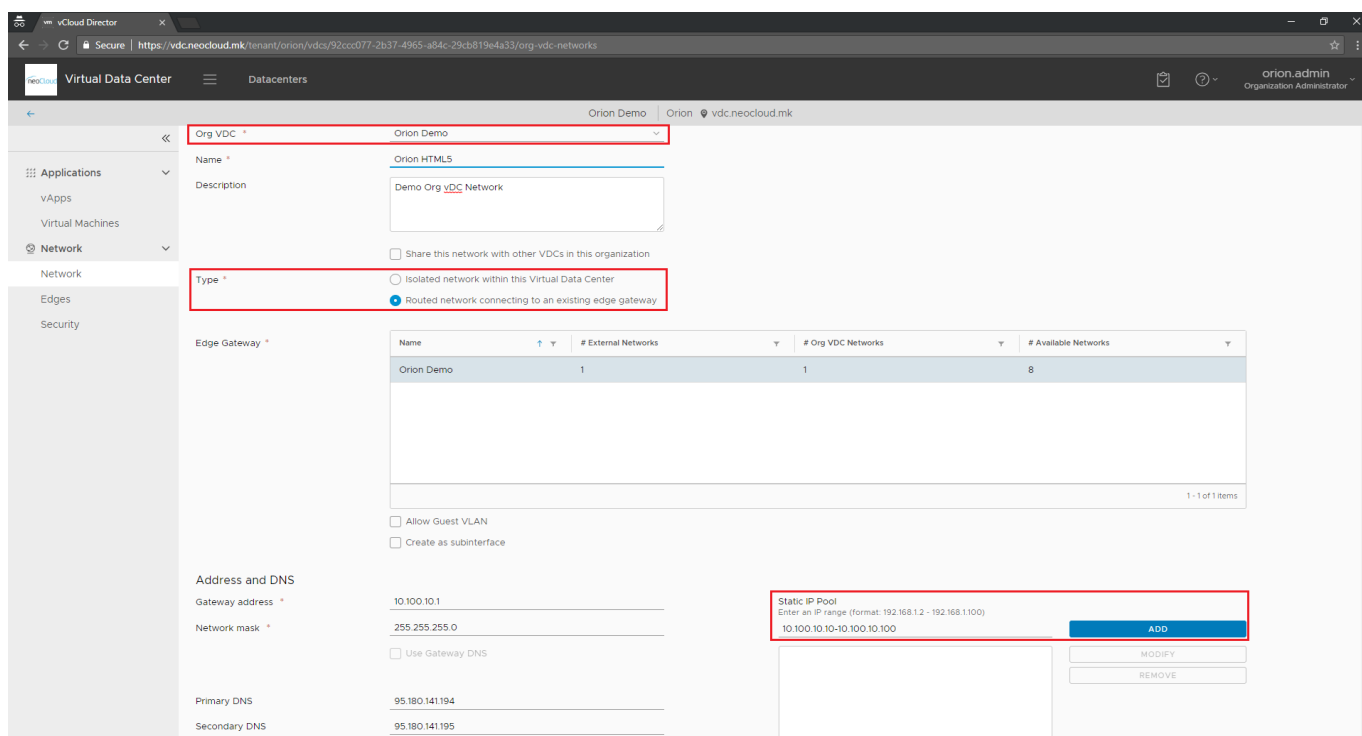
Создавање на нова мрежа

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).



Слика 3

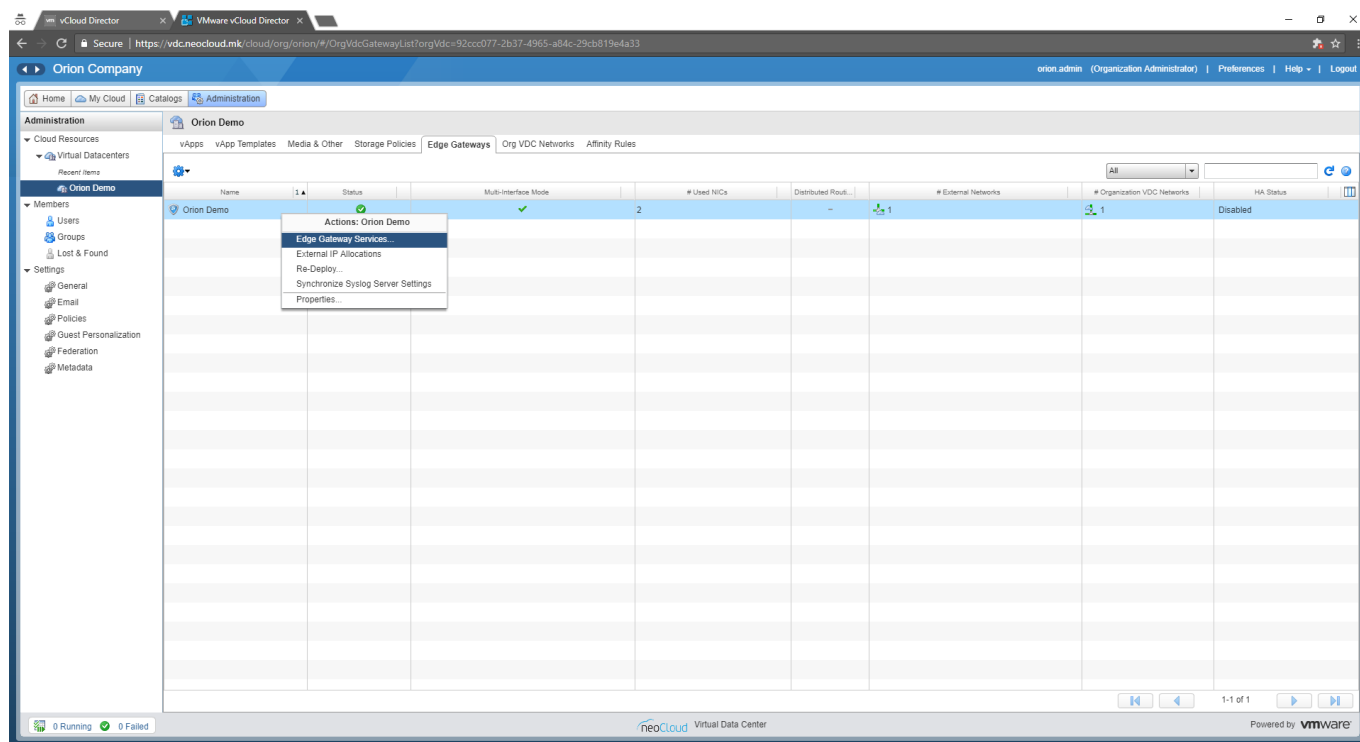
Покрај стандардните параметри потребно е да се одбере и каков тип ќе биде новата мрежа, дали ќе функционира како изолирана внатрешна мрежа, без пристап до Edge Gateway или рутирани мрежа. Во примерот е прикажано создавање на нова мрежа од типот **Routed network connecting to an existing edge gateway**, 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).



Слика 4

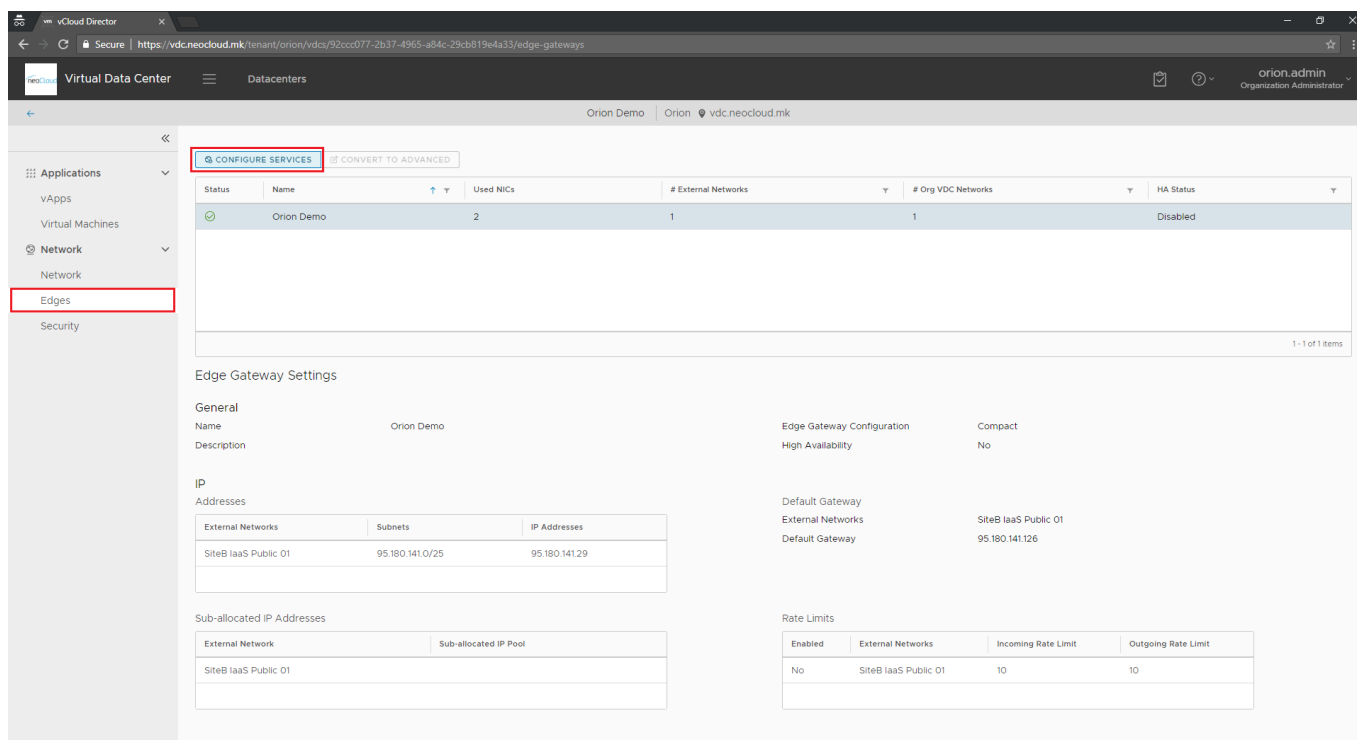
Edge Gateways

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.



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.

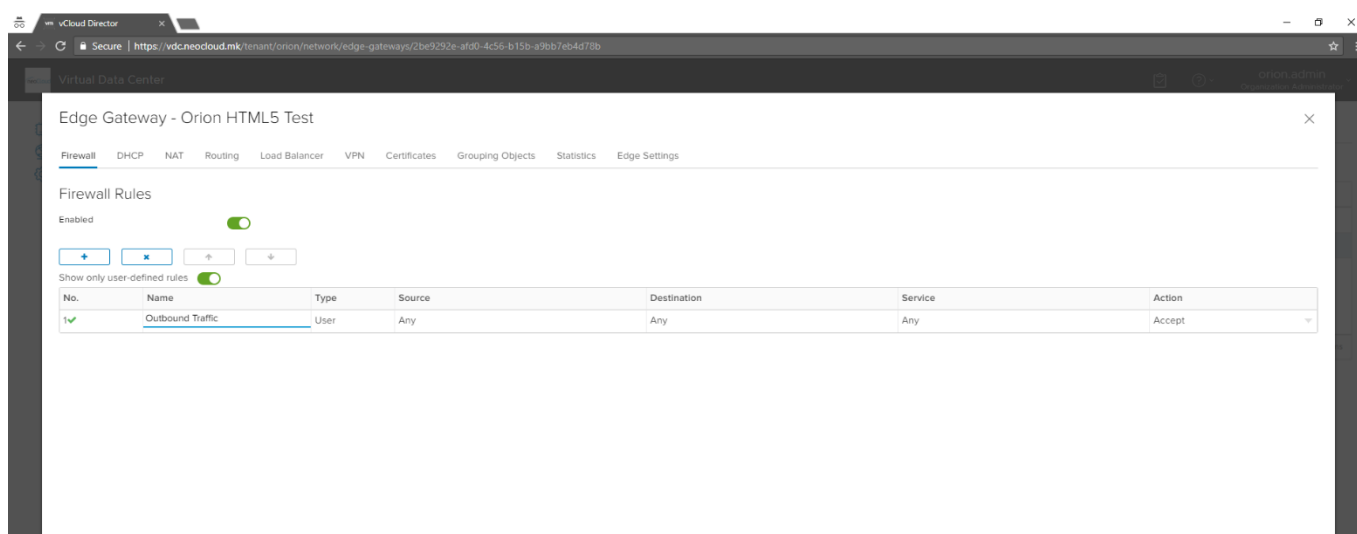


Слика 6

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.

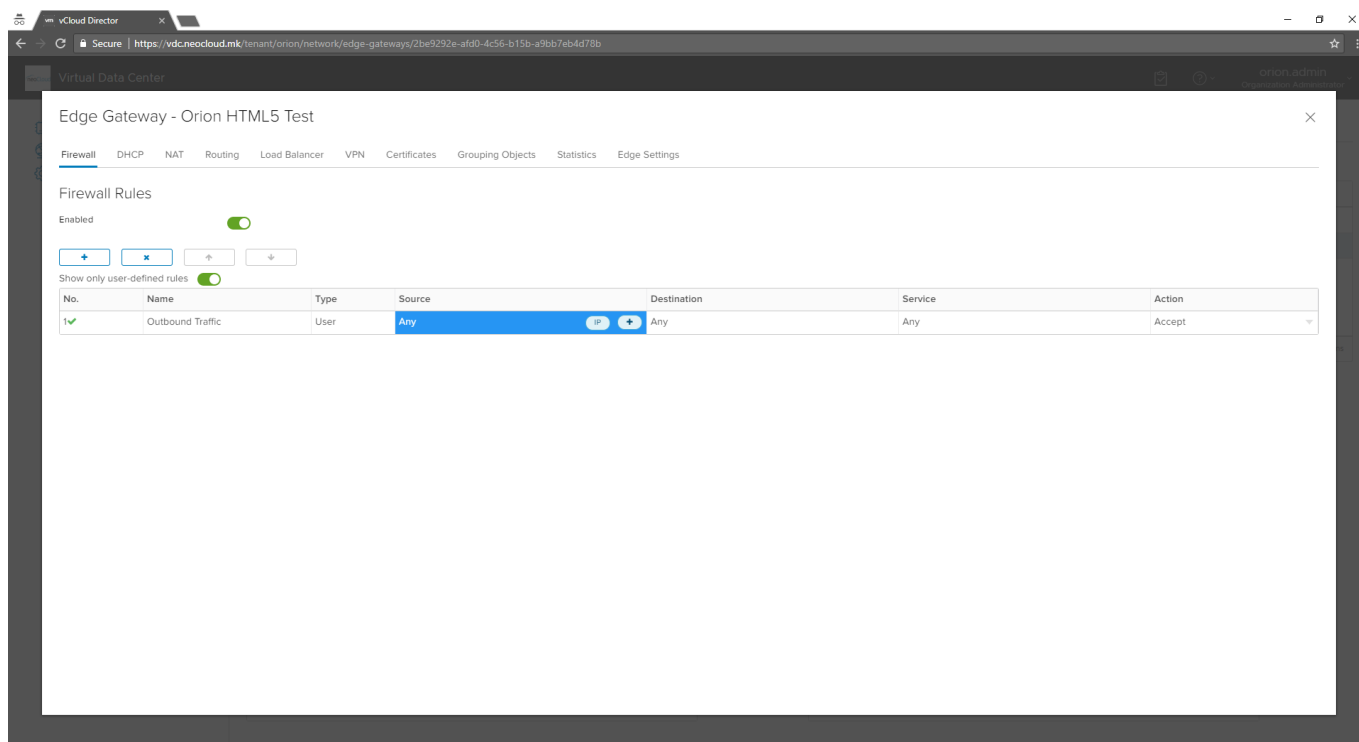
Firewall

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.



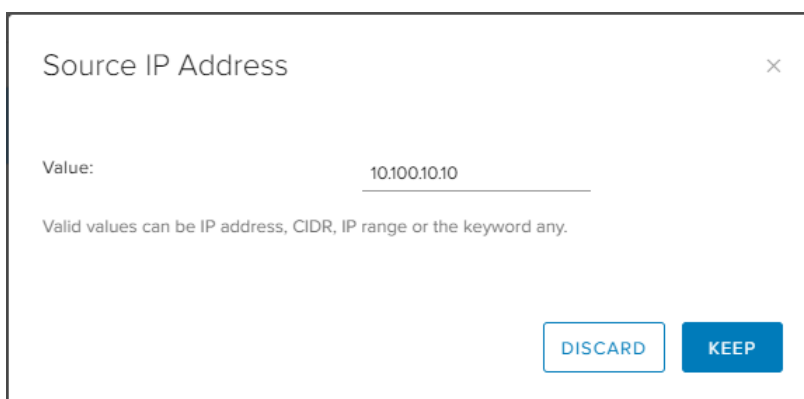
Слика 7

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 или 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 или објект (Слика 8).



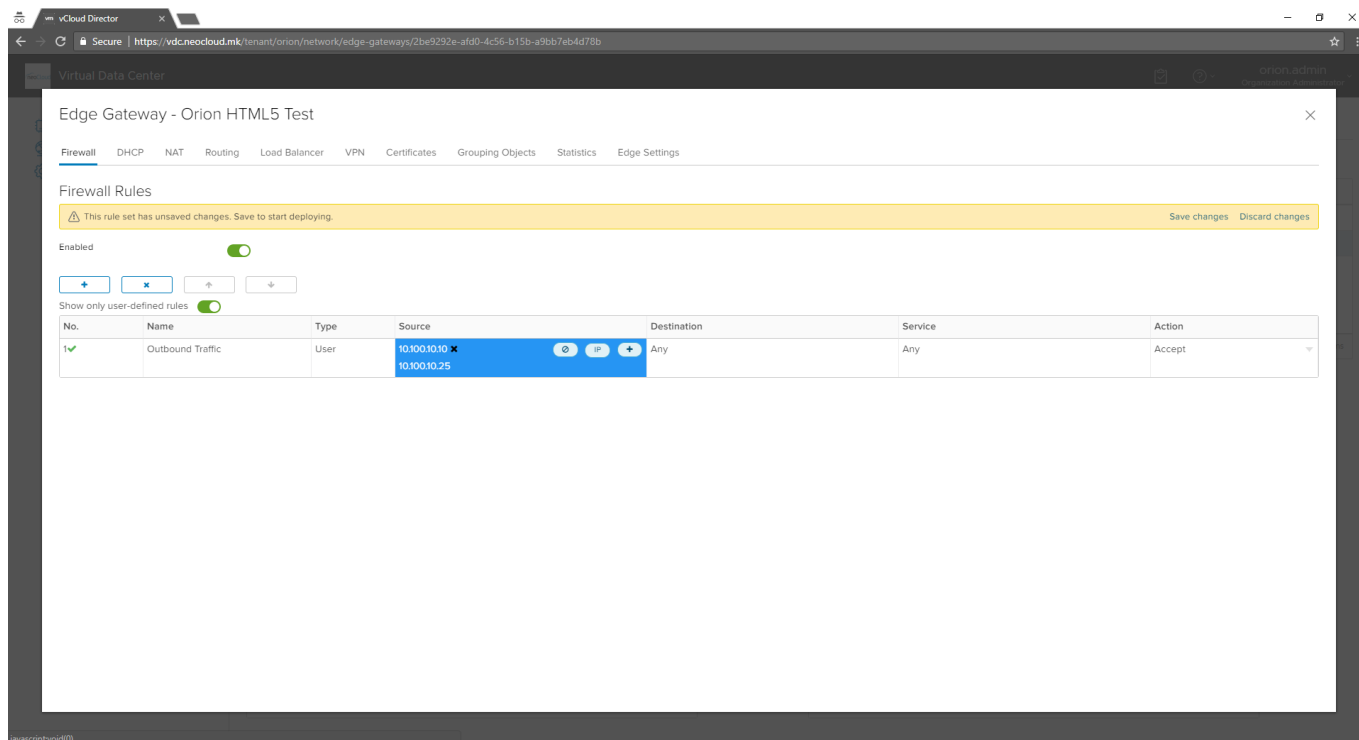
Слика 8

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.



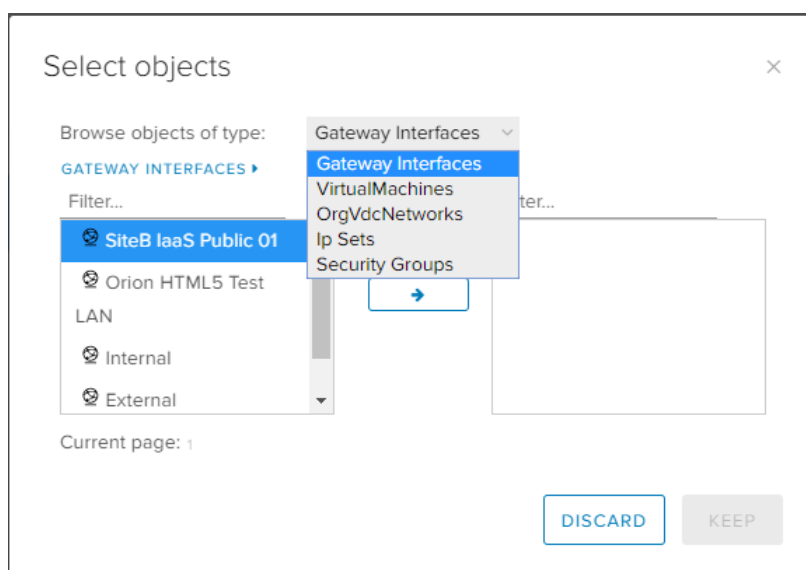
Слика 9

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



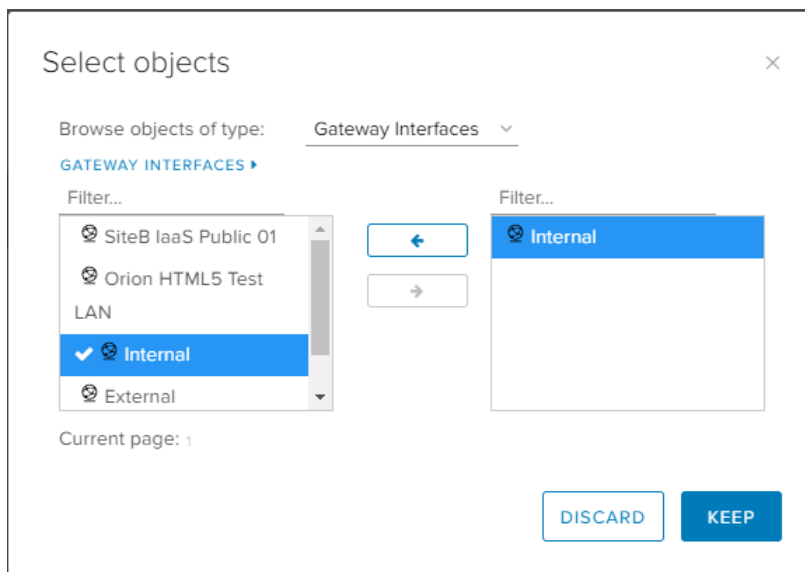
Слика 10

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).



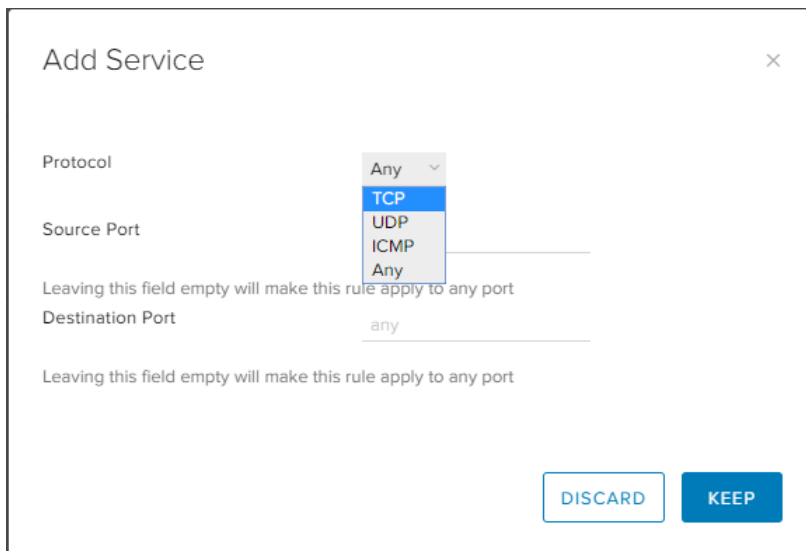
Слика 11

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.



Слика 12

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).



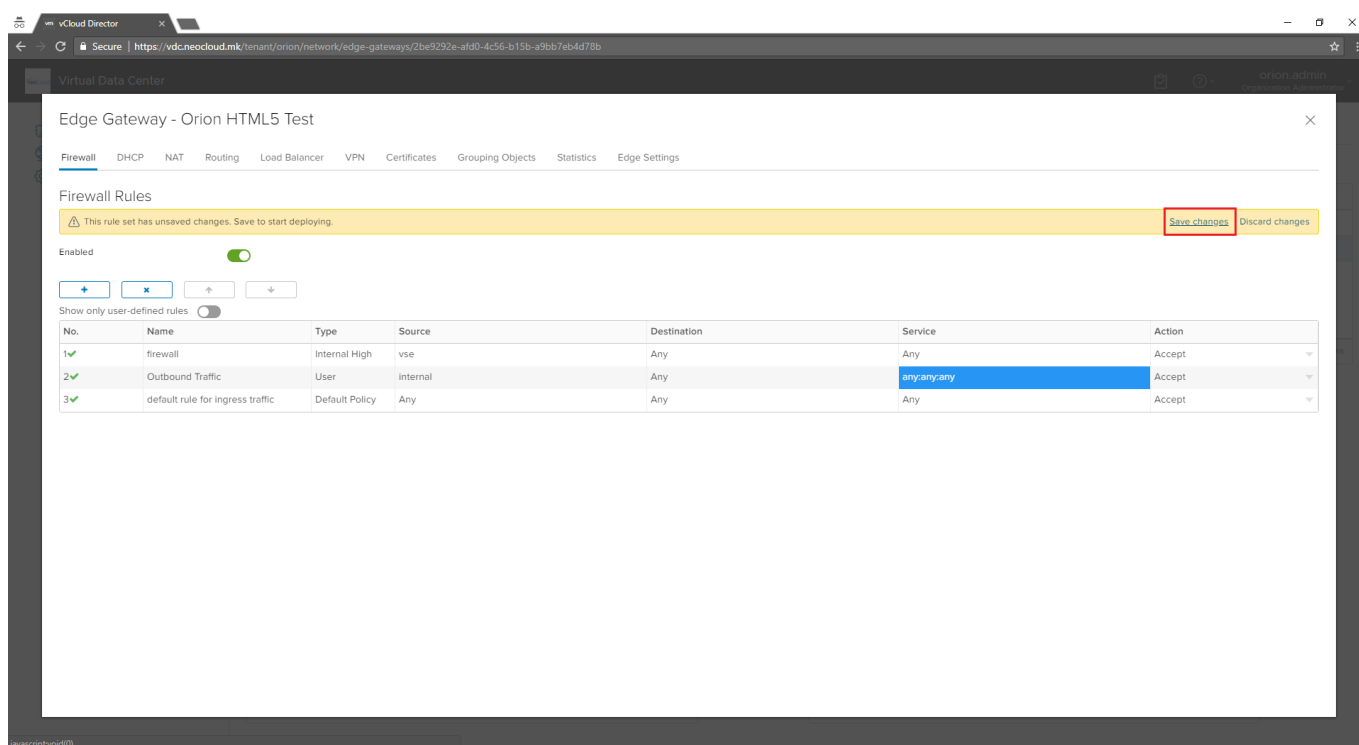
Слика 13

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).



Слика 14

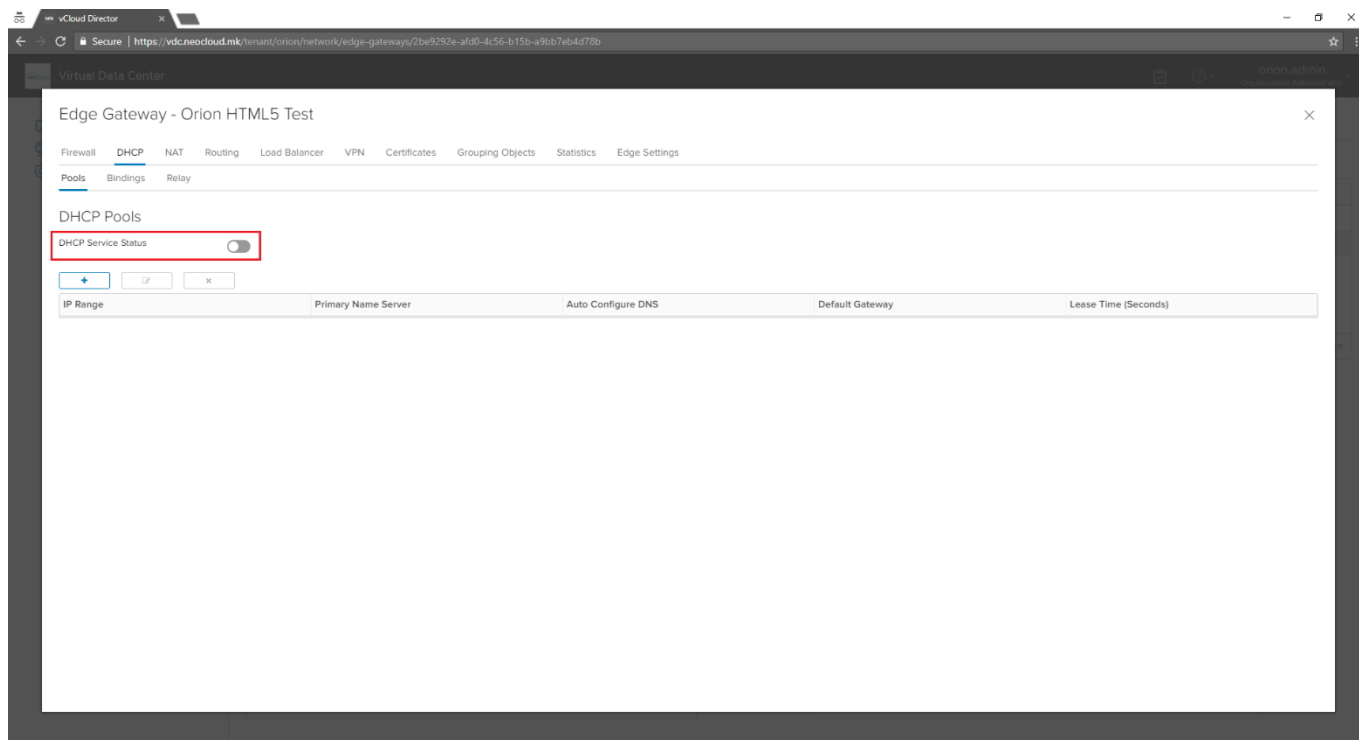
Откако ќе се постават сите firewall правила во последниот чекор потребно е да се зачува новата конфигурација на Edge gateway рутерот. Истото се прави со притиснување на *Save Changes* во жолтата статусна лента, која е позиционирана во горниот дел (Слика 15).



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*)

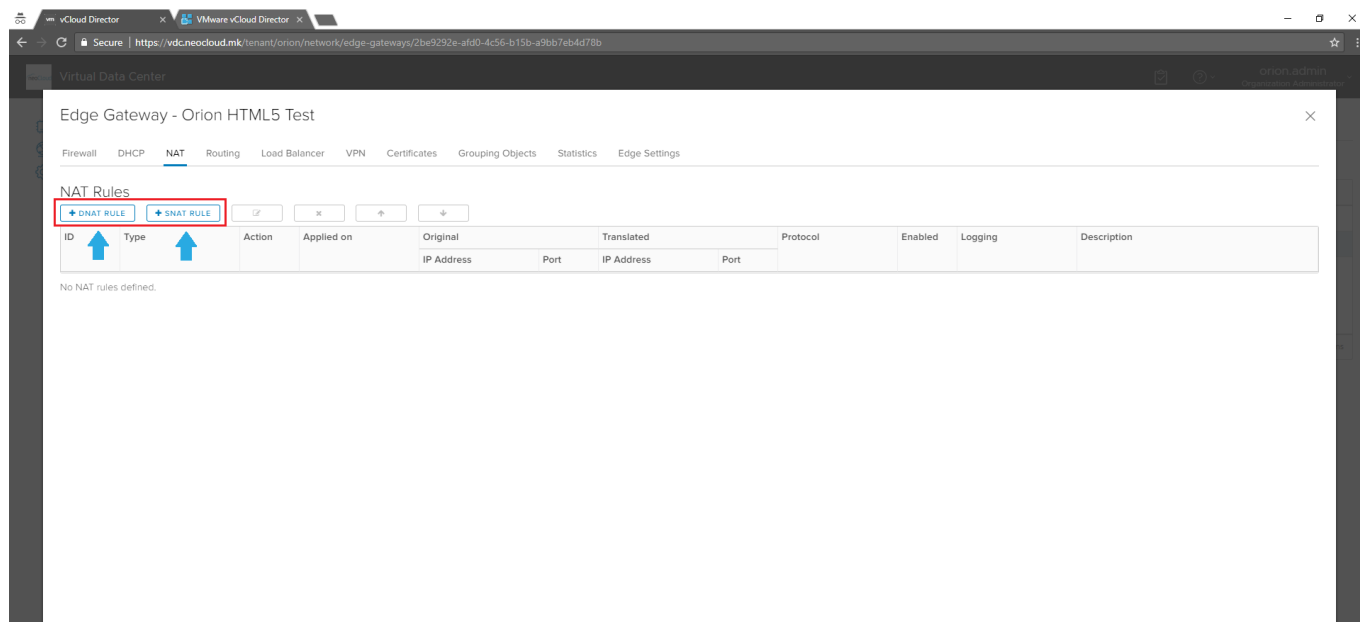


Слика 16

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.

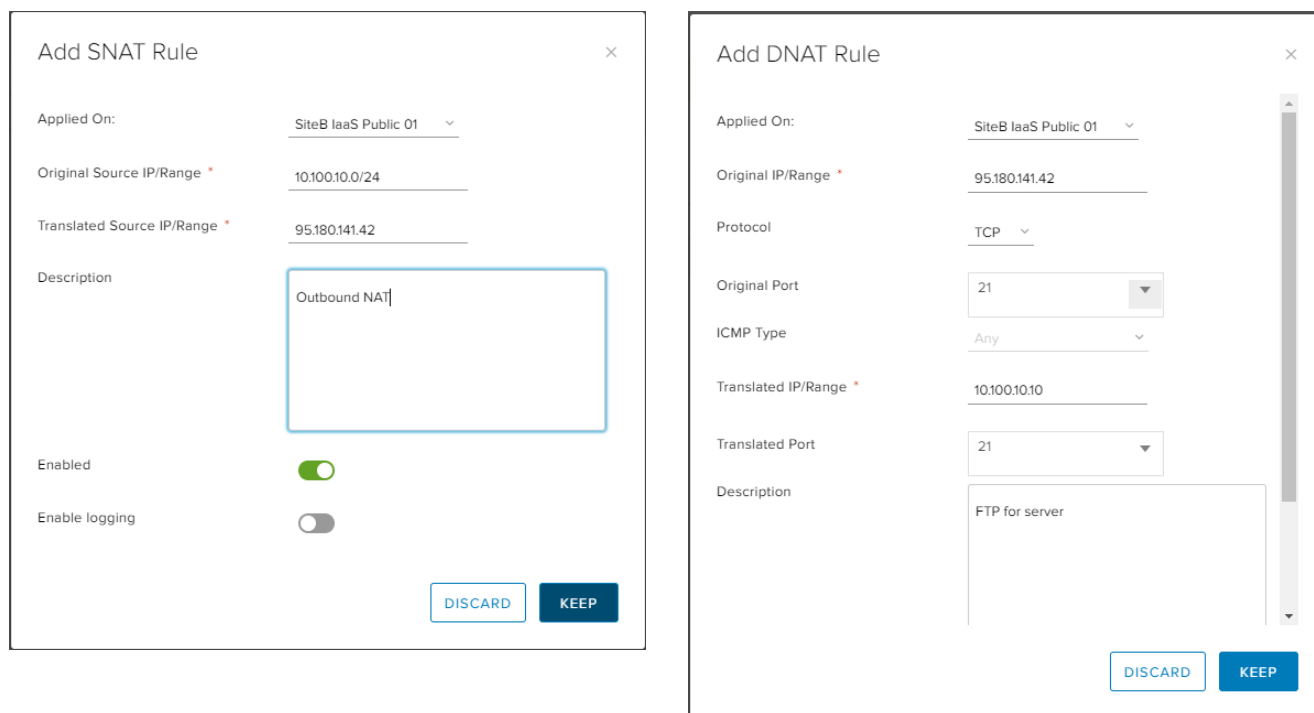
NAT

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 трансляциски правила (Слика 17).



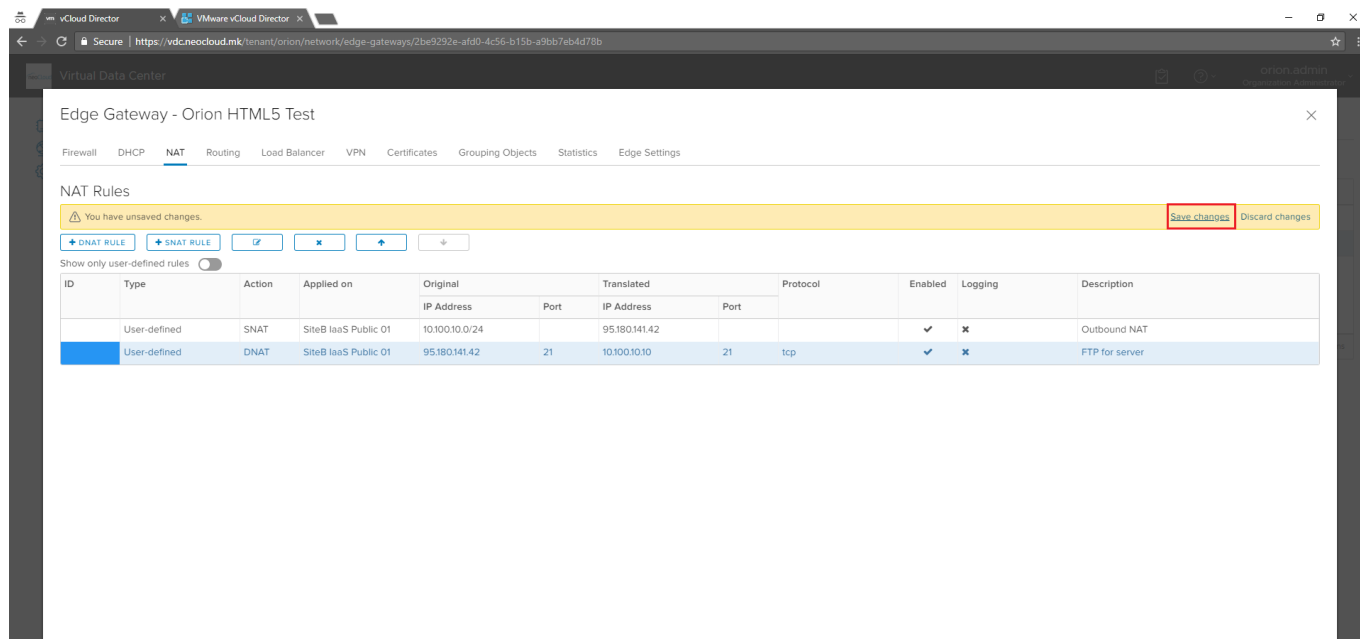
Слика 17

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).



Слика 18

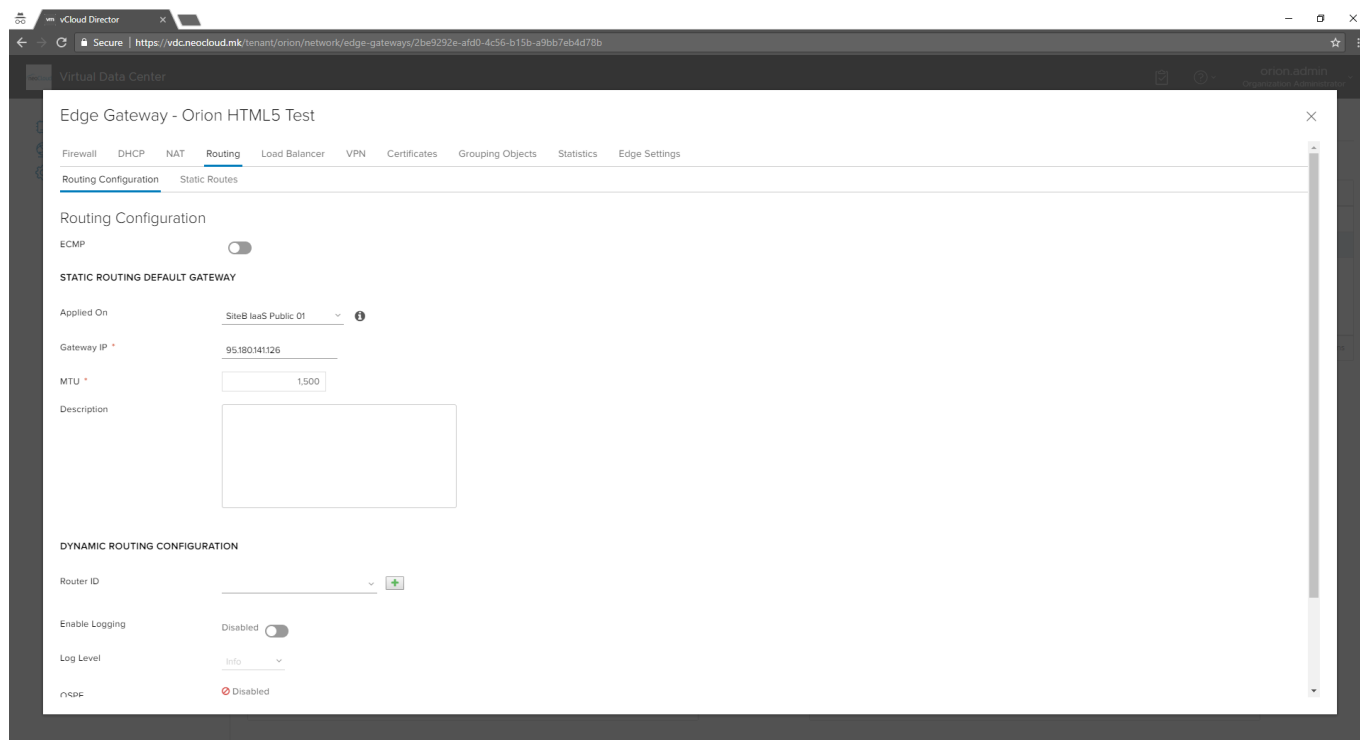
Како и досега потребно е да се зачува промената во главниот предлог (Слика 19).



Слика 19

Routing

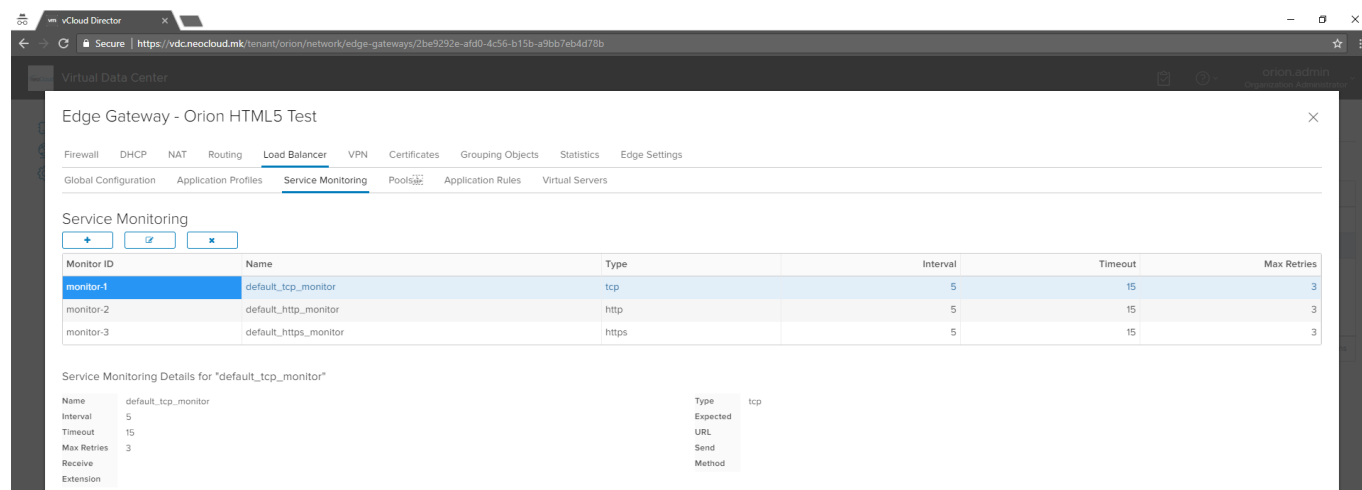
Како и во претходната верзија постои можност за рутирање на сообраќајот, доколку е потребно. Во новата верзија покрај статичкото рутирање, постои можност за динамичко рутирање со помош на OSPF и BGP протоколите (Слика 20).



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, MSRP 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).



Слика 21

Четвртиот чекор е делот за **Pools** или дефинирање на сервери кои ќе бидат дел од Load Balancer групата. Покрај стандардните параметри при додавање на нов Pool потребно е да се одбере алгоритмот 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** алгоритмот 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 HTTP 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 *

Description

Algorithm

Algorithm Parameters

Monitors

Transparent

Members

En...	Name	IP Address	We...	Mo...	Port	Min Conn...	Max Conn...

DISCARD KEEP

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 Member

Enabled

Name *

IP Address *

Port

Monitor Port

Weight *

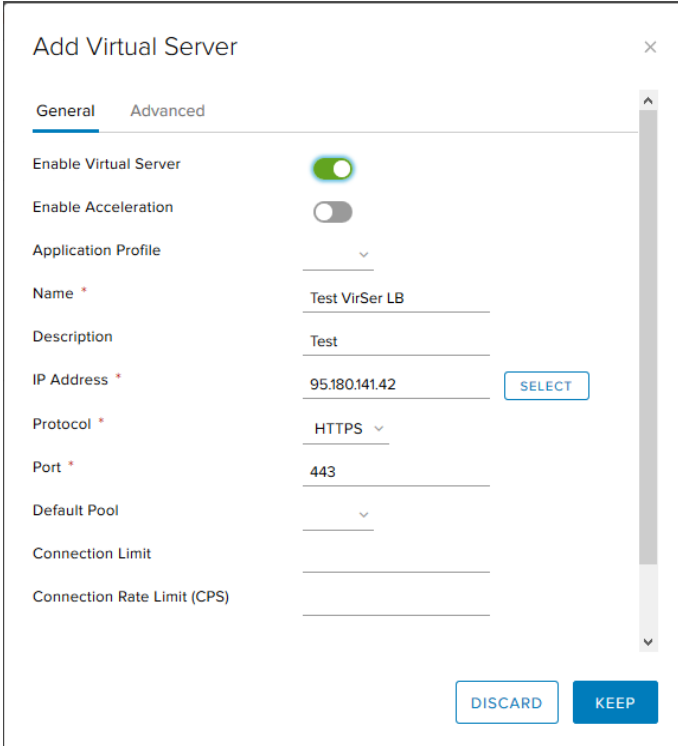
Max Connections

Min Connections

DISCARD KEEP

Слика 23

Во [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).



The screenshot shows the 'Add Virtual Server' dialog box with the following configuration:

- Enable Virtual Server:
- Enable Acceleration:
- Application Profile: [Dropdown]
- Name: Test VirSer LB
- Description: Test
- IP Address: 95.180.141.42 (with a 'SELECT' button)
- Protocol: HTTPS
- Port: 443
- Default Pool: [Dropdown]
- Connection Limit: [Input field]
- Connection Rate Limit (CPS): [Input field]

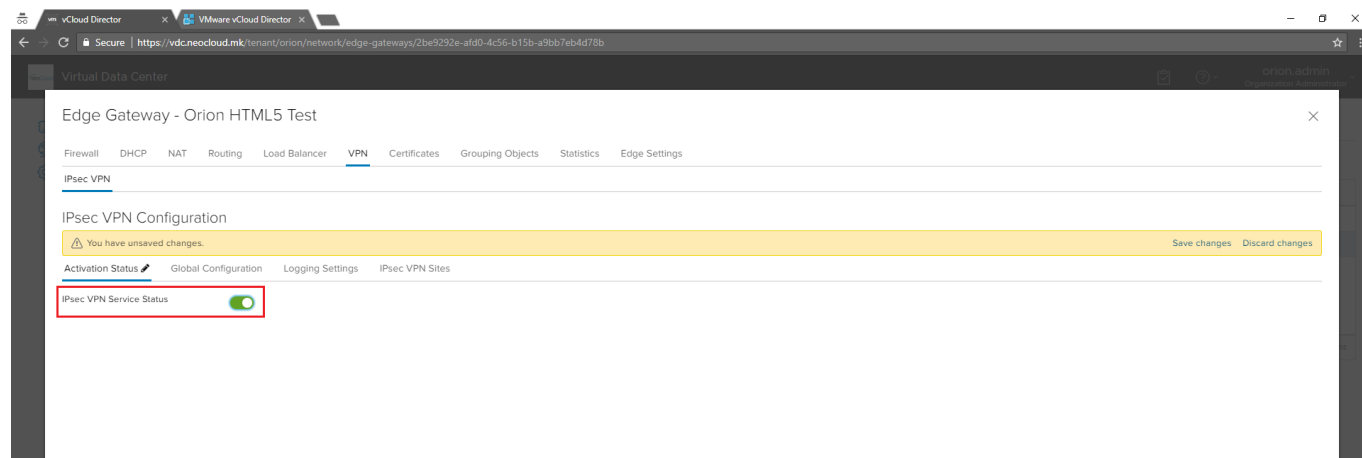
Buttons: DISCARD, KEEP

Слика 24

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

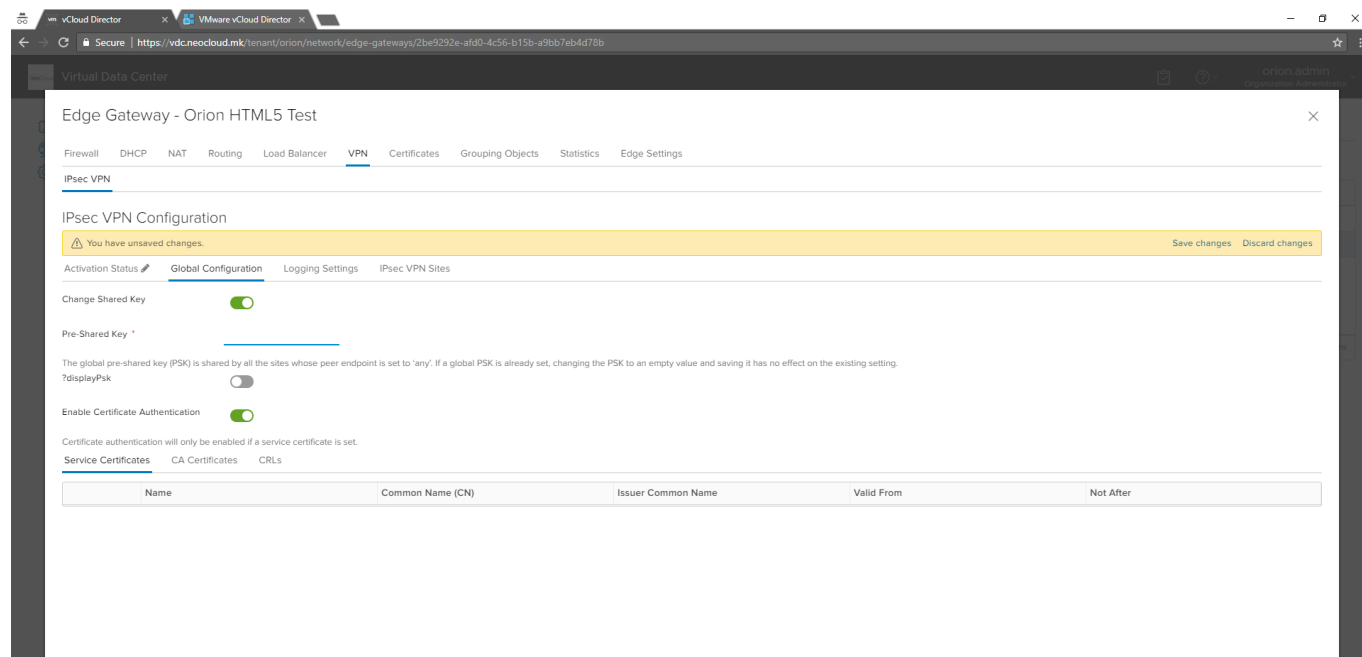
VPN

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).



Слика 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.



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

Local Id *

Local Endpoint *

Local Subnets *

Subnets should be entered in CIDR format with comma as separator.

Peer Id *

Peer Endpoint *

Endpoint should be a valid IP, FQDN or any.

Peer Subnets *

Subnets should be entered in CIDR format with comma as separator.

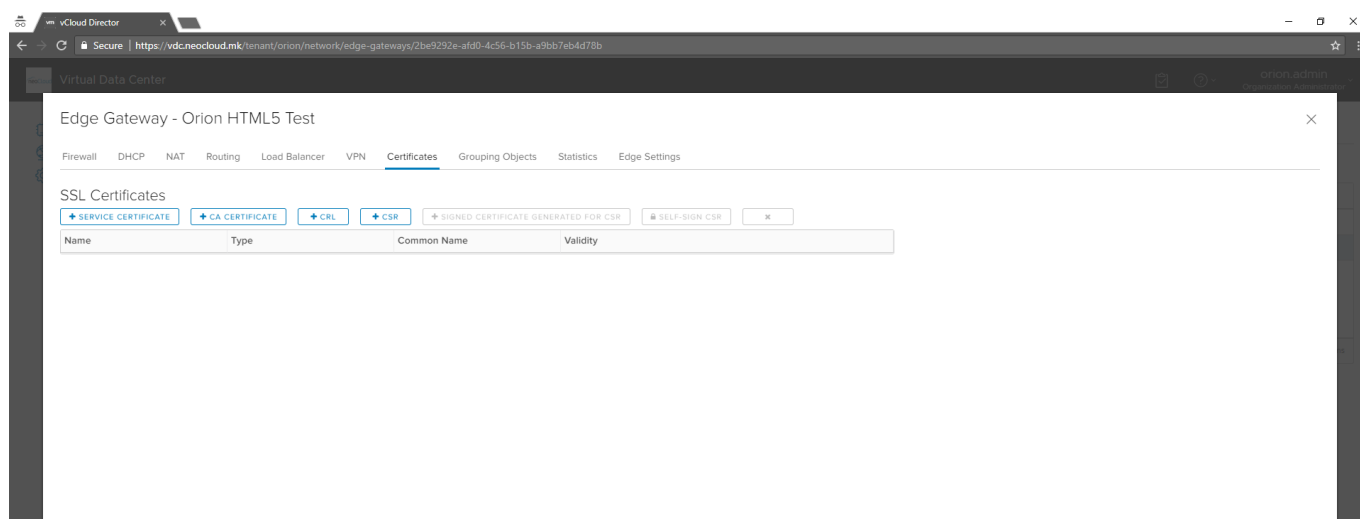
DISCARD
KEEP

Слика 27

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

Certificates

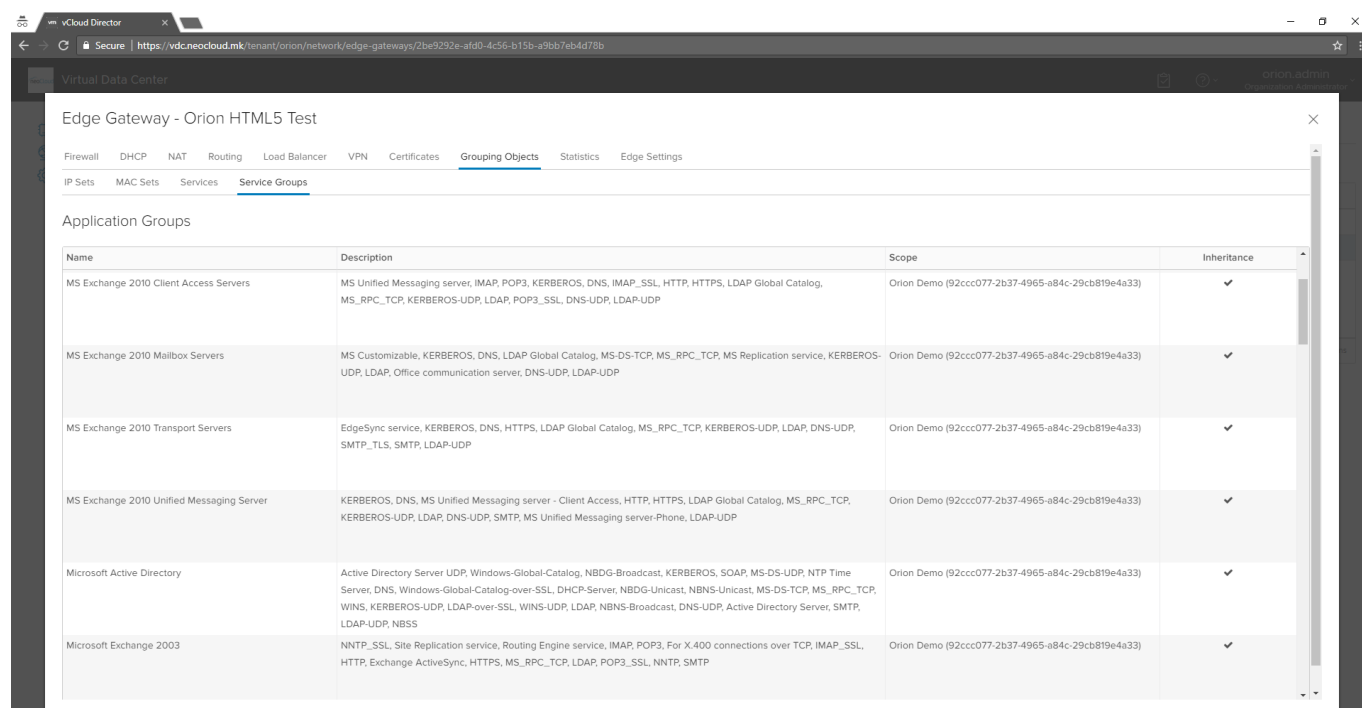
Како една од дополнителните опции во новата верзија е секако и можноста за користење на сертификати, за сервисите Load Balancer или VPN. Потребно е да се додадат потребните параметри и да се прикачат постоечки сертификати или пак да се генерира CSR (Слика 28). Доколку има потреба од користење на сертификати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



Слика 28

Grouping Objects

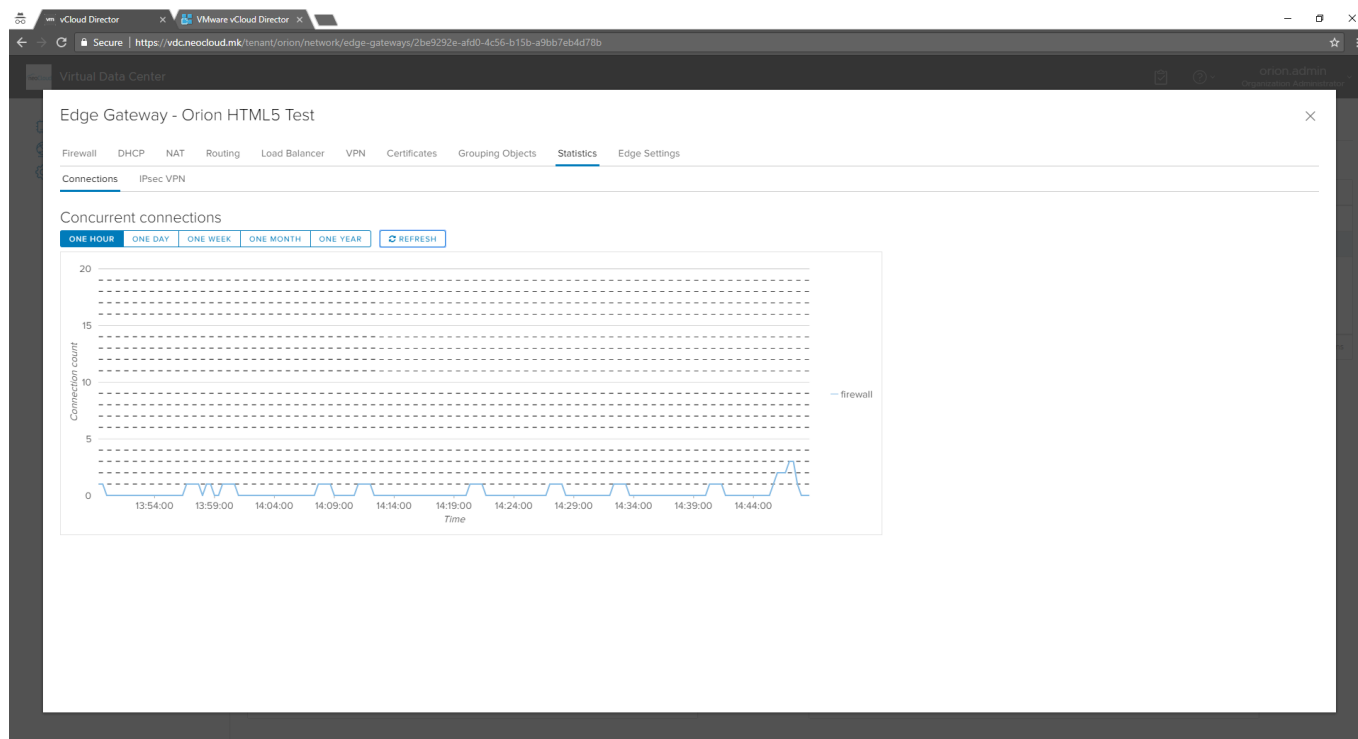
Grouping Objects е новитет преку кој го поедноставува процесот на создавање на безбедносни правила. Grouping Objects се објекти кои се дефинираат (**IP Sets** и **MAC Sets**) или се претходно дефинирани (**Services** и **Service Groups**) и понатаму може да се употребуваат при додавање на firewall правила (*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.)



Слика 29

Statistics

Уште еден новитет покрај претходно споменатите во оваа верзија на порталот, покрај метриците за секоја виртуелна 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 нé на support@neocloud.mk за повеќе информации.