

КОНФИГУРАЦИЈА НА EDGE GATEWAY

Прирачник за конфигурација на уредот Edge Gateways, задолжен за рутирање и периметарска заштита во Вашиот виртуелен дата центар.



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

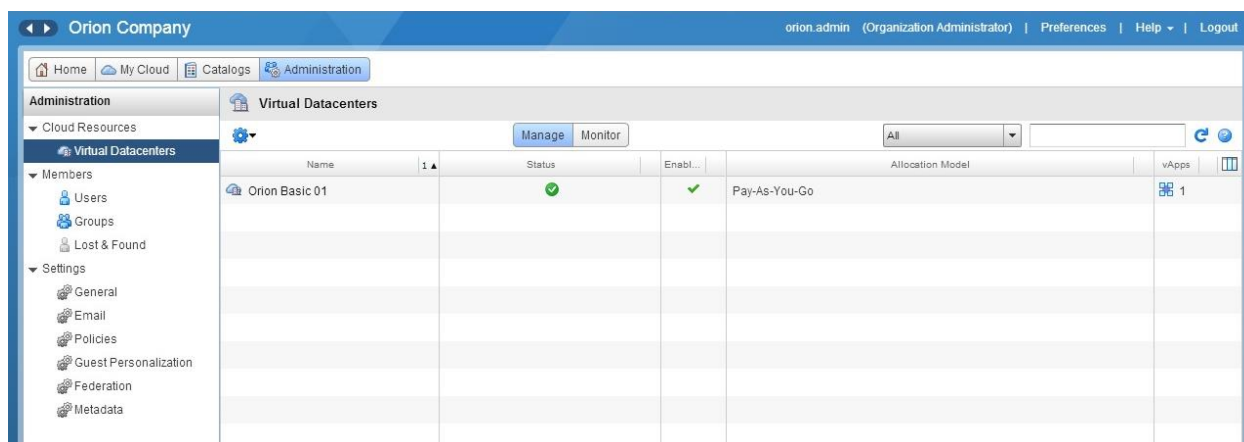
Неотел ДОО е телекомуникациски оператор основан во 2004 година со македонски капитал обезбеден од страна на Неоком. На пазарот нуди широк спектар на услуги од областа на широкопојасен интернет пристап, телефонија, изнајмени линии, хостирање и колокација на опрема. Започнува со нудење на услуги на бизнис-корисници 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

Edge Gateway.....	3
Services	5
DHCP.....	5
NAT	6
Firewall.....	7
Static Routing	8
VPN	9
Load Balancer	11
External IP Allocations	16

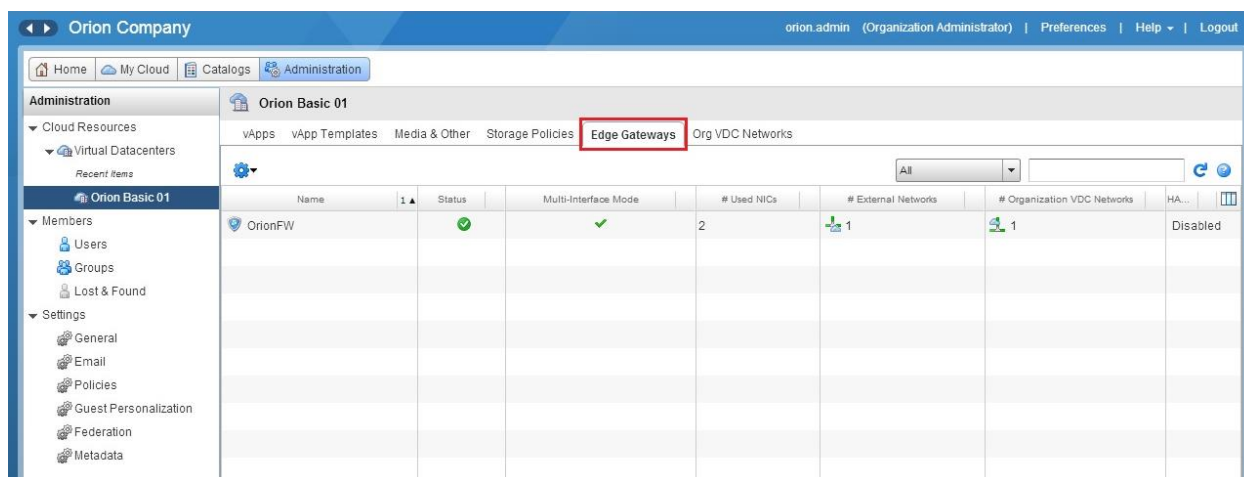
Edge Gateway

За конфигурација на Вашиот Edge Gateway уред кој служи за рутирање (router) и периметарска безбедност (firewall), неопходно е да бидете лоцирани во прегледот **Administration**. Од менито од левата страна одберете **Cloud Resources** → **Virtual Datacenter** (Слика 1).



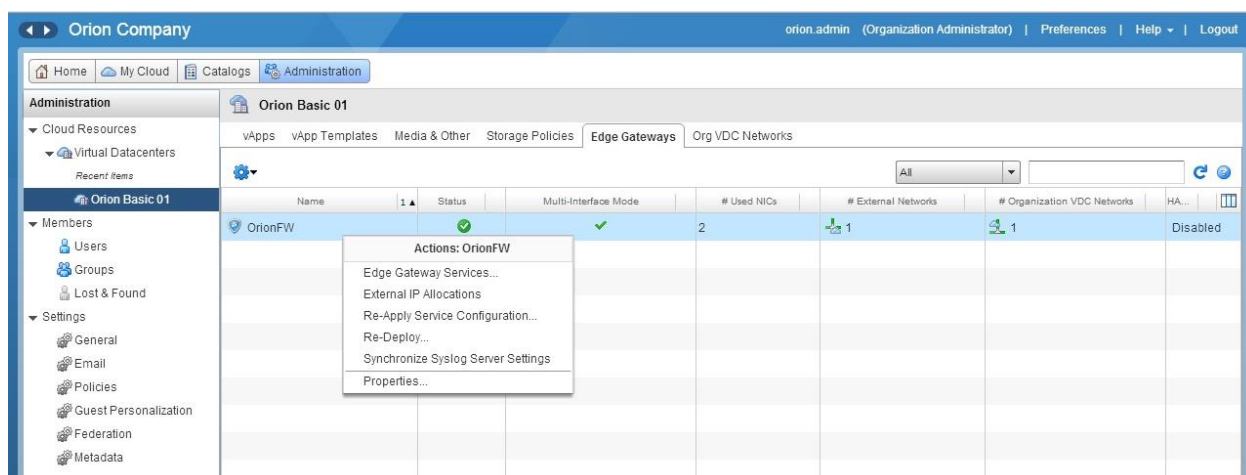
Слика 1

Во новиот приказ одберете го виртуелниот дата центар за кој што сакате да го конфигурирате Edge Gateway уредот; со притиснување на двоен клик на името на виртуелниот дата центар, ќе ги добиете сите параметри и поставки за одредениот дата центар. Од менито кое е позиционирано во горниот дел на табелата, одберете **Edge Gateways** (Слика 2).



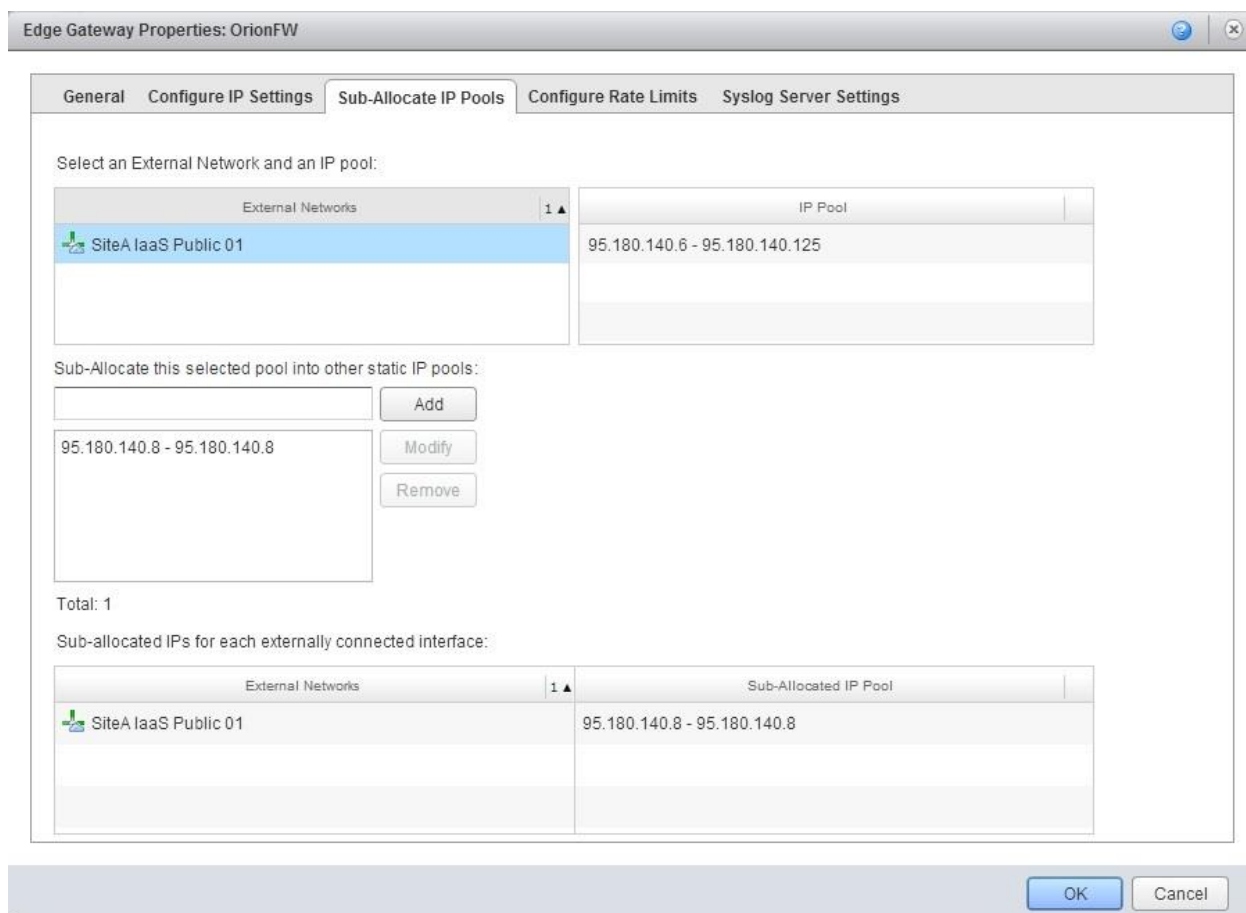
Слика 2

Во новиот приказ се прикажани сите Edge уреди кои се асоцирани со овој виртуелен дата центар. Со десен клик на името на уредот се појавуваат повеќе опции каде ќе можете да го менувате името на Edge уредот, која IP адреса ја поседува или да конфигурирате некој од дополнителните сервиси: DHCP, NAT, Firewall, Static Routing, VPN и Load Balancer (Слика 3).



Слика 3

Во **Properties** може да ги прегледате некои од основите параметри за одбраниот Edge. Во делот **General** може да ги менувате основните параметри, како на пример името на самиот уредот. Во следниот прозор е прикажана доделената IP адреса за самиот уред од страна на операторот. Во **Sub-Allocate IP Pools** е адресниот простор достапен за дополнителни сервиси на Edge уредот (Слика 4). **Configure Rate Limits**, ги содржи потребните параметрите за брзина на линкот. Во зависност од пакетот кој го поседувате, брзините на линкот варираат.

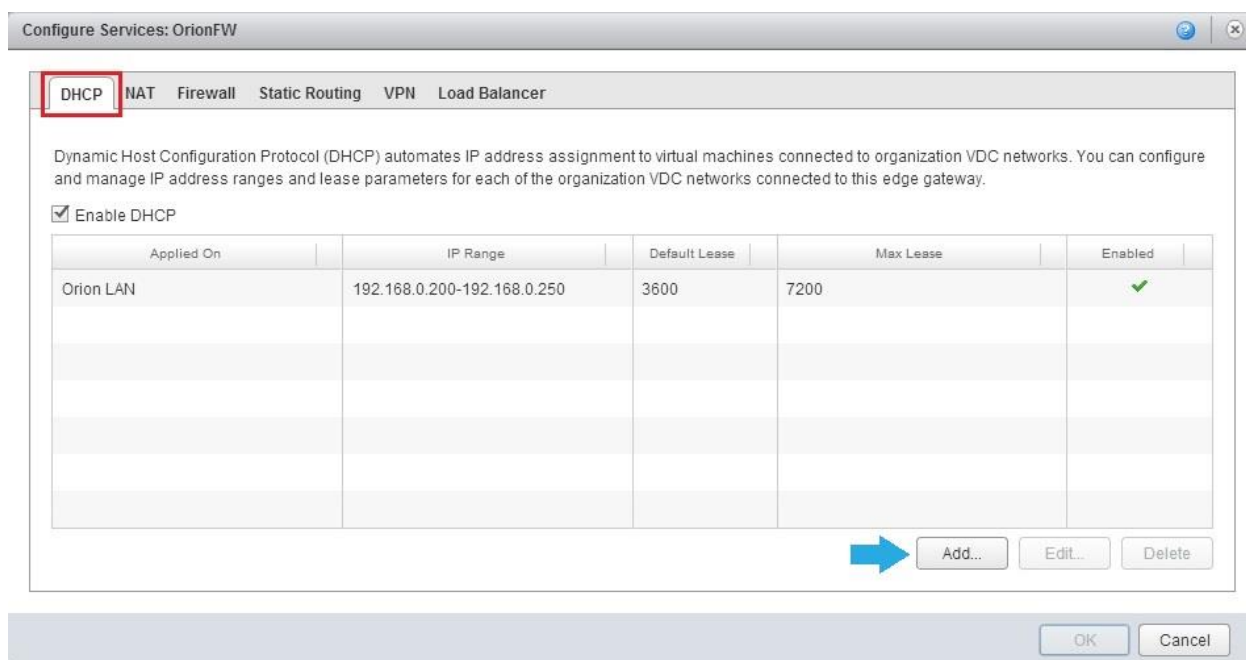


Слика 4

Services

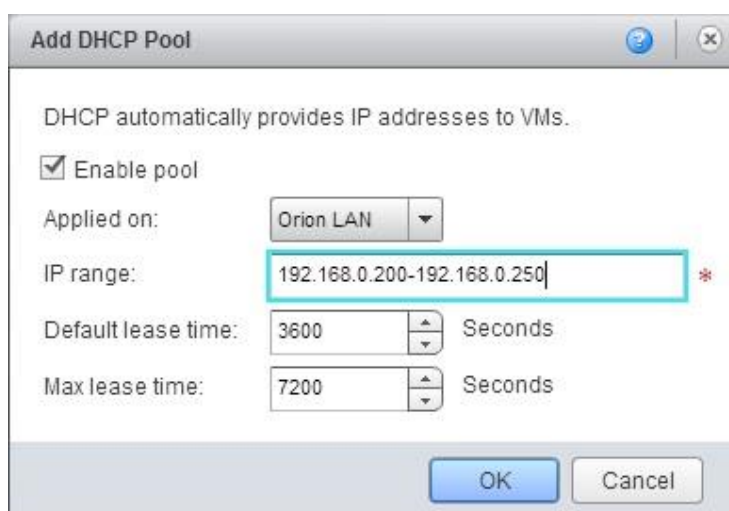
Откако ќе го затворите претходниот прозор, повторно со десен клик на името на уредот одбираме од менито **Edge Gateway Services** (Слика 3). Во новиот прозор, се прикажани сите дополнителни сервиси поврзани со уредот кои можете да ги конфигурирате. Прв е делот за **DHCP** (Слика 5).

DHCP



Слика 5

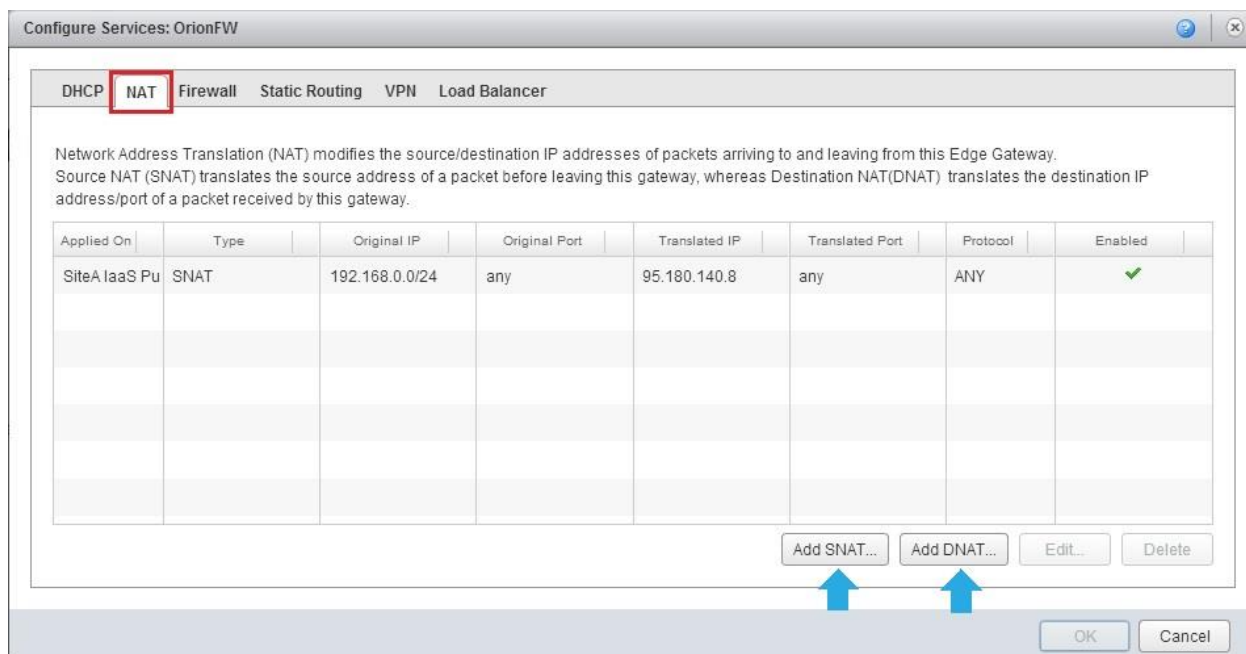
На копчето *Add* можете да додадете нов адресен простор за потребите на DHCP. Доколку постојат повеќе LAN мрежи во вашиот виртуелен дата центар, од менито *Applied on* можете да одберете за кој точно LAN ќе соодветствува одредениот DHCP адресен простор. Во полето за *IP range*, потребно е да го внесете опсегот, почетна и крајна адреса, која ќе се користи за автоматско доделување на адреси. Исто така можете да го менувате и времетраењето на доделените IP адреси (Слика 6).



Слика 6

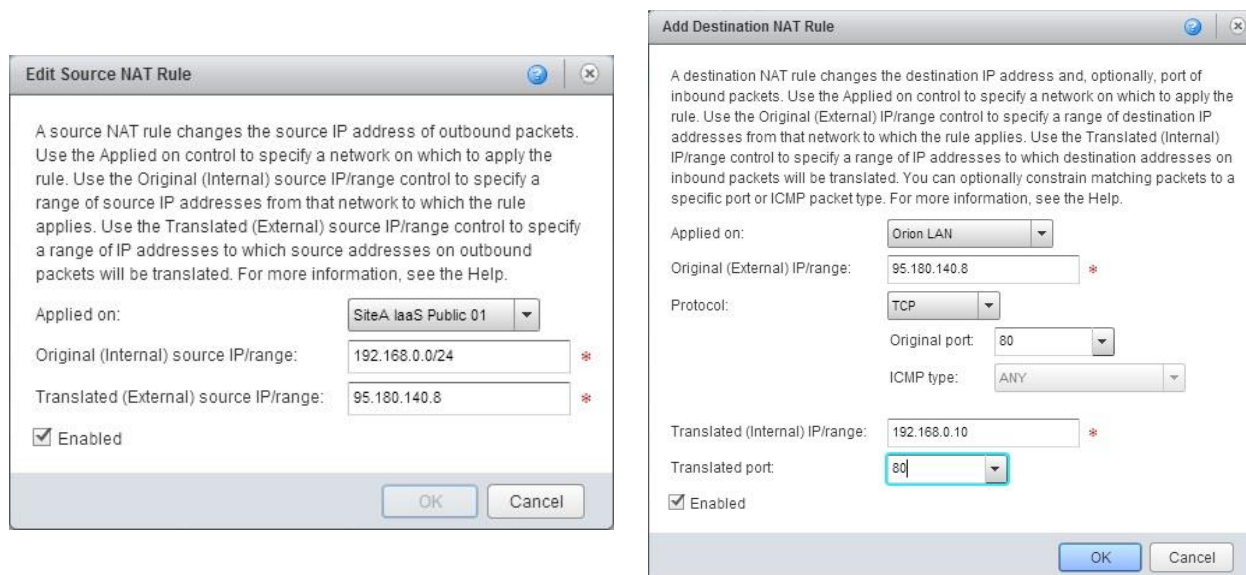
NAT

Во следниот преглед можете да конфигурирате **NAT** (Слика 7). Можете да одберете помеѓу двата типа SNAT (*Source NAT*) или DNAT (*Destination NAT*). Во прирачникот даден е пример и за двата типа.



Слика 7

Со клик на Add SNAT или Add DNAT од долниот дел на прозорот, се прикажуваат два нови различни прозорци, во кои ќе треба да ги внесете потребните параметри за конфигурирање на NAT правилата.



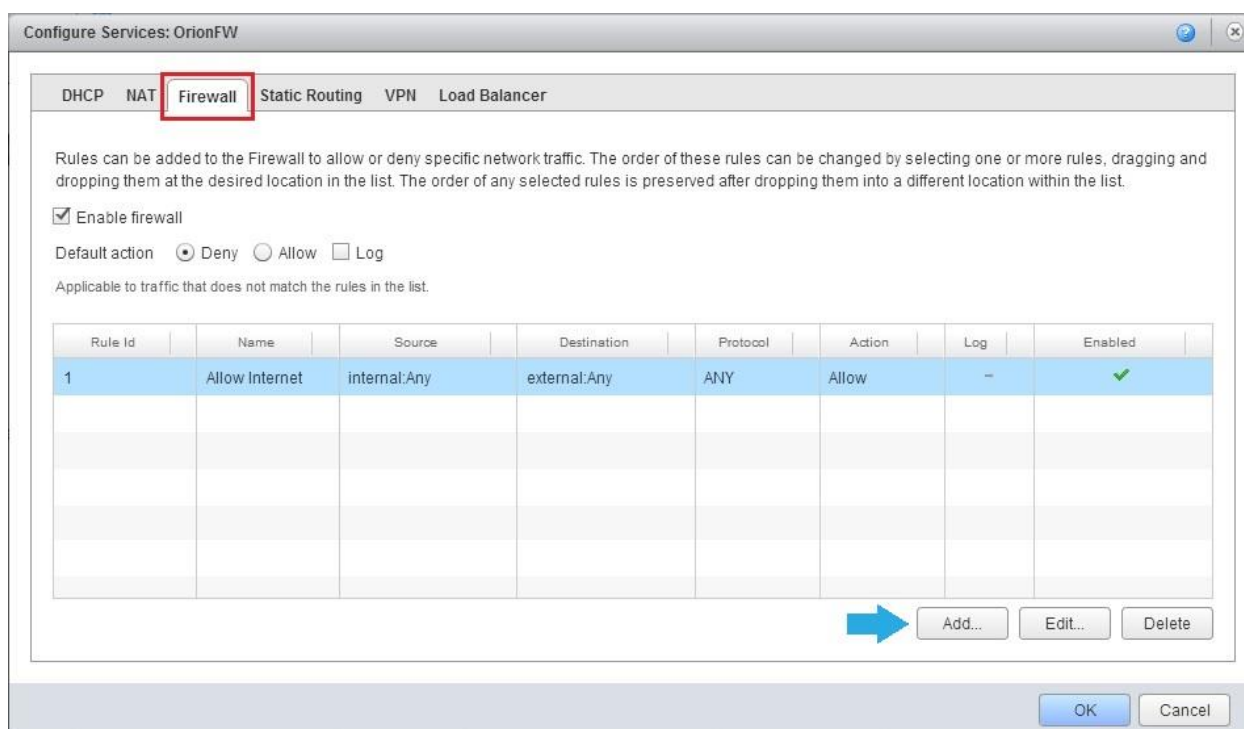
Слика 8

На *Слика 8*, во левиот прозор, е даден пример за Source NAT, правило за NAT-ирање на сообраќај од LAN транслиран во доделената јавна IP адреса. Оттука во делот *Applied on* го одбираме WAN интерфејсот (*SiteA laas Public 01*), каде внатрешниот извор (IP адреса или опсег) е опсегот на адреси од постоечкиот LAN, а за надворешен извор (IP адреса или опсег) е поставена доделената јавна IP адреса. Откако ќе се примени правилото, сообраќај кон интернет е овозможен.

На *Слика 8*, во десниот прозор, е даден пример за Destination NAT, правило за NAT-ирање на сообраќај од WAN транслиран на одредена приватна IP адреса. Во *Applied on* одбираме за која приватната мрежа (*Orion LAN*) ќе се однесува правилото, каде внатрешниот извор (IP адреса или опсег) е поставена доделената јавна IP адреса. Во делот за протокол можете да одберете од неколкуте типови: TCP, UDP, TCP & UDP, ICMP или ANY. Во полето за порта пишувате од која порта треба да биде транслиран сообраќајот. Кај полето за транслирана внатрешна IP адреса или опсег одбираме постоечка приватна IP адреса и транслираната порта.

Firewall

Следниот сервис од листата е периметарската заштита или **Firewall** (*Слика 9*). Во овој дел можете да создавате одредени правила за самиот firewall. Притоа во делот *default action* може да одберете што ќе се случува со останатиот сообраќај, кој не е опфатен со правилата кои сте ги создале.



Слика 9

Со клик на *Add* можете да додадете правила. Во примерот е прикажано правило за пристап на интернет од било која внатрешна IP адреса кон било која надворешна IP адреса. Во делот за *Source* треба да внесете IP адреса или опсег, можете за вредност да внесете и "Internal", "External" или "Any". Истото важи и за *Destination*. Од менито *Protocol* може да се одбере од неколкуте типови: Any, TCP, UDP, TCP & UDP и ICMP. Последен параметар е дали ова правило да го одбива или пропушта сообраќајот (*Слика 10*).

Edit Firewall Rule

Enabled

Name: *

Source: *

Valid values can be IP address, CIDR, IP range, "any", "internal" and "external".

Source port:

Destination: *

Valid values can be IP address, CIDR, IP range, "any", "internal" and "external".

Destination port:

Protocol:

Action: Allow Deny

Log network traffic for firewall rule

OK Cancel

Слика 10

Static Routing

Исто така доколку е потребно можете да направите и статичко рутирање. Со клик на *Add* од долниот десен агол, се отвара нов прозор каде потребни се неколку параметри (Слика 11).

Configure Services: OrionFW

DHCP NAT Firewall **Static Routing** VPN Load Balancer

Static routes allow traffic between networks. Ensure that the firewall rules are configured appropriately.

Enable static routing

Name	Network	Next Hop IP	Applied On

Add Static Route

Applied on:

Name: *

Network: *

Enter network address in CIDR format. For example: 192.168.2.0/24.

Next Hop IP: *

Enter next hop router IP address. For example: 192.168.0.100.

OK Cancel

Add... Edit... Delete

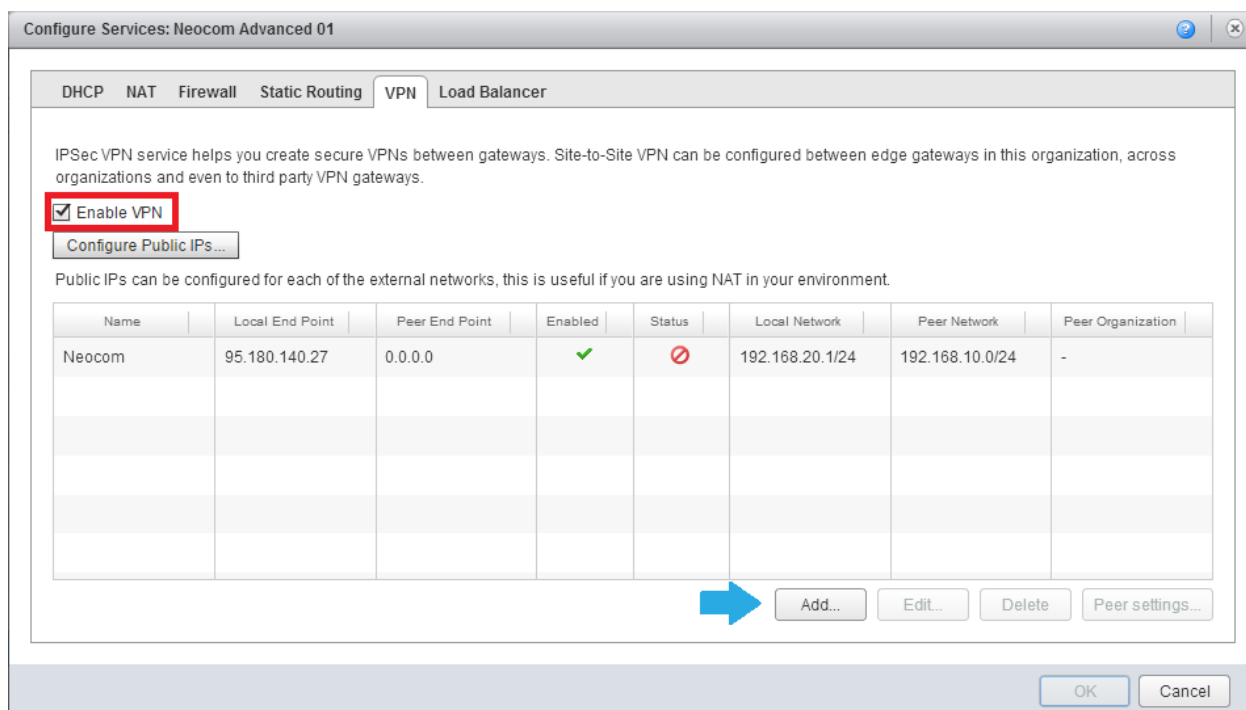
OK Cancel

Слика 11

Мрежа за која ќе се однесува статичкото рутирање, јавната или приватната мрежа, име, за која внатрешна мрежа (доколку има повеќе) ќе се однесува и кон каде ќе треба да се рутира сообраќајот (Next Hop IP).

VPN

VPN опцијата Ви е достапна во neoCloud виртуелниот дата центар. Пред да додадете нов VPN, важно е да ја овозможите оваа опција со едноставно штиклирање на полето Enable VPN (Слика 12). Со клик на Add копчето се отвара нов прозор.



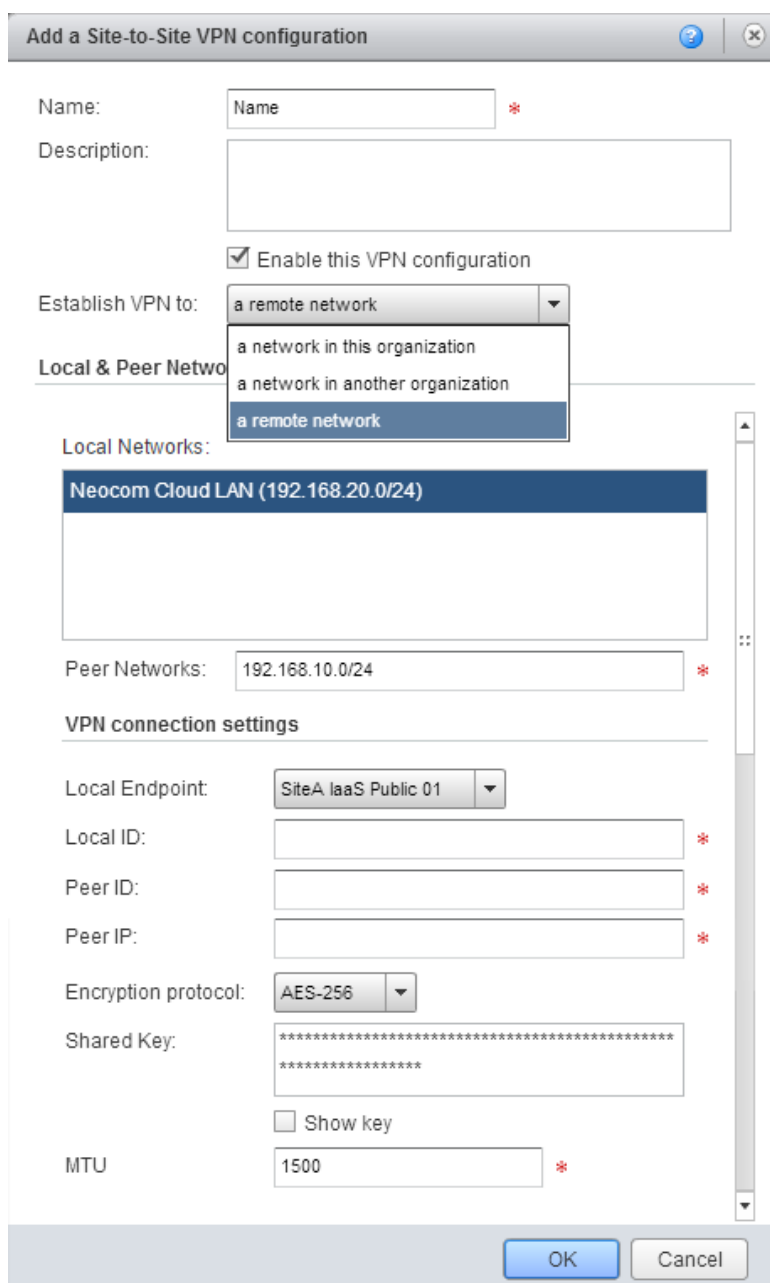
Слика 12

Потребно е да ги внесете следните параметрите за Site-to-Site VPN. Во првото и второто поле се внесуваат информации, име и опис за новиот VPN. *Establish VPN to* е поле во кое треба да одберете каков VPN ќе треба да се постави. Постојат три опции:

- *a network in this organization*, каде VPN поврзувањето ќе биде помеѓу две различни мрежи во самиот vDC
- *a network in another organization*, односно поврзување со друга мрежа во neoCloud (пример друг пакет и vDC).
- *a remote network*, која и најчесто се користи, поврзување помеѓу мрежата во vDC и Вашата локалната мрежа.

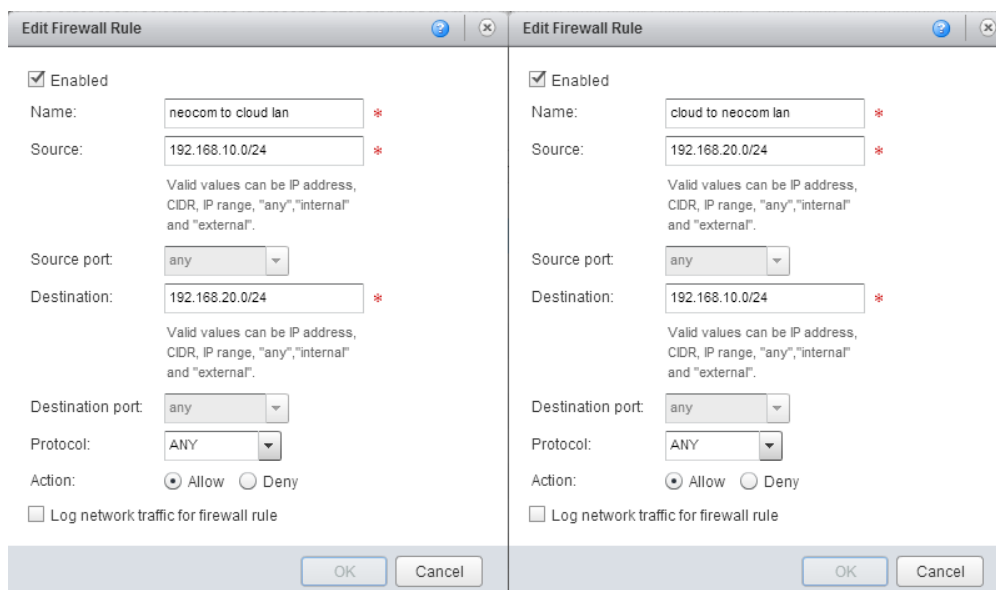
Во нашиот пример прикажуваме како да направите Site-to-Site VPN со надворешна мрежа (Слика 13).

Во делот за *Local & Peer Networks* ги внесувате потребните параметри за двете страни. Одбирате локална мрежа од вашиот vDC и Peer Networks, мрежа со која сакате да го направите поврзувањето. Во *Local ID* ја внесувате вашата јавна адреса од Edge Gateway, додека во *Peer ID/IP* ја внесувате IP адресата на уредот од другата страна преку кој ќе се овозможи овој VPN. Во делот за енкрипциски протокол можете да одбирате помеѓу: AES, AES-256 и 3DES. Наша препорака е да го користите протоколот AES-256. *Shared key* е клучот кој се користи при договарање на двата уреда за VPN. Со клик на *Show key* се прикажува автоматски генерираниот клуч од страна на vDC.



Слика 13

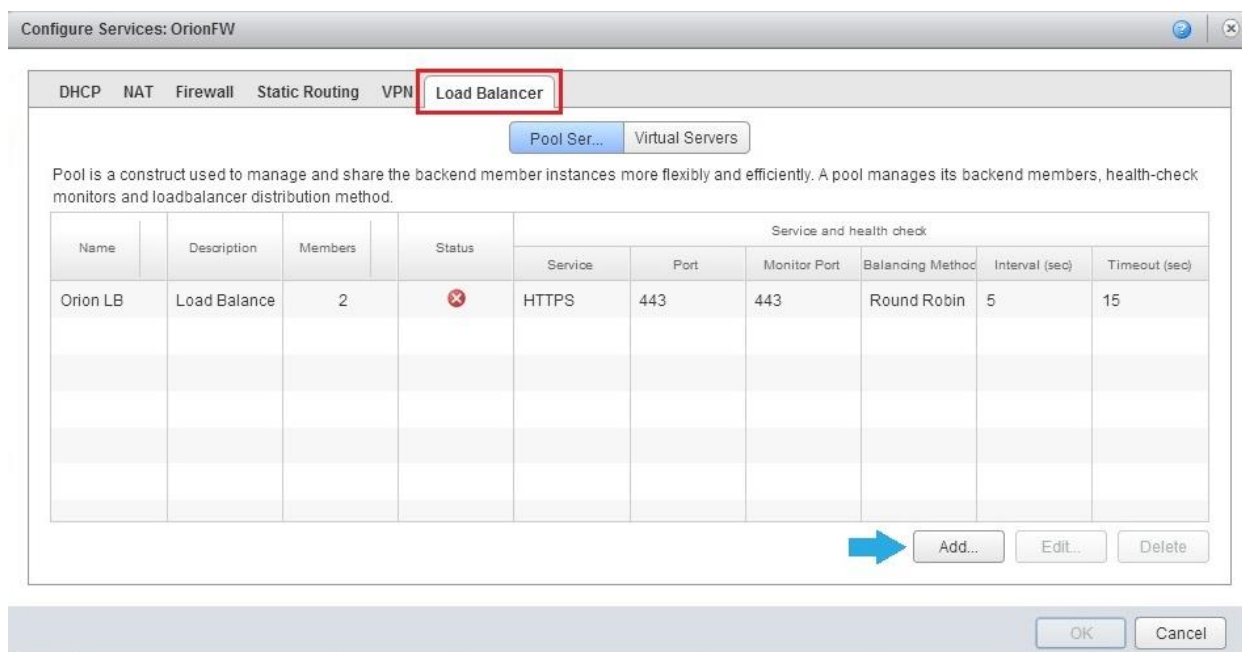
Откако завршивте со сите потребни параметри за конфигурација на Вашиот VPN потребно е да се додадат и две правила во делот за Firewall. Првото правило е наменето за пропуст на сообраќај од Вашата локација до виртуелниот дата центар. Второто правило е за сообраќајот наменет во спротивниот правец.



Firewall Rules

Load Balancer

Доколку е потребно, последен сервис во Edge Gateways е и конфигурирање на **Load Balancer** (Слика 14). Load Balancer делот е составен од два одделни прегледи, *Pool Servers* и *Virtual Servers*. Во првиот, ги дефинираме сервери кои се членови на одредена load balance група, а во вториот преглед го дефинираме виртуелниот сервер кој ќе биде задолжен за таа група. Со клик на *Add* се отвара нов прозор, каде на самиот почеток потребно е да внесете име.

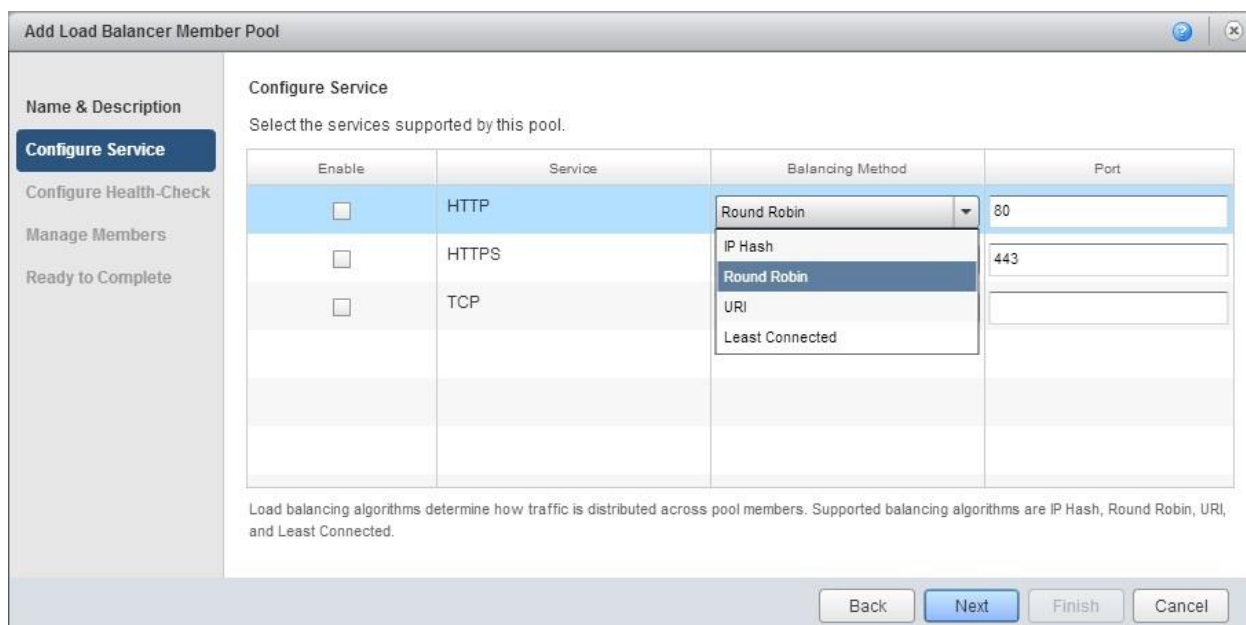


Слика 14

Во вториот чекор, *Configure Services* (Слика 15), треба да одберете параметри за самиот load balancer, да овозможите тип на сервис, метод на балансирање и која порта ќе се користи. Во делот за одбирање на метод постојат четири избора: *IP Hash*, *Round Robin*, *URI* и *Least Connected*.

- **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.
- **Round Robin** претставува алгоритам каде пренасочувањето на сообраќајот се одлучува по пат на одбирање на следната дестинација од листата на членови.
- **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.
- **Least Connected** алгоритмот поседува евиденција на активни конекции за секој од членовите и испраќа нова конекција до серверот со најмал број на активни конекции.

Во нашиот пример во *Configure Service*, е одбрана HTTPS сервис со Round Robin метод на балансирање, притоа оставена е стандардната порта 443.



Слика 15

Следниот чекор, *Configure Health-Check*, треба да се внесат параметри за портата на која ќе се следи/мониторира сервисот и режимот (mode). Останатите параметри во нашиот пример се оставени стандардни. Изборот на режимот кај HTTP сервисот е помеѓу HTTP и TCP, додека кај HTTPS е SSL и TCP. Доколку е активен HTTP сервисот, во долниот дел на прозорот е полето наменето за URI линкот кој ќе се користи за мониторинг (Слика 16).

Add Load Balancer Member Pool

Configure Health-Check
Define the default health check parameters for each service.

Service	Port	Monitor Port	Mode	Interval (sec)	Timeout (sec)	Health Threshold	Unhealth Threshold
HTTP	80		HTTP	5	15	2	3
HTTPS	443	443	SSL	5	15	2	3
TCP			TCP	5	15	2	3

URI for HTTP service:

The URI that will be polled at regular intervals to check the health of HTTP service.

Back Next Finish Cancel

Слика 16

Следниот чекор е дефинирање на сервер членовите од кои ќе биде сочинета load balance групата (Слика 17). Повторно со клик на *Add* додаваме нови членови. Дефинираме IP адреса, тежинска вредност и портата на која ќе се мониторира, во нашиот случај HTTPS 443.

Add Load Balancer Member Pool

Manage Members
Add back-end servers which will be part of this pool.

IP Address	Ratio Weight	Service and health check		
		Service	Port	Monitor Port
192.168.0.21	1	HTTPS	443	443
192.168.0.22	1	HTTPS	443	443

Back Next Finish Cancel

Слика 17

IP Address: *
 Ratio weight: *

Specify how requests will be proportionately routed to an instance. Setting ratio weight to 0 will disable the member.

Services & Monitoring:

Service	Port	Monitor Port
HTTP	<input type="text"/>	<input type="text"/>
HTTPS	<input type="text" value="443"/>	<input type="text" value="443"/>
TCP	<input type="text"/>	<input type="text"/>

OK Cancel

Add Member

Откако ќе ги додадете двата сервера, во последниот чекор имате краток преглед на сите параметри и што сè е дефинирано за овој load balancer (Слика 18).

Ready to Complete

You are about to create a new load balancer pool. Review the settings and click on Finish to complete.

Name: Orion LoadBalance

Description:

Services and Health check:

Enable	Service	Port	Monitor Port	Balancing Method	Interval (sec)	Timeout (sec)	Health Threshold	Unhealth Threshold
<input type="checkbox"/>	HTTP	80		Round Robin	5	15	2	3
<input checked="" type="checkbox"/>	HTTPS	443	443	Round Robin	5	15	2	3
<input type="checkbox"/>	TCP			Round Robin	5	15	2	3

URI for HTTP service: /

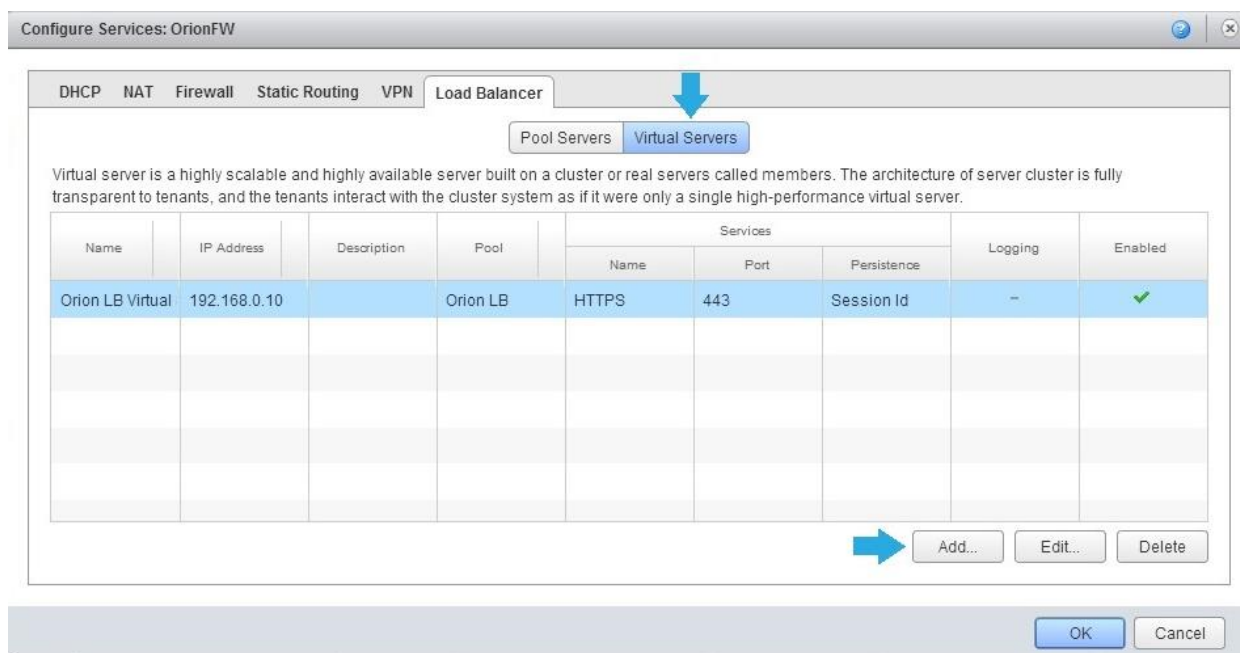
Members:

IP Address	Ratio Weight	Service and health check		
		Service	Port	Monitor Port
192.168.0.21	1	HTTPS	443	443
192.168.0.22	1	HTTPS	443	443

Back Next Finish Cancel

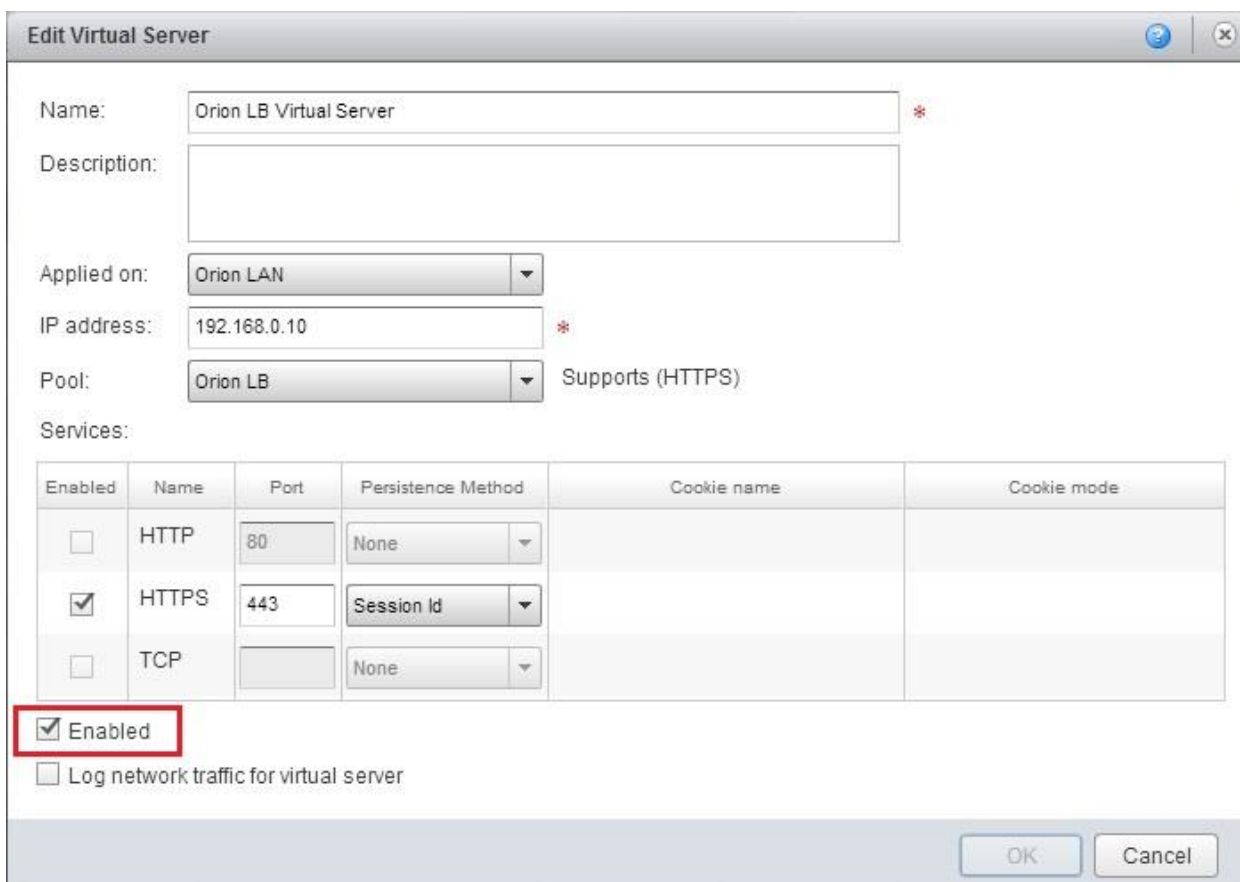
Слика 18

Откако завршивте со дефинирање на членовите кои ја сочинуваат load balancer групата, од Load Balancer делот го одбираме *Virtual Servers* прегледот (Слика 19). Следно е создавање на виртуелен сервер кој ќе биде одговорен за примање на сообраќајот наменет за load balancer групата. Како и претходно, клик на *Add*.



Слика 19

Пишувате име за виртуелниот сервер, ја одбирате мрежата (локална или јавна), IP адреса, и за која група на сервери ќе биде одговорен. Во нашиот пример тоа е Orion LB кој го создадовме погоре (Слика 20).



Слика 20

Во делот сервиси е овозможен само сервисот кој е претходно дефиниран во load balance групата. Постојат неколку типови на *Persistence Method*, кај HTTPS се *None* и *Session ID*.

Session ID е потребен при користење на SSL, со цел да се оствари сесија помеѓу клиентот и серверот, load balancer-от ја идентифицира сесијата и знае на кој член од групата се пристапува. *None* е спротивно од *Session ID* т.е. нема persistence method.

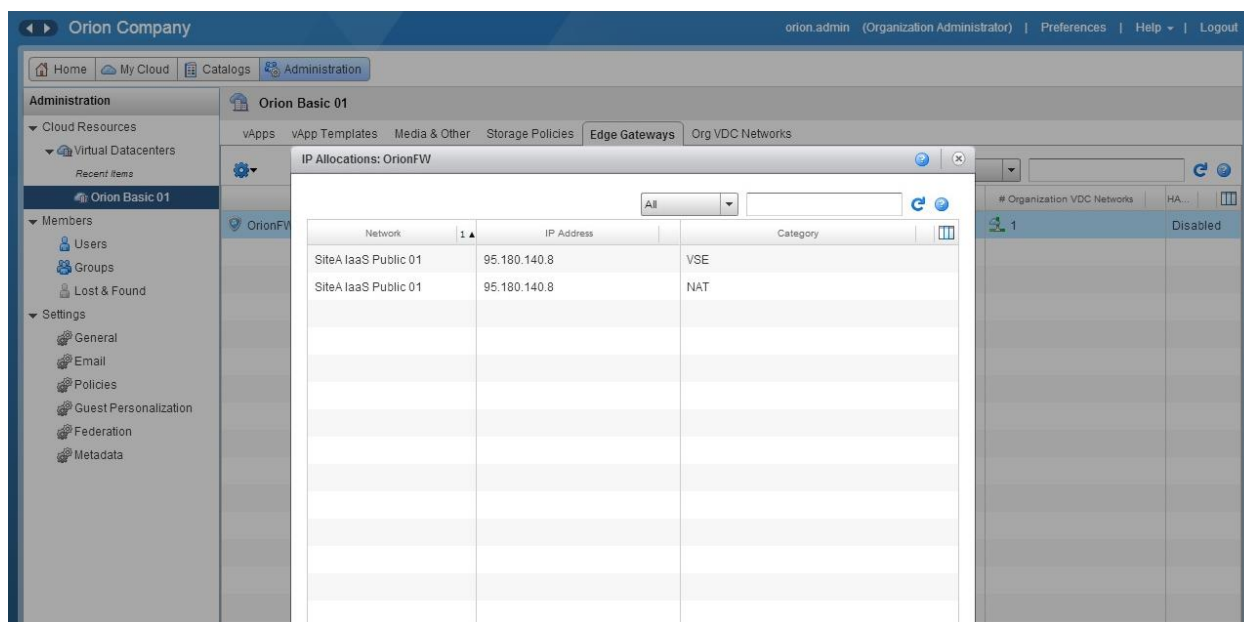
Кај HTTP постојат повторно два типа: *None* и *Cookie*. *None* методот како и кај HTTPS, така и кај HTTP, нема persistence метод. Додека методот *Cookie* функционира на сличен начин како и *Session ID*, каде е потребно дополнително во делот *Cookie mode* да одберете и режим. Постојат три типа: *Insert*, *Prefix* или *App*.

- **Insert** е метод во кој самиот load balancer испраќа persistence cookie преку HTTP од серверот до клиентот. На тој начин ја одржува сесијата со клиентскиот прелистувач при било какви барања и промени од страна на клиентот од истиот веб прелистувач.
- **Prefix** е метод во кој наместо load balancer-от, серверот испраќа cookie до клиентот. Load balancer-от го мониторира и го менува cookie-то со помош на префикси кои ги додава самиот load balancer за секој сервер посебно, секогаш кога ќе помине сообраќај преку него.
- **App** е метод во кој не се испраќа, ниту мониторира постоечко cookie од страна на load balancer-от. Во овој случај, load balancer-от ја мониторира вредноста на cookie header-от во самите параметри на URL линкот.

Исто така важно е полето Enabled да биде штиклирано.

External IP Allocations

Откако ќе завршите со конфигурирање на потребните сервиси на Edge Gateway уредот, доколку сакате да ги прегледате сите IP адреси и сервиси, повторно десен клик на името на Edge уредот од главниот преглед за Edge Gateways и одбирате **External IP Allocations** (Слика 3). Во примерот се прикажани записите за NAT и firewall кои се конфигурирани во овој виртуелен дата центар (Слика 21).



Слика 21