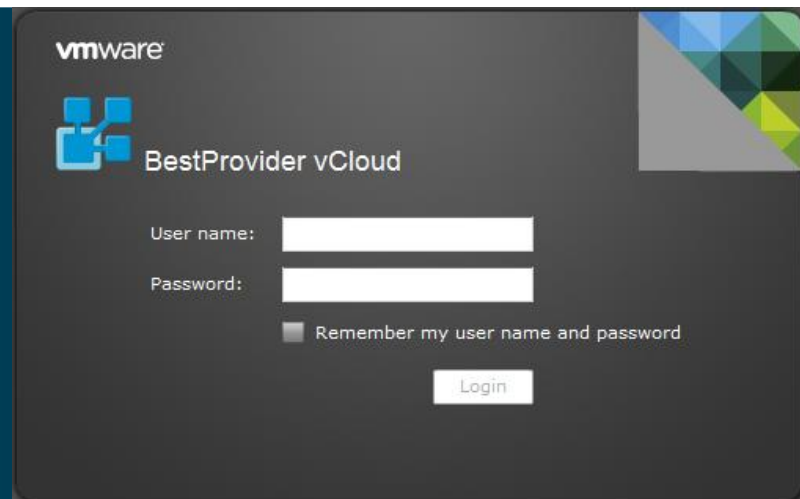




Настройка виртуальных сетей в VMware vCloud Director



Евгений Киселев

Инструктор

Учебный Центр Сиско Системс

kiselev@ciscotrain.ru

+7-916-137-88-96

IT как услуга

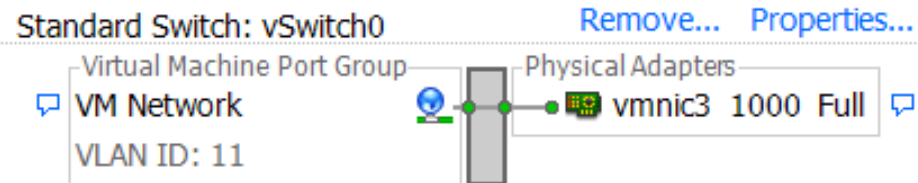
IT as a Service =

Optimizing IT
production
for business
consumption

Виртуальные коммутаторы VMware vSphere

View: **vSphere Standard Switch** vSphere Distributed Switch

Networking



View: **vSphere Standard Switch** vSphere Distributed Switch

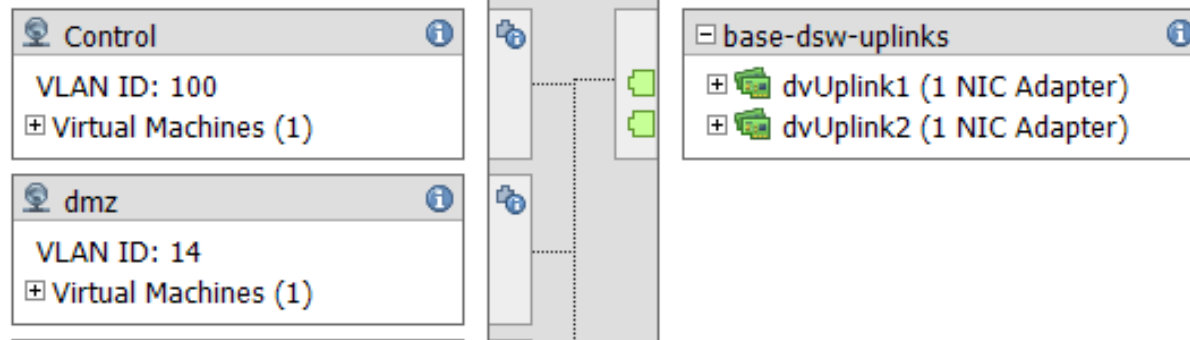
Networking

[Refresh](#)

▼ Distributed Switch: base-dsw

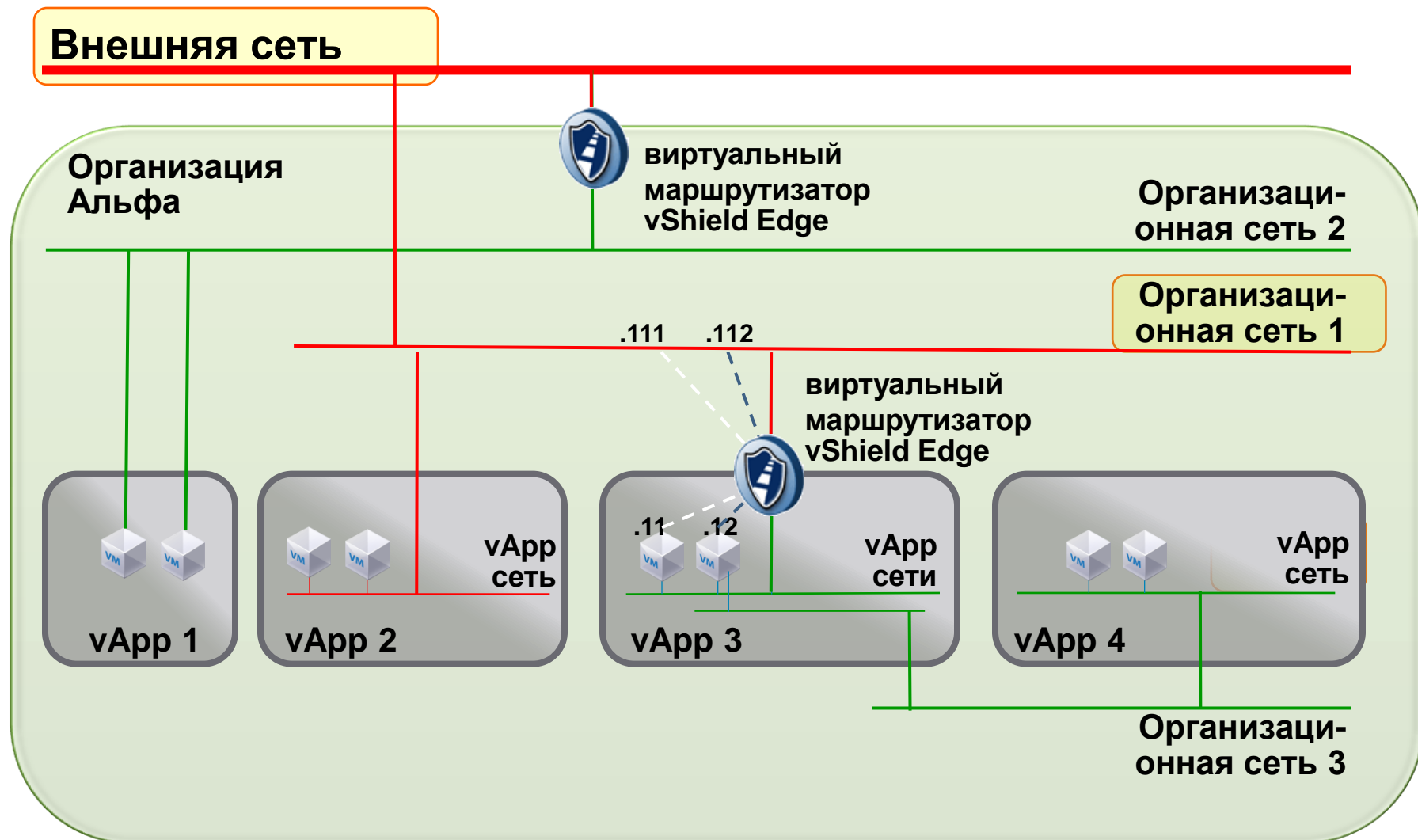
[Manage Virtual Adap](#)

base-dsw ⓘ



Типы виртуальных сетей в vCloud Director

Внешняя сеть

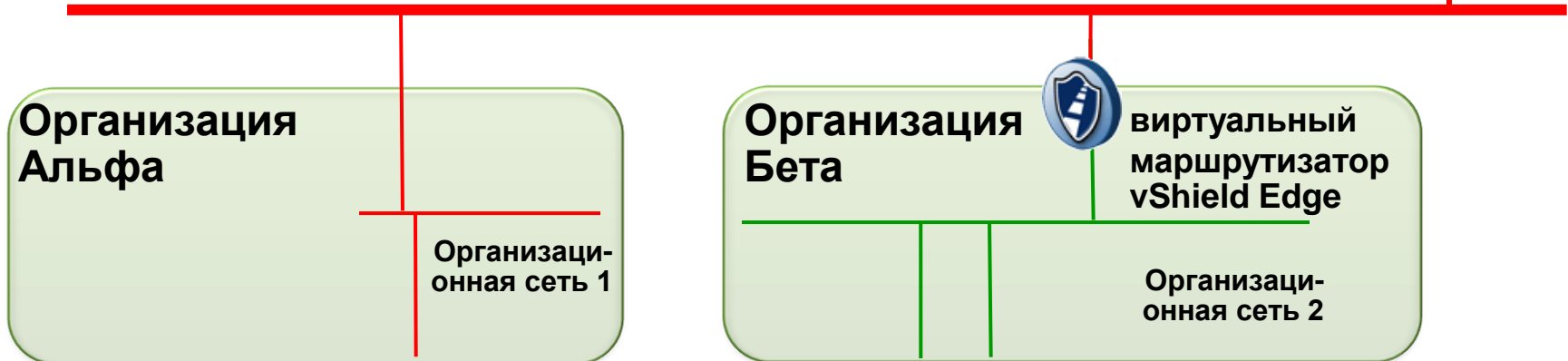


Внешняя сеть

- Обеспечивает связь за пределы облака
- Соответствует порт-группе виртуального свича (а порт-группа, в свою очередь, может соответствовать VLAN)
- К ней подключаются сети организаций
- Ей могут пользоваться несколько организаций

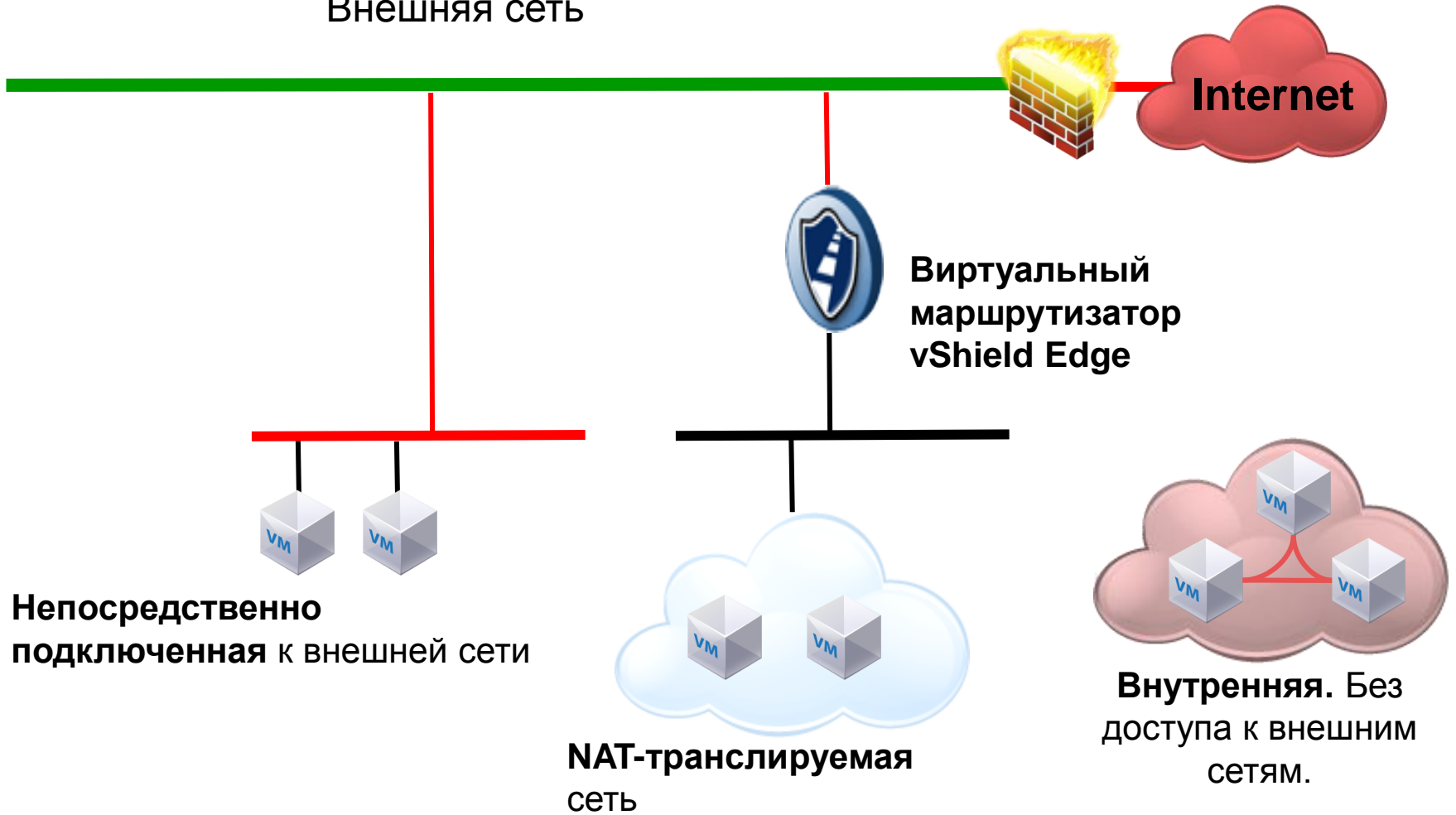


Внешняя сеть



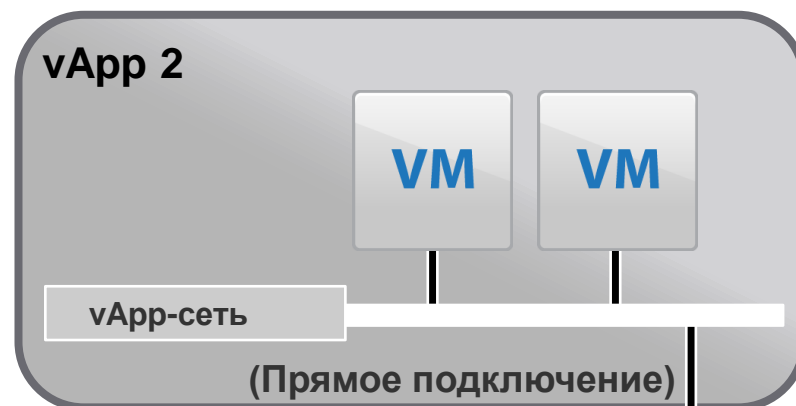
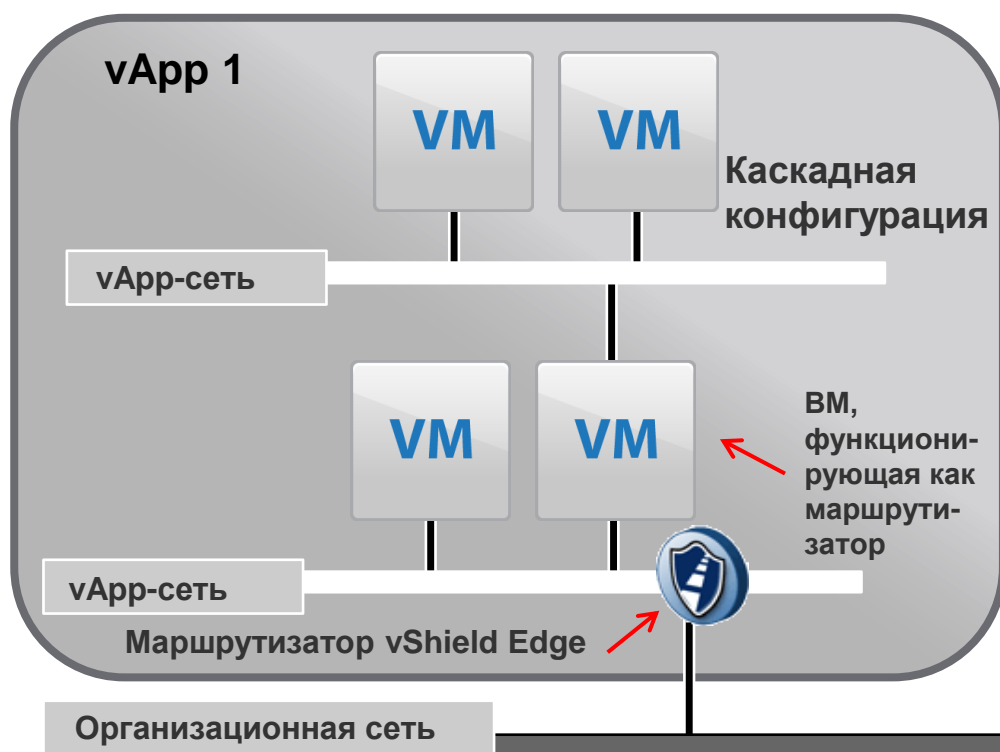
Типы организационных сетей

Внешняя сеть



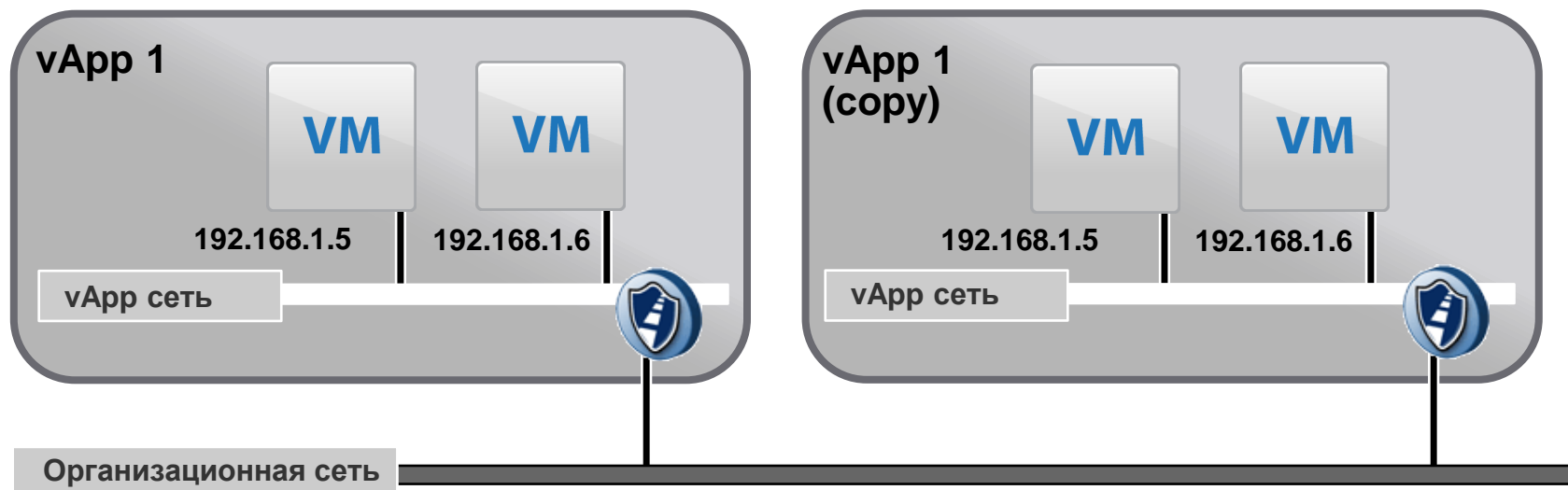
Сети для vApp

- Нужны для взаимодействия виртуальных машин внутри vApp
- Могут подключаться к организационным сетям
- Подключение может быть напрямую или через маршрутизатор vShield Edge



Fenced-сети

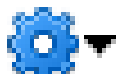
- Позволяет идентичным vApp с пересекающейся адресацией быть подключенным к одной организационной сети.



Пулы сетей



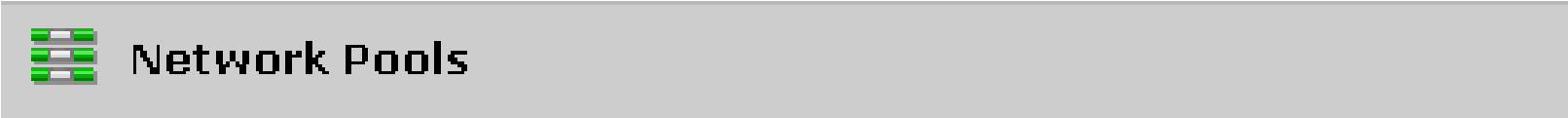
Network Pools



- Это шаблоны для создания сетей:
 - Организационных сетей (как маршрутизируемых, так и внутренних)
 - vApp-сетей
- Организационному виртуальному ЦОД можно поставить в соответствие только один пул сетей







Обеспечение сетевых пулов

- Каждый сетевой пул может быть обеспечен 3-мя видами ресурсов:
 - VLAN
 - vCD-Network Isolation
 - Созданными заранее порт-группами виртуальных свичей



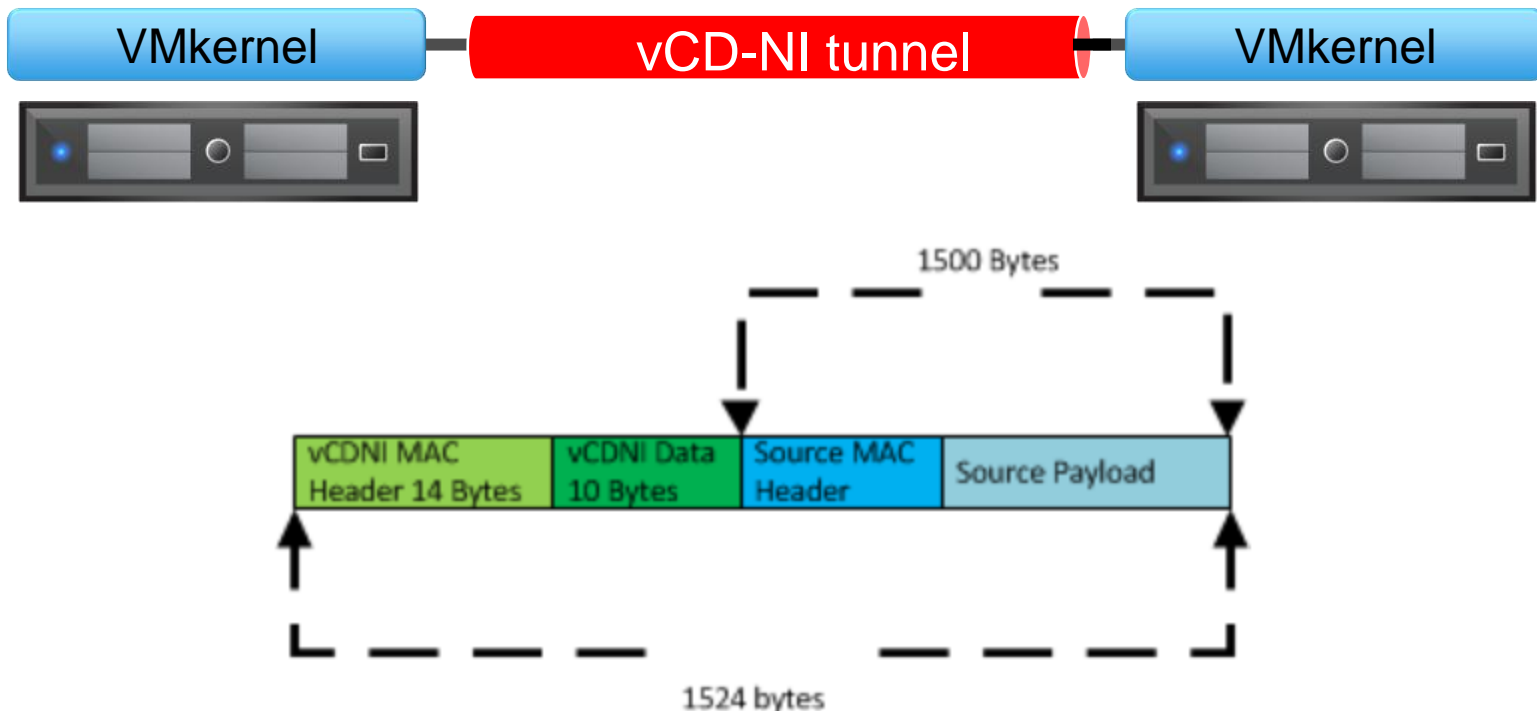
Network Pools

+ [gear icon]

Name	Status	Type
 NetworkPool PG		Portgroup
 NetworkPool vCD-NI 10		vCloud Network Isolation
 NetworkPool VLAN 10-2		VLAN

Изоляция трафика средствами VCD

- Используется MAC-in-MAC encapsulation
- Требуется транспортный VLAN
- Порт-группы на виртуальных коммутаторах создаются автоматически (требуется распределенный виртуальный свич, Nexus1000V пока не поддерживается)



Постановка задачи

Внешняя сеть

172.30.5.0 /24

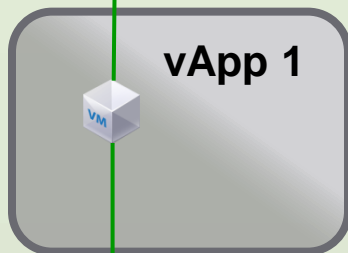
**Организация
Альфа**



виртуальный
маршрутизатор
vShield Edge

192.168.0.0 /24

**Организационная
сеть NAT-
транслируемая**



vApp 1

192.168.1.0 /24

**Организационная
сеть внутренняя**

Создание внешней сети (провайдер)

Select vSphere Network

An external network uses a network in vSphere to connect to a network outside of your cloud. The network can be a public network such as the Internet, or even an external IPsec-VPN network that connects to a given organization.

If you don't see the vCenter you need: [attach a different vCenter](#)

Select vCenter and vSphere Network

vCenter	vSphere Network	VLAN	Datacenter
Base-vCenter	Main-VMs	11	Base
	MGMT	-1	Nested
	MGMT	11	Base
	Nested-extcloud	15	Nested

! This port group has a fixed number of ports. If you try to use more ports than are available, virtual machine deployments will fail. You can try using ephemeral port groups.

These provider vDCs will connect to this new external network:

Nested-vDC

IP-адресация для внешней сети (провайдер)

New External Network

- Select vSphere Network
- Configure External Network**
- Name this External Network
- Ready to Complete

Configure External Network

Specify the network settings for this new external network. You can have this network used by VMs in organizations by adding IP address ranges or IP addresses using the Static IP pool.

Network mask:	<input type="text" value="255.255.255.0"/>	*
Default gateway:	<input type="text" value="172.30.5.1"/>	*
Primary DNS:	<input type="text" value="10.110.0.2"/>	
Secondary DNS:	<input type="text" value="10.110.0.5"/>	
DNS suffix:	<input type="text"/>	

Static IP pool:

Enter an IP range (format: 192.168.1.2 - 192.168.1.100) or IP address and click Add.

<input type="text" value="172.30.5.128 - 172.30.5.159"/>	<input type="button" value="Add"/>	*
<input type="text" value="172.30.5.128 - 172.30.5.159"/>	<input type="button" value="Modify"/>	
	<input type="button" value="Remove"/>	

Имя для внешней сети (провайдер)

New External Network

Select vSphere Network

Configure External Network

Name this External Network

Ready to Complete

Name this External Network

Enter a name and description for the new external network.

Network name: *

Description:

Создание пула сетей (провайдер)

Network Pool Type

A network pool is a collection of virtual machine networks that are available to be consumed by vDCs to create vApp networks and by organizations to create organization networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Select a network pool type from the list below:

- VLAN-backed**
Create a network pool backed by a range of VLAN IDs. The VLANs must be pre-provisioned.
- Network isolation-backed**
Create a network pool backed by Cloud isolated networks. A Cloud isolated network spans hosts and provides traffic isolation from other hosts. The system provisions Cloud isolated networks automatically.
- vSphere port group-backed**
Create a network pool backed by a vSphere port group. The port group must be pre-provisioned.

Настройка VLAN-backed пула (провайдер)

Configure VLAN-backed Pool

Enter the settings for the new network pool below:

VLAN ID Range

Enter a VLAN ID range (format: 1-1000) and click Add.

<input type="text"/>	<input type="button" value="Add"/> *
113 - 114	<input type="button" value="Modify"/>
	<input type="button" value="Remove"/>

Select vNetwork Distributed Switch

<input type="text"/>	<input type="button" value="Refresh"/>	All	<input type="text"/>														
<table border="1"><thead><tr><th>vCenter</th><th>1</th></tr></thead><tbody><tr><td>Base-vCenter</td><td><input type="checkbox"/></td></tr></tbody></table>	vCenter	1	Base-vCenter	<input type="checkbox"/>	<table border="1"><thead><tr><th>vDS</th><th>1</th><th>vCenter</th></tr></thead><tbody><tr><td>base-dsw</td><td><input type="checkbox"/></td><td>Base-vCenter</td></tr><tr><td>ek-nexus</td><td><input type="checkbox"/></td><td>Base-vCenter</td></tr><tr><td>nested-dsw</td><td><input checked="" type="checkbox"/></td><td>Base-vCenter</td></tr></tbody></table>	vDS	1	vCenter	base-dsw	<input type="checkbox"/>	Base-vCenter	ek-nexus	<input type="checkbox"/>	Base-vCenter	nested-dsw	<input checked="" type="checkbox"/>	Base-vCenter
vCenter	1																
Base-vCenter	<input type="checkbox"/>																
vDS	1	vCenter															
base-dsw	<input type="checkbox"/>	Base-vCenter															
ek-nexus	<input type="checkbox"/>	Base-vCenter															
nested-dsw	<input checked="" type="checkbox"/>	Base-vCenter															
<input type="button" value="Previous"/> <input type="button" value="Next"/> 1-1 of 1 <input type="button" value="Refresh"/>	<input type="button" value="Previous"/> <input type="button" value="Next"/> 1-3 of 3 <input type="button" value="Refresh"/>																

These provider vDCs will connect to networks allocated from this new network pool:

Provider vDC
Nested-vDC

Имя для VLAN-backed пула (провайдер)

Create Network Pool Wizard

[Network Pool Type](#)
[Configure VLAN-backed Pool](#)
Name this Network Pool
[Ready to Complete](#)

Name this Network Pool
Enter profile settings for the new network pool below:

Name:
 *

Description:

Create Network Pool Wizard

[Network Pool Type](#)
[Configure VLAN-backed Pool](#)
[Name this Network Pool](#)
Ready to Complete

Ready to Complete
You are about to create a network pool with the following settings:

Name:	DemoOrg-VLAN-pool
Description:	
VLAN ID Range:	113 - 114
Selected vNetwork Distributed Switch:	nested-dsw

Создание пула сетей для vApp (провайдер)

Create Network Pool Wizard

Network Pool Type

Configure Isolation-backed Pool

Name this Network Pool

Ready to Complete

Network Pool Type

A network pool is a collection of virtual machine networks that are available to be consumed by vDCs to create vApp networks and by organizations to create organization networks. Network traffic on each network in a pool is isolated at layer 2 from all other networks.

Select a network pool type from the list below:

- VLAN-backed
Create a network pool backed by a range of VLAN IDs. The VLANs must be pre-provisioned.
- Network isolation-backed
Create a network pool backed by Cloud isolated networks. A Cloud isolated network spans hosts and provides traffic isolation from other hosts. The system provisions Cloud isolated networks automatically.
- vSphere port group-backed
Create a network pool backed by a vSphere port group. The port group must be pre-provisioned.

Настройка VCDNI-пула (провайдер)

Configure Isolation-backed Pool


Enter the settings for the new network pool below:


Number of VCD isolated networks:

*

VLAN ID:

Select vNetwork Distributed Switch



vCenter	1 ▲	
Base-vCenter		

▼

vDS	1 ▲	vCenter
base-dsw		Base-vCenter
ek-nexus		Base-vCenter
nested-dsw		Base-vCenter

Navigation: 1-1 of 1 | 1-3 of 3

These provider vDCs will connect to networks allocated from this new network pool:

Provider vDC
Nested-vDC

Создание новой организации (провайдер)

New Organization

- Name this Organization**
- LDAP Options
- Add Local Users
- Catalog Publishing
- Email Preferences
- Policies
- Ready to Complete

Name this Organization

An Organization is the fundamental VCD grouping. An Organization vApps use. An organization can be a department in your own company.

Organization name:

 *

The unique identifier in the full URL with which users log in to this organization.

Default organization URL:

<https://172.30.1.60/cloud/org/DemoOrg/>

Organization full name:

 *

Appears in the Cloud application header when users log in. An organization a

Description:

Создание администратора организации (провайдер)

New Organization

New User

Name this Organization

LDAP Options

Add Local Users

Catalog Publishing

Email Preferences

Policies

Ready to Complete

Add Local Users

Even if you use LDAP, you can add a local user who will be the administrator.

Local users:

User Name

Credentials

User name: *

Password: *

Confirm password: *

Enable

Role

Roles available to this user:

▼

Contact Info


Full name:



Email address:





Создание виртуального ЦОД организации – на базе виртуального ЦОД провайдера (провайдер)

Select Provider vDC

You can allocate resources to an organization by creating an Organization vDC that is partitioned from a Provider vDC. Select the Provider vDC.

All 

Provider vDC	Processor (Used/Total)	Memory (Used/Total)	Storage (Used/Total)
 Base-vDC	0.13%	0.08%	23.10%
 Nested-vDC	0.00%	0.00%	23.75%

  1-2 of 2  

The following networks are available to the Provider vDC you selected:

Network	Gateway	Subnet	DNS
 Nested-extcloud-vlan15	172.30.5.1	255.255.255.0	10.110.0.2

Выбор модели выделения ресурсов (провайдер)

Select Allocation Model

The Organization vDC's allocation model allows you to control the quality of the service you're providing and the cost of providing these resources.

- Allocation Pool
Only a percentage of the resources you allocate are committed to the organization vDC. The system administrator controls overcommitment of capacity on the following pages.
- Pay-As-You-Go
Resources are committed only when vApps are created in the organization vDC. The system administrator controls overcommitment of capacity on the following pages. When backed by a provider vDC that has multiple resource pools, compute resources are Elastic.
- Reservation Pool
All of the resources you allocate are committed to the organization vDC. Users can control the overcommitment of capacity at any time.

Настройки модели Pay-As-You Go (провайдер)

Configure Pay-As-You-Go Model

In this model, compute resources are committed only when vApps are running in this Organization VDC.

CPU resources guaranteed: %

The percentage of CPU resources that are guaranteed to a virtual machine running within this organization vDC. You can use this option to control overcommitment of CPU resources.

vCPU speed: GHz

This value defines what a virtual machine with one vCPU will consume at maximum when running within this organization vDC. A virtual machine with two vCPUs would consume a maximum of twice this value.

Memory resources guaranteed: %

The percentage of memory that is guaranteed to a virtual machine running within this organization vDC. You can use this option to control overcommitment of memory resources.

Maximum number of VMs: Unlimited

A safeguard that allows you to control the number of vApps or VMs in this vDC.

The committed resources from Provider vDC, 'Nested-vDC' using these allocation settings:

0 GHz CPU reservation, 12.03 GHz free

0 GB Memory reservation, and 10.88 GB free

The typical number of vApps or VMs you can expect using these allocation settings at this time:

21 'small' VMs: 260.00 MHz CPU = 1 vCPUs * 260.00 MHz vCPU Rating, 512.00 MB RAM

10 'medium' VMs: 520.00 MHz CPU = 2 vCPUs * 260.00 MHz vCPU Rating, 1.0 GB RAM

5 'large' VMs: 1.0 GHz CPU = 4 vCPUs * 260.00 MHz vCPU Rating, 2.0 GB RAM

Настройки виртуального хранилища (провайдер)

Allocate Storage

As the service provider, you control the storage allocation to the organization by setting a limit, enabling thin provisioning of live storage and fast provisioning of virtual machines.

Storage limit: 50 Unlimited GB (4% of 1,397.07 GB available)

- Enable thin provisioning**
Enabling thin provisioning will save storage space by committing it on demand. This will allow over-allocation of storage.
- Enable fast provisioning**
Enabling fast provisioning can reduce the time it takes to create virtual machines by using vSphere linked clones. If you disable fast provisioning, all provisioning operations will result in full clones.

Выбор пула для сетей vApp (провайдер)

Select Network Pool

Select the network pool that provides vApp networks to this organization vDC and specify the vApp network quota from this pool.

Network pool:

Total available networks: 30

Quota for this organization:

⚠ The configured quota is greater than the total number of networks available in the selected network pool. The maximum number of networks that can be provisioned is 30.

Создание сетей организации (провайдер)

Select Typical or Advanced Setup

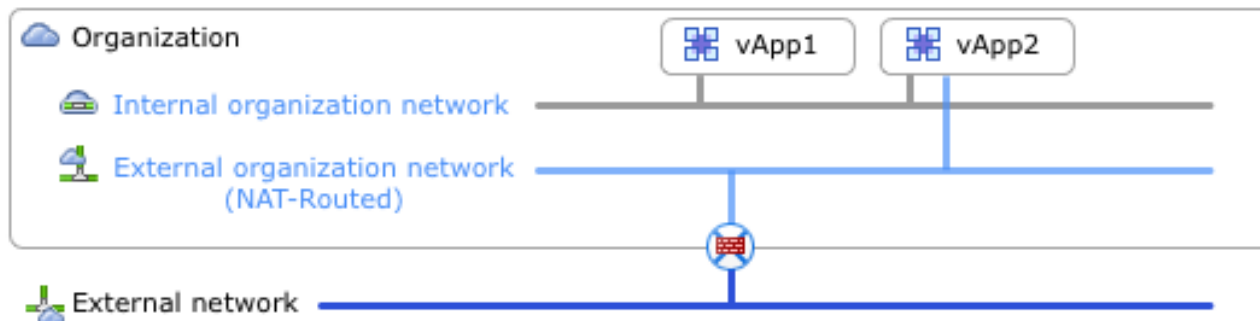
The default options are the most common setup for a new organization.

What type of network access do you want to give this organization?

- Typical
The quickest and most common way to set up networks for an organization.

Create an internal network

Create an external network via: Routed connection



An internal organization network is accessible only by this organization. It provides the organization with a private network to which multiple vApps can connect. An external organization network provides an organization with external connectivity, such as to the Internet. Virtual machines from multiple organizations can communicate over this network.

- Advanced
Add a new network and specify its detailed settings.

Создание внутренней сети организации (провайдер)

Configure Internal Organization Network


Select the network pool that allocates the internal network.

If you don't see the network pool you need:

[create a new network pool](#)

Only use networks that are accessible by this organization.

Select Network Pool

All 

Name	vCenter	Type	Network (Used/Total)
DemoOrg-VCDNI-pool	Base-vCenter	Cloud Network Isolator	0 / 30 0%
DemoOrg-VLAN-pool	Base-vCenter	VLAN	0 / 2 0%

Настройка IP-адресации для внутренней сети организации (провайдер)

Configure IP Settings

Enter the network settings of the new organization network below:

Network mask:	<input type="text" value="255.255.255.0"/>	*
Default gateway:	<input type="text" value="192.168.1.1"/>	*
Primary DNS:	<input type="text" value="10.110.0.2"/>	
Secondary DNS:	<input type="text" value="10.110.0.5"/>	
DNS suffix:	<input type="text"/>	

Static IP pool:

Enter an IP range (format: 192.168.1.2 - 192.168.1.100) or IP address and click Add.

<input type="text"/>	<input type="button" value="Add"/>
<input type="text" value="192.168.1.100 - 192.168.1.199"/>	<input type="button" value="Modify"/>
	<input type="button" value="Remove"/>

Создание «внешней» (маршрутизируемой) сети организации (провайдер)


Configure External Organization Network


Select the external network you want to connect to, and select the network pool that allocates the internal network.





If you don't see the network you need: [create a new external network](#) or [create a new network pool](#)

Only use networks that are accessible by this organization.


Select External Network


All 

Name <small>1 ▲</small>	VLAN	Default Gateway	vCenter	IP Pool (Used/Total)	
Nested-extclou	15	172.30.5.1	Base-vCenter	0 / 32 0%	

  1-1 of 1  

Select Network Pool

All 

Name <small>1 ▲</small>	vCenter	Type	Network (Used/Total)	
DemoOrg-VCDNI-pool	Base-vCenter	Cloud Network Isolator	0 / 30 0%	
DemoOrg-VLAN-pool	Base-vCenter	VLAN	0 / 2 0%	

Настройка IP-адресации для маршрутизируемой сети организации (провайдер)

Configure IP Settings

Enter the network settings of the new organization network below:

Network mask:	<input type="text" value="255.255.255.0"/>	*
Default gateway:	<input type="text" value="192.168.0.1"/>	*
Primary DNS:	<input type="text" value="10.110.0.2"/>	
Secondary DNS:	<input type="text" value="10.110.0.5"/>	
DNS suffix:	<input type="text"/>	

Static IP pool:

Enter an IP range (format: 192.168.1.2 - 192.168.1.100) or IP address and click Add.

<input type="text"/>	<input type="button" value="Add"/>	*
<input type="text" value="192.168.0.100 - 192.168.0.199"/>	<input type="button" value="Modify"/>	
	<input type="button" value="Remove"/>	

Как это отображается в vSphere

- [-]  Nested
 - [+]  ek-nexus
 -  VM Network
 - [-]  nested-dsw
 -  nested-dsw-uplinks
 -  dvs.VCDVSDemoOrg-Internal-netw-9eb2eee5-80ae-40c0-a640-bb1519448d6a
 -  dvs.VCDVSDemoOrg-Routed-netw-c50b9c32-d2a6-49b6-a5f5-3894607e03de
 -  Nested-extcloud

- [-]  Nested
 - [-]  ek-VCD
 - [-]  DemoOrg (05426f40-c54f-4c76-9fca-bb9f2dfe3194)
 -  DemoOrg-vDC (c9ac5085-88c2-4e27-b403-f48474117309)
 - [-]  Service VMs
 - [-]  vse-c50b9c32-d2a6-49b6-a5f5-3894607e03de
 -  vse-DemoOrg-Routed-netw (c50b9c32-d2a6-49b6-a5f5-3894607e03de)
 - [-]  System (a93c9db9-7471-3192-8d09-a8f7eeda85f9)
 -  System vDC (09b8b317-c18a-477a-ac26-43082b46a677)

Создание vApp (потребитель)

New vApp

- Name this vApp
- Add Virtual Machines
- Configure Virtual Machines
- Configure Networking
- Ready to Complete

Name this vApp

A vApp is a cloud computer system that contains one or more virtual machines (VMs). Name and describe the leases.

Name: *

Description:

Leases


Runtime lease: Days Expires on: 11/30/2011 2:35 AM
How long this vApp can run before it is automatically stopped.

Storage lease: Days Expires on: 12/23/2011 2:35 AM
When this vApp is stopped, how long it is available before being automatically cleaned up.







Добавление виртуальных машин (потребитель)

Add Virtual Machines


You can search the catalog for virtual machines to add to this vApp or add a new, blank VM. Once the vApp is created, you can power on the new VM and install an operating system.

Look in: My organization's catalogs All 

Name	OS	Gold Master	vApp	Catalog	Created On	Disk Info

 Add  Remove   0-0 of 0  

Name	OS	Gold Master	vApp	Catalog	Created On	Disk Info

 New Virtual Machine...

Создание новой виртуальной машины (потребитель)

New Virtual Machine ✕

Full name: *

A label for this VM that appears in VCD lists.

Computer name: *

The computer name / host name set in the guest OS of this VM that identifies it on a network.
This field is restricted to 15 characters because of a Windows OS limitation on computer names.

Description:

Operating System Family:

Operating System:

Virtual hardware version:

Number of CPUs:

Memory:

Hard disk size:

Bus type:

Number of NICs:

Подключение сетевых адаптеров VM к сетям (потребитель)



Configure Virtual Machines

Select the virtual datacenter (vDC) in which this vApp is stored and runs when it's started. Name each virtual machine and select the network to which you want it to connect. You can configure additional properties for virtual machines after you complete this wizard.

Select virtual datacenter:

Show network adapter type

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapter support for various guest operating systems and hosts.



Full Name	Computer Name	Primary NIC	Network	IP Assignment
<input type="text" value="Demo-VM-1"/>	<input type="text" value="Demo-VM-1"/>	<input checked="" type="radio"/> NIC 0	 DemoOrg-Routed-	Static - IP Pool <input type="text"/> *
		<input type="radio"/> NIC 1	 DemoOrg-Interna	Static - IP Pool <input type="text"/> *
				Static - IP Pool Static - Manual DHCP

Настройки подключения к сетям (потребитель)

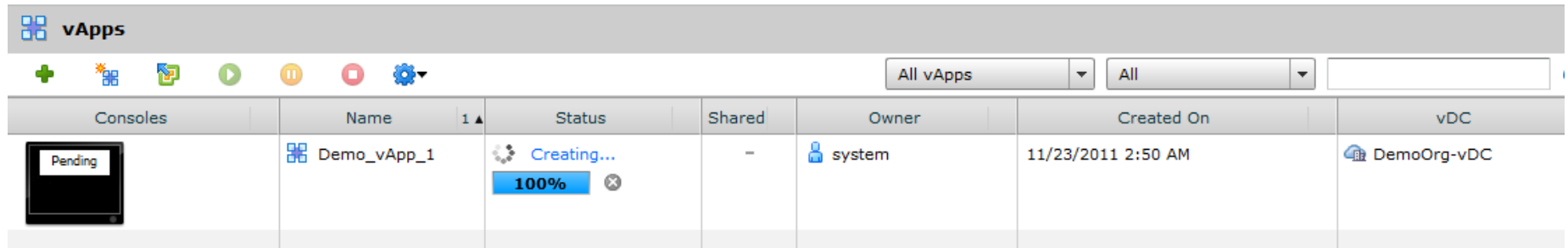
Configure Networking


Specify how this vApp, its virtual machines, and its vApp networks connect to the organization networks that are accessed in this vApp.

- Fence vApp
Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.
- Always use assigned IP addresses until this vApp or associated networks are deleted.
By default, when a vApp is stopped, public IP and MAC addresses for the network are relinquished to pool. Select this option if you intend to retain IP and MAC addresses of router across deployments.
- Show networking details

Name	Type	Default Gateway	Network Mask	Connection	DHCP
 DemoOrg-Routed	organization	192.168.0.1	255.255.255.0	Direct	-
 DemoOrg-Internal	organization	192.168.1.1	255.255.255.0	Direct	-

Как это отображается в vSphere



Consoles	Name	Status	Shared	Owner	Created On	vDC
	Demo_vApp_1	Creating... 100%	-	system	11/23/2011 2:50 AM	DemoOrg-vDC

- [-] Nested
 - [-] ek-VCD
 - [-] DemoOrg (05426f40-c54f-4c76-9fca-bb9f2dfe3194)
 - [-] DemoOrg-vDC (c9ac5085-88c2-4e27-b403-f48474117309)
 - [-] Demo_vApp_1 (17f14240-f199-4a01-82f8-62fbe2af89cf)
 - [-] Demo-VM-1 (8633cc1b-8962-4944-b206-da68acbae19f)
 - [-] Service VMs
 - [-] vse-c50b9c32-d2a6-49b6-a5f5-3894607e03de
 - [-] vse-DemoOrg-Routed-netw (c50b9c32-d2a6-49b6-a5f5-3894607e03de)
 - [-] System (a93c9db9-7471-3192-8d09-a8f7eeda85f9)
 - [-] System vDC (09b8b317-c18a-477a-ac26-43082b46a677)

Настройка сервисов для сети организации (потребитель)

Home My Cloud Catalogs Administration

Administration

- Cloud Resources
 - Virtual Datacenters (1 re)
 - DemoOrg-vDC
 - Networks**
- Members
 - Users
 - Lost & Found
- Settings
 - General
 - Email
 - LDAP
 - Policies
 - Guest Personalization

Networks

+ ⚙

Name	Status	Default Gateway	Type
DemoOrg-Internal-netw	✓	192.168.1.1/24	Internal
DemoOrg-Routed-netw	✓	192.168.0.1/24	Routed

Network Menu

- Configure Services...
- IP Allocations
- Connected vApps
- Reset Network
- Delete
- Synchronize syslog server settings
- Properties

Настройка DHCP (потребитель)

Configure Services: DemoOrg-Routed-netw

DHCP

Firewall

NAT - External IPs

NAT Mapping

Site-to-Site VPN

Static Routing

DHCP automatically provides IP addresses to VMs.

Enable DHCP

Network mask: 255.255.255.0

Gateway: 192.168.0.1

IP range: *

Default lease time: ▲▼

Max lease time: ▲▼

Настройка МСЭ (потребитель)

Configure Services: DemoOrg-Routed-netw

DHCP | **Firewall** | NAT - External IPs | NAT Mapping | Site-to-Site VPN | Static Routing

Rules can be added to the Firewall to allow or deny specific network traffic. The order of these rules can be changed by selecting one or more rules, dragging and dropping them at the desired location in the list. The order of any selected rules is preserved after dropping them into a different location within the list.

Enable firewall

Default action Deny Allow Log

Applicable to traffic that does not match the rules in the list.

Firewall Rule	Source	Destination	Protocol	Traffic ...	Action	Log	Ena...
Allow all outgoir	Any:Any				Allow		

Add Firewall Rule

Name:

Traffic direction Incoming Outgoing

Source IP: *

Enter IP address or * for any IP address

Source Port: ▾

Destination IP: *

Enter IP address or * for any IP address

Destination Port: ▾

Protocol: ▾

Action Allow Deny

Enabled

Log network traffic for firewall rule

OK Cancel

Add... Edit... Delete

OK Cancel

Провайдер выделяет “публичный” IP

Configure Services: DemoOrg-Routed-netw

DHCP

Firewall

NAT - External IPs

NAT Mapping

Site-to-Site VPN

Static Routing

Organization VMs can be accessed from outside the organization using these external IP addresses. The IP addresses must be routable on the external network and unique across internal networks.

External network gateway: 172.30.5.1

External network mask: 255.255.255.0

External IPs

Enter an IP address (format: 10.1.1.1) and click Add.

172.30.5.5

Add

172.30.5.5

Modify

Remove

Настройка NAT с использованием адреса, выданного провайдером (потребитель)

Configure Services: DemoOrg-Routed-netw

DHCP

Firewall

NAT - External IPs

NAT Mapping

Site-to-Site VPN

Static Routing

Organization administrators typically handle network address translation (NAT) of external IP addresses specified on the previous tab to internal IP addresses. Ensure that the firewall rules are configured appropriately. NAT rules are applied in the order in which they appear below. The order of these NAT rules can be changed by selecting one or more rules, dragging and dropping them at the desired location in the list. The order of any selected rules is preserved after dropping them into a different location within the list.

Router external IP: 172.30.5.128

Enable IP Masquerade

Map External IP	Port	To Internal IP	Port	Protocol	Rule Type

Add NAT Rule

Port Forwarding IP Translation

External IP: 172.30.5.5 *

Port: 80

Internal IP: 192.168.0.100 *

Port: 80

Protocol: TCP

OK Cancel

Add... Edit... Delete

Резюме по настройке МСЭ совместно с NAT

DHCP Firewall **NAT - External IPs** NAT Mapping Site-to-Site VPN Static Routing

Rules can be added to the Firewall to allow or deny specific network traffic. The order of these rules can be changed by selecting one or more rules, dragging and dropping them at the desired location in the list. The order of any selected rules is preserved after dropping them into a different location within the list.

Enable firewall

Default action Deny Allow Log

Applicable to traffic that does not match the rules in the list.

Firewall Rule	Source	Destination	Protocol	Traffic ...	Acti...	Log	Ena...
permit-RDP	Any:Any	192.168.0.100:3389	TCP	Incoming	Allow		
permit-HTTP	Any:Any	192.168.0.100:80	TCP	Incoming	Allow		
Allow all outgoir	Any:Any	Any:Any	ANY	Outgoing	Allow		

DHCP Firewall NAT - External IPs **NAT Mapping** Site-to-Site VPN Static Routing

Organization administrators typically handle network address translation (NAT) of external IP addresses specified on the previous tab to internal IP addresses. Ensure that the firewall rules are configured appropriately. NAT rules are applied in the order in which they appear below. The order of these NAT rules can be changed by selecting one or more rules, dragging and dropping them at the desired location in the list. The order of any selected rules is preserved after dropping them into a different location within the list.

Router external IP: 172.30.5.128

Enable IP Masquerade

Map External IP	Port	To Internal IP	Port	Protocol	Rule Type
172.30.5.5	80	192.168.0.100	80	TCP	Port Forwarding
172.30.5.5	3389	192.168.0.100	3389	TCP	Port Forwarding

Настройка Site-to-Site VPN (потребитель)

DHCP

Firewall

NAT - External IPs

NAT Mapping

Site-to-Site VPN

Static Routing

Site-to-site VPN allows you to create secure tunnels to other networks. Ensure that the firewall rules are configured appropriately.

Enable site-to-site VPN

External IP address: 172.30.5.128

This is the IP address of the external interface of the vShield edge router deployed for this network.

Public IP address:

This field is optional. It is required so that entities from different external networks (across WAN/Internet) can reach the external interface of the vShield edge router.

Tunnels to other networks

Name	Status	Peer Network	Organization

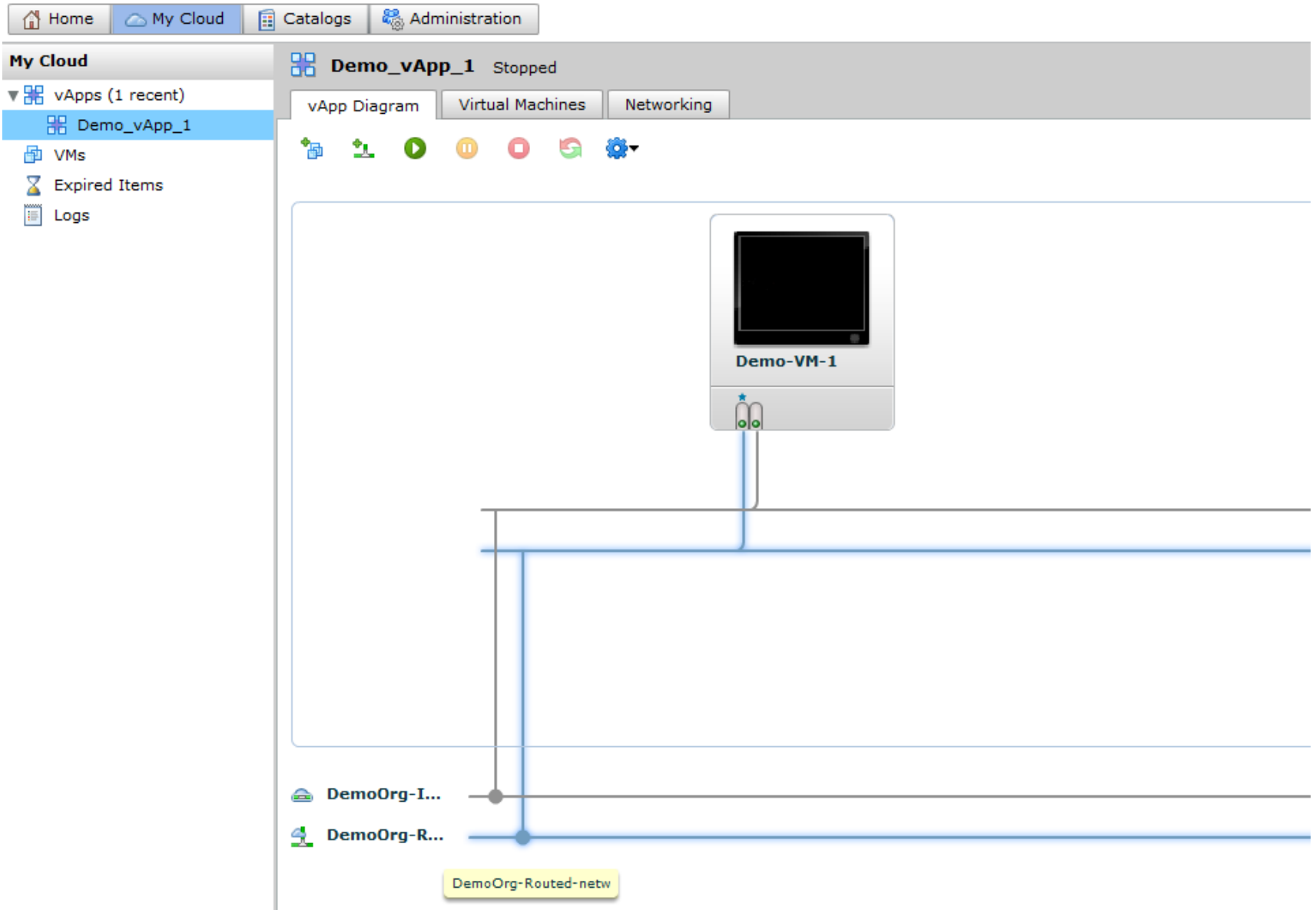
Add...

Edit...

Delete

i VPN tunnel status takes approximately 2 minutes to update after a connect or disconnect.

Сетевая диаграмма





Постановка задачи 2

