Using Amazon VPC

1. Overview

Simply put, [AWS’s latest VPC release](http://aws.typepad.com/aws/2013/03/amazon-ec2-update-virtual-private-clouds-for-everyone.html) gives users two modes to launch resources (instance, ELBs, etc):

if your AWS account registration < this release:

for region in all AWS regions:

if you have launched EC2, RDS, ElasticCache instance, ELBs in region:

You have

- EC2-Classic # same with EC2 before

- EC2-VPC # same with VPC before

else: # your AWS account > this release

You have only EC-VPC

And AWS pre-creates a Default VPC for you # very similar with EC2

Or you can define VPC by yourself # we call Custom VPC

IDE will detect your supported platform , whether you have a default VPC, and prompt to let you choose which platform or VPC you want to use when creating a new blank stack. Also, we predefine some rules to make VPC easier to use and less error-prone:

* You cannot have both EC2 resources and VPC resources in one stack.
* One VPC per stack max (either Default VPC or Custom VPC). Multi-VPC in one stack is forbidden (why)
* Don’t delete or modify Default VPC. Otherwise, a default-vpc-stack launch probably fails

We believe the rules will serve most scenarios well. If you don’t like them or have particular requirements, [let’s know](mailto:support@madeiracloud.com).

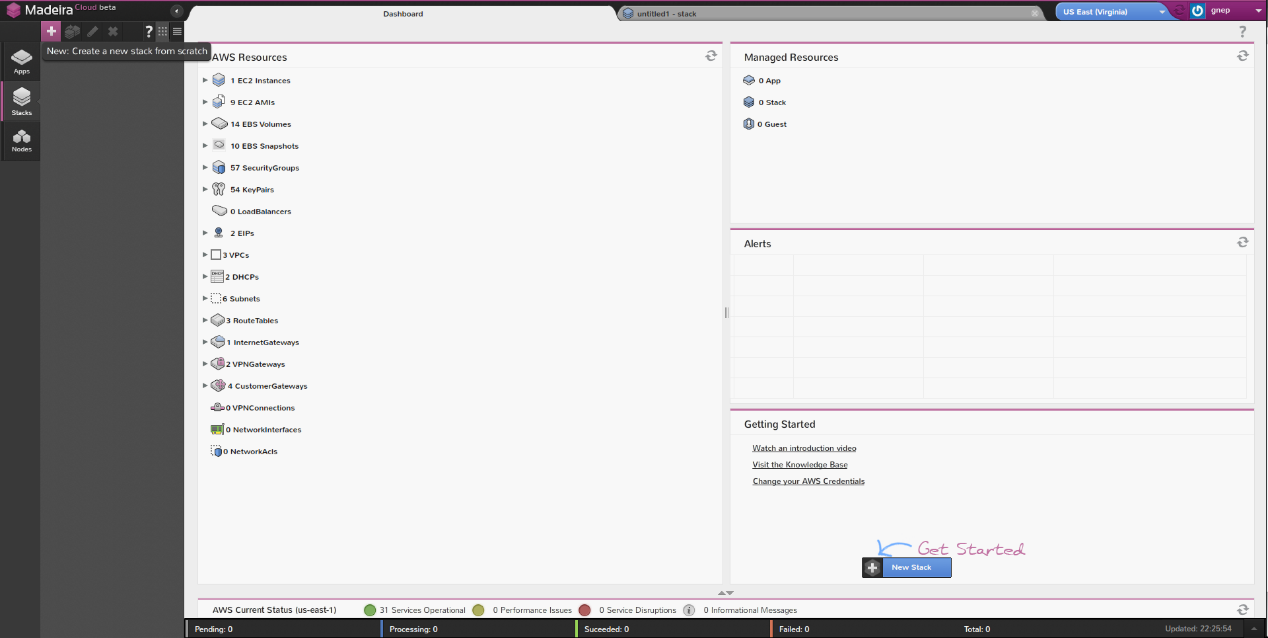
Next, we will use the VPC examples in AWS’s documents to demonstrate you how easy and brain-friendly to design and create VPC environments with our IDE.

1.1 [VPC with a Public Subnet Only](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario1.html)

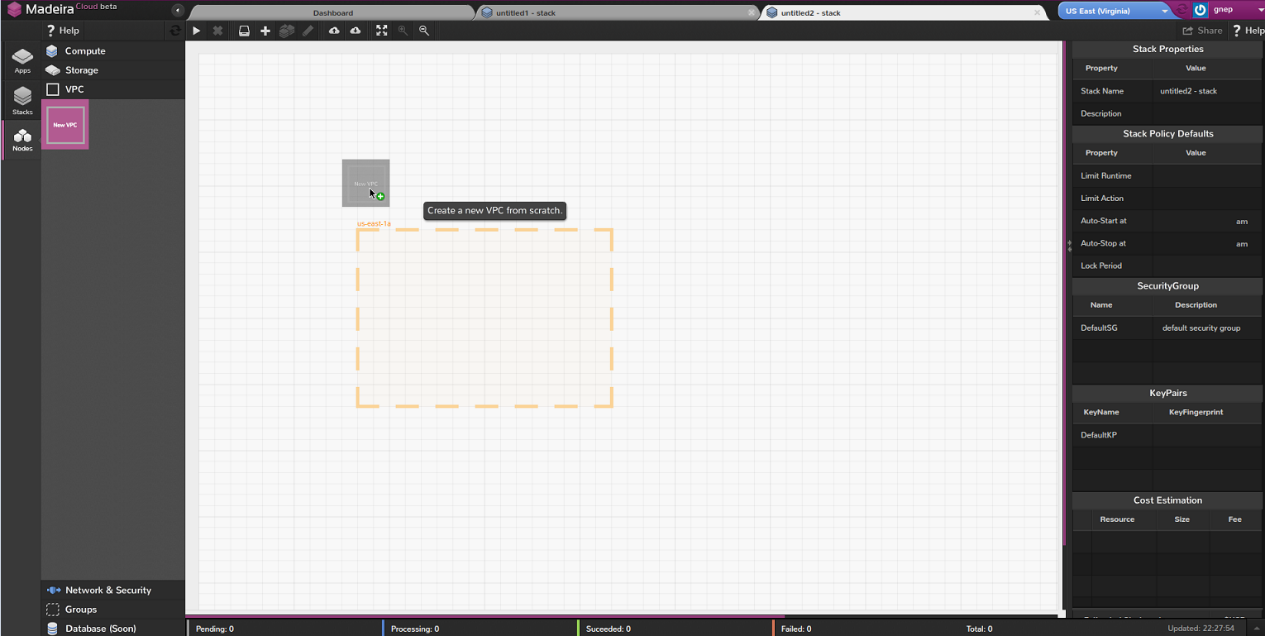
**Description**: “The configuration for this scenario includes a virtual private cloud (VPC) with a single public subnet, and an Internet gateway to enable communication over the Internet. We recommend this configuration if you need to run a single-tier, public-facing web application, such as a blog or a simple website.”

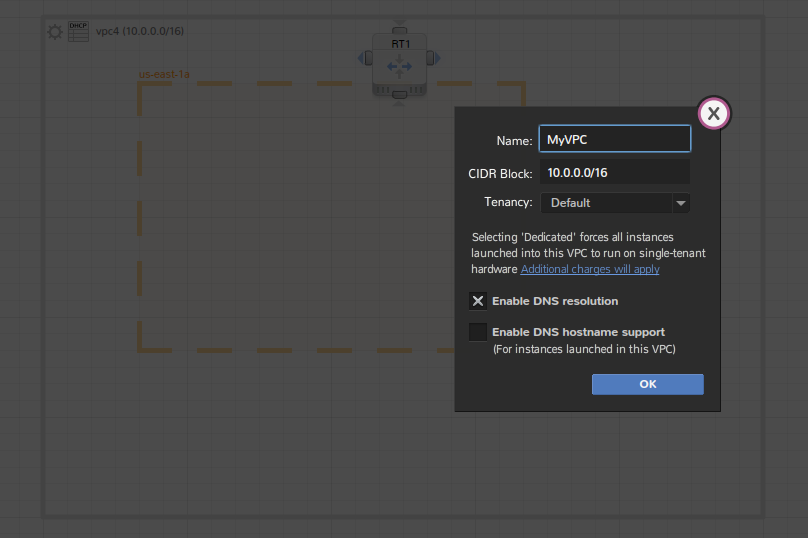
**Step by step:**

1. Create a new stack



1. Add a new VPC

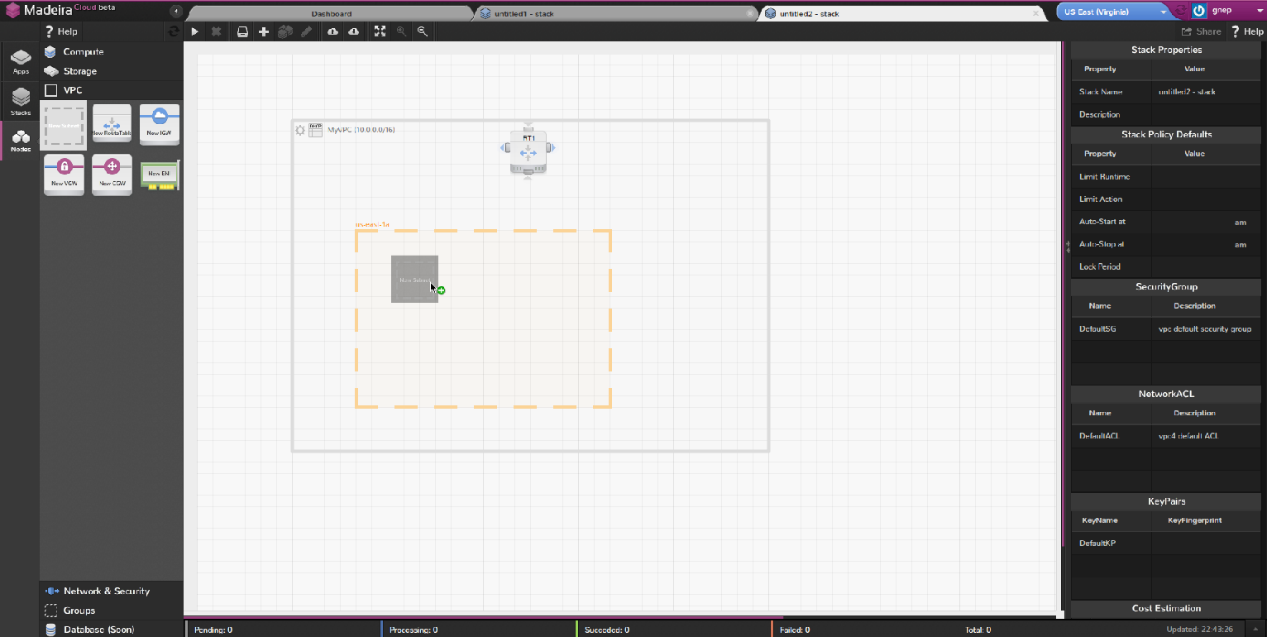


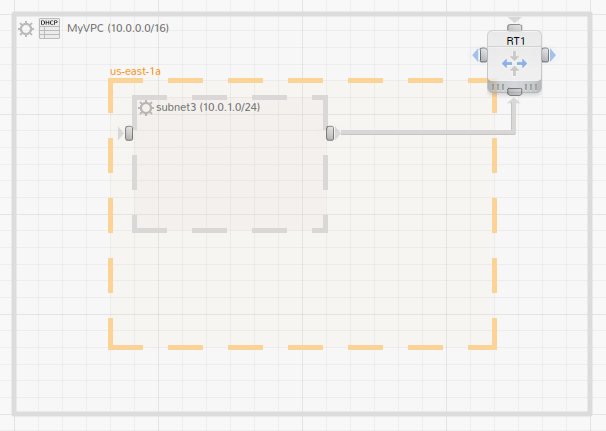


NOTE: make sure Availability Zone is completely located inside of the VPC

1. Add a new subnet

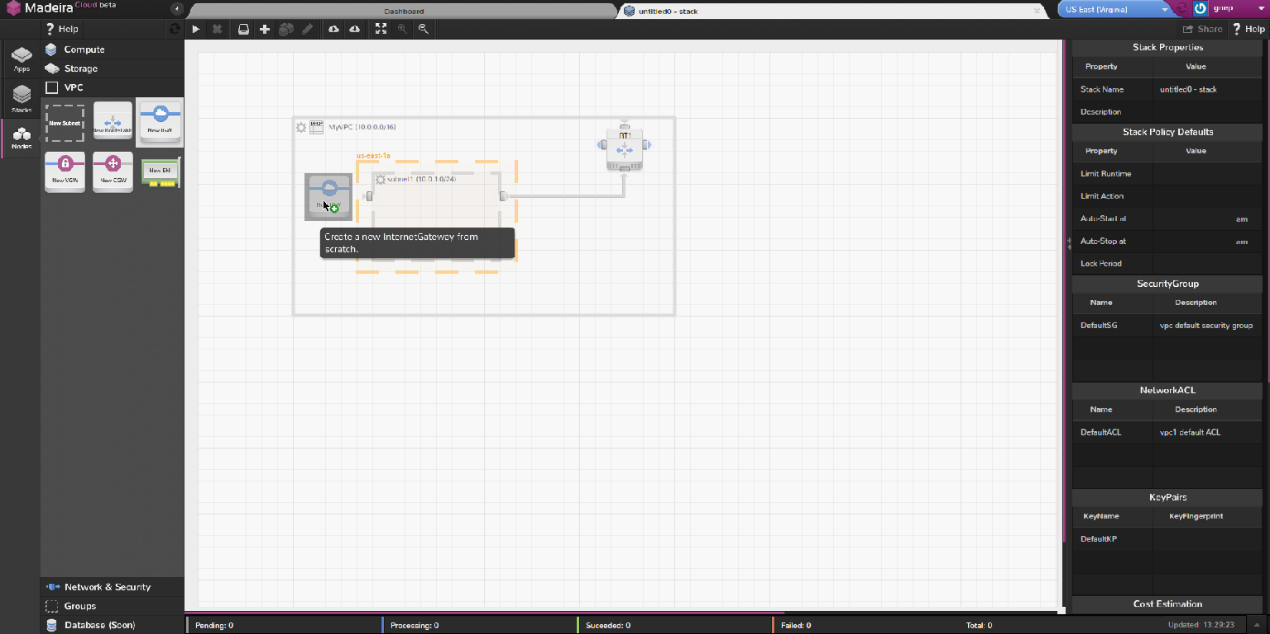
NOTE: Subnet must be placed inside of Availability Zone



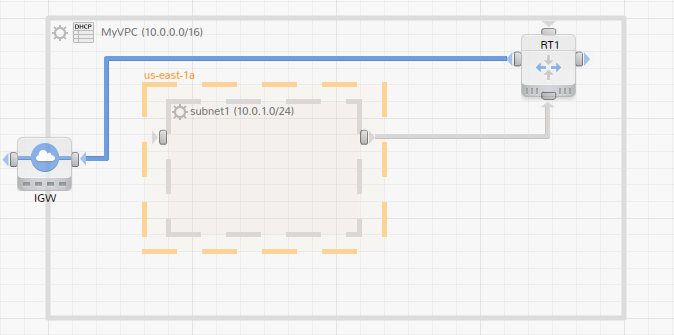


By default, subnet will be associated with the main route table. You can add/remove route table and re-associate subnets.

1. Add a new Internet Gateway and connect main Route Table with it

After dropping the icon in the VPC, Internet Gateway will be auto-placed at the VPC’s left rim. 

NOTE: One Internet Gateway per VPC at max.

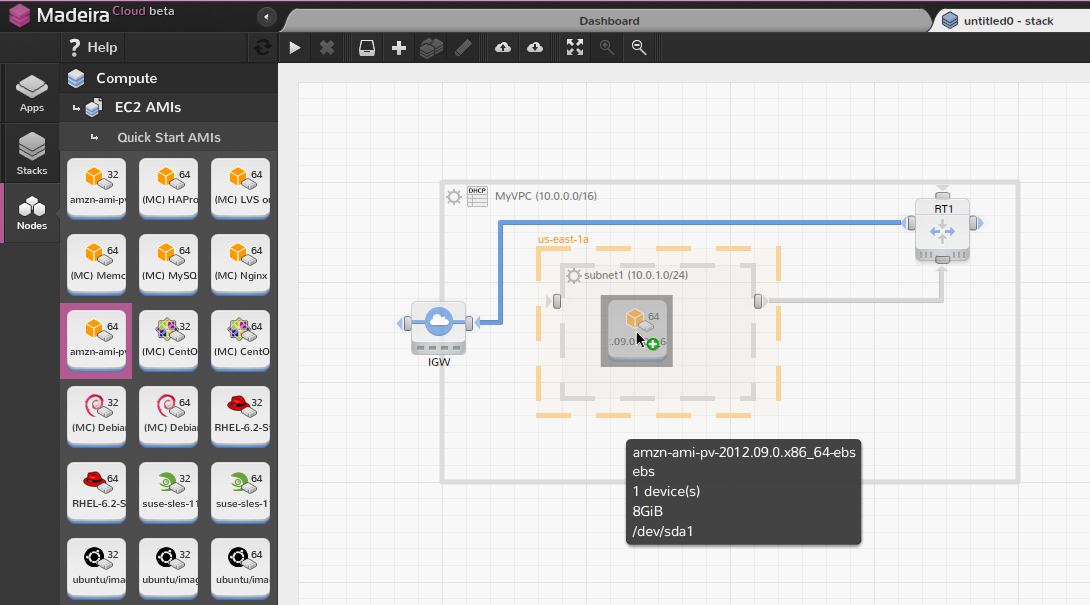


Done!

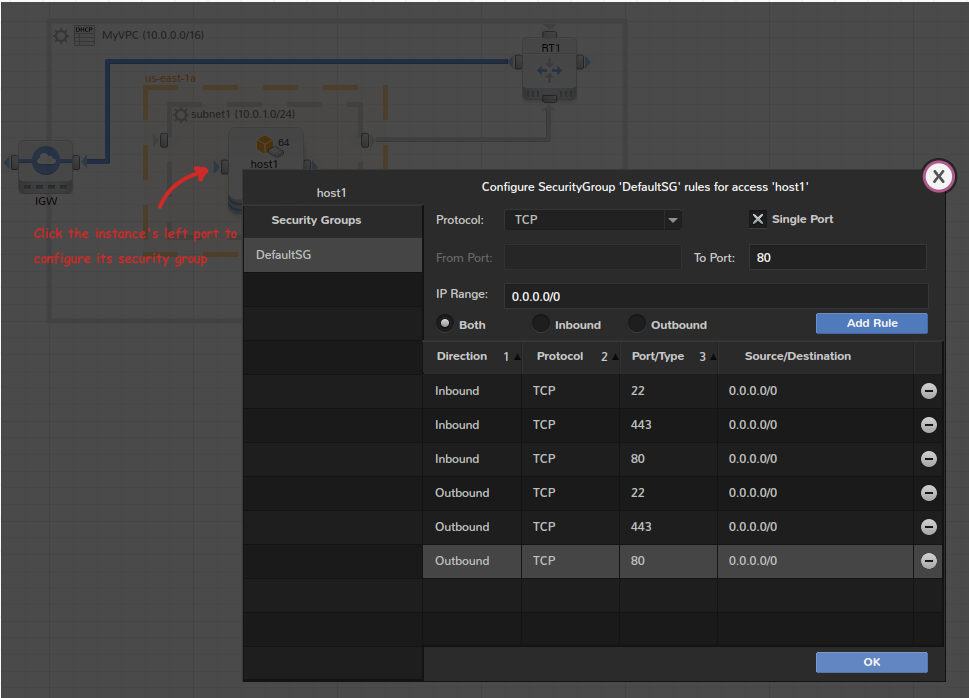
Now you can save the stack as a network template.

(Optional) Add a new Instance and setup the configuration

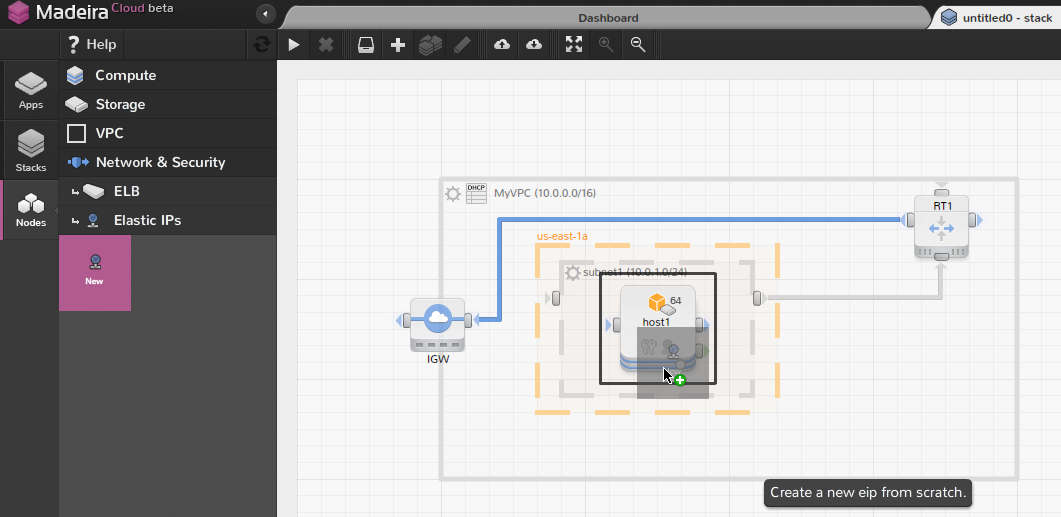
NOTE: Instance must be placed inside of subnet (in VPC).



Configure Security Group



Allocate a new Elastic IP to the instance



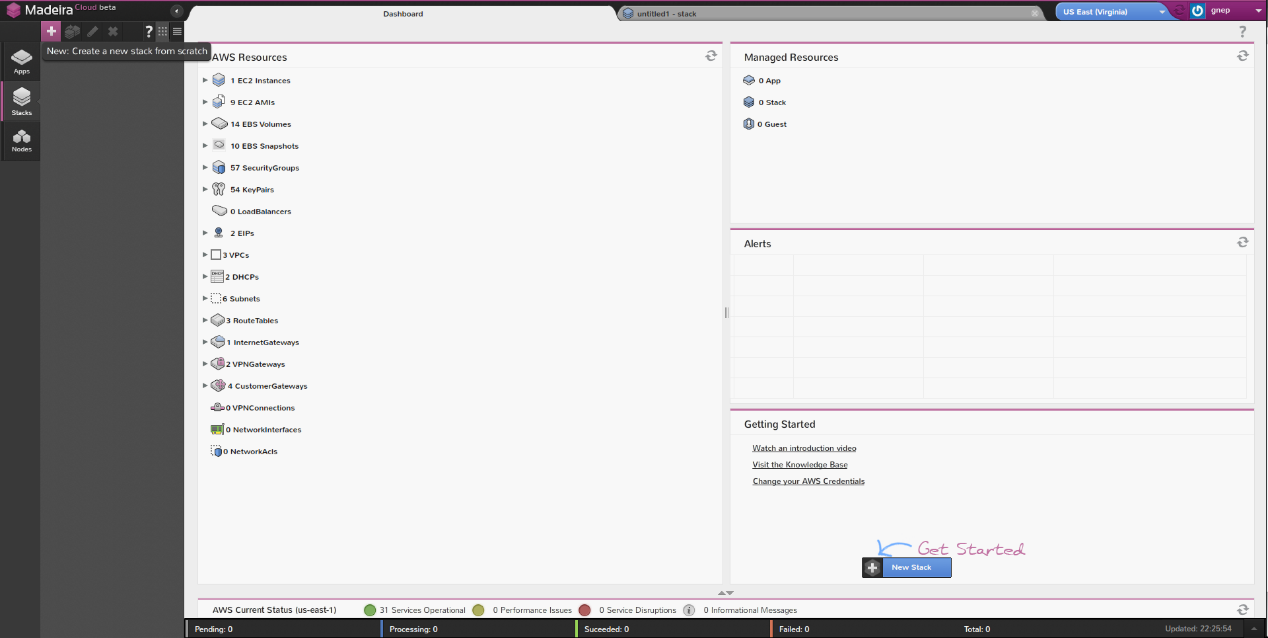
Now you can launch the stack into a real environment (App).

1.2 [VPC with Public and Private Subnets](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario2.html)

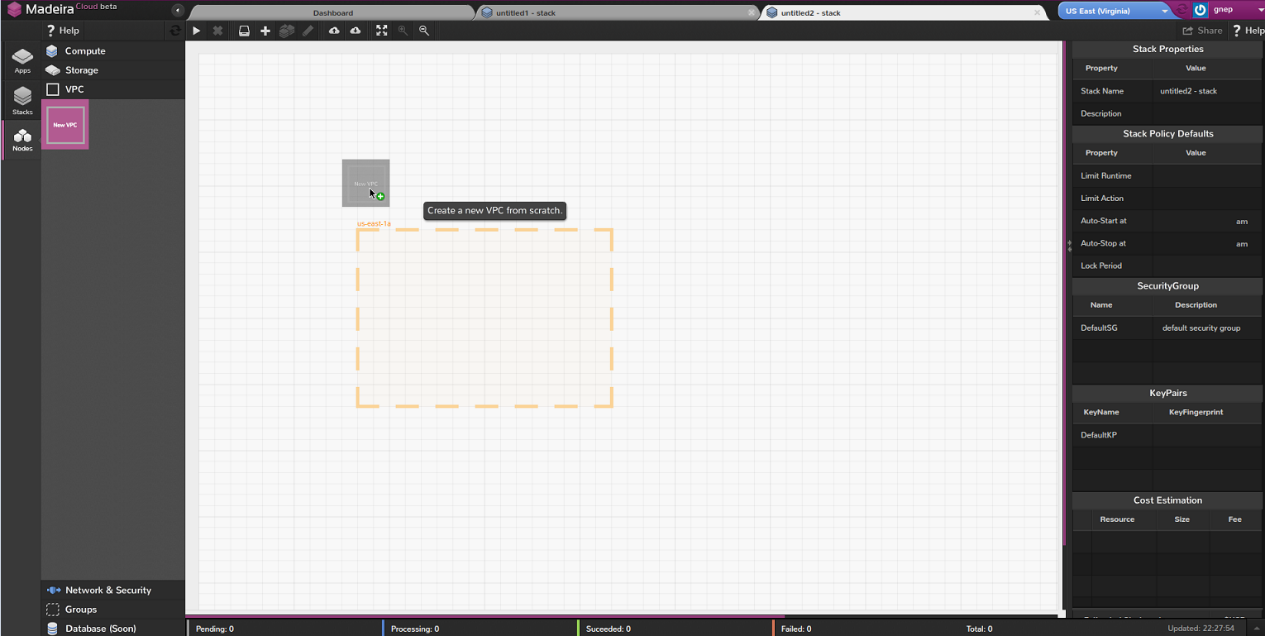
**Description**: “The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet. The instances in the public subnet can receive inbound traffic directly from the Internet, whereas the instances in the private subnet can't. The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can't. Instead, the instances in the private subnet can access the Internet by using a network address translation (NAT) instance that you launch into the public subnet.”

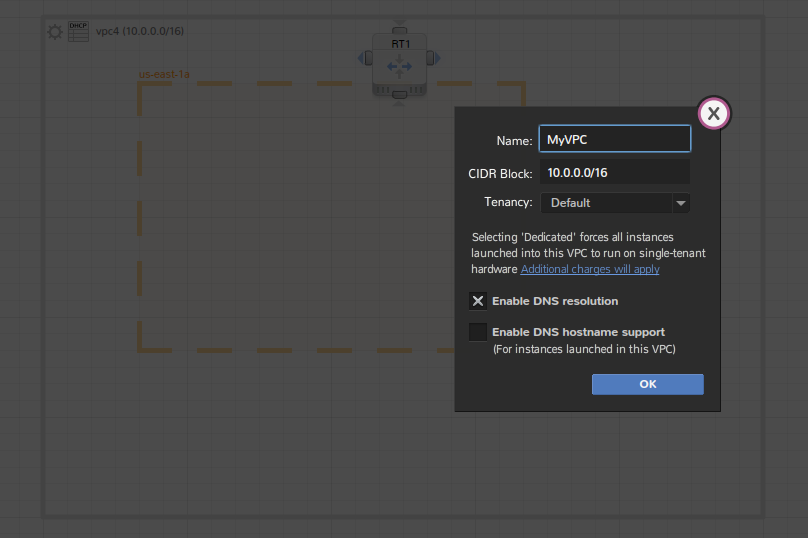
**Step by step:**

1. Create a new stack



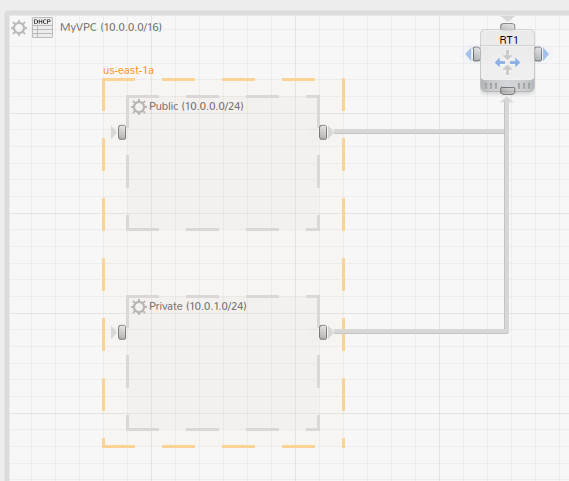
2. Setup VPC



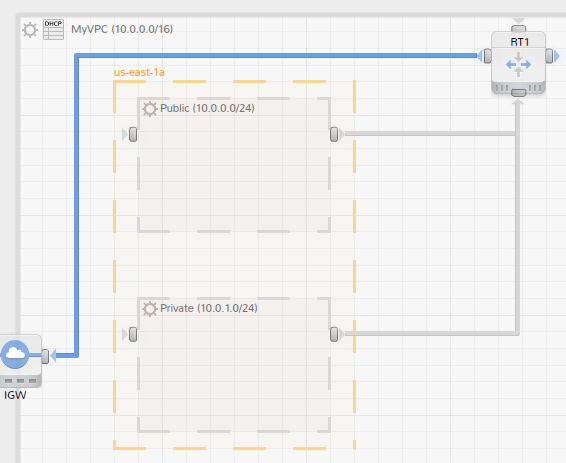


3. Add and configure two new subnets

|  |  |
| --- | --- |
|  | CIDR IP |
| Public Subnet | 10.0.0.0/24 |
| Private Subnet | 10.0.1.0/24 |

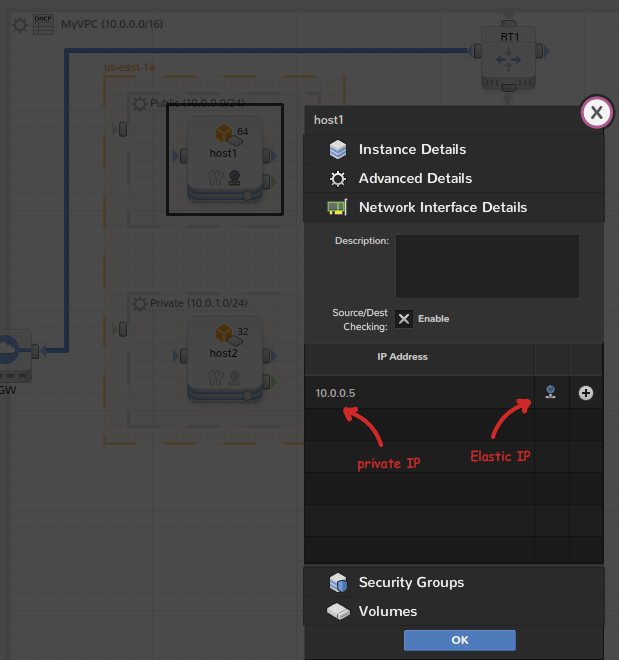


1. Add Internet Gateway

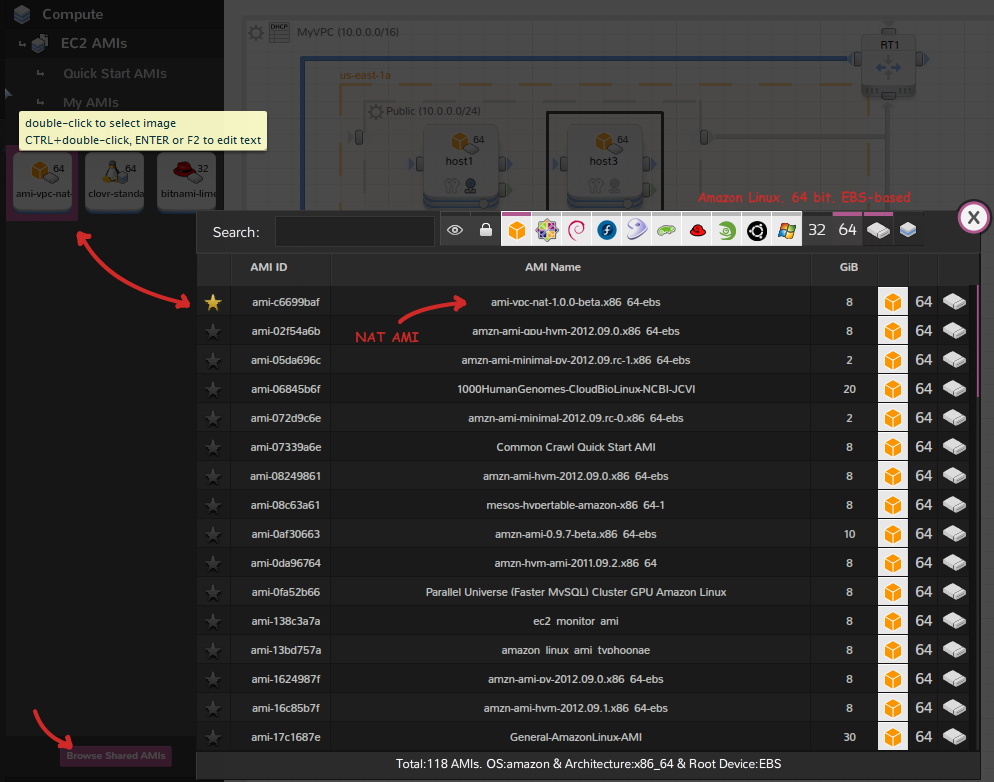


5. Add and configure instances

|  |  |  |  |
| --- | --- | --- | --- |
|  | Private IP | Elastic IP | Subnet |
| host1 | 10.0.0.5 | Yes | Public |
| host2 | 10.0.1.5 | No | Private |
| host3 (NAT) | Any | Yes | Public |

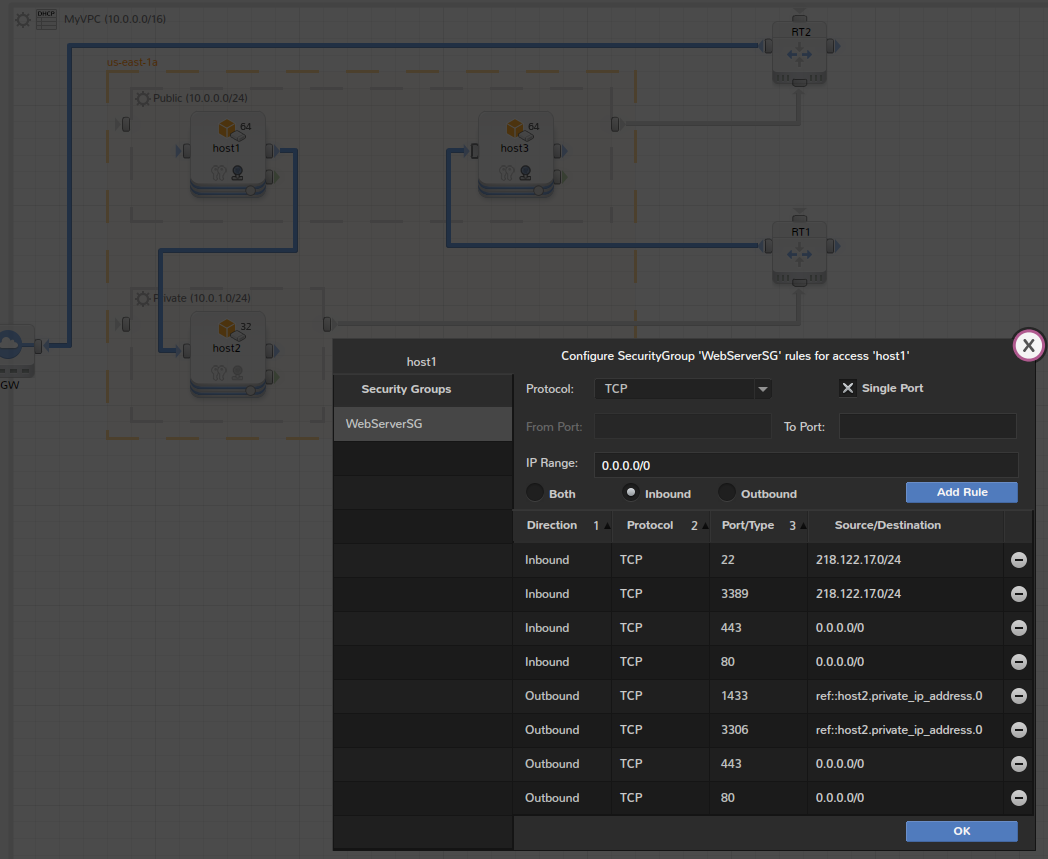


NOTE: When you enable Elastic IP in the instance configuration window, we will allocate a new Elastic IP automatically upon launching. There is no way to specify the Elastic IP address explicitly, because that will make the stack non-reusable.



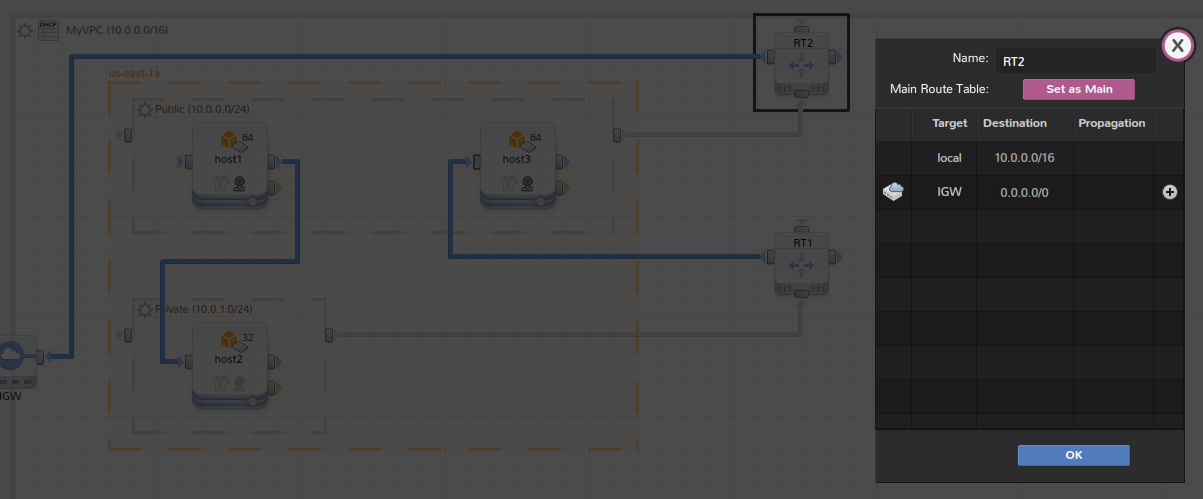
And configure the security groups:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Instance | Security Group Rules | | | |
| In/Out | Source | Protocol | Port Range |
| WebServerSG | host1 | In | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |
| Your network’s public IP address range | TCP | 22 |
| Your network’s public IP address range | TCP | 3389 |
| Out | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |
| host2.private\_ip\_address | TCP | 1433 |
| host2.private\_ip\_address | TCP | 3306 |
| DBServerSG | host2 | In | host1.private\_ip\_address | TCP | 1433 |
| host1.private\_ip\_address | TCP | 3306 |
| Out | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |
| NATSG | host3 | In | 10.0.1.0/24 | TCP | 80 |
| 10.0.1.0/24 | TCP | 443 |
| Your network’s public IP address range | TCP | 22 |
| Out | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |



1. Configure route tables

|  |  |  |  |
| --- | --- | --- | --- |
|  | Routing Rules (Target, Destination) | | Associated Subnet |
| RT1 | local | 10.0.0.0/16 | Private |
| host3 | 0.0.0.0/0 |
| RT2 | local | 10.0.0.0/16 | Public |
| Internet Gateway | 0.0.0.0/0 |



Done!

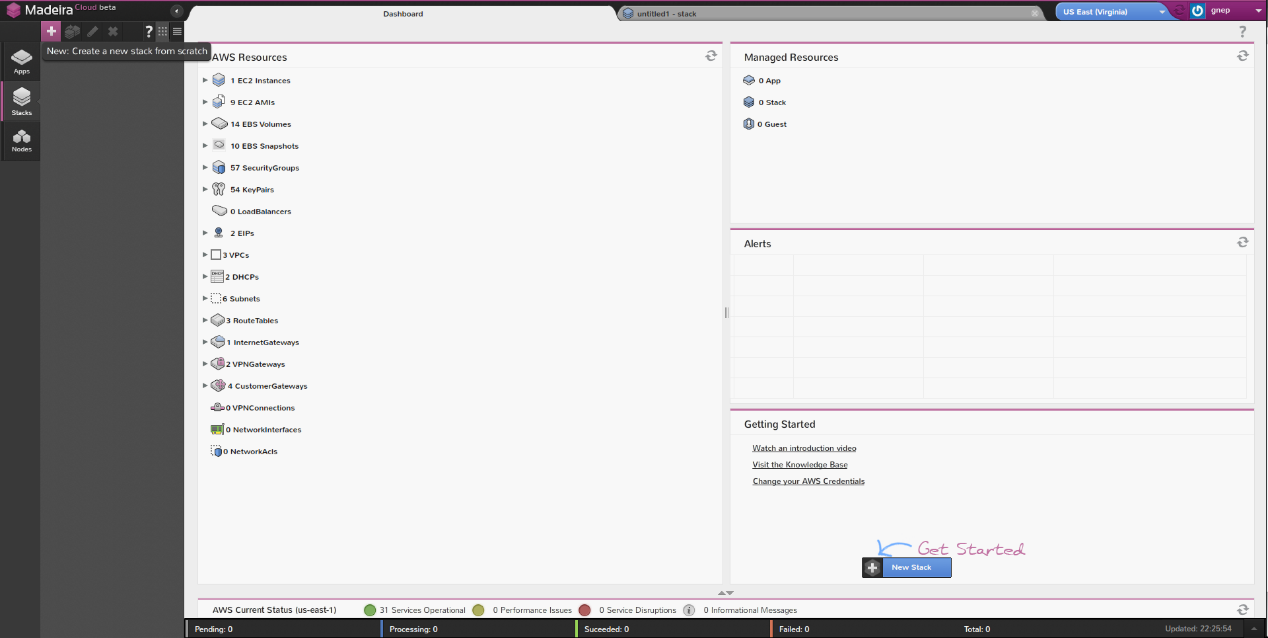
Now you can save the stack and launch it into a real environment (App).

# 1.3 [VPC with Public and Private Subnets and Hardware VPN Access](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario3.html)

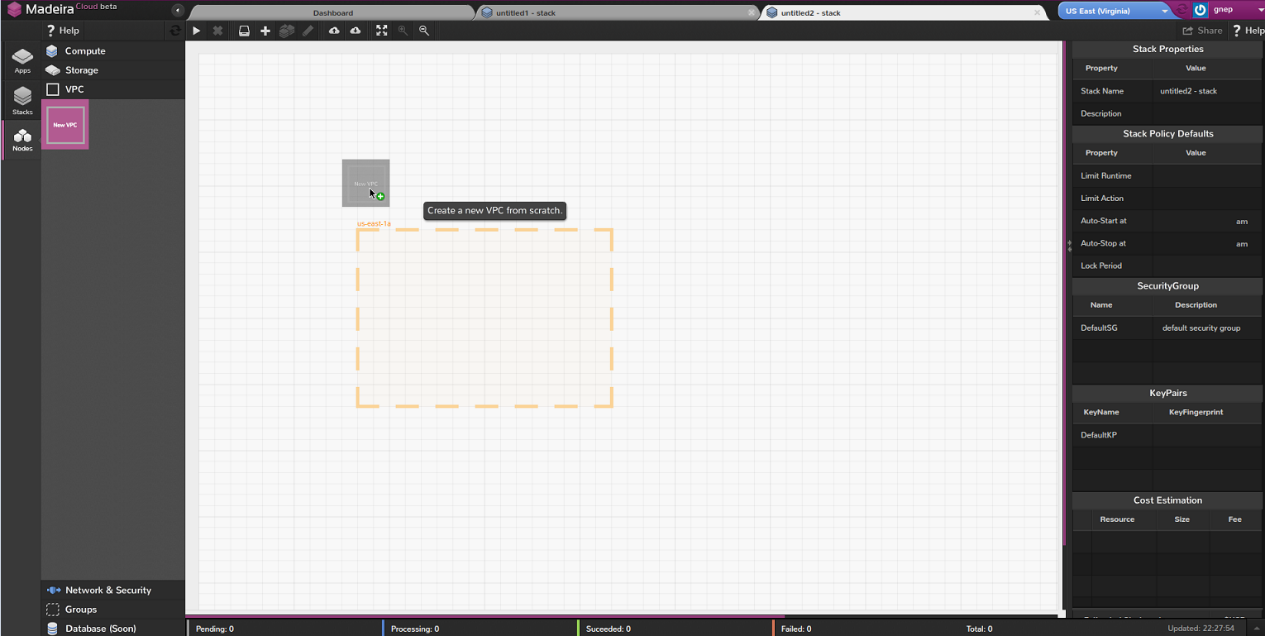
**Description**: “The configuration for this scenario includes a virtual private cloud (VPC) with a public subnet and a private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel. We recommend this scenario if you want to extend your network into the cloud and also directly access the Internet from your VPC. This scenario enables you to run a multi-tiered application with a scalable web front end in a public subnet, and to house your data in a private subnet that is connected to your network by an IPsec VPN connection.”

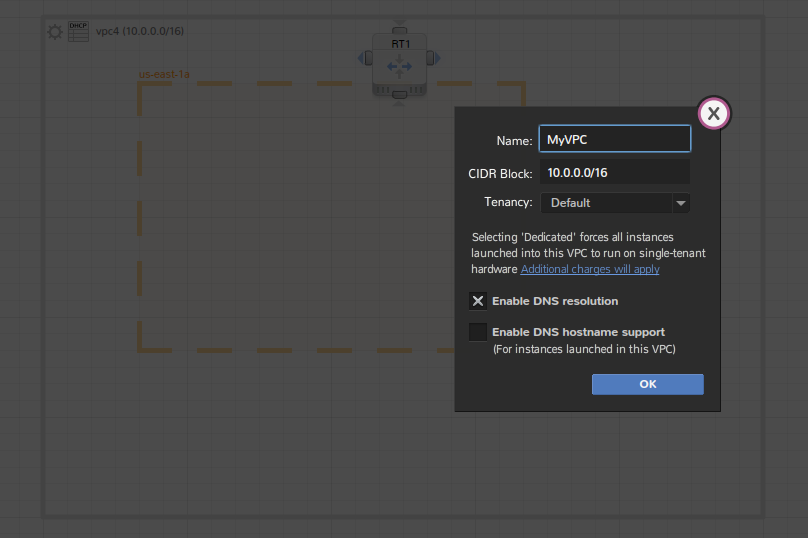
**Step by step:**

1. Create a new stack



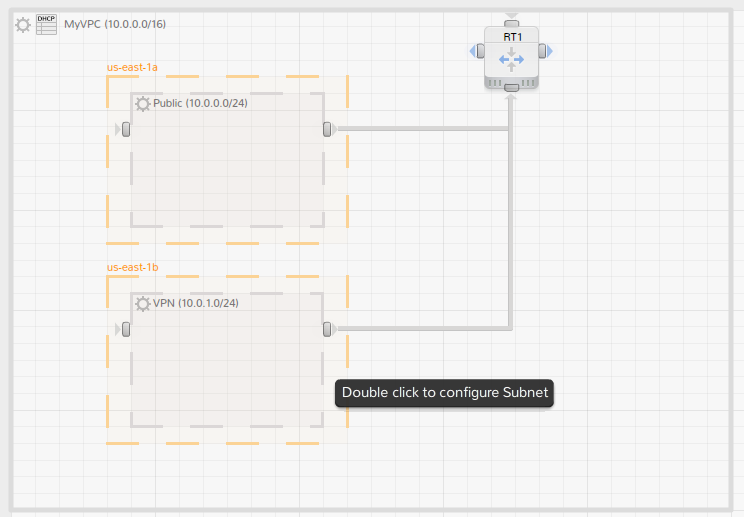
2. Setup VPC



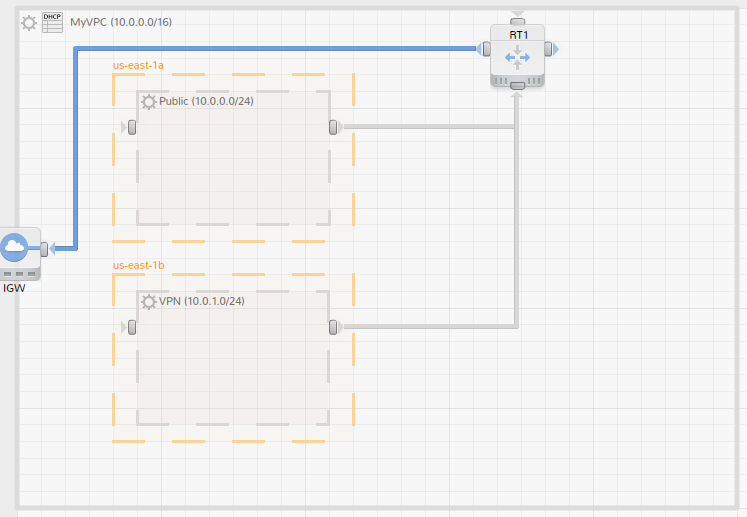


3. Add and configure two new subnets

|  |  |  |
| --- | --- | --- |
|  | CIDR IP | Zone |
| Public Subnet | 10.0.0.0/24 | us-east-1a |
| VPN-only Subnet | 10.0.1.0/24 | us-east-1b |

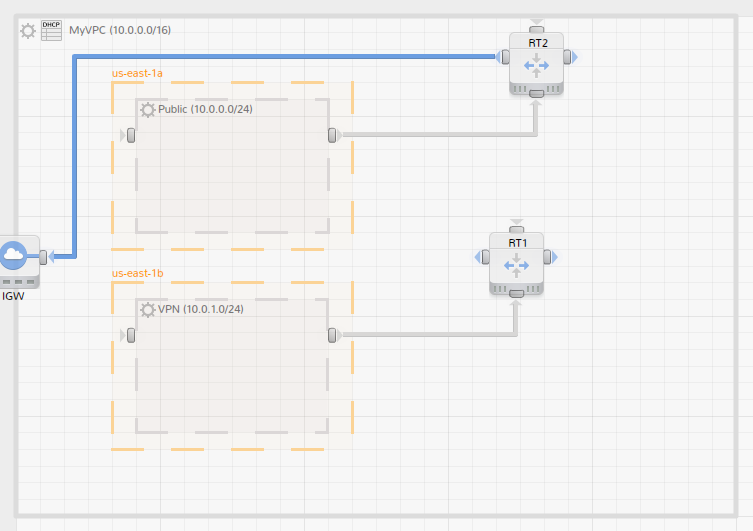


1. Add Internet Gateway



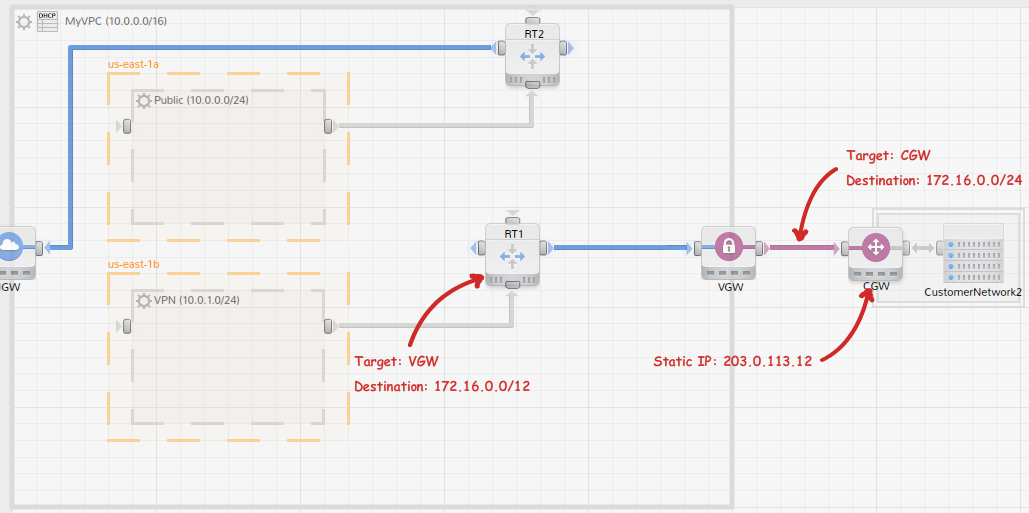
5. Add and configure route tables

|  |  |  |  |
| --- | --- | --- | --- |
|  | Routing Rules (Target, Destination) | | Associated Subnet |
| RT1 | local | 10.0.0.0/16 | VPN |
| RT2 | local | 10.0.0.0/16 | Public |
| Internet Gateway | 0.0.0.0/0 |



6. Add VPN connection to your private network

|  |  |
| --- | --- |
| RT1 | Target: VGW Destination: 172.16.0.0/12 |
| VPN | 172.16.0.0/24 |
| CGW IP | 203.0.113.12 |

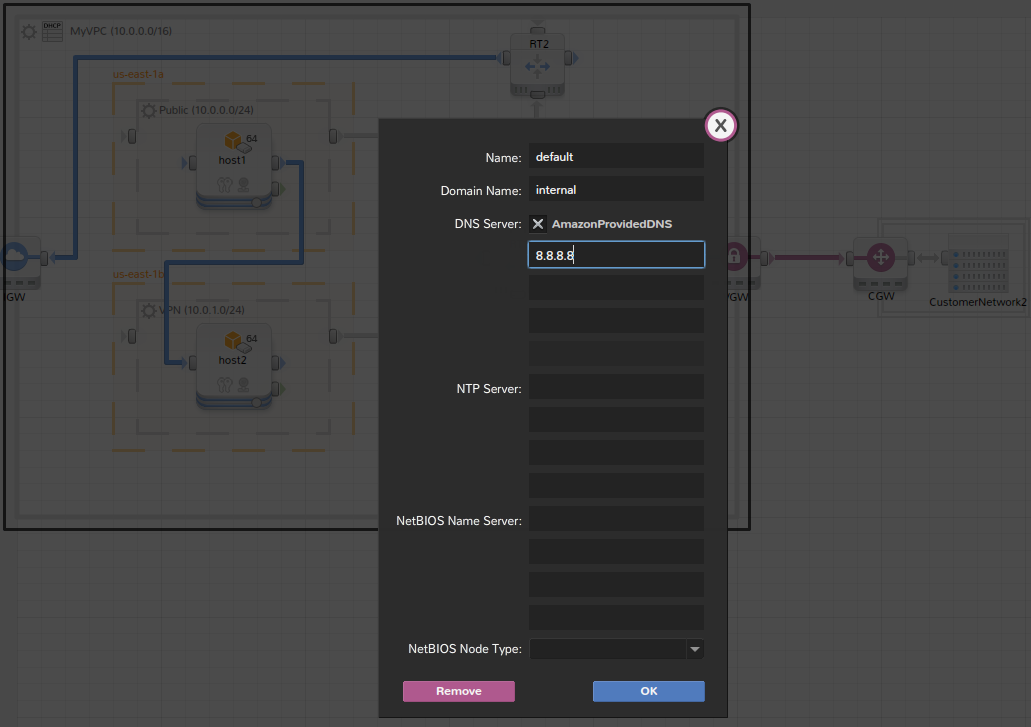


Done!

Now you can save the stack as a VPC template.

7. (Optional) Add instances and configure security groups, DHCP:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Security Group Rules | | | |
| In/Out | Source | Protocol | Port Range |
| WebServerSG | In | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |
| Your network’s public IP address range | TCP | 22 |
| Your network’s public IP address range | TCP | 3389 |
| Out | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |
| host2.private\_ip\_address | TCP | 1433 |
| host2.private\_ip\_address | TCP | 3306 |
| DBServerSG | In | host1.private\_ip\_address | TCP | 1433 |
| host1.private\_ip\_address | TCP | 3306 |
| 172.16.0.0/24 | TCP | 22 |
| 172.16.0.0/24 | TCP | 3389 |
| Out | 0.0.0.0/0 | TCP | 80 |
| 0.0.0.0/0 | TCP | 443 |

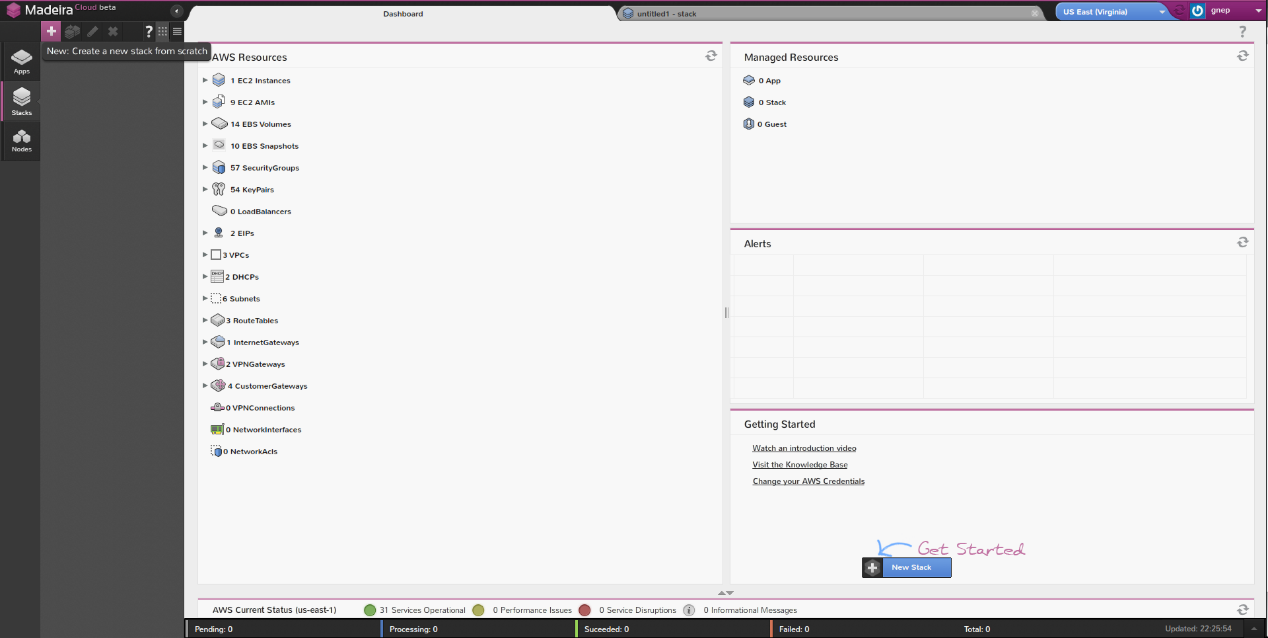


1.4 [VPC with a Private Subnet Only and Hardware VPN Access](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Scenario4.html)

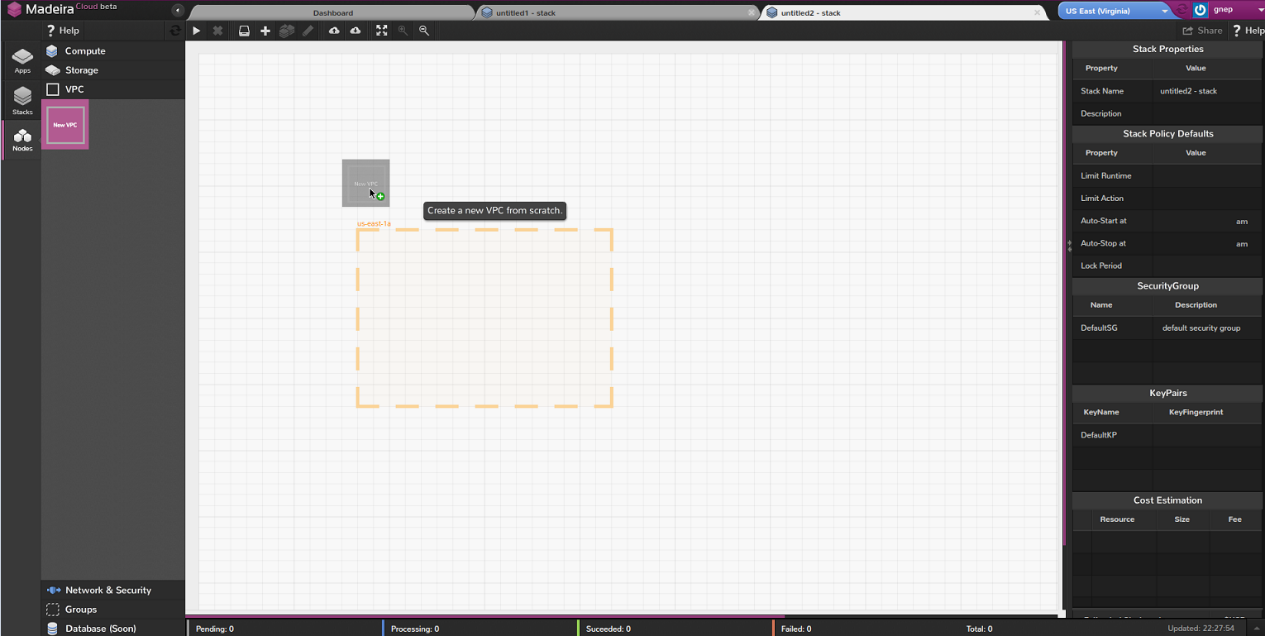
**Description**: “The configuration for this scenario includes a virtual private cloud (VPC) with a single private subnet, and a virtual private gateway to enable communication with your own network over an IPsec VPN tunnel. There is no Internet gateway to enable communication over the Internet. We recommend this scenario if you want to extend your network into the cloud using Amazon's infrastructure without exposing your network to the Internet.”

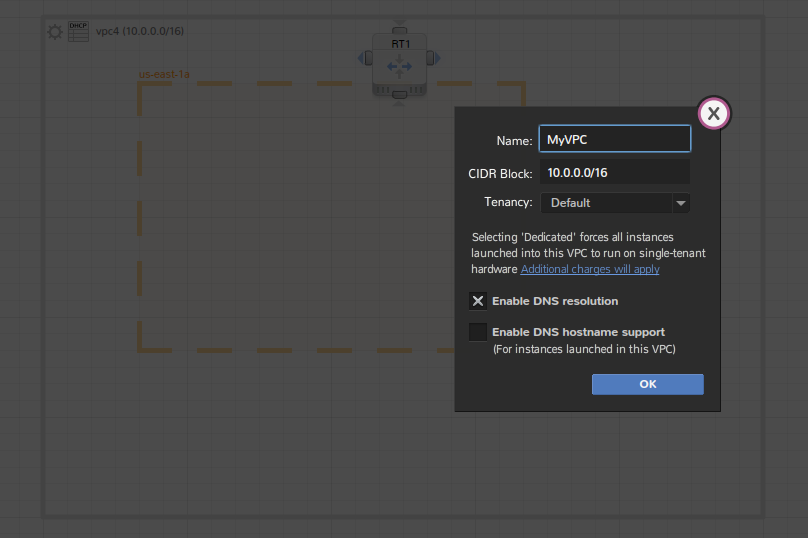
**Step by step:**

1. Create a new stack



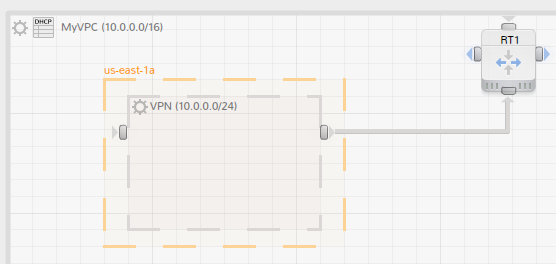
2. Setup VPC





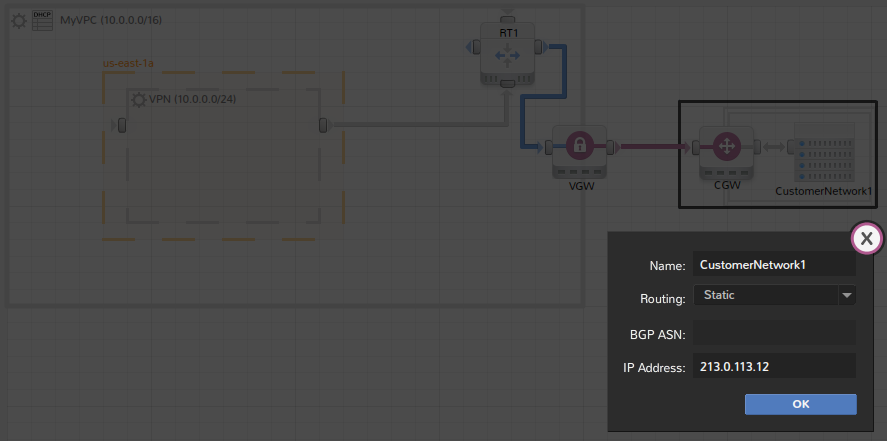
3. Add and configure subnet

|  |  |
| --- | --- |
|  | CIDR IP |
| VPN-only Subnet | 10.0.0.0/24 |



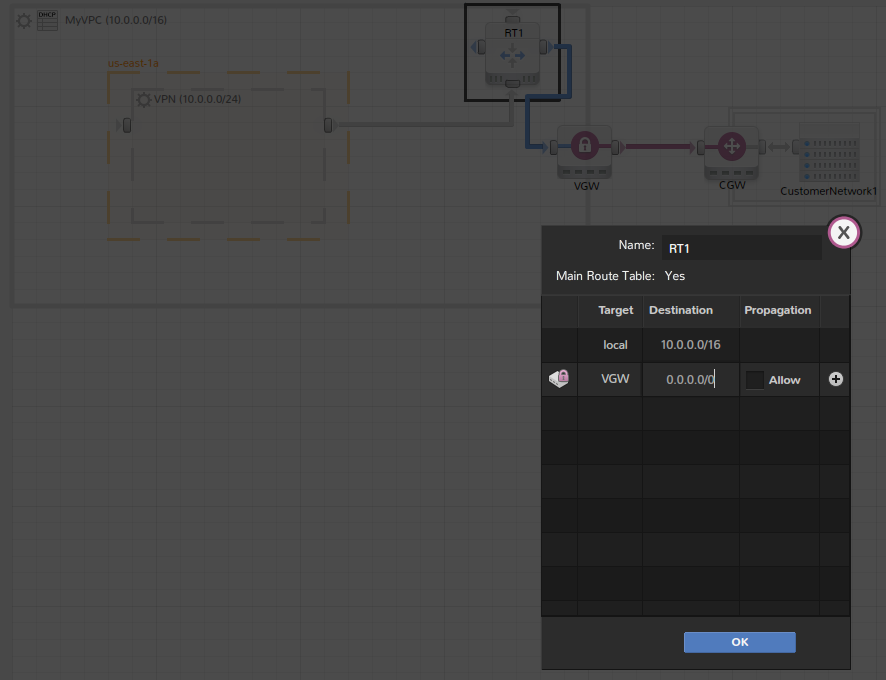
4. Add and configure VPN connection to your private network

|  |  |
| --- | --- |
| RT1 | Target: VGW Destination: 172.16.0.0/12 |
| VPN | 172.16.0.0/24 |
| CGW IP | 203.0.113.12 |



5. Configure route tables

|  |  |  |  |
| --- | --- | --- | --- |
|  | Routing Rules (Target, Destination) | | Associated Subnet |
| RT1 | local | 10.0.0.0/16 | VPN |
| Internet Gateway | 0.0.0.0/0 |



Done!

Now you can save the stack as a VPC template.

1. (Optional) Add instances and configure security groups:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| DefaultSG | Security Group Rules | | | |
| In/Out | Source | Protocol | Port Range |
| In | Your network’s public IP address range | TCP | 22 |
| Your network’s public IP address range | TCP | 3389 |
| Out | 0.0.0.0/0 | ALL | ALL |

