VMWARE NSX TECH NOTE

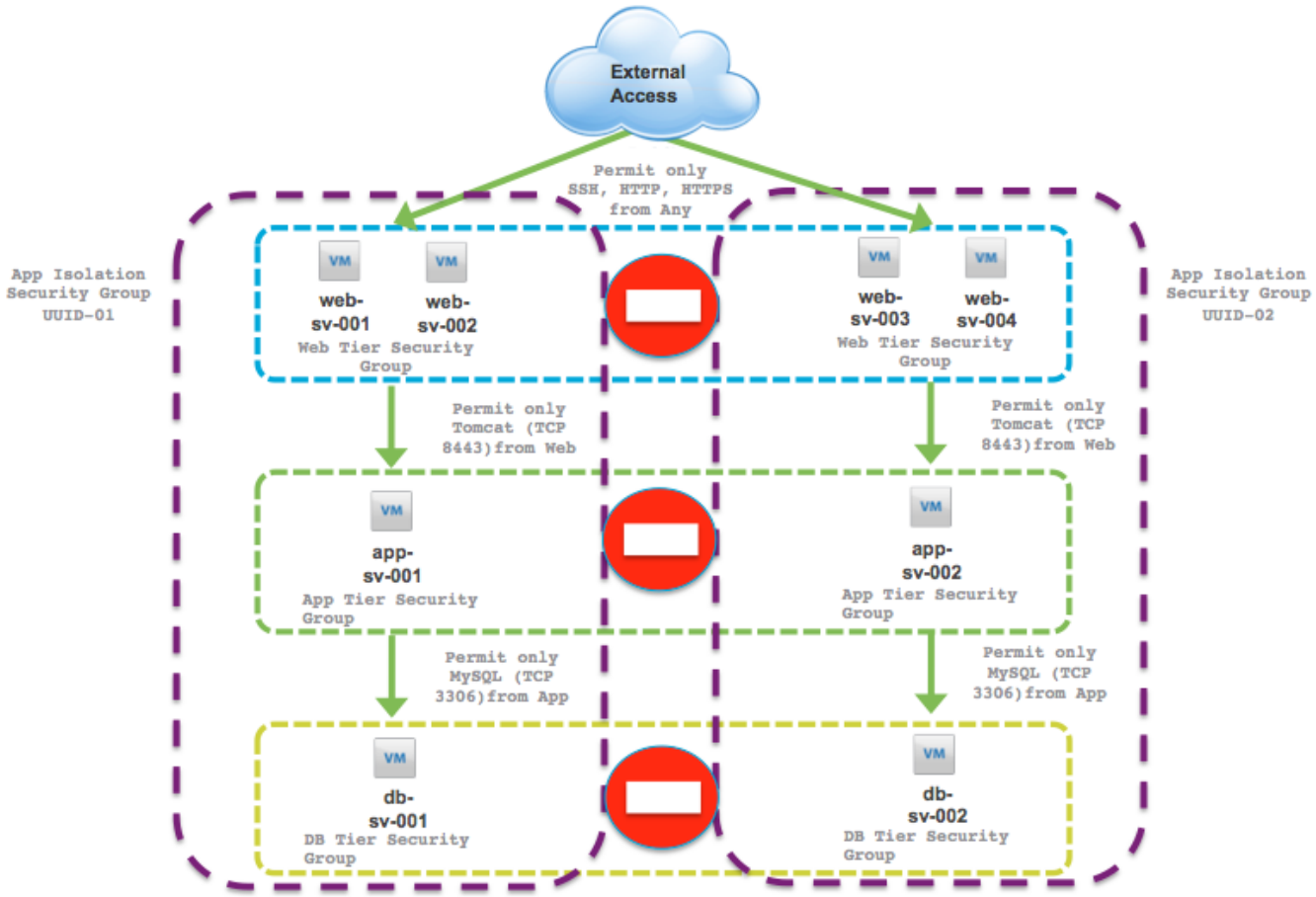
vRealize Automation and NSX Micro-Segmentation

Background

This guide explains how to configure a granular security policy leveraging NSX Micro-Segmentation for multi-tier workloads deployed via vRealize Automation, utilizing the integration of these two VMware products. The security policy provides the following controls:

- External access only to permitted services to a selected tier
- Ability to restrict VM to VM communication within a tier
- Controlled communication path limited to specific ports and protocols between tiers
- Restrict access between different application instances

Our example multi-tier application scenario is described below, where the green arrows highlight permitted traffic and all other traffic is blocked.



ENABLEMENT

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vRealize Automation and NSX Micro-Segmentation

Requirements

- NSX vSphere 6.1.x or later
- vRealize Automation 6.2.x or later
- NSX vRealize Orchestrator Plugin (supported vRO and plugin versions are linked to NSX and vRA releases)
- Configured vCenter Server, Orchestrator and NSX Endpoints within vRealize Orchestrator
- For NSX 6.1.x: Run the workflow included in the NSX vRO Plugin called '**Enable security policy support for overlapping subnets'**.
  NSX 6.2.x: Configure Service Composer to apply rules to Policy's SGs:

  This is a requirement for the NSX and vRA integration and ensures that Firewall Rules in Service Composer Security Policies are only applied to the vNICs of VMs that are members of the Security Group
- Refer to: http://www.vmware.com/resources/compatibility/sim/interop_matrix.php for additional compatibility information

Author

Ray Budavari, Senior Staff Technical Product Manager - NSX, VMware

Version

1.0 published 8/30/2016

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

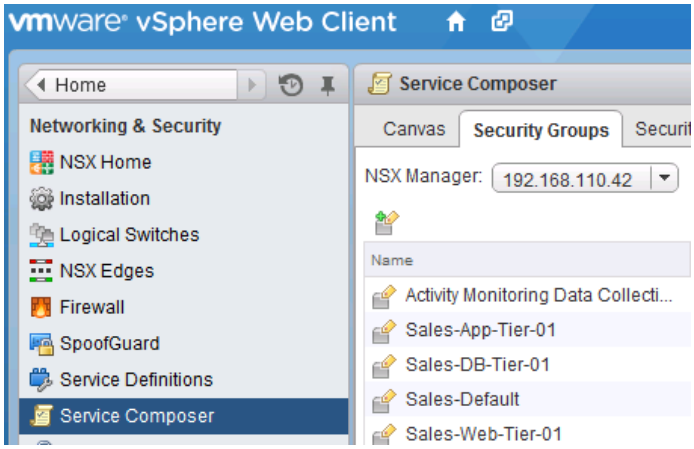
vRealize Automation and NSX Micro-Segmentation

Procedure

Define NSX Security Groups

Rather than using dynamically created Security Groups (which cannot be referenced within a Security Policy as they are created at the time of application deployment), this approach will use pre-created Security Groups and utilize the App Isolation Feature of the vRA and NSX integration.

As a first step, define Security Groups for the different tiers of your application. In our example we have three tiers, a Web Tier (**Sales-Web-Tier-01**), App Tier (**Sales-App-Tier-01**) and DB Tier (**Sales-DB-Tier-01**):



These three security groups are used for all instances of the multi-tier application deployed via vRA using the same blueprint.
In addition there is also a default security group (**Sales-Default**), which will be used to control access to shared services for all VMs.

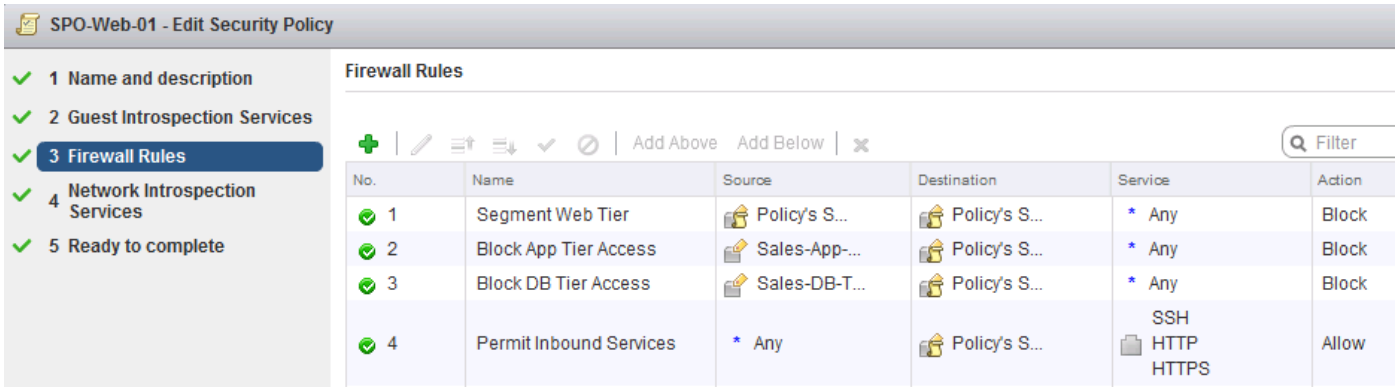
Define NSX Security Policies

Next we will define the NSX Security Policies that contain Distributed Firewall rules and are applied to the respective Security Groups created in the previous step.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

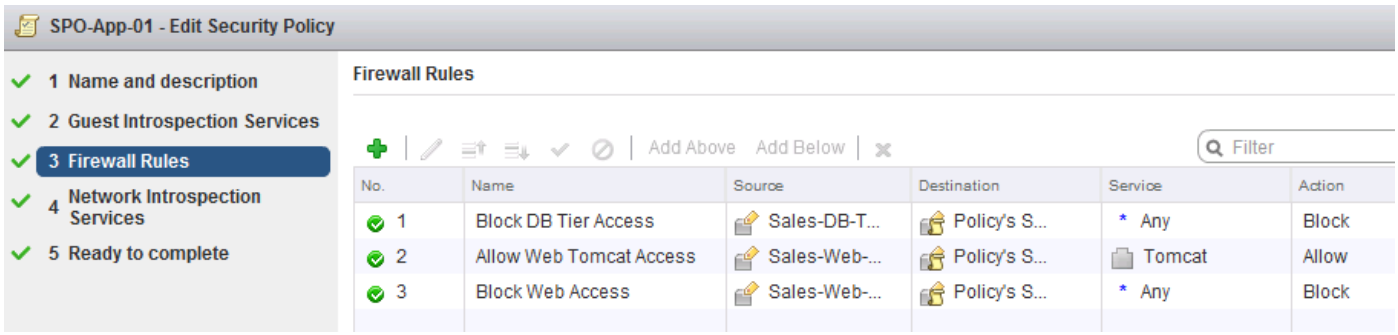
vRealize Automation and NSX Micro-Segmentation

Here is the **SPO-Web-01** Policy applied to the **Sales-Web-Tier-01** Security Group**:**



Firewall Rule 1 blocks any communication between Web VMs, Rule 2 blocks access from the Sales-App-Tier-01 VMs to Web VMs, Rule 3 blocks Sales-DB-Tier-01 Access and Rule 4 Permits selective Inbound Services from External Networks (any). This policy has a weight of **4300.**

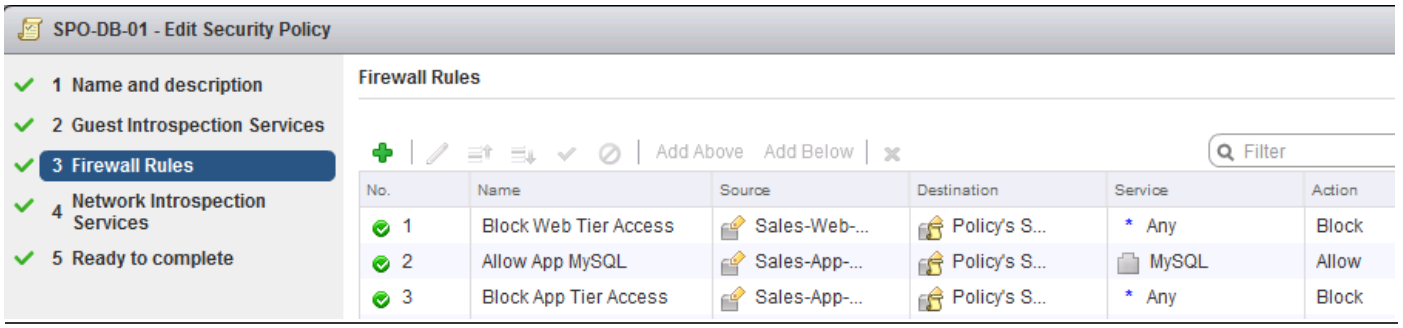
The **SPO-App-01** Policy applied to **Sales-App-Tier-01** SG:



FW Rule 1 blocks access from the Sales-DB-Tier-01 VMs to App VMs, Rule 2 permits only the Tomcat Service from Web VMs and Rule 3 blocks all other traffic from Web VMs. This policy has a weight of **4200.**

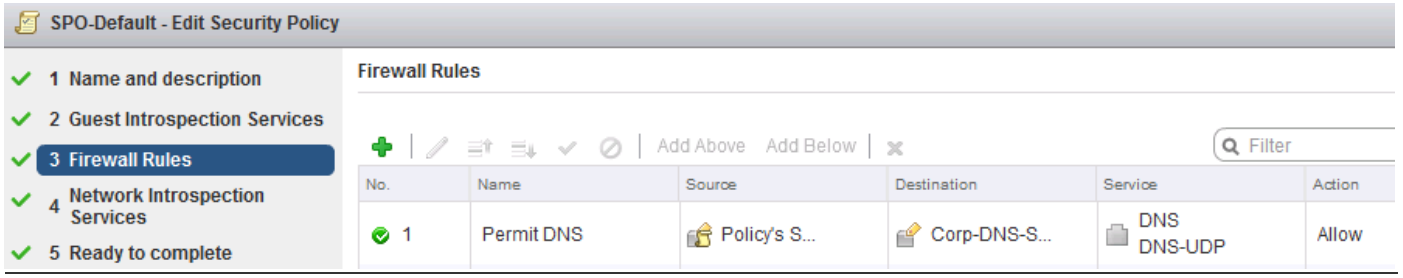
vRealize Automation and NSX Micro-Segmentation

And similarly the **SPO-DB-01** Policy applied to **Sales-DB-Tier-01** SG:

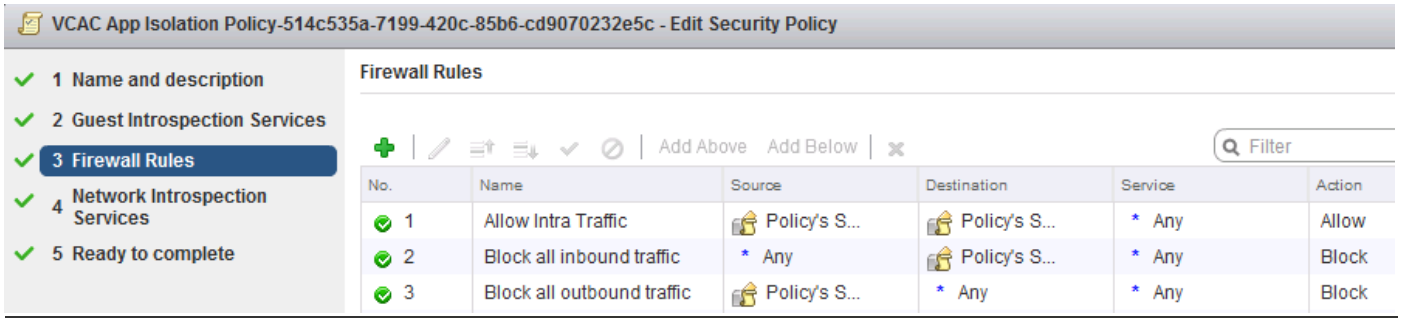


FW Rule 1 blocks direct access from the Sales-Web-Tier-01 VMs to DB VMs, Rule 2 permits only MySQL from App VMs and Rule 3 blocks all other traffic from the App VMs. This policy has a weight of **4100.** If there were multiple App & DB VMs per application that didn't need to communicate within their tiers you could also add a rule to segment within the App & DB Security Groups similar to Rule 1 on the Web Security Policy. In our example scenario this is only required for the Web Tier.

Access to shared services is provided by the **SPO-Default** Security Policy, which has a weight of **5000** and allows VMs to connect to approved DNS Servers (this can be extended as required, eg Directory Services, Monitoring, Patch Management etc):



Finally, when **App Isolation** is enabled on a vRealize Automation Blueprint, the following Security Policy is automatically created the first time a Multi-Machine Service is deployed, so no configuration is required:



vRealize Automation and NSX Micro-Segmentation

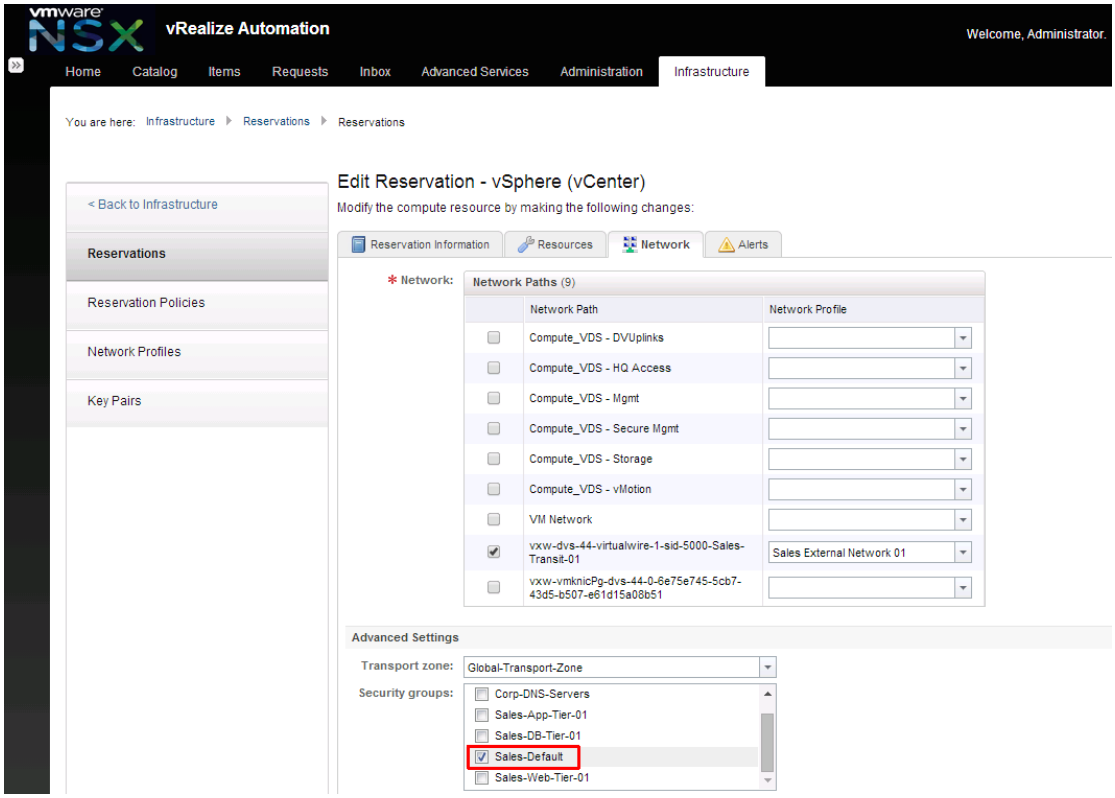
This App Isolation Security Policy is applied to a Dynamically Created Security Group, which contains all Component VMs in the Deployment provisioned by vRealize Automation. So each Deployment will have a dedicated App Isolation Security Group, which allows the Deployment to be used as a security container. As you can see the App Isolation Policy allows Intra Tier traffic between VMs in the same Deployment, but blocks all other inbound and outbound traffic outside of the Security Group. This provides isolation between Deployment instances deployed from the same Blueprint even though they are sharing common Security Groups for the Web, App and DB Tiers.

As the App Isolation Security Policy is created with a Weight of **3456** it has a lower precedence than the other Security Policies, so the Web, App and DB Policies will block any intra tier traffic that is not explicitly permitted by a firewall rule before we reach Rule 1 of the App Isolation policy which would otherwise permit it. There is no dependency on the DFW Default Rule and the enforcement covered in this document will work the same whether the default is set to Allow or Block.

These NSX Security Policies allow us to meet the requirement to provide a controlled communication path between tiers of our application where only traffic related to explicitly allowed ports and protocols is permitted.

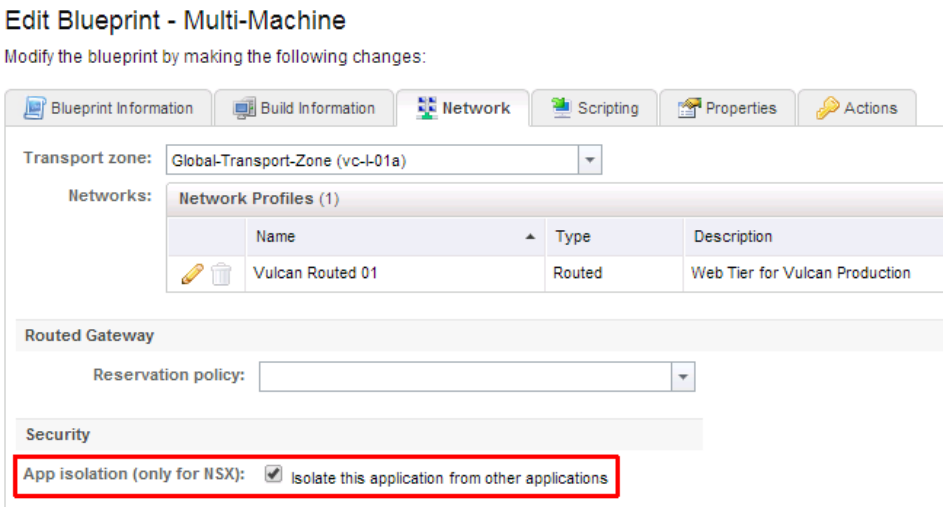
Configure vRA Blueprints

Now we will apply the appropriate configuration within vRealize Automation. First at the Reservation level we will select the **Sales-Default** Security Group, which ensures all VMs deployed within this Reservation will be added to this SG:



vRealize Automation and NSX Micro-Segmentation

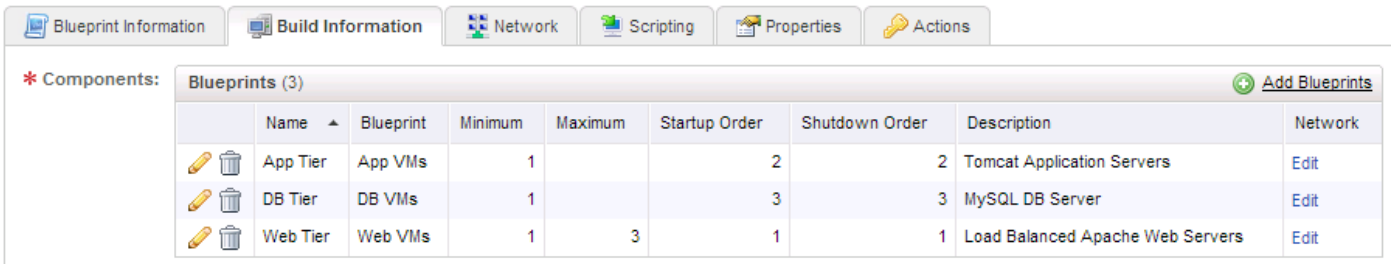
Next in our example 3-tier Blueprint, on the **Network** tab ensure the Checkbox for **App isolation** is checked:



In this example I have defined a single Routed Network Profile in the Blueprint, which means that one VXLAN Logical Switch will be created dynamically for each Deployment instance deployed from this blueprint connected to an NSX Distributed Logical Router.

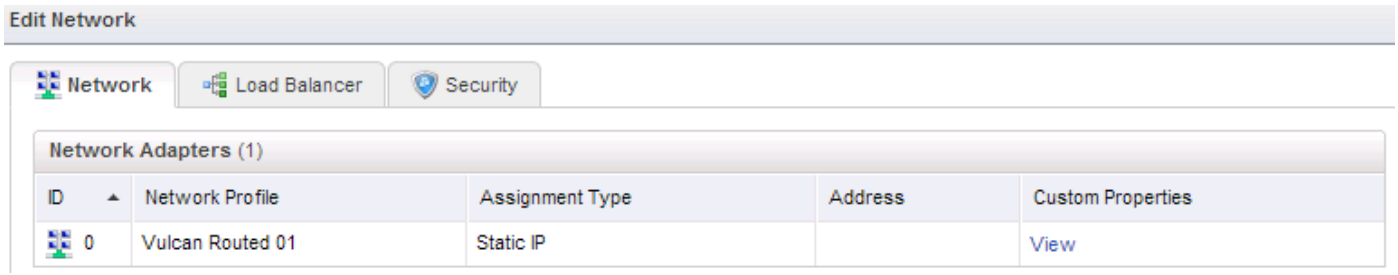
This highlights one of the important benefits of a policy-based security model provided by NSX compared to an infrastructure-based approach. Which is that exactly the same policy will apply independent of the underlying network topology. So here I could also choose to have each tier of the application on its own Routed Network, or instead of dynamically created networks use existing External Networks (so a common network is shared across multiple application instances), with no change to the previously defined NSX Security Groups and Policies.

Then on the Build Information tab we can see there are 3 Components within this Blueprint, one for each tier of the application:

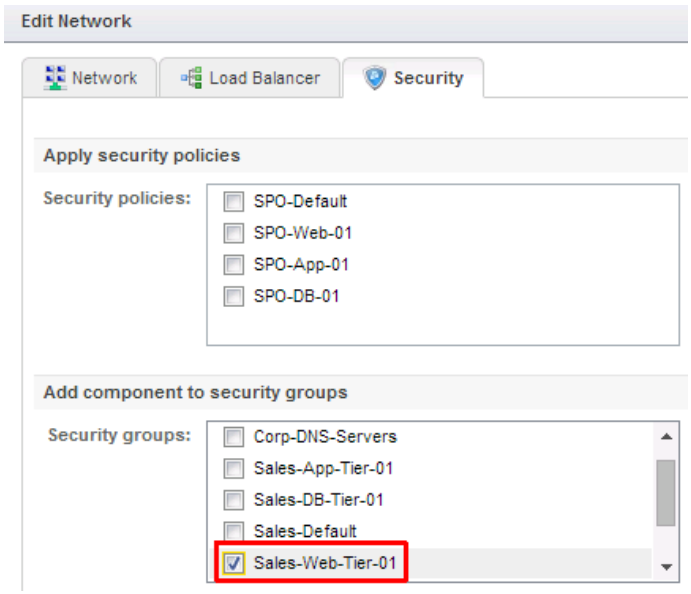


vRealize Automation and NSX Micro-Segmentation

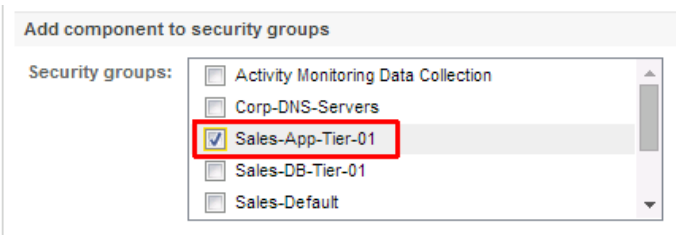
In our scenario all of the Components Virtual Machines from the App, Web and DB Tiers connected to the same Routed Network Profile:



On the **Security** tab, Web Component VMs are added to the **Sales-Web-Tier-01** Security Group:



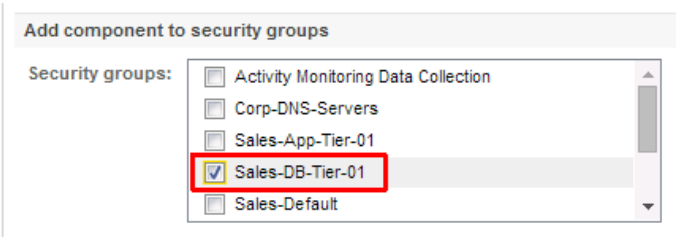
While for App Component VMs select the **Sales-App-Tier-01** Security Group:



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vRealize Automation and NSX Micro-Segmentation

And finally DB VMs will use the respective **Sales-DB-Tier-01** Security Group:



Now when you deploy an instance of this Blueprint from the Catalog, the vRealize Automation and NSX integration will ensure all networking & security configurations are applied at deployment time along with the application virtual machines. VMware NSX is a platform build for automation, as all operations can be performed through the northbound REST API available on NSX Manager.

NSX Distributed Firewall Rules

To fully understand how Micro-Segmentation is enabled by this configuration it is important to consider the point of enforcement with the NSX Distributed Firewall and the direction in which each rule is applied. The Firewall rule that permits inter tier traffic (using Web to App on 8443 as an example) is enforced on ingress to the vNIC of the App Servers, while the Firewall Rule in the App Isolation policy that blocks traffic is applied on egress of the vNIC of a Web server in a different Deployment instance.

From the Distributed Firewall Rule table, you can see that all other Security Policies are applied before the App Isolation policy. And any allowed traffic is only within the same Dynamically Created Security Group, while blocked traffic applies across all App Isolation Security Groups. So in the example below we have two instances of the same Blueprint deployed, resulting in two App Isolation Security Groups with a suffix that matches the Deployment UUID (**SG-0d64731d-13a4-4817-a15c-42f61109e8c4** and **SG-c07b5064-d07d-4af5-9ff7-6aaebb9c200e**):

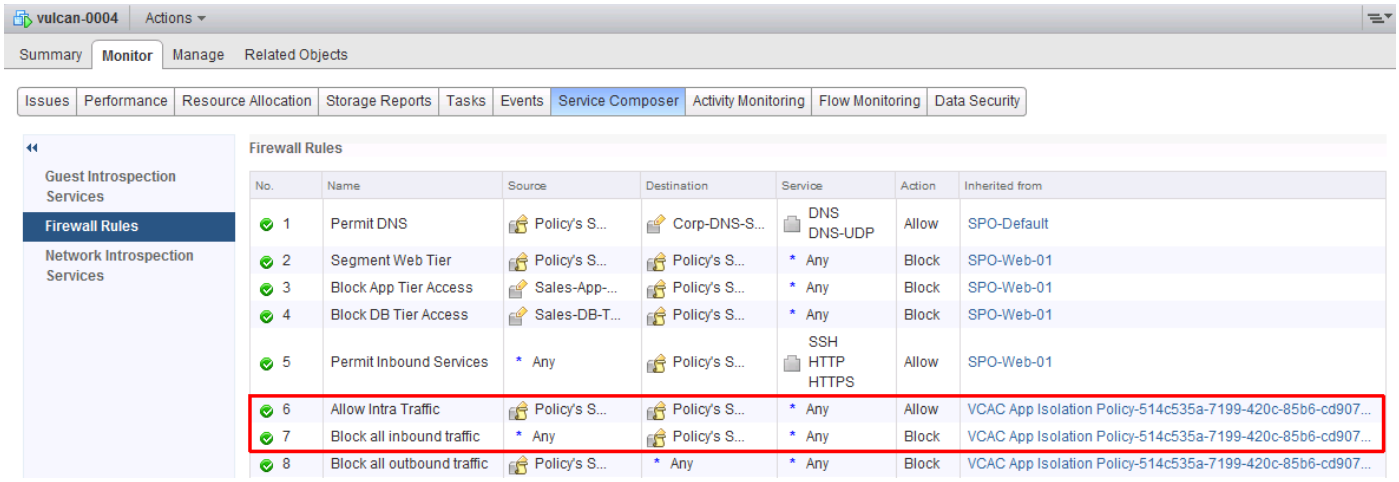
▶ SPO-Default :: NSX Service Composer - Firewall (Rule 1)					
▶ SPO-Web-01 :: NSX Service Composer - Firewall (Rule 2 - 5)					
▶ SPO-App-01 :: NSX Service Composer - Firewall (Rule 6 - 8)					
▶ SPO-DB-01 :: NSX Service Composer - Firewall (Rule 9 - 11)					
▼ VCAC App Isolation Policy-514c535a-7199-420c-85b6-cd9070232e5c :: NSX Service Composer - Firewall (Rule 12 - 15)					
12	Allow Intra Traffic	SG-c07b5064-d07d-4af5-9ff...	SG-c07b5064-d07d-4af5-9ff...	* any	Allow
13	Allow Intra Traffic	SG-0d64731d-13a4-4817-a...	SG-0d64731d-13a4-4817-a...	* any	Allow
14	Block all inbound traffic	* any	SG-0d64731d-13a4-4817-a... SG-c07b5064-d07d-4af5-9ff...	* any	Block
15	Block all outbound traffic	SG-0d64731d-13a4-4817-a... SG-c07b5064-d07d-4af5-9ff...	* any	* any	Block

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

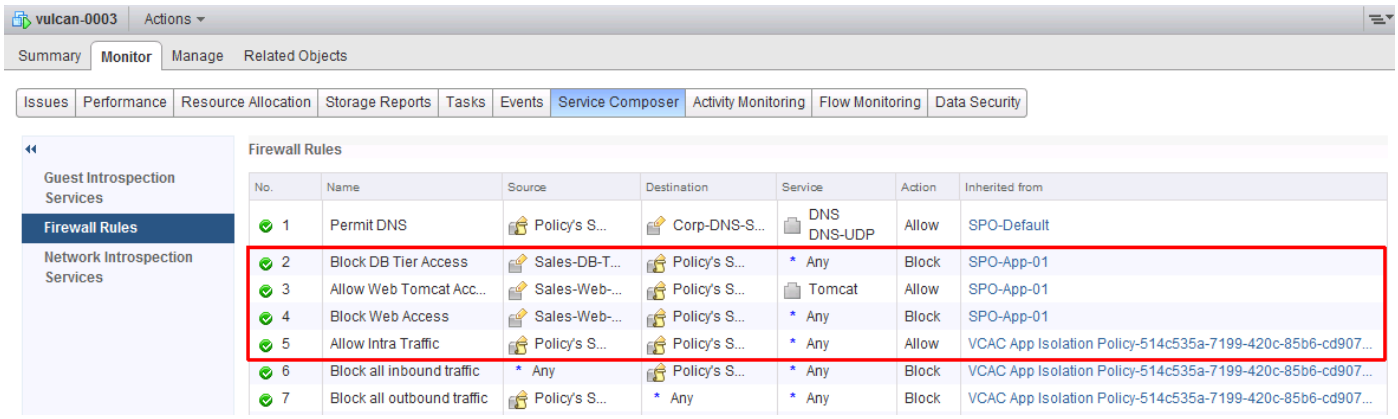
vRealize Automation and NSX Micro-Segmentation

In the VM & Templates view of the vSphere Web Client, you can display the Firewall Rules from Service Composer Security Policies that apply to a specific virtual machine by navigating to the VM and selecting **Monitor -> Service Composer -> Firewall Rules.**

Using an example of the Web Tier to App Tier connectivity, looking at a Web VM from our example Multi-Machine Service you can see that on egress for access to App Tier VMs the first rule that applies is Rule 6 from the App Isolation Policy. This permits traffic to App VMs within the same Deployment only, while Rule 7 blocks any traffic to another Deployment instance:



While from the same view of an App Tier VM, you can see that on ingress Rule number 3 permits traffic from Web Tier VMs to the App VMs for the Tomcat Service, while Rules 2 & 4 block any other communication between tiers before Rule 5 from the App Isolation policy would permit it:



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vRealize Automation and NSX Micro-Segmentation

So the effective Security Policy is that traffic from Web to App Tiers is only permitted at the vNIC of Web VMs when the destination App VM is in the same Deployment, and then at the vNIC of the App VMs further rules are applied to restrict traffic to TCP Port 8443 only. The same approach is used to secure connectivity between any of the other Tiers also.

Another view of the Security Policy is available if we look at the actual Distributed Firewall rules applied to the vNIC of a Web VM deployed by vRealize Automation directly at the ESXi host level:

```
  # Filter rules
  rule 1011 at 1 inout protocol udp from addrset ip-securitygroup-16 to addrset ip-securitygroup-36 port 53 accept;
  rule 1011 at 2 inout protocol tcp from addrset ip-securitygroup-16 to addrset ip-securitygroup-36 port 53 accept;
  rule 1041 at 3 inout protocol any from addrset ip-securitygroup-19 to addrset ip-securitygroup-19 drop;
  rule 1006 at 4 inout protocol any from addrset ip-securitygroup-20 to addrset ip-securitygroup-19 drop;
  rule 1005 at 5 inout protocol any from addrset ip-securitygroup-21 to addrset ip-securitygroup-19 drop;
  rule 1007 at 6 inout protocol tcp from any to addrset ip-securitygroup-19 port 22 accept;
  rule 1007 at 7 inout protocol tcp from any to addrset ip-securitygroup-19 port 443 accept;
  rule 1007 at 8 inout protocol tcp from any to addrset ip-securitygroup-19 port 80 accept;
  rule 1014 at 9 inout protocol any from addrset ip-securitygroup-23 to addrset ip-securitygroup-23 accept;
  rule 1016 at 10 inout protocol any from addrset ip-securitygroup-24 to addrset ip-securitygroup-24 accept;
  rule 1013 at 11 inout protocol any from any to addrset dst1013 drop;
  rule 1012 at 12 inout protocol any from addrset dst1013 to any drop;
  rule 1004 at 13 inout protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 1004 at 14 inout protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 1003 at 15 inout protocol udp from any to any port 67 accept;
  rule 1003 at 16 inout protocol udp from any to any port 68 accept;
  rule 1002 at 17 inout protocol any from any to any accept;
}
```

Here you can see that on egress the first rule highlighted in Green permits traffic to destination VMs in the same App Isolation Security Group, while the rules in Red drop any other traffic. So before traffic even reaches the App VMs in a different Deployment, it is blocked by the App Isolation rules applies to the Web VMs.

While from the DFW rules applied to an App VM:

```
  # Filter rules
  rule 1011 at 1 inout protocol udp from addrset ip-securitygroup-16 to addrset ip-securitygroup-36 port 53 accept;
  rule 1011 at 2 inout protocol tcp from addrset ip-securitygroup-16 to addrset ip-securitygroup-36 port 53 accept;
  rule 1009 at 3 inout protocol any from addrset ip-securitygroup-21 to addrset ip-securitygroup-20 drop;
  rule 1037 at 4 inout protocol tcp from addrset ip-securitygroup-19 to addrset ip-securitygroup-20 port 8443 accept;
  rule 1036 at 5 inout protocol any from addrset ip-securitygroup-19 to addrset ip-securitygroup-20 drop;
  rule 1014 at 6 inout protocol any from addrset ip-securitygroup-23 to addrset ip-securitygroup-23 accept;
  rule 1016 at 7 inout protocol any from addrset ip-securitygroup-24 to addrset ip-securitygroup-24 accept;
  rule 1013 at 8 inout protocol any from any to addrset dst1013 drop;
  rule 1012 at 9 inout protocol any from addrset dst1013 to any drop;
  rule 1004 at 10 inout protocol ipv6-icmp icmptype 135 from any to any accept;
  rule 1004 at 11 inout protocol ipv6-icmp icmptype 136 from any to any accept;
  rule 1003 at 12 inout protocol udp from any to any port 67 accept;
  rule 1003 at 13 inout protocol udp from any to any port 68 accept;
  rule 1002 at 14 inout protocol any from any to any accept;
}
```

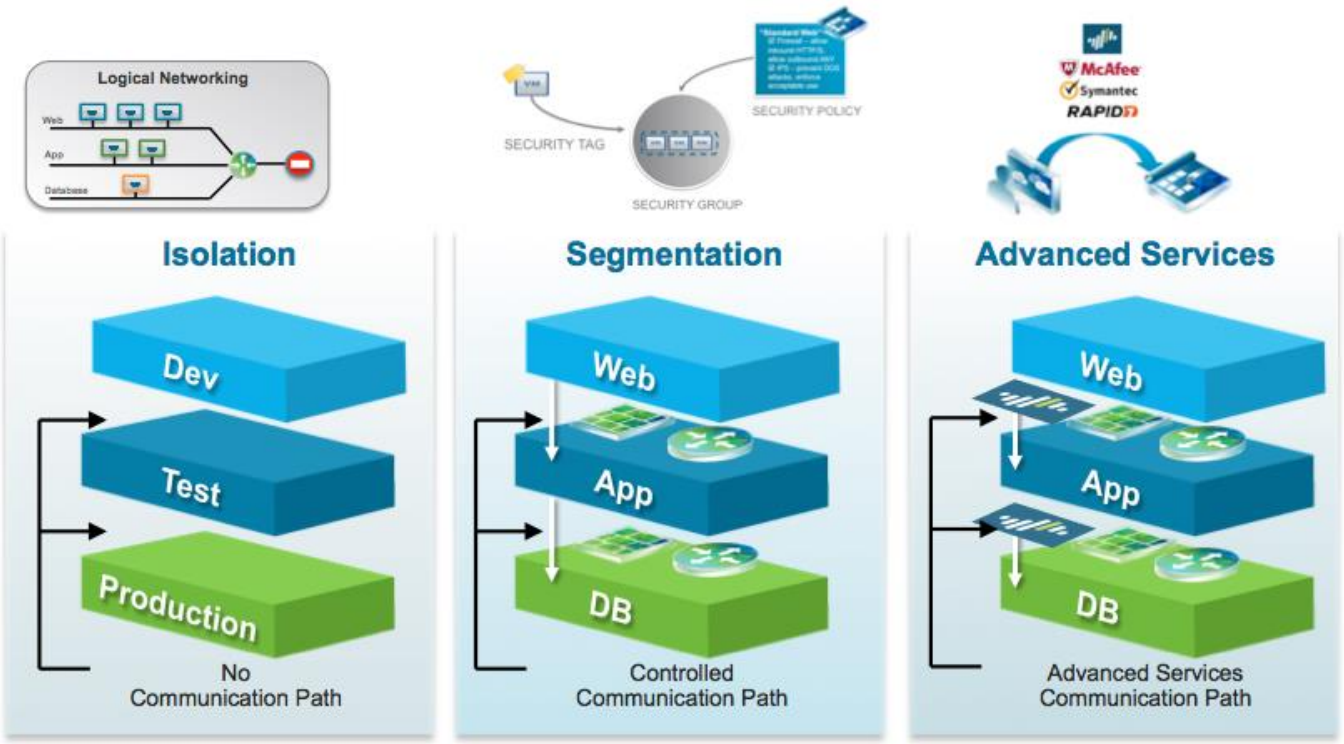
The rule highlighted in Green permits traffic from Web VMs on ingress to the App VMs limited to port 8443. It is only traffic VMs within the same Deployment that will reach this point in the FW rule processing, so we maintain the required segmentation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

vRealize Automation and NSX Micro-Segmentation

Conclusion

Leveraging the vRealize Automation and NSX integration you can provide secure, automated micro-segmentation for workloads deployed on demand via templates using self-service.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com