# Table of Contents

Lab Overview - HOL-1903-02-NET - VMware NSX - Distributed Firewall and Micro-Segmentation .................................................................................................................. 2
Lab Guidance ........................................................................................................ 3

Module 1 - Service Composer and Distributed Firewall Overview (45 minutes) .......... 9
  Distributed Firewall - Micro-segmentation Overview ............................................. 10
  Improved IP Discovery Mechanism for Virtual Machines and SpoofGuard .......... 38
  Security Groups Overview.................................................................................... 53
  Security Policy Overview..................................................................................... 57
  Module 1 - Conclusion ........................................................................................ 66

Module 2 - Collapse 3-Tier Application Feature Walk-Through (15 minutes) .......... 69
  Securing Collapsed Architectures with NSX's Distributed Firewall Capability ....... 70
  Module 2 - Conclusion ....................................................................................... 101

Module 3 - Intelligent Grouping (30 minutes) ...................................................... 103
  Intelligent Grouping .......................................................................................... 104
  Log on to the End of Support Virtual Machines ................................................. 105
  Security Group Creation...................................................................................... 112
  Limit VM Access ............................................................................................... 121
  Verify Limited Access from Windows XP VMs .................................................. 133
  Module 3 Conclusion ......................................................................................... 136

Module 4 - User Based Security with a Jump Box (45 minutes) ............................ 138
  User Based Security in a Jump Box Scenario ..................................................... 139
  Explore Link between NSX and Active Directory ............................................. 140
  NSX Guest Introspection .................................................................................... 146
  Use Security Objects based on AD Groups ....................................................... 151
  Define Internal Application Firewall Rules ..................................................... 170
  Testing User Identity Based Rules ..................................................................... 177
  Module 4 Conclusion ......................................................................................... 185

Module 5 - NSX Application Rule Manager (30 minutes) .................................... 187
  Application Rule Manager Introduction ............................................................ 188
  Application Micro segmentation ...................................................................... 189
  Module 5 Conclusion ......................................................................................... 235

Module 6 - NSX Troubleshooting & Maintenance (30 Minutes) ........................... 236
  NSX Troubleshooting & Backups with vRealize Network Insight Overview ....... 237
  NSX Troubleshooting & Backups with vRealize Network Insight - Lab Tasks ....... 239
  NSX Data Center with NSX-PowerOps Overview .............................................. 253
  NSX Data Center with NSX-PowerOps - Lab Tasks .......................................... 254
  Module 6 Conclusion ......................................................................................... 265
Lab Overview -
HOL-1903-02-NET -
VMware NSX - Distributed
Firewall and Micro-
Segmentation
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

In this lab we will explore use cases around VMware NSX and Micro Segmentation, including more in depth reviews of the Distributed Firewall and Service Composer UI. Use cases include solutions around collapsing segmented networks, intelligent grouping of servers, and user based security.

Lab Module List:

- **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
- **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to collapsed single tier architecture.
- **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
- **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
- **Module 5 - Application Micro-segmentation with Application Rule Manager** (45 minutes) - Basic - This module will demonstrate application micro-segmentation with Application Rule Manager.
- **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

- **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**

This lab manual can be downloaded from the Hands-on Labs Document site found here:
http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:


**Location of the Main Console**

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

**Alternate Methods of Keyboard Data Entry**

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the **Shift** key.

Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.
Module 1 - Service Composer and Distributed Firewall Overview (45 minutes)
Distributed Firewall - Micro-segmentation Overview

NSX Distributed firewall (DFW) is a hypervisor kernel-embedded firewall that provides visibility and control for virtualized workloads and networks. You can create access control policies based on VMware vCenter objects like datacenters and clusters and virtual machine names; network constructs like IP or IPSets, VLAN (DVS port-groups), VXLAN (logical switches), security groups, as well as user group identity from Active Directory. Firewall rules are enforced at the vNIC level of each virtual machine to provide consistent access control even when the virtual machine gets vMotioned. The hypervisor-embedded nature of the firewall delivers close to line rate throughput to enable higher workload consolidation on physical servers. The distributed nature of the firewall provides a scale-out architecture that automatically extends firewall capacity when additional hosts are added to a datacenter.

Micro-segmentation is powered by the Distributed Firewall (DFW) component of NSX. DFW operates at the ESXi hypervisor kernel layer and processes packets at near line-rate speed. Each VM has its own firewall rules and context. Workload mobility (vMotion) is fully supported with DFW, and active connections remain intact during the move. This advance security capability makes the data center network more secure by isolating each related group of virtual machines onto a distinct logical network segment, allowing the administrator to firewall traffic traveling from one segment of the data center to another (east-west traffic). This limits attackers’ ability to move laterally in the data center.

The outline of this module is:

**Distributed Firewall Basic Functionality**

- Check the status of the Distributed Firewall on vSphere hosts.
- Verify full open communication to the web application and between the 3-tiers.
- Block access to 3-tier app and verify.
- Create a security group for the web tier.
- Create Firewall rules to allow secure access to the web application.

**Improved IP discovery mechanism for Firewall function**

- Review existing rule rejecting access to Linux-01a VM
- Enable IP discovery with Arp Snooping
- Verify that the reject rule now takes effect and denies access to Linux-01a VM

**Logically apply Security with Service Composer**

- Review and create a Security Group for VMs, defined by dynamic membership
• Review, create, and apply a firewall rule to the Security Group via a Security Policy
• **Service Composer Canvas is no longer available in NSX 6.4.x versions!**
  Please review the following link for more information: [https://tinyurl.com/y9fe6w8v](https://tinyurl.com/y9fe6w8v)

**New with NSX 6.4, there is some layer 7 functionality which becomes available.** This is done by pushing a new VIB to ESXi hosts which looks inside the traffic flows. This newest change recognizes App ID inside network traffic. For example: AD, KMS, DNS, RDP, SSH, SMB, TLS versions, etc.

Start the module from your desktop. The desktop is your **Control center** jumpbox in the virtual environment. From this desktop you will access the **vCenter Server Appliance** deployed in your virtual datacenter. Another important task is to always choose to save each time a Firewall Rule is created.

**Special Note: On the desktop you will find a file names README.txt. It contains the user accounts and passwords used for all the virtual devices and VM's in the lab.**

**Notice to User about Distributed Firewall - Micro-segmentation Section**

If you have completed HOL-1903-01-NET, Module 6 - Distributed Firewall, then it is important to note that this section titled, Distributed Firewall in this lab is a repeat of that module, and is not required to continue on with this lab. If you would like to skip this section and move to the next section in this lab, we provide a link below to skip ahead.

**Alternate Methods of Keyboard Data Entry**

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Access vSphere Web Client

1. Bring up the vSphere Web Client (Flash) via the icon on the desktop labeled, Google Chrome.

Login to the vSphere Web Client (Flash)
If you are not already logged into the vSphere Web Client (Flash):

(The home page should be the vSphere Web Client(Flash). If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Type in **administrator@corp.local** into User name  
2. Type in **VMware1!** into Password  
3. Click **Login**

## Configure Rules for Web Application Access

You will now configure Distributed Firewall access to a 3-tier application. The application has two web servers, and one each of an application and database server. There is also a Load Balancer servicing the two web servers.

## Test 3-tier VM to VM connectivity using Putty

![Putty Configuration](image)

Next you will test communication and access between the network segments and guest VMs making up the 3-tier application. Your first test will be to open a console to web-sv-01a and ping the other members.

1. **Click on the PuTTY shortcut on the desktop taskbar**  
2. Select **web-01a.corp.local**  
3. Click on **Open**
Ping from web-01a to other 3-tier members

1. First you will show that **web-01a** can Ping **web-02a** by entering:

```
ping -c 2 172.16.10.12
```

Now test connectivity between **web-01a to app-01a** and **db-01a**:

```
ping -c 2 172.16.20.11
```

```
ping -c 2 172.16.30.11
```

(Note: You might see DUP! at the end of a Ping line. This is due to the nature of the virtual lab environment using nested virtualization and promiscuous mode on the virtual routers. You will not see this in production.)

Don't close the window just minimize it for later use.

**Demonstrate 3-tier application using a web browser**

Using a browser you will access the 3-tier application to demonstrate the function between the 3 parts.
1. Open a new browser tab
2. Click on the bookmark "Customer DB App"

**Demonstrate 3-tier application using a web browser-cont**

![External Customer Database](image)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name</th>
<th>Universe</th>
<th>Revenue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CHOAM</td>
<td>Dune</td>
<td>$1.7 trillion</td>
</tr>
<tr>
<td>2</td>
<td>Acme Corp.</td>
<td>Looney Tunes</td>
<td>$348.7 billion</td>
</tr>
<tr>
<td>3</td>
<td>Sirius Cybernetics Corp.</td>
<td>Hitchhiker's Guide</td>
<td>$327.2 billion</td>
</tr>
<tr>
<td>4</td>
<td>Buy n Large</td>
<td>Wall-E</td>
<td>$291.8 billion</td>
</tr>
<tr>
<td>5</td>
<td>Aperture Science, Inc.</td>
<td>Valve</td>
<td>$163.4 billion</td>
</tr>
<tr>
<td>6</td>
<td>SPECTRE</td>
<td>007</td>
<td>$157.1 billion</td>
</tr>
<tr>
<td>7</td>
<td>Very Big Corp. of America</td>
<td>Monty Python</td>
<td>$146.6 billion</td>
</tr>
</tbody>
</table>

1. Result is data that passed from the web tier to the **app-01a** vm and finally queried the **db-01a** vm
Change the default firewall policy from Allow to Block

In this section you will change the default Allow rule to Block and show communication to the 3-tier application to be broken. After that you will create new access rules to re-establish communication in a secure method.

1. Click the browser tab for the vSphere Web Client (Flash).
2. Click Home and select Networking and Security
3. Select Firewall on the left. You will see the Default Section Layer3 on the General Section (Select the + sign to expand to bottom of list).
Examine the Default Rules

1. Expand the section using the drop down arrow

Notice the Rules have green check marks. This means a rule is enabled. However, the "Default Rule" is active even without green indicator as shown. Rules are built in the typical fashion with source, destination, and service fields. Services are a combination of protocols and ports.

The last Default Rule is a basic any-to-any-allow.

Explore Default Rule - FireWall

Scroll to the right and you can see the Action choices for the Default Rule by placing the cursor in the field for Action: Allow drop down selection on rule 5. This will bring up a selection of either: "Allow, Block, or Reject" that allows you to see the choices for this field.
Change the Last Default Rule Action from Allow to Block

Choose Block to enforce "Zero Trust" goal

1. Select on **Block**
2. Click **Publish**  (Choose the Publish button near top of the screen)

Verify the Rule change blocks communication
To test the block rule using your previous Putty and browser sessions

- **Putty:** In a few moments opening Putty will show it is no longer active due to the default rule now blocks everything including SSH. Minimize the console again.

**Verify the Rule blocks https using Web Browser**

1. Open the tab for the **Customer DB App**
2. **Refresh your browser.** You will get an error
3. Click the browser tab for **vSphere Web client**
Create 3-Tier Security Groups

1. Click on Service Composer.

Service Composer defines a new model for consuming network and security services in virtual and cloud environments. Policies are made actionable through simple visualization and consumption of services that are built-in or enhanced by 3rd party solutions. These same policies can be made repeatable through export/import capabilities, which would help make it easier to stand up and recover an environment when there is an issue. One of those objects for repeatable use is a Security Group. We will cover Service Composer and Security Groups in depth in a later the module, called "Service Compose and DFW Overview."
Add Security Group

1. Select **Security Groups**. Note: there may be existing security groups to be used in another lab module
2. To add a new security group click the **+ ADD** icon

**New Security Group - Web**

1. Once selecting the + Add then choose Name this first group "**Web-Tier**"
2. Click the "**Select objects to include**" section
Select objects to include

1. Pull down the **Object Types** and select **Virtual Machines**
2. You can filter by typing "web" into the search widow
3. Select **web-01a**
4. Click the **Right Hand arrow** to push the VM to the Selected Objects window
5. Repeat for **web-02a**
6. Click **Finish**

Note: As a shortcut you can double-click the VMs on the left and they will move to the right in this one step.
Verify Security Group Creation

You have created a security group named **Web-tier** having 2 VMs assigned.

1. Validate by choosing "Groups and Tags section
2. Notice newly created "Web-Tier" Security Group
3. Verify that there is now Quantity of 2 static Members

Create 3-Tier Access Rules

Next you will add new rules to allow access to the web vm and then set up access between the tiers.

1. On the left hand menu, select **Firewall**
Create New Firewall Section

1. In middle of screen select the + **ADD SECTION** button to add another Firewall section above the "Flow Monitoring & Trace Flow Rules-Disabled by Default (Rule 1)" row

Add New Rule Section for 3-Tier Application

1. Name the section "**3-Tier App**"
2. Select **Add** button
**Add Rule to New Section**

1. On the new "3-Tier App" section please choose the three dot as indicated with the arrow
2. Click on the **Add rule** icon

**Edit New Rule name**

1. Notice new default rule under the section called "3-Tier App"
2. Click Name area of the new rule "[Enter rule name] to change to new name
Edit New Rule name cont

1. Enter "Ext to Web" for the name
2. Click on Enter Key of your keyboard

Set Rule Source and Destination

Source: Leave the Rule Source set to any.

1. Hover the mouse pointer in the Destination field and select box to modify Destination from Any
Set Security Group values

1. Pull down the Object Type and scroll down until you find Security Group
2. Click on Web-Tier
3. Click on the top arrow to move the object to the right
4. Click SAVE

Edit Service

1. Again hover in the Service field and click on the box to change from Any
Set Rule Service

In the search field you can search for service pattern matches.

1. Enter "https" and press enter to see all services associated with the name https
2. Select the simple HTTPS service
3. Click on the top arrow
4. Repeat the above steps 1-3 to find and add SSH. (You will see later in the module that we need SSH.)
5. Click SAVE

Note: DO NOT Publish - as you have more rules to create first
Create Rule to Allow Web Security Group Access to App Logical Switch

You will now add a second rule to allow the Web Security Group to access the App Security Group via the App port.

1. Start by selecting the three dots next to "Ext to Web" rule as shown
2. You want this rule to be processed below the previous rule so choose Add Below from the drop down box

Create Second Rule Name and Source fields

1. As you did before hover the mouse over the Name field and click the pencil. Enter "Web to App" for the name
2. Choose Web-tier Security Group for the Source field
Create Second Rule Destination

1. **Hover** over the Destination Field - **Click the Destination** to edit from Any

Create Second Rule Destination field: Choose Logical Network

In the first rule, the **Web-tier** security group was chosen as the destination. You could proceed with the remaining rules in the same fashion. But as seen from the drop-down you can use several vCenter objects already defined. A powerful time saving aspect of the integrated vSphere with NSX Security is the selection of using existing virtual datacenter objects for your rules rather having to start from scratch. Example uses a VXLAN Logical Switch as the destination. This allows the selection of creating a rule to be applied to any VM attached to this network.
1. Scroll down in the Object Type drop-down and click on Logical Switch choice
2. Select App_Tier-Logical_Switch
3. Click on the top arrow to move the object to the right
4. Click SAVE

Create Second Rule Service

![](image)

1. Hover over the Destination Field - Click the "Service Field" to edit from Any

Create Second Rule Service Field: New Service (Please review both screen steps for this task)

![](image)

The 3-tier application uses tcp port 8443 between the web and app tiers. You will create a new Service called MyApp to be the allowed service.
1. Click on New Service

**New Service for Second Rule Creation**

![New Service interface with labeled steps]

1. **Enter MyApp** for the new service name
2. **Select TCP** for the Protocol
3. **Enter 8443** for the Port number
4. **Click ADD**

*Note - Ensure that Layer 3 is chosen and than none of the other fields are filled out other than illustrated for this task*
Click SAVE

1. Click Save

Create Third Rule: Allow Logical Switch App to Access Logical Switch Database

Repeating the previous steps:
On your own create the third and last rule below your last rule to give access between the App Tier Logical Switch and the DB Tier Logical Switch.

1. Create the final rule allowing the **App Logical Switch** to communicate with the **Database Logical Switch** via the **HTTP service**.

Your new rule should look like the one listed in the example.

2. **Publish** Changes

**Verify New Rule Allow 3-Tier Application Communication**

1. Return to the tab you used previously for the Web App.
2. **Refresh the browser** to show you are getting the data via the 3-tier app.

Your new "3-tier App" section allows access to the application.
Restart Putty Session to web-01a

1. Click the **Session icon** in the upper left
2. Click **Restart Session**

Ping Test between Tiers

```
[root@web-01a ~]# ping -c 2 172.16.10.12
PING 172.16.10.12 (172.16.10.12) 56(84) bytes of data.

--- 172.16.10.12 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 11000ms

[root@web-01a ~]# ping -c 2 172.16.20.11
PING 172.16.20.11 (172.16.20.11) 56(84) bytes of data.

--- 172.16.20.11 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 11000ms

[root@web-01a ~]# ping -c 2 172.16.30.11
PING 172.16.30.11 (172.16.30.11) 56(84) bytes of data.

--- 172.16.30.11 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 11000ms
```

Try to ping 3-tier application guest VMs.
Note: Remember to use the Click and Drag feature.

**web-02a**

```bash
ping -c 2 172.16.10.12
```

**app-01a**

```bash
ping -c 2 172.16.20.11
```

**db-01a**

```bash
ping -c 2 172.16.30.11
```

Pings are not allowed and will fail as ICMP is not allowed between tiers or tier members in your rules. Without allowing for ICMP between the tiers the Default Rule now blocks all other traffic.

- Minimize Putty Session to web-01a.

**Topology After Adding Distributed Firewall Rules for the 3-Tier Application**
The diagram shows the relative enforcement point of the vNIC level firewall. Although the DFW is a Kernel Loadable Module (KLM) of the vSphere ESXi Host the rules are enforced at the vNIC of the guest VM. This protection moves with the VM during vMotion to provide complete fulltime protection not allowing for a "window of opportunity" during which the VM is susceptible to attack.

**Module Clean Up**

1. Change the Default Rule Action back to Allow.
2. Publish Changes.
Improved IP Discovery Mechanism for Virtual Machines and SpoofGuard

After synchronizing with the vCenter Server, NSX Manager collects the IP addresses of all vCenter guest virtual machines. If a virtual machine has been compromised, the IP address can be spoofed and malicious transmissions can bypass firewall policies.

You create a SpoofGuard policy for specific networks that allows you to authorize the IP addresses reported and alter them if necessary to prevent spoofing. SpoofGuard inherently trusts the MAC addresses of virtual machines collected from the VMX files and vSphere SDK. Operating separately from Firewall rules, you can use SpoofGuard to block traffic determined to be spoofed.

SpoofGuard supports both IPv4 and IPv6 addresses. When using IPv4, the SpoofGuard policy supports a single IP address assigned to a vNIC. IPv6 supports multiple IP addresses assigned to a vNIC. The SpoofGuard policy monitors and manages the IP addresses reported by your virtual machines in one of the following modes:

• **Automatically Trust IP Assignments On Their First Use**

This mode allows all traffic from your virtual machines to pass while building a table of vNIC-to-IP address assignments. We can review this table at our convenience and make IP address changes. This mode automatically approves all ipv4 and ipv6 address on a vNIC.

• **Manually Inspect and Approve All IP Assignments Before Use**

This mode blocks all traffic until there is an approval each vNIC-to-IP address assignment.

**Note:** SpoofGuard inherently allows DHCP requests regardless of enabled mode. However, if in manual inspection mode, traffic does not pass until the DHCP-assigned IP address has been approved.

SpoofGuard includes a system-generated default policy that applies to port groups and logical networks not covered by the other SpoofGuard policies. A newly added network is automatically added to the default policy until the administrator adds the network to an existing policy or creates a new policy for it.

NSX distributed firewall operation requires discovery of IP addressees for objects that are specified as a source or a destination. Prior to NSX 6.2, this was achieved by VMtools inside the VM. This exercise will show you how to discover IP addresses with VMtools and Trust-On-First-Use.
Review SpoofGuard

Click on the browser tab for the vSphere Web Client

1. Click the **Home Icon**
2. Click **Networking & Security**

Explore SpoofGuard Options
1. Click **SpoofGuard** in the Navigator

**Enable IP address discovery via ARP Snooping**

1. Click **Gear wheel icon**

**Change IP detection type to ARP Snooping**

Now we will enable IP address discovery with “ARP Snooping”
1. Check **ARP Snooping**
2. Click **SAVE**

**Edit Default SpoofGuard Policy**

1. Click on **Default Policy**
2. Click on **EDIT** button

**Enable SpoofGuard**

1. Click the **Radio button** for **Enabled** - "Ensure Manually inspect and approve all IP assignment before use" is chosen
2. Click **Finish**
Migrate Linux-01a from vDS to a new Logical Switch

First, we must migrate the **Linux-01a** VM from its existing vDS to a Logical Switch to leverage SpoofGuard IP Discovery capabilities.

**Navigate to Logical Switches**

1. Click the **Logical Switches** section
2. Click the **Green plus icon** to create a new Logical Switch
Name the New Logical Switch

1. Name the Logical Switch, "Linux_Logical_Switch"
2. Click OK

Add Virtual Machines to the Logical Switch
1. To add virtual machines, we will right-click the Linux_Logical_Switch.
2. Select the Add VM option.

**Select the Virtual Machine to Migrate**

1. Enter "linux" into the Filter
2. Select the linux-01a VM
3. Click the "right arrow" to add the linux-01a VM to the Selected Objects list
4. Click Next
Select vNIC to Migrate to new Logical Switch

1. Check the box for the linux-01a vNIC to migrate to the Logical Switch
2. Click Next

Finish Migration of VMs to Collapsed Logical Switch

1. Click Finish to complete the migration of the linux-01a VM to the new Linux_Logical_Switch.
Access the Logical Switch

1. Double-click the new **Linux_Logical_Switch** to view the associated virtual machines.

View Related Virtual Machines

1. Click the **Virtual Machines** section
2. Verify the **linux-01a** VM is listed
Open Console to linux-01a VM

1. Select the **linux-01a VM**
2. Click **Gear Icon**
3. Select **Launch Remote Console**

**Enter Username and Password to linux-01a**

Remember you can use the "click and drag" feature to copy CLI commands into the active window

1. Enter "**root**" at the login prompt
2. Enter "**VMware1!**" at the password prompt
Verify IP Configuration

1. Enter "ifconfig" in the command line

ifconfig

Note: the IP address of the linux-01a VM is 192.168.120.115.

Test Network Connectivity

1. Enter "ping -c 2 192.168.120.1" to initiate a ping test to an assumed default gateway

ping -c 2 192.168.120.1

Note: the ping test in this step will fail because we have not connected the Linux_Logical_Switch to an NSX Edge to provide routing. We only want to initiate traffic from the VM in order for SpoofGuard to identify this VM.
Exit the Remote Console

1. Press Control+Alt to move your cursor out of the Remote Console Window
2. Return to the vSphere Web Client browser tab by clicking on it

Navigate back to Networking & Security

1. Under the Navigator, click the Back button in the history field until you get back to the NSX configuration interface.
Verify that Linux-01a was discovered via ARP Snooping

1. Select **SpoofGuard** from the Navigator menu
2. Click on **Default Policy**

**SpoofGuard Active NICs**

1. Pick **All Virtual NICs** in the View dropdown
2. Enter "lin" and press enter to filter for linux-01a
Approve Linux-01a new IP Address

1. Click **APPROVE**

Prompt for Approval

1. Do you want to approve IP for selected vNIC?  - Yes

Publish IP Approval

1. Click on **Publish** Changes (Only if not already saved and "PUBLISH" has not been chosen in this section with prompts as indicated)
SpoofGuard Wrap Up

This concludes the section on Improved IP Discovery Mechanism for Virtual Machines and SpoofGuard. We have successfully migrated a VM into the NSX environment, and leveraged SpoofGuard to learn the IP address of the VM with the new Trust-On-First-Use ARP feature.
Security Groups Overview

We will now build upon the Security Group capabilities we discovered in the Distributed Firewall - Micro-segmentation Overview. NSX Security Groups are a way to logically group and define assets that you want to protect. Security groups may be static (including specific virtual machines) or dynamic where membership may be defined in one or more of the following ways:

- vCenter containers (clusters, port groups, or datacenters)
- Security tags, IPset, MACset, or even other security groups. For example, you may include a criteria to add all members tagged with the specified security tag (such as AntiVirus.virusFound) to the security group
- Directory Groups (if NSX Manager is registered with Active Directory)
- Regular expressions such as virtual machines with VM1 in their name

Note that security group membership changes constantly. For example, a virtual machine tagged with the AntiVirus.virusFound tag is moved into the Quarantine security group. When the virus is cleaned and this tag is removed from the virtual machine, it again moves out of the Quarantine security group.

Access the Service Composer

1. Click the **Service Composer** on the left panel
2. Ensure **Security Groups** tab is selected
3. Select **+ADD** to create new Security Group
Create the Web Security Group

1. Enter "Web Security Group" in the Name dialog box
2. Click Next

Explore Object List

1. Open the Object Drop Down box

You will see that you can use Computer OS Name, Computer Name, VM Name, Security Tag, or Entity. Entity allows you to pick from many elements of the vCenter including Resource Pool, Directory Domain Group, Logical Switches, Distributed Port Group and many more.
Explore Object member criteria list

The Criteria choices will vary depending on the Object Type chosen.

Define Dynamic Membership

1. Select **VM Name** from the first **Criteria Details** drop down list
2. Verify **Contains** is selected in the middle drop down of the page
3. Enter **web** in the dialog box
4. Click **Finish**

**Validate Dynamic Security Group Membership**

1. Select **Groups and Tags**
2. Notice newly created Security Group with **NO Static Members**
3. Dynamic Security group has been defined with criteria
4. Double click on "**1 Criteria**" to see the logic for this dynamic security group

**Dynamic Member Validation**

1. Criteria is met according to the defined value
Security Policy Overview

NSX Security Policies can be a collection of the following service configurations; Firewall rules; Endpoint services; and Network introspection services. Firewall rules can consist of rules that define the traffic to be allowed to, from, or within the security group. Endpoint services can be implemented via third party solution provider services such as anti-virus or vulnerability management services. Network introspection services are services that monitor your network such as IPS.

During service deployment in NSX, the third party vendor selects the service category for the service being deployed. A default service profile is created for each vendor template.

*Note* When you have many security groups to which you need to attach the same security policy, create an umbrella security group that includes all these child security groups, and apply the common security policy to the umbrella security group. This will ensure that the NSX distributed firewall utilizes ESXi host memory efficiently.

Create a New Security Policy

1. Select **Service Composer**
2. Select the **Security Policies** tab in the Service Composer panel
3. Click **+ADD** to create Security Policy
Name new Security Policy

1. Type in "Block Web-to-Web Traffic" in the Name field
2. Click Firewall Rules in the left panel
Create a New Firewall Rule

1. Click the **ADD icon** to add a New Firewall Rule
New Firewall Rule

1. Type in "Block Web-to-Web Traffic" in the Name field
2. Select Block from the Action list
3. For the Destination field, change Any to Policy's Security Groups
4. Services select Any
5. Select State - Enabled
6. Log - No
7. Select OK for New Firewall Rule

Note: We are going to apply this Security Policy to the Policy's Security Group, which is now defined as the Source and Destination for our Firewall rule.
Finish Security Policy Definition

1. Click **Finish**

Apply the Security Policy to a Security Group

1. Highlight the **Block Web-to-Web Traffic** security policy
2. Click the **Apply Security Policy** icon
Filter Security Group to be in Security Policy

1. Select the **Web Security Group**
2. Select **Arrow** to move over to Selected Objects
3. Click **APPLY**

Verify Security Policy Application

1. Verify the **Sync Status** column changed to **Published**
2. Verify the **Applied to** have a **1** in the column
3. Verify **Firewall Rules** associated should be **1**
Security Policy Status

1. Final Validation & "Sync Status"

This information verifies that our rules have successfully synced with the Firewall rules in NSX, and are being correctly applied to the Security Groups

Verify Firewall Rule Synchronization

1. Click on Firewall
View Service Composer Firewall rules

1. Expand the firewall section "Block Web-to-Web Traffic" and verify the rules creation

Test Web VM to Web VM connectivity using Putty

Test communication and access between the Web VMs making up the 3-tier application. Our first test will be to open a console to web-01a and ping web-02a.

1. Click on the PuTTY shortcut on the desktop taskbar
2. Select web-01a.corp.local
3. Click on Open
Ping from web-01a to web-02a

We will show that **web-01a** cannot ping **web-02a** by entering:

1. Ping web-02a

```bash
ping -c 2 web-02a
```

Pings will fail between the Web VMs per the Security Policy.
Module 1 - Conclusion

This now completes Module 1 on Service Composer and Distributed Firewall. We have created both static and dynamic Security Groups, applied both static and dynamic Security Policies, including firewall rules, and used SpoofGuard to discover and allow VMs on to the network that are not running VMTools.

Module 1 Clean Up

Prior to finishing Module 1, you need to remove the rule that was created during this section.

1. Navigate back to Service Composer
2. Select Security Policies tab
3. select radio button for "Block Web-to-Web Traffic" row
4. Select the Delete option. When prompted "Are you sure you want to delete the selected - Block Web-to-Web Traffic?", click DELETE

Module 1 Cleanup - SpoofGuard
Prior to finishing Module 1, you need to disable SpoofGuard Default Policy

1. Select Default Policy
2. Choose EDIT

Module 1 Cleanup - Disable SpoofGuard

![](image)

1. Ensure Enable is off to save Default Policy SpoofGuard settings

You've finished Module 1

Congratulations on completing Module 1.

If you are looking for additional information on NSX Routing capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL:

- Go to [https://tinyurl.com/y9fe6w8v](https://tinyurl.com/y9fe6w8v)

Proceed to any module below which interests you the most:

Lab Module List:

- **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
- **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
- **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
- **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
- **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application micro segmentation.
• **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

**Lab Captain:**

• **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**

**How to End Lab**

To end your lab click on the **END** button.
Module 2 - Collapse 3-Tier Application Feature Walk-Through (15 minutes)
Securing Collapsed Architectures with NSX's Distributed Firewall Capability

In this module, you will explore how the Distributed Firewall (DFW) functionality in NSX allows customers to collapse traditional multi-tier network architectures into single, flat networks while maintaining application isolation at the same time. This is essential to getting away from a network-centric approach to security and moving to a workload-centric approach. You will be using two different applications (HR and Finance) that have been placed on the same logical switch and subnet.

You will then configure and test the following:

- Test communication between the HR and Finance application VMs on the same network prior to isolation
- Create logical groupings of VMs using Security Groups
- Create Distributed Firewall rules to protect communication between the applications
- Verify each application can still function correctly and that communication is blocked *between* the HR and Finance application VMs
- Clean up lab security policies prior to moving on the next lab

When you have completed this lab module, you have proven that NSX DFW has secured and isolated the applications from each other while allowing intra-application communication to function as normal on the same network infrastructure.

Review Sample Network Architecture

Before we collapse a 3-tier application network into a single network, let's look at an example of a 3-tier application segmented into individual network subnets to provide Layer 3 isolation between the web, application, and database tiers. It is important to note that we were missing security firewall rules protecting communication between VMs resident on the same layer 2 domain, and even between tiers of the application. When organizations begin to scale out multiples of these multi-tier workloads the
Choice is to either deploy more subnets or deploy application components (e.g. databases from different applications) on the same L2 domain.

For example, an organization may have the database components for multiple applications resident on the "DB-Tier" network. With traditional firewalls, there is no protection between those databases. This could potentially allow someone with approved access to one DB machine the ability to access another DB on the same network. NSX's DFW allows organizations collapse the entire network structure into a single L2 segment and provide intra-application functionality while providing inter-app application isolation.

**Review Collapsed Network Topology**

In an effort to save time, we have created a logical switch named **Collapsed_Logical_Switch** with a subnet of 172.16.60.0/24. We have migrated two multi-tier apps (HR and Finance) to this single subnet. There is currently no security implemented on this network.

Once communication between VMs associated to the HR and Finance applications is verified, you will create security groups to logically apply firewall rules to protect and control communication between them.

**Access vSphere Web Client**

1. Click on the shortcut to **Google Chrome** on the Main Console window.
Login to the vSphere Web Client(Flash)

If you are not already logged into the vSphere Web Client(Flash):

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client bookmark icon for Google Chrome.)

1. Type in administrator@corp.local into User name
2. Type in VMware1! into Password
3. Click Login

Access Networking & Security UI

1. Click on Networking & Security.
Navigate to Logical Switches

1. Click Logical Switches in the left menu.
2. Double-click the Collapsed_Logical_Switch (Segment ID - 5003).

View Connected Virtual Machines

1. Click the Virtual Machines selection
2. Review VMs from both the HR and Finance applications: fin-db-01a.corp.local, fin-app-01a.corp.local, fin-web-01a.corp.local, hr-web-01a.corp.local, hr-db-01a.corp.local, and hr-app-01a.corp.local.
Validate Finance Application is working

1. Open a New Tab in Chrome.
2. Click on the Finance DB App bookmark.
3. Validate you are accessing the Financial Department Cost Centers Database. Result will be received data from fin-web-01a.

Validate the HR Application

1. Open a New Tab in Chrome
2. Click on the HR DB App bookmark
3. Validate you are accessing the HR Employee Salary Database
Launch a Remote Console to fin-web-01a VM

1. Click the tab for vSphere Web Client.
2. Click fin-web-01a.corp.local.
3. Click on the Summary tab.
4. Click Gear Icon and Launch Remote Console.

Login into fin-web-01a VM

When the VMRC window first opens, it will appear black. Click inside the window and press enter a couple of times to make the console appear from the screensaver.

1. Login as "root"
2. Type the password "VMware1!"
Test ping between Finance Web VM to HR App VMs

We will now test communication between the HR and Finance applications by sending a ping from **fin-web-01a** to **hr-web-01a**, and **hr-db-01a** by entering the following commands:

1. **ping -c 3 hr-web-01a**

   ```
   # ping -c 3 hr-web-01a
   ```

2. **ping -c 3 hr-db-01a**

   ```
   # ping -c 3 hr-db-01a
   ```

We have verified HR and Finance application VMs can communicate with each other. This is not a desirable security model. Users who have access to HR, for example, could now have easier access to the Finance application components.

**Note**: To release your cursor from the remote console window, press **Ctrl+Alt** keys.

**Return to the vSphere Web Client Session**

1. Click the **vSphere Web Client(Flash)** browser icon on the Taskbar
Launch a Remote Console to hr-db-01a VM

1. Click hr-db-01a.corp.local
2. Click on the Summary
3. Click Gear Icon and Launch Remote Console

Note: in order to Launch Remote Console we must be on the Summary tab of the VM, and may have to click the Summary tab if not already selected by default.

Login into hr-web-01a VM

When the VMRC window first opens, it will appear black. Click inside the window and press enter a couple of times to make the console appear from the screensaver.

1. Login as "root"
2. Type the password "VMware1!"
We will now test communication between the HR and Finance applications by sending a ping from hr-db-01a to fin-app-01a, and fin-db-01a by entering the following commands:

1. **ping -c 3 fin-app-01a**

   ```
   # ping -c 3 fin-app-01a
   ```

2. **ping -c 3 fin-db-01a**

   ```
   # ping -c 3 fin-db-01a
   ```

We have verified HR and Finance application VMs can communicate with each other. Enable application isolation on the collapsed application tier by configuring the Distributed Firewall, and Security Groups to prevent communication.

**Note:** To release your cursor from the remote console window, press **Ctrl+Alt** keys.

**Return the vSphere Web Client**

1. Click the **vSphere Web Client Chrome** browser icon on the Taskbar or shortcut on desktop
Go back to Networking & Security

1. Click the Back button twice to go back to Networking & Security

Access the Firewall Configuration

1. Click the Firewall from the Navigator menu on the left.
Add a New Section

1. Click the **ADD SECTION** icon in the top row of the Firewall Configuration rules

Name New Firewall Section

1. Enter "**Collapsed App Tier Rules**" to name the new section
2. Click the **Add** button

**Note:** DO NOT PUBLISH CHANGES YET.

Create a New Firewall Rule

Now we will create a new firewall rule.
Open up New Rule

1. Click the "Add Rule" on the **Collapsed App Tier Rules** section

Create Block HR to Finance Traffic rule

1. Select new Rule row and change Name field (Double click in Name field for ability to change name)

Rename newly created Rule

1. Enter "**Block HR to Finance Traffic**" in the Rule Name field and hit enter on keyboard
Edit Source Object

1. Click the edit icon to edit the Source Object from Any

Create HR App Security Group

1. Select Security Group from the Object Type drop down menu
2. Click New Security Group to define the HR App security group
Name HR App Security Group

1. Enter "HR App" as the Name of the security group
2. Click Next

Define Dynamic Membership

1. Select VM Name from the Criteria Details drop down menu
2. Enter "hr" into the text field to set the criteria for VM name
3. Click Finish

Note: We left the center drop down menu of the Criteria Details at Contains to specify that the VM Name contains the letters "hr" to find all HR VMs in the lab environment.

Confirm HR App Selected

1. Verify the new HR App security group has been added to the Selected Objects
2. Click SAVE

Edit Destination Object

1. Click the Destination field to edit the Destination Object from Any
Create Finance App Security Group

1. Select **Security Group** from the **Object Type** drop down menu.
2. Click **New Security Group** to define the Finance App security group.
Name Finance App Security Group

1. Enter "Finance App" as the **Name** of the security group
2. Click **Next**

Define Dynamic Membership

1. Select **VM Name** from the **Criteria Details** drop down menu
2. Enter "fin" into the text field to set the criteria for VM name
3. Click **Finish**

**Note:** We left the center drop down menu of the **Criteria Details** at **Contains** to specify that the **VM Name** contains the letters "fin" to find all finance VMs in the lab environment.

**Confirm Finance App Selected**

![Image of Specify Destination | Block HR to Finance Traffic]

1. Verify the new **Finance App** security group has been added to the **Selected Objects**
2. Click **SAVE**
Confirm HR App VM Membership

1. Click on the **HR App** name in the firewall rule **Source** field to expose the VM membership of this security group.
2. Validate that you see all VMs with "hr" in the name listed, like in the image above (hr-web-01a, hr-db-01a, & hr-app-01a)
3. Click the "X" in the top right corner of the window to close it.

Confirm Finance App VM Membership

1. Click on the **Finance App** name in the firewall rule **Destination** field to expose the VM membership of this security group.
2. Validate you see all VMs with "fin" in the name listed, like in the image above (fin-app-01a, fin-web-01a, fin-db-01a)
3. Click the "X" in the top right corner of the window to close it.
**Edit Action Settings**

1. Hover of the right hand side of the Action cell of the Firewall rule, and click the Allow Field drop down to edit the action

**Select Block Action**

1. Select Block from the Action drop down menu.
2. Click Save.

**Add a New Firewall Rule**

1. Click the three dots icon of the Collapsed App Tier Rules section
2. Select "Add Rule Above"
Edit Rule Name

1. Hover over the right side of the **Name** box to click the Name field to edit the name of the new rule

**Name Block Finance to HR Traffic rule**

1. Enter "**Block Finance to HR Traffic**" in the Rule Name field and then hit enter on keyboard

Edit Source Object

1. Click the Source Field and edit the Source Object
Select Finance App Security Group

1. Select **Security Group** from the **Object Type** drop down menu
2. Select the **Finance App** security group
3. Click the **Arrow** icon to move the object to the **Selected Objects** list
4. Click **SAVE**

Edit Destination Object

1. Click the Destination Field to edit the Destination Object
Select HR App Security Group

1. Select **Security Group** from the **Object Type** drop down menu
2. Select the **HR App** security group
3. Click the **Arrow** icon to move the object to the **Selected Objects** list
4. Click **SAVE**

Edit Action Settings

1. Hover of the right hand side of the **Action** cell of the Firewall rule, and click the Action Field to edit the action from **Allow**
Select Block Action

1. Select **Block** from the **Action** drop down menu

Publish Changes

1. Click **Publish Changes** to deploy the new firewall rules to the effected VMs and hosts.

Verify Collapsed App Tier Rules

Click the + icon to drop down the **Collapsed App Tier Rules** section

1. The new firewall rules do not have a **Rule ID number** until the rules are published to the lab environment.

Note: Your rule numbers may be different depending on the order you take the lab modules.
Validate Finance Application is working

1. Click the tab "HOL- Finance Department"
2. Click the Refresh button
3. Validate you are accessing the Financial Department Cost Centers Database.

Return to Open Remote Console for Finance Web VM

We are now going to test communication between the VM applications after the new firewall rules have been deployed.

1. Click the fin-web-01a.corp.local remote console session on the Taskbar.
Test ping between Finance Web VM to HR App VMs

We will start with testing communication between the Finance web VM and the HR application VMs by sending a ping from `fin-web-01a` to `hr-web-01a`, and `hr-db-01a` by entering the following commands:

1. `ping -c 3 hr-web-01a`

   ```
   # ping -c 3 hr-web-01a
   ```

2. `ping -c 3 hr-db-01a`

   ```
   # ping -c 3 hr-db-01a
   ```

   The **100% packet loss** indicates that the Finance web VM cannot communicate with the HR application VMs on the same L2 network.
Next, we will verify communication between the Finance application VMs by sending a ping from **fin-web-01a** to **fin-app-01a**, and **fin-db-01a** by entering the following commands:

1. **ping -c 3 fin-app-01a**

   ```
   # ping -c 3 fin-app-01a
   ```

2. **ping -c 3 fin-db-01a**

   ```
   # ping -c 3 fin-db-01a
   ```

The **100% success rate** indicates that the all the finance VMs can communicate with each other on the same L2 network.

**Note:** To release your cursor from the remote console window, press **Ctrl+Alt** keys.
Validate the HR Application

1. Click on the tab "HOL - HR Department"
2. Click the **Refresh button**
3. Validate you are accessing the **HR Employee Salary Database**

Return Remote Console to HR DB VM

1. Click the **hr-db-01a.corp.local** remote console session on the Taskbar

Test ping between HR DB VM to Finance App VMs

1. `ping -c 3 fin-app-01a`
2. `ping -c 3 fin-db-01a`
We will now test communication between the HR database VM and the Finance application VMs by sending a ping from `hr-db-01a` to `fin-app-01a`, and `fin-db-01a` by entering the following commands:

1. **ping -c 3 fin-app-01a**

```
# ping -c 3 fin-app-01a
```

2. **ping -c 3 fin-db-01a**

```
# ping -c 3 fin-db-01a
```

**Note:** the **100% packet loss** indicates that the Finance web VM cannot communicate with the HR application VMs on the same L2 network.

**Test ping between HR App VMs**

Last, we will verify communication between the HR application VMs by sending a ping from `hr-db-01a` to `hr-web-01a`, and `hr-app-01a` by entering the following commands:

1. **ping -c 3 hr-web-01a**

```
# ping -c 3 hr-web-01a
```

2. **ping -c 3 hr-app-01a**

```
# ping -c 3 hr-app-01a
```
You will be able to have traffic between the app tiers.

3. **Close the console window to hr-db-01a. Note:** To release your cursor from the remote console window, press **Ctrl+Alt** keys.

This concludes our verification of application isolation via the Distributed Firewall. Even though the HR and Finance applications reside on the same layer 2 logical switch, we have prevented communication between them.

**Lab Clean Up prior to moving to next Lab Module**

Before proceeding to the next module, we must first clean up the firewall rules.

1. Click the *vSphere Web Client*(Flash) browser tab.

**Deleted Collapsed App Tier Section**

1. Select the box for all Rules related to "**Collapsed App Tier Rules**" section to delete the entire section
2. Select **DELETE**

**Prompt for Rule Deletion**

1. Select **YES** when the new window prompt to confirm deletion of the rule section
1. Click Publish Changes to save the changes to the firewall rules and remove the firewall rules from the application VMs.
Module 2 - Conclusion

This now completes Module 2, a guided walk through of application isolation with NSX Distributed Firewall (DFW) for a single flat network. In this module, we showed how collapsing a 3-tier network application into a single NSX Logical Switch does not impact how NSX provides zero-trust security via the Distributed Firewall. We started this lab with verifying communication between the HR and Finance application VMs on the same network. Then we created firewall rules with logical groupings of VMs to protect and prevent communication between the HR and Finance applications, and verified the enforcement of the rules we created by testing VM communication across and within the application stacks. After verifying the applications were isolated from each other, we deleted our firewall rules to prepare for another module of the lab.

We hope you enjoyed learning about the application isolation and zero-trust capabilities of NSX DFW.

You've finished Module 2

Congratulations on completing Module 2.

If you are looking for additional information on NSX Routing capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL below:

- Go to https://tinyurl.com/y9fe6w8v

Proceed to any module below which interests you the most:

- **Lab Module List:**
  - **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
  - **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
  - **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
  - **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
  - **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application microsegmentation.
• **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

• **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**

How to End Lab

To end your lab click on the **END** button.
Module 3 - Intelligent Grouping (30 minutes)
Intelligent Grouping

Module 3 Intelligent Grouping

Introduction

**The End of Support (EOS)** of major enterprise platforms like Windows XP, Windows 2000 Server, and Windows Server 2003 are a major challenge for organizations running mission-critical applications necessary for day-to-day business. For example, in July 2015, when Microsoft ended support for Windows 2003, it put millions of enterprise servers at risk.

Organizations using Operating Systems that are EOS likely introduced serious security risks into their environments, unless they are fully prepared to migrate to a new platform or put compensating controls in place. Hackers know that platform providers like Microsoft will no longer acknowledge or patch vulnerabilities, so these systems quickly become a favorite target for attacks, and the risks of running an unsupported platform after EOS will increase over time as more issues are found and not patched.

NSX can help mitigate the issue of EOS Operating Systems by providing additional security via the Distributed FireWall (DFW) and Service Composer. In this lab you will use NSX Security Groups to corral windows XP VMs and provide firewall polices to protect them in a simulated environment.

The outline of this module is:

- Create Security Group For Windows XP VM & Security Group for Module 4
- Create IP Set's
- Use Dynamic Inclusion to automatically group Windows XP VM
- Apply Firewall rules to provide protection of Windows XP VM
- Test Windows XP VM access to external networks

Lab Captain:

**Module 3 - James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**
Log on to the End of Support Virtual Machines

Using Windows XP VMs we will determine the current security access to external and internal resources.

Login to the vSphere Web Client

If you are not already logged into the vSphere Web Client:

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Type in **administrator@corp.local** into User name
2. Type in **VMware1!** into Password
3. Click **Login**
Log on to EOS Virtual Machines

1. Select **Home**
2. Select **VMs and Templates**
Launch the VM console for win-xp-01

1. Select win-xp-01.corp.local
2. Select the Summary tab
3. Click to launch the console

Wake up win-xp-01 desktop

Click to wake desktop

1. Click Send Ctrl+Alt+Delete button to log in
Log on to win-xp-01 desktop

![Log on to Windows interface]

1. User name: Administrator
2. Password: VMware1!
3. Click OK

Verify Internal Access

![Mozilla Firefox Start Page]

Launch Mozilla Browser from desktop

1. Click **Customer DB-App** link to launch internal application (Make certain url is https://web-01a.corp.local/cgi-bin/app.py)
Also accept the certificate warning on web-01a if needed. (Advanced -> Add Exception -> Confirm Security Exception.)

**Internal application launches**

We see the Windows XP VM has full access to our internal applications. This is the desired security posture.
Open Command Prompt for External Access

1. Click Start menu
2. Launch Command prompt

If “Command Prompt” icon not shown. Click “Run” and type “cmd” and press Enter to bring up the Command Prompt”

Verify External Access

First you will show that win-xp-01 can reach the external network by pinging a vm external to the defined virtual datacenter. In this case you will use the address of the Main Console (192.168.110.10). This represents the Internet.
As you can see as illustrated by the ping we can reach External Services. This creates a large potential security concern for VMs running End of Support Operating Systems.
Security Group Creation

Now that we see the potential vulnerability of allowing end of support VMs to access external resources we want to find a way to secure them. We will use Security Groups in NSX to quickly identify machines running End of Service (EOS) Operating Systems and secure them using policy enforcement.

Networking & Security - Service Composer

1. Click the vSphere Web Client (Flash) browser tab
2. Click the HOME icon
3. Select Networking & Security
Select Service Composer

1. Click on Service Composer

New Security Group

1. Select the Security Groups Tab
2. Click +ADD for new security group
Name New Security Group

1. Name type: **Windows XP EOS**.
2. Click **Next**.

Define Security Group

1. Select **Computer OS Name**
2. Select **Contains**
3. Enter **Windows XP**
4. Click **Finish**

**Verify Security Group Membership**

The Security Group has been created and has Dynamically included the windows XP VM.

1. Click "Groups and Tags" section to find out what Security Groups are created
2. Notice newly created Dynamic Security Group "Windows XP EOS"
3. Double click the Dynamic Member Sets Criteria

**Validate Dynamic Criteria**

1. Notice field criteria
2. Close once validated
New "IP SET"

**NOTE:** We will first create an IP Set that defines all lab virtual machine infrastructure.

What is an "IP SET"?

"IP Sets" can contain any combination of individual IP addresses, IP ranges and/or subnets to be used as sources and destinations for firewall rules or as members of Security groups.

Please follow the steps below with illustrations that are then to follow:

1. Select: "Groups and Tags"
2. Select: "IP Sets" tab
3. Click **+ADD** to create new IP Set
1. Create new IP Set name: **Internal Services**
2. Select IP Address ranges to add with **+ADD** and choice ranges of **172.16.0.1/18**
3. Create this new IP Set by choosing **ADD** button
Validate IP Set

1. Validate that the New "IP Set" is created

New Security Group with "IP SET"

Please follow the steps below with illustrations that are then to follow with creating new Security Group via Service Composer:

1. Select the **Security Groups** Tab
2. Click **+ADD** for new security group
Name IP Set Security Group

1. Create new Security Group name: **Internal Services**
2. Click on **"3 Select Objects to include"**

Define IP Set Security Group

1. **Internal Services**
2. **Internal Services**
3. **Internal Services**
4. **FINISH**
1. Once new screen shows please select choice for the object type drop down "IP Sets"
2. Select IP Sets object: Internal Services
3. Select Arrow to right with the selected object
4. Click FINISH

**Validate IP Set Security Group**

1. Validate that the New "IP Set" is created with "Internal Services" Security Group
**Limit VM Access**

We will now apply rules to limit VM external access.

**Apply New Policy**

1. Go to **Service Composer**
2. **Security Policies** tab should be selected
3. Select +**ADD** for new Security Policy
New Security Policy

1. Type the name "Security Policy Internal Only Access"
2. Click the "3 Firewall Rules"

Add New Firewall Rule
1. Select **ADD** to create new Firewall Rule

Create Firewall Rule

1. Type Name: **Access Internal Resources**
2. Choose the Action radio button for **Allow**
3. Ensure State is set **Enabled**
5. **Destination** - Select Security Groups choice which will open new window
Define Security Group

1. Select **Internal Services** Security Group
2. Right **Arrow** the selected to be the chosen Object
3. Click **OK** to complete Destination Security Group
Approve Firewall Rule Settings

1. Click **OK** to complete Firewall Rule

Finalilze Firewall Rule Settings
1. Click **FINISH** to complete Security Policy

**Add Firewall Rule**

1. Choose Firewall from Navigation menu

We have created a Security Group to allow Windows XP VM to access the Internal Services (Internal Applications). However we still need to Add an additional rule to allow access between internal services as well as modifying the Default firewall rule to block all other access including External access.

**Edit Section Name**

On the **Firewall configuration** tab.
1. Click **Firewall** to access the firewall rules
2. Select three dots for adding section or rules
3. Click the **Add Section Below** icon

### Name Section for Firewall Rules

1. Create Section Name: **Internal Services to Internal Services**
2. Click **ADD**

### Publish Changes

1. Click **Publish Changes**.
Firewall Rule to the New Section

1. Click three dots for adding to the section
2. Click **Add Rule**

Edit Firewall Rule Name

1. Hover and Click the **Name Field** to Edit the Firewall Name. Type the rule name: **App to App** and select enter with your keyboard.
Define Firewall Rule

Click the Source Field to change Any

1. Select **Security Group** as the **Object Type**
2. Select the **Internal Services** security group
3. Click the arrow to add it to **Selected Objects**
4. Click **SAVE**
Define the Firewall Rule Destination

Click the Destination Field to change Any

1. Select Security Group as the Object Type
2. Select the Internal Services security group
3. Click the arrow to add it to Selected Objects
4. Click SAVE

Verify Firewall Rule
Our new firewall rule will allow our internal application to communicate between Application Tiers.

Verify the **Source** security group is **Internal Services**; the **Destination** security group is **Internal Services**; verify **Action Allow**

1. Click **Publish Changes**

**Modify Default Firewall Rule**

In order to block any unwanted traffic including traffic to external services from the Windows XP EOS VMs, we need to enable blocking on the default firewall rule. The default firewall rule is in the default firewall section.

1. Click to **expand** the **Default Firewall Rule section**. Click the Drop Down on the Action Column of the Default Rule. Select **Block** as the action.
Publish Changes

1. Click **Publish Changes**.
Verify Limited Access from Windows XP VMs

We now have rules in place for the EOS windows XP VMs. We can proceed with testing access to internal and external services.

Reopen Console to win-xp-01

1. Click the browser tab for "win-xp-01"

Verify Internal Services are Allowed

1. Refresh your browser tab for "Customer DB-App".

You will see that the page is refreshed. This is allowed by your firewall rule between Internal Services.
Verify External Access is Blocked

1. Reopen the Command Prompt on the win-xp-01 desktop
2. In the Command Prompt, enter: `ping 192.168.110.10`
3. Verify that external access to the Control Center is now **blocked**

```
ping 192.168.110.10
```

Now we can see that win-xp-01 has access to internal services, but its external access has been completely blocked per the Group Policy.
Module Clean-Up: Set Default Rule to Allow

Select the + to expand the Default Section Layer3.

1. Select the Drop Down field on the Action column of the Default Rule Select the Allow Action

Publish Changes

1. Publish Changes
Module 3 Conclusion

Congratulations on completing Module 3.

In the lab we have seen how using intelligent grouping can quickly containerize End of Support Operating Systems via security groups. Once security groups are in place we can use them to create firewall rules that can both limit access to and from the virtual machines contained within. The Security Groups are a versatile tool and can be reused to change or create new policies as our security requirements evolve.

If you are looking for additional information on NSX Security Groups capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL below:

- Go to https://tinyurl.com/y9fe6w8v

You've finished Module 3

Lab Module List:

- **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
- **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
- **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
- **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
- **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application microsegmentation.
- **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

- Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States
How to End Lab

To end the lab click on the **END** button.
Module 4 - User Based Security with a Jump Box (45 minutes)
User Based Security in a Jump Box Scenario

Module 4

User Based Security in a Jump Box Scenario.

Introduction

In this Lab Module, you will create firewall rules using the NSX Identity Based Firewall feature. This feature uses a connection to Active Directory from the NSX manager. The NSX manager scans the event log of the AD Server to determine log on credentials and events. Users logging on to VMs can have their VMs instantly assigned to Security Groups based on their AD groups. The Security Groups combined with firewall rules allow us to control access within our environment.

This lab uses different Active Directory groups and two different users. The first user, a network administrator who should be able to get to any application in the environment and a Human Resources administrator who should only have access to a specific HR web based application.

This is the outline for this module:

- Configure NSX link to Active Directory
- Create Security Groups Based on AD Groups
- Create IP SETS with Security Groups
- Add Application Rules for Internal Applications
- Verify and Test AD Based Rules

Lab Captain:

Module 4 James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States
Explore Link between NSX and Active Directory

NSX links with Active Directory to use AD groups to provide identity based firewall rules.

Launch Browser and vSphere Web Client(Flash)

- Double click on Chrome icon on the desktop.

Login to the vSphere Web Client(Flash)

If you are not already logged into the vSphere Web Client(Flash):

(The home page should be the vSphere Web Client. If not, Click on the vSphere Web Client Taskbar icon for Google Chrome.)
1. Type in **administrator@corp.local** into User name
2. Type in **VMware1!** into Password
3. Click **Login**

**Explore Link between NSX and Active Directory**

![NSX Manager Interface]

1. Click on **Home** icon
2. Click on **Networking & Security**

**Select NSX Manager**

![NSX Manager Interface]

1. Click on **NSX Home**
2. Click on **NSX Manager**
Explore Domain Connector

1. Click on **Users and Domains**
2. Click on **Domains tab**
3. Click on **Green + Sign** to add domain

This connection requires you to provide AD information so that vCenter can access AD for group information. NOTE: This is different from associating a vCenter to AD for permissions used in Users/Roles.

**Provide NetBIOS Name**

For the name field you would enter a name. You would next enter the NetBIOS name for the domain.
1. Fill in for Domain Name: \textit{corp.local}
2. Fill in for NetBIOS Name: \textit{corp}
3. Click \textit{Next}

Provide LDAP Options

Here, you will complete the configuration.

1. Enter a Server address of \textbf{192.168.110.10}
2. Enter User Name: \\	extit{“administrator”}
3. Enter \textbf{VMware1!} for the password
4. Click \textit{Next}
Security Event Log Access Options

Here you would enter settings for the log access and leave the choice of YES for logs available

1. **Uncheck** the **Use Domain Credentials** box
2. Enter **administrator** and **VMware1!** for the Credentials
3. Click **Next**

Ready to Complete - Verify Settings
Now you would verify all your settings.

1. Click **Finish**

**AD Synchronization**

1. Notice Successful AD Sync

Note this may take 2-3 minutes to succeed.

With a configured and synchronized AD connection you are ready to make use of the AD Groups in your security policies.
NSX Guest Introspection

Before creating Identity Based Firewall (IDFW) rules, we will need to configure NSX Guest Introspection.

Networking & Security Navigation

1. Click Home icon.
2. Click Networking & Security

Guest Introspection Deployments

1. Select Installation and Upgrades
2. Select Service Deployments tab
3. Click + ADD icon to deploy Guest Introspection
Service deployment wizard

1. Select **Guest Introspection** service
2. Click **Next**

Select Cluster to Install
1. Select RegionA01-COMP02.
2. Click Next.

Select Storage and Management Network

1. Leave existing selected values as it may not match the example illustration
2. Click Next
Starting Data Collection

1. Click **Finish**

Validate Install Success

1. Validate that is successful

(Wait a few minutes for the installation to complete and then confirm successful installation to the cluster - may need time and do refresh to change from Unknown to Warning which is acceptable for this lab environment)
Verify Guest Introspection installation on hosts

1. Click **Home** icon
2. Click **Hosts and Clusters**

Verify Cluster Status

1. Expand the **RegionA01-COMP02** cluster
2. Verify the Guest Introspection VM is operational and deployed on the esx-03a.corp.local host
3. Verify the Guest Introspection VM has an IP address assigned
Use Security Objects based on AD Groups

1. In this lab example, Security Objects are defined based on AD group membership and will be used to enforce security policy.

Prerequisite create IP Set & Security Group

Note: Requires creating IP Set and Security Group first if not already completed from Module 3 Intelligent Grouping

New "IP SET"

![VMware vSphere Web Client interface showing steps to create an IP Set and Security Group]

**NOTE:** We will first create an IP Set that defines all lab virtual machine infrastructure

What is an "IP SET"?

"IP Sets" can contain any combination of individual IP addresses, IP ranges and/or subnets to be used as sources and destinations for firewall rules or as members of Security groups.

Please follow the steps below (with illustrations that follow) to create the defined Security Group:

1. From "Home-> Network & Security Select: "Groups and Tags"
2. Select: "IP Sets" tab
3. Click +ADD to create new IP Set
Name IP Set - Internal Services

1. Create new IP Set name: Internal Services
2. Select IP Address ranges to add with +ADD and choice ranges of 172.16.0.1/18
3. Create this new IP Set by choosing ADD button
Validate IP Set - Internal Services

1. Validate that the New "IP Set" is created

New Security Group with "IP SET"

Please follow the steps below with illustrations that are then to follow with creating new Security Group via Service Composer:

1. Select the Security Groups Tab
2. Click +ADD for new security group
Name IP Set Security Group

1. Create new Security Group name: **Internal Services**
2. Click on "3 Select Objects to include"

Define Security Group with IP Set criteria
1. Once new screen shows please select choice for the object type drop down "**IP Sets**
2. Select IP Sets object: **Internal Services**
3. Select **Arrow** to right with the selected object
4. Click **FINISH**

**Validate IP Set with new Security Group**

![Image of IP Set with new Security Group]

1. Validate that the New "**IP Set**" is created with "**Internal Services**" Security Group

**Create New Firewall Rule Section (Security Object based with Active Directory Groups)**

![Image of Firewall Rule Section]

1. Click the **Firewall** link on the navigation pane
2. Select **three dots**
3. Click the "**Add Section Above**" icon on the "**Flow Monitoring & Traceflow Rule section**"
AD-Group Firewall Rule Section

1. Name the new section **AD Based Firewall Rules**
2. Click **ADD**

Add Rule Net-Admin

1. Select **three dots** on "AD Based Firewall Rules"
2. Click the **Add rule** icon on the newly created rule section

Rename New Rule

1. Click the **field** on the **Name** column to edit the new rule
Name Rule

1. Type name: **Network Admin Access** and hit enter on your keyboard to have it saved

Select Source Rule - Network Admin Access

You are going to add a Domain Group to the Source field of the Network Admin rule.

1. Hover on to source field and click on the **Field** to change from **Any**

Define Source Network Admin Access
1. Select Security Group in the Object Type pull-down
2. Click on New Security Group.

Name New Security Group - Net-Admin

1. Enter Net-Admin for the name
2. Click on Define Dynamic membership

Define Dynamic Membership

1. Ensure the first line shows "Entity" and "Belongs to"
2. Click the blank line to bring up "Select Entity" screen
Choose AD Group

1. Select type "Directory Group"
2. Type "app" in search box
3. Select "AppConfiguration"
4. Click on "OK"

Complete AD Group

1. Click Finish
Verify Security Group Selection

1. Click **SAVE**

Edit Rule Destination

1. **Hover and Click Destination Field** in the Destination Column of the new created rule
Select the Internal Services Security Group (* Requires creating IP Set and Security Group from Module 3 Intelligent Grouping)

1. Select **Security Group** from the Object type Pull down menu
2. **Select** the previously created **Internal Services** IP-Set security group
3. **Click** the **Right-arrow icon** to add it to the Selected Objects
4. **Click SAVE**

The "Internal Services" security group is made up of all the VMs in the internal environment. This rule will allows the admin to connect to any application and or any VM in the internal environment.
Verify Rule Settings.

The new rule should Allow Net-Admin (AppConfiguration AD group members) to access Internal Services (all internal applications) using Any Service.

1. Click Publish changes

Add Rule HR-Admin

1. Select three dots on "AD Based Firewall Rules"
2. Click the Add rule icon on the newly created rule section

Edit Newly Created Rule

1. Click the field on the Name column to edit the new rule
Name Rule

1. Type name: **Human Resources Access** and hit enter on your keyboard to have it save

Select Source Firewall Rule

You are going to add a Domain Group to the Source field of the HR-Admin rule.

1. Hover over the source field and click on the **Field** to change from **Any**
Define Source Firewall Rule

1. Select **Security Group** in the Object Type pull-down
2. Click on **New Security Group**

Name New Security Group - HR-Admin

1. Enter **HR-Admin** for the name
2. Click on **Define Dynamic membership**
Define Dynamic Membership

1. Ensure the first line shows "Entity" and "Belongs to"
2. Click on the blank line to bring up the "Select Entity" screen

Choose Directory Group

1. Select Type "Directory Group"
2. Type "Hr" in search box
3. Select "HResources"
4. Click on "OK"
Complete Security Group Creation

1. Click on "Finish".

Verify Security Group Selection
1. Click SAVE

**Edit Rule Destination**

1. Hover and Click Destination Field in the Destination Column of the new created rule

**Define Destination selection**

HR Admins should only have access to the HR web application.

1. Select Virtual Machine from the Object type Pull down menu.
2. Enter "web" in search field.
3. Select hr-web-01a from the Available Objects window.
4. Click the arrow icon to add it to the Selected Objects.
5. Click SAVE
Define Service

1. Hover and Click the **Field to edit Service**

**Limit the Allowed services.**

HR Admins should only have access to the applications via web access. (HTTP and HTTPS)

1. Confirm **Service** is shown in the **Object type Pull down menu**
2. Type **http** in to the search window
3. Select **HTTP** and **HTTPS** from the Available Objects window
4. Click the **arrow icon** to add it to the Selected Objects
5. **Click SAVE**
Verify Rule Settings.

The new rule should Allow **HR-Admin (Human Resources AD group members)** to access the **HR and Web Applications** using **HTTP and HTTPS Services**.

1. Click **Publish** changes
Define Internal Application Firewall Rules

Internal applications in this lab will require additional rules to allow for communication between application tiers.

Add Additional Firewall Rules

We have created a AD based firewall rules to allow HR admins and Net admins to access the appropriate applications based on there role. However, we still need to Add an additional rule to allow access between internal services as well as modifying the Default firewall rule to block all other access including External access.

1. Click **Firewall** to access the firewall rules.
New Section Below

On the Firewall configuration tab

1. Click the three dots area on the "Flow Monitoring & Traceflow Rule Section"
2. Select "Add Section Below"

Name Section Rule Internal Services to Internal Services

1. Type Name: Internal Services to Internal Services
2. Click ADD
Publish Changes

1. Click **Publish** changes

Add rules to the New Firewall Section

1. Click on three dots from section "**Internal Services to Internal Services**"
2. Click **Add Rule**
Name App to App

1. Click on new rule and rename to "App to App"

Select the Source Field

1. Click the Source Field to change from "Any" in the Source column
Define the Source Field

1. **Select** Security Group as the **Object Type**
2. **Select the "Internal Services" security group** (*This Security Group was created in Module 3 - Security Group Creations and also discussed earlier in this lab module as a Prerequisite task)*
3. **Click the arrow** to add it to Selected Objects
4. **Click SAVE**

Select the Destination - App to App

1. **Click the Destination Field** in the Destination column
Define the Destination - App to App

1. Select Security Group as the **Object Type**
2. Select the "**Internal Services**" security group
3. **Click the arrow** to add it to Selected Objects
4. **Click SAVE**

Verify Firewall Rule

Our new firewall rule will allow our internal application to communicate between Application Tiers.
1. Verify the Source and Destination are security group "Internal Services"
2. Verify Action Allow
3. Click Publish changes

Modify Default Firewall Rule

In order to block any unwanted traffic we need to enable blocking on the default firewall rule. The default firewall rule is in the default firewall section.

1. Click the Drop Down Action column of the Default Rule then Select Block as the action and then enter on your keyboard to ensure chosen

Publish Changes

1. Click Publish changes
Testing User Identity Based Rules

In order to test the newly created rules we must log on to the win12-jump VM with different user AD credentials.

Test User Identity Rule

You can test the new Identity based rules by opening a console to the Jump Box (win-12-jump) VM in the domain and logging in as a member of the Active Directory AppConfiguration group or the Human Resources group. User Netadmin is a member of the AppConfiguration group and therefore can login into any internal application or application tier. User HRadmin is a member of the Human Resources group and can only login into HR web application and the Financial web application. You will login as each and see the results of trying to access the multiple 3-tier applications.

1. Clicking on the Home icon
2. Click on the VMs and Templates
Open Console to Jumpbox

1. Expand Misc VMs
2. Right Click on "win12-jump"
3. Click on "Open Console"

Login in as HRadmin
1. Send **Ctrl-Alt-Del**. Use the console button
2. Click the **Left Arrow**
3. Choose **Other user**
4. Enter User name = **hradmin**
5. Password = **VMware1!**
6. Click on the **arrow**

**Open Chrome browser**

![Chrome Browser Icon]

1. Start **Chrome Browser** from desktop icon

**Launch the HR DB App**

![HR Employee Salary Database]

Accessed via: hr-web-01a

<table>
<thead>
<tr>
<th>Last Name</th>
<th>First Name</th>
<th>Department</th>
<th>Salary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watson</td>
<td>Daniel</td>
<td>NSBU</td>
<td>$750,000</td>
</tr>
</tbody>
</table>
1. Click on the bookmark, "HR DB App"

User HRadmin is part of the Hresources domain group and is **ONLY** allowed to access the HR Medical application.

**Attempt to launch the Finance DB App**

![Image of Finance DB App failing to load](image)

1. Click on the bookmark, **Finance DB App**.

This link will **FAIL**. Again user HRadmin is part of the Hresources domain group and is **ONLY** allowed to access the HR Medical application.

**Log Off as HRadmin**

![Image of log off process](image)

1. Click on Send **Ctrl-Alt-Del**
2. Click **"Sign Out"**
Switch to other user

1. Click on **Send Ctrl-Alt-Del**
2. Click on "**Other user**"

Login in as **NetAdmin**

1. Enter User name = **NetAdmin**
2. Password = **VMware1!**
3. Click on the **arrow**
Open Chrome browser

1. Start Chrome Browser from desktop icon

Launch the HR DB App

1. Click on the bookmark, "HR DB App" APP

User NetAdmin is part of the AppConfiguration domain group and is allowed to access all applications
Launch the HOL-Finance App

1. Click on the bookmark, "Finance DB App"

User NetAdmin is part of the AppConfiguration domain group and is allowed to access all applications.

Launch the Customer DB App

1. Click on the bookmark, "Customer DB App"
User NetAdmin is part of the AppConfiguration domain group and is allowed to access all applications

You can close the console to jumpbox

**Module 4 Clean-Up: Set Default Rule to Allow**

Expand the Default Section Layer3

1. Select the Drop Down field on the Action column of the Default Rule **Select the Allow Action**

**Publish Changes**

1. **Publish** Changes
Module 4 Conclusion

Congratulations on completing Module 4.

In the lab we have seen how using Identity Based Firewall features within NSX we can control access to internal applications. We created AD based firewall rules for both a Network Administrator and a Human Resources Administrator. These rules allow the HR admin to only connect to the HR web application via HTTP protocol. The rules also allow the Network Admin to connect to any of the applications via any protocol. In this way we can control access to the correct applications with the correct level of privilege based on roles within the organization.

You've finished Module 4

If you are looking for additional information on NSX Identity Based Firewall capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL below:

- Go to https://tinyurl.com/y9fe6w8v

Proceed to any module below which interests you the most:

- **Lab Module List:**
  - **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
  - **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
  - **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
  - **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
  - **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application microsegmentation.
  - **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

- **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**
How to End Lab

To end the lab click on the **END** button.
Module 5 - NSX
Application Rule Manager
(30 minutes)
Application Rule Manager Introduction

The Application Rule Manager (ARM) is a new toolset introduced in NSX 6.3. Application Rule Manager utilizes real-time flow data to enable quick and efficient micro-segmentation planning and implementation of Zero Trust security models. ARM provides a new way to help secure new or existing applications on scales larger than what Log Insight can handle, and environments on a smaller scale than what vRealize Network Insight (vRNI) would address.

ARM gathers real-time flow data both IN, OUT and between application workloads allowing for the creation of app-centric security models. ARM can monitor up to 30 VMs per session and a total of 5 sessions can be running at any given time. ARM also provides visibility into blocked flows and the firewall rules that are blocking the traffic.

There are three steps in the application rule manager workflow:

1. Select virtual machines (VMs) that form the application and need to be monitored. Once configured, all incoming and outgoing flows for a defined set of VNICS (Virtualized Network Interface Cards) on the VMs are monitored. There can be up to five sessions collecting flows at a time.
2. Stop the monitoring to generate the flow tables. The flows are analyzed to reveal the interaction between VMs. The flows can be filtered to bring the flow records to a limited working set.
3. Use flow tables to create grouping object such as security groups, IP sets, services and service groups and firewall rules.

Application Rule Manager 6.4 introduces:

- Auto-recommendations for DFW rules based on Flow data
- Automatic Intelligent Object grouping
- Application and Protocol Identification built-in

Notice the new benefits of ARM 6.4 are being used in this lab module:

- Additional context gained from Flow data for even further granular security controls
- Easier to Micro-segment applications for Day 2 operations
- Faster time to value

Lab Captain:

Module 5 - James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States
Application Micro segmentation

In this lesson, we will review some examples of the new changes to Application Micro-Segmentation in NSX 6.4.x.

Launch Chrome Browser and vSphere Web Client

1. Double-click on Chrome icon on the desktop
Login to the vSphere Web Client

If you are not already logged into the vSphere Web Client (Flash):

(The home page should be the vSphere Web Client. If not, click on the vSphere Web Client Taskbar icon for Google Chrome.)

1. Type in administrator@corp.local in to User name and Type in VMware1! into Password
2. Click Login
1. Click the **Home** menu
2. Select **Networking & Security**

**Select Flow Monitoring**
1. Select **Flow Monitoring**
2. Notice the active "Top Flows" being collected (Activity may vary depending on what lab modules have been completed)

**Create Live Flow - Flow Monitoring**

Next we will create a live flow.

**Live Flow**

![Flow Monitoring UI](image)

1. Select **Live Flow** tab
2. Click "**Select vNIC**"
1. Type **hr** to filter the search
2. Double-click "**hr-web-01a_corp.local**"
Select vNIC

1. Select "hr-web-01a_corp.local" Network adapter 1
2. Click "OK"

Start Monitoring

1. Click "START"
Stop Monitoring

1. Click "STOP"

Results
Notice Example Source and Destination captured from Live Monitoring

**Application Rule Manager with "Auto-recommendations" - Start New Session for HR Application**

1. Select **Application Rule Manager** from Navigator menu
2. Click **+Start Session** to start collecting application flow data

**Start New Session**

Fill in the Start New Session window with the following information:
1. Session Name: **HR_DB_App**
2. Verify that **Object Type** is set to **Virtual Machine**
3. In the Search field, type **HR**

### Select the HR VMs

![Start New Session](image)

1. Tick the box next to each of the three **HR virtual machines** *(hr-web-01a.corp.local, hr-db-01a.corp.local, and hr-app-01a.corp.local)*
2. Click the **right arrow** to move the three virtual machines to the **Selected Objects** box
3. Click **Start**

### Create Some Traffic Flows - ICMP

Application Rule Manager is now collecting flow data from the three HR_App virtual machines. The longer the collection process runs, the more data you will have to analyze. For our purposes, we will collect flow data for three minutes.
Open PuTTY

1. From the taskbar, click the PuTTY icon.
2. In the list of Saved Sessions, double-click on hr-web-01a.corp.local (you will have to scroll down to see it).
Ping

1. Type `ping -c 2 172.16.60.12`

```
ping -c 2 172.16.60.12
```

NOTE: Do not close your PuTTY session as you will be using it later.
Windows Command Prompt

1. Open the **Command Prompt** on the Main Console
2. Type `ping 172.16.60.10`

```
ping 172.16.60.10
```
Create More Traffic Flows - HTTPS

1. Open a new **Chrome browser tab**
2. Click the ‘>>’ and select the **HR DB App** bookmark.

Refreshing the Page

1. **Refresh** the page several times to generate more traffic flows.
Data Collection Session Capture

Within three minutes, you will see Flows in the Flow Monitoring console. The number of flows will vary in each lab.

1. Back in the vSphere Web Client, ensure Application Rule Manager is selected from Navigator menu.
Stop Data Collection

1. Ensure "HR_DB_App" Session is selected
2. Choose STOP to review captured flow information

Confirm Stop

1. Click STOP to confirm
Review Flow Data

Within three minutes, you will see Flows in the Flow Monitoring console. The number of flows will vary in each lab.

1. Select the "HR_DB_APP Virtual Machines" Session
2. Select Analyze

Analyze Session

1. Select "OBJECT" based rules for recommendation for this lab
Wait for Analysis to Complete

1. Wait for the analysis to complete. The time will vary based on the amount collected
2. Click the selection "HR_DB_APP" Session

View Results
1. Notice ARM Recommended Rules that could be implemented ASAP that can be exported or published to the firewall from this activity:  
   Here we can see source and destination IPs as well as services like HTTP, HTTPS, etc.

**Start New Session for Finance_DB_App**

Before we analyze the data collected for HR_App, we will configure a second session for Fin_App in order to demonstrate collecting multiple data flow sessions.

**Return to Main Screen**

![Application Rule Manager](image)

1. Click the '<' to return the Application Rule Manager main screen.

**Start Session for Finance_App Virtual Machines**

![Application Rule Manager](image)

1. Click Start Session
Select Finance_App Virtual Machines

Fill in the Start New Session window with the following information:

1. Session Name: **Finance_DB_App**
2. Verify that **Object Type** is set to **Virtual Machine**
3. In the Search filed, type **fin**
Select the Finance VMs

1. Tick the box next to each of the three Finance virtual machines (fin-web-01a.corp.local, fin-db-01a.corp.local, and fin-app-01a.corp.local)
2. Click the right arrow to move the three virtual machines to the Selected Objects box
3. Click Start
Finance_App Data Collection

1. Wait a minute or two until you see a few flows appear.
2. Select Finance_DB_App
3. Select STOP

Confirm Stop

1. Click STOP to confirm
Analyze Finance_DB_App

1. Ensure "Finance_DB_App" is still selected
2. Click "ANALYZE"

Analyze Session

1. Ensure Object based rules for recommendations is selected
2. Click the "ANALYZE" button
Review Sessions

We can now see that Application Rule Manager has successfully collected flow data for both the **HR_DB_App** and **Finance_DB_App** virtual machines.

Review Sources

1. Click on **Details** to review vNICs being monitored.
## Review Flow Duration

1. Notice **Flows** with collection time and duration

### HR_DB_App Flows

1. Click on **HR_DB_App**
1. Click the **Flows** tab
2. After analyzing and processing flow data, NSX has replaced the IPs with VM names, making it easier to logically map flows between objects.
HR-DB IP Address

1. Find an entry for `hr-db-01a_corp.local` in the Destination column and click on it.
2. Note the IP Address. It should be **172.16.60.12**
3. Click the 'X' to close the window.
PuTTY Session

We will use the information ARM has given us to micro segment virtual machines within and between HR_DB_App & Finance_DB_App. Let's see if hr-web-01a can communicate with hr-db-01a.

Go back to your PuTTY session to hr-web-01a.corp.local. If you closed it, you will need to open it again and reconnect.

Ping 172.16.60.12 by typing:

```
ping -c 2 172.16.60.12
```

We just verified that the HR_DB_App web-01a virtual machine can communicate directly with the db-01a virtual machine. This is not an ideal situation! Next, we will configure appropriate firewall rules to control traffic between the 3-tiered virtual machines.
New Firewall Rules from "ARM Rule Planning"

1. Ensure **Application Rule Manager** is selected from Navigator Menu
2. Select created session "**HR_DB_APP_Virtual**"
3. Select "**Rule Planning**" tab

**Update Pre-Created Rule**

1. Find pre-created rule with the flow with Source (**192.168.110.10**)
2. With pre-created rule with Destination (**hr-web-01a.corp.local**)
3. With pre-created rule with Service (**SSH**)
4. Select "**ARM-Recommended**" rule to rename
1. Name: **Control Center to HR_Web** then hit enter on your keyboard to save changes

**Add HTTPS**

1. Move your mouse over SSH and click on the edit icon.
Specify Service

1. Enter https in the search field
2. Scroll down until you see HTTPS
3. Tick the box next to HTTPS
4. Click the right area to add HTTPS to the Selected Objects box
5. Click Save
Review recommended ARM Security Group

1. Select "Save"

Verify Security Group

1. Click on ARM in the Applied To column for "Control Center to HR_Web"
Validate Virtual Machines

1. **Validate** that the group has the three HR virtual machines; hr-web-01a, hr-db-01a and hr-app-01a.

Note that you will need to use the scroll bar to see all three virtual machines.

Modify recommended ARM Security Group

1. Ensure "HR_DB_APP Virtual Machines" ARM Session has been selected
2. Select "Security Group" tab under Rule Planning
Edit ARM Security Group

1. Select the first ARM Generated security group to rename
2. Choose to Edit selected security group

HR_Machine_SG

1. Rename existing Security Group to "HR_Machine_SG"
2. Click the Select Objects to Include step
1. Validate that the objects in this security group include "hr-app01a, hr-db-01a, hr-web-01a". If you only see hr-db-01a and hr-web-01a on the list, click Cancel and select the other ARM security group in the list.

2. Click Finish

Modify recommended ARM Security Group #2
1. Select the second **ARM** Generated security group to rename
2. Choose to **Edit** selected security group

**HR_Machine_DB_WEB**

1. Rename existing Security Group to "**HR_Machine_DB_WEB**"
2. Click the **Select Objects to Include** link
Validate Virtual Machines

1. Validate that the objects in this security group include "hr-db-01a, hr-web-01a"
2. Click the Finish button

Validate ARM configuration changes
1. Notice the names changed from previous steps

**Firewall Rules**

![Firewall Rules Tab](image1)

1. Click on the **Firewall Rules** tab

**Validate ARM firewall changes**

![Control Center for HR_WEB Firewall Rule](image2)

1. Notice changes to **Control Center for HR_WEB** firewall rule

*NOTE: You may have to refresh to see the change.*
Configure HR_Web to HR_App Firewall Rule

1. Select the row that lists hr-app-01a as the Destination and hr-web-01a as the Source
2. Click the Name Field to rename generated ARM name

New Firewall Rule: HR_Web to HR_App
1. Rename: **HR_Web to HR_App** and press enter on keyboard
2. Leave everything else as default and click **SAVE**

**Configure New Firewall Rule: HR_App to HR_DB**

1. Select the row with **hr-db-01a** as the Destination and **hr-app-01** as the Source
2. Click Name Field to rename generated ARM Firewall Rule

**New Firewall Rule: HR_App to HR_DB**

1. Rename: **HR_App to HR_DB** and press enter on keyboard
2. Leave everything else as default and click **SAVE**
Publish Firewall Rules

1. Click **Publish To Firewall**

Firewall Publish
1. In the **Section Name** field, enter **HR_DB_APP**
2. Click **OK**

**Review HR_DB_App Firewall Rule**

Here, we can review the firewall rules we just configured in Application Rule Manager. Next, we will test the HR_DB_App to make the web page still resolves and unsecured traffic has been blocked.
Expand Default Section

1. Click the '+' to expand the Default Section Layer3 section.
2. Scroll down until you see the Default Rule

Block Traffic
1. Under the **Default Rule** and in the **Action** column (you may have to scroll to see it), change the rule from **Allow** to **Block**. Press **Enter** on the keyboard

**Publish Changes**

1. Click the **Publish** button

**Verify HR_DB_App is working**

If you closed the HOL-HR Department tab:

1. Open a new Chrome browser tab
2. Click on the **HR DB App** bookmark.

You should be able to see the **HR Employee Salary Database**.
Testing Access

Go back to your command prompt. If you closed, you will need to open the command prompt again.

Let's test if we can successfully ping the web, application, and database servers from the Main Console:

1. ping 172.16.60.10
2. ping 172.16.60.11
3. ping 172.16.60.12

Now we can see that ICMP traffic is being blocked. The only allowed traffic is HTTPS.
Note: In this lab, we configured the web-01a firewall rule to allow SSH so we can access the virtual machine via Putty to do the next test.

Next, go back to the SSH session to hr-web-01a.

**Open Putty**

1. ping -c 2 172.16.60.12
2. After about 10 seconds, enter Control+C to terminate.

Now we can see traffic from the **web-01a** to **db-01a** has been blocked!

```
ping -c 2 172.16.60.12
```

**Module 5 Clean-Up: Set Default Rule to Allow**

**Expand the Default Section Layer3**

1. Select the Drop Down field on the Action column of the Default Rule **Select the Allow Action**
Publish Changes

1. Publish Changes
Module 5 Conclusion

You've finished module 5

Congratulations on completing Module 5!

If you are looking for additional information on NSX Application Rule Manager capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL below:

- Go to [https://tinyurl.com/y9fe6w8v](https://tinyurl.com/y9fe6w8v)

Proceed to any module below which interests you the most:

- **Lab Module List:**
  - **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
  - **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
  - **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
  - **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
  - **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application microsegmentation.
  - **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

- **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**

How to End Lab

To end the lab click on the **END** button.
Module 6 - NSX
Troubleshooting & Maintenance (30 Minutes)
NSX Troubleshooting & Backups with vRealize Network Insight Overview

How is my NSX environment doing? I logged into vRealize Network Insight (vRNI) and noticed multiple active events among other items that could be reviewed such as Micro Segmentation, Application, Network, and VM Security. This lab provides numerous sample real time events. One example shows quickly backup risks outlined from the configured lab vRNI / VMware NSX environment.

Why use vRealize Network Insight (vRNI)?

VMware vRealize Network Insight helps customers build an optimized, highly available and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation deployment, minimizes business risk during application migration and enables customers to confidently manage and scale NSX deployments.

Why NSX Backup and Restore?

Proper backup of all NSX components is crucial to restore the system to its working state in the event of a failure. The NSX Manager backup contains all of the NSX configuration, including controllers, logical switching and routing entities, security, firewall rules, and everything else that you configure within the NSX Manager UI or API.

At a minimum, we recommend taking regular backups of NSX Manager and vCenter. However, all VMware invested products are recommended to have a backup strategy.

Your backup frequency and schedule might vary based on your business needs and operational procedures. We recommend taking NSX backups frequently during times of frequent configuration changes. NSX Manager backups can be taken on demand or on an hourly, daily, or weekly basis.

We recommend taking backups in the following scenarios:

- Before an NSX or vCenter upgrade
- After an NSX or vCenter upgrade
- After Day Zero deployment and initial configuration of NSX components, such as after the creation of NSX Controllers, logical switches, logical routers, edge services gateways, security, and firewall policies
- After infrastructure or topology changes
- After any major Day 2 change

VMware NSX Backup guide defined at the following: [https://tinyurl.com/y98d98nd](https://tinyurl.com/y98d98nd)
VMware Best Practices for VMware NSX 6.4.x are referenced at the following: https://tinyurl.com/ycfy45sz

Lab Activities

This lab will provide the following tasks to be completed in this order:

1. Quick Overview of vRealize Network Insight environment
2. Validation Overview of vSphere Web “Flash” connection to vCenter / NSX environment
3. Backup Configuration via NSX Manager
4. Updated changes reviewed via vRealize Network Insight
5. vRealize Network Insight NSX changes to environment - Security Group & Firewall examples

Lab Captain:

Module 6 NSX Troubleshooting & Backups with vRealize Network Insight

- James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States
This lab is configured to run all tasks from "Main Console" machine as illustration:

1. Verify that you are connected to "Main Console" and "HOL-1903" is the defined lab that is displayed

2. Select web browser "Google Chrome" for access to this labs tasks
vRealize Network Insight Login

1. Select Bookmark "vRealize Network Insight" from Google Browser
3. Log into vRNI with User name: admin@corp.local Password: VMware1!
4. Click on button "Login"

vRealize Network Insight review of "Operate and Troubleshoot" dashboard
"Operate and Troubleshoot" dashboard in illustration

1. Notice alerts from home page of vRealize Network Insight “Operate and Troubleshoot”
2. NSX Manager backups are not enabled and click on event for more details

View the Event Details

1. The Event Details list pertinent information about the selected event.
vCenter Login

vCenter review of "Network & Security as illustrated:

1. Select Bookmark "vSphere Web(Flash)" from Google Browser
3. Log into vCenter with User name: administrator@corp.local Password: VMware1!
4. Click on button "Login"
vCenter Review of NSX Manager Backups

vCenter review of “NSX Manager Backups" in illustration:

1. Select “Networking & Security" from the Navigation Menu

vCenter - NSX Manager Backup Review
1. Once logged in then choose "Overview" tab after selecting "Dashboard" and notice Backup Status

**NSX Manager Login**

NSX Manager Configuring Backup Tasks - Login Steps

1. Select Bookmark folder "**HOL Admin**" from Google Browser
2. Select Bookmark "**nsxmgr-01a**" from Google Browser
3. Notice URL of web link: [https://nsxmgr-01a.corp.local](https://nsxmgr-01a.corp.local)
4. Log into NSX Manager with User name: **admin** Password: **VMware1!**
5. Click on button "Login"
**NSX Backup & Restore Button**

![NSX Manager Virtual Appliance Management](image)

NSX Manager Configuring Backup Tasks Illustrated:

1. Click on "Backup & Restore" button from NSX Manager Dashboard

**NSX Backup & Restore FTP Settings**

![FTP Server Settings](image)

Backup & Restore button will open new window for FTP Server Settings as shown:

1. Click on "Change" button to define FTP Server Settings
NSX Backup Configuration

NSX Manager Configuring Backup Tasks - Configuring FTP Server:

1. Fill out Backup Location with the following items:
   - IP/Host name: **192.168.110.91**
   - Transfer Protocol: **FTP**
   - Port: **21**
   - User name: **admin**
   - Password: **VMware1!**
   - Backup Directory: **ftp://192.168.110.91**
   - Filename Prefix: **nsxmgr**
   - Pass Phrase: **VMware1!**

2. Once all fields have been filled out - Click **OK**
FTP Backup Server Validation

1. **Notice** Successful configuration with FTP server

NSX Backup Schedule Change

NSX Manager Configuring Backup Tasks - FTP Backup Schedule

1. Now select **Change** Scheduling

NSX Backup Schedule Frequency

NSX Manager Configuring Backup Tasks - FTP Backup Schedule
1. Choose options as shown:
   - Backup Frequency: **Hourly**
   - Minute: **5**

2. Now select **Schedule** button

**Execute NSX Manager Backup**

![NSX Manager Backup Configuration](image)

**NSX Manager Configuring Backup Tasks - Final Step**

1. Now select **Backup**

**Start Backup**

![Backup Confirmation](image)

1. Additional Window will pop open and ask "Would you like to start a backup process now?" Choose **Start** (Backup will take a few minutes then this task is completed)
vRealize Network Insight - Operate and Troubleshooting

Follow Up

"Operate and Troubleshoot" Follow up review of changes in illustration:

1. Notice alert from home page of vRNI “Operate and Troubleshoot” which have changed since earlier review
2. NSX Manager backups are enabled but not with preferred SFTP choice and click on event for more details

Event Details

1. Notice SFTP Risk around Backups (Before lab tasks there were NO backups but now it is stating that FTP backups were configured)
vRealize Network Insight Security Group NSX changes to environment

"Operate and Troubleshoot" Follow up review of changes in illustration from this main dashboard:

1. Double Click "**NSX Security Group**"

**NSX Security Group Events**

1. Notice filter "**security groups**"
2. Notice example "**RDSH SG1**" as was created in Lab Module 3 or Lab Module 4

(Please note that the name of the Security Groups will be different depending on the examples created in earlier Modules)
"Operate and Troubleshoot" dashboard review of changes in illustration *(Firewall Deletions)*:

1. Click on "**VM - vRealize Network Insight**" on far upper left corner of dashboard
2. Hover over with mouse to select "**Events**"
3. Select "**Delete change**"
vRealize Network Insight - Delete Event

1. Notice Event "Delete Event"
2. Notice example delete events from lab module tasks if completed before doing Module 6 (Requires that Module clean up was executed from previous modules)
NSX Data Center with NSX-PowerOps

Overview

NSX Power Operations is a platform that provides NSX users a way to document their VMware NSX for vSphere environment in Microsoft Excel and Visio files that are easily consumable and referable. The documentation not only captures the desired state (configuration) but also the Realized State (for example: routing & forwarding tables) across the distributed environment. The platform also embeds rich health check tools.

Please note the following link for more details and updates to this tool set by original authors: https://tinyurl.com/ybdsdxf3

There are at least 3 steps in order to use this tool set:

1. Follow complete steps to install the tool set and required supporting applications (This is already completed during HOL-1903-NET Lab)
2. Establish connection from machine where the NSX-PowerOps is installed
3. Choose to complete one of the following tasks
   - **Environment Documentation**
     - Document All NSX Components
     - Document ESXi Host(s) Info
   - **Network Documentation**
     - Document NSX Environment via Visio Diagramming Tool
     - Document Routing Information
     - Document Load Balancing Information
   - **Security Documentation**
     - Document NSX DFW info to Excel via DFW2Excel (small environments)
     - Document NSX DFW info to Excel via DFW2Excel (large environments)

Lab Captain:

Module 6 Section NSX Data Center with NSX-PowerOps - James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States
NSX Data Center with NSX-PowerOps - Lab Tasks

NSX Configuration Review with NSX-PowerOps

Validate NSX PowerOps Location

Establish connection NSX-PowerOps - continued as illustrated (DO NOT use the Quotes in the commands):

1. NSX PowerOps is installed in the following Directory location "c:\NSX-PowerOps\nsx-powerops-master"
Start NSX-PowerOps Tool

Establish connection from machine where the NSX-PowerOps is installed as illustrated:

1. **Right Click** on Icon of the **Windows PowerShell** from shortcut on Main Console Windows Server
2. Select **“Run as Administrator”**
Start Windows PowerShell

1. Change directory from root of C drive with command : "cd nsx-powerops\nsx-powerops-master"
2. While in Windows PowerShell please select `dir` if your would like to validate that directory for NSX PowerOps has been installed as shown
3. Please now type the following command: ".
sx-PowerOps.ps1"

Load NSX-PowerOps

1. Once command is typed then hit enter which will now show executed command (LOADING PowerNSX):
PowerNSX - PowerOps

PowerOPS - PowerNSX is Loaded

Time to Establish Connection to VMware Infrastructure

1. Notice **NSX PowerOps Main Menu**

2. Select then number 2 to establish connection profile (Requirement to complete these tasks  *MUST DO THIS BEFORE DOING ANY OTHER OPTION (Selecting #2)
Establish Connection with NSX-PowerOps

Establish connection from machine where the NSX-PowerOps is installed

1. Select 1 "Create Connection Profile"

Create Default Connection Profile
Begin Default Connection Profile setup

1. Create Connection Profile with steps in the following order as prompts arise and hit enter after each selection
   - Enter NSX Server address: 192.168.110.42
   - Enter NSX username: admin
   - Enter NSX password: VMware1!
   - Enter vCenter username (vcsa-01a.corp.local): administrator@vsphere.local
   - Enter vCenter password: VMware1!
   - Enter a unique connection profile name: 192.168.110.42

Save new Default Connection Profile

1. Additional Settings needed "Default Connection Profile"
   - Passwords can be saved to disk - (Default is N) Choose Y
   - Enter NSX Controller Credentials? Choose Y
   - Enter NSX Controller Password: VMware1!
   - Plugins require ESXi Host Credentials? Choose Y
   - Enter ESXi Host Username: root
   - Enter ESXi Host Password: VMware1!
   - Set this profile as the default? Choose Y
Select Default Connection Profile

Once "Default Connection Profile" has been created and saved it now can be selected to begin using the NSX-PowerOps toolset

1. Select #4 by pressing 4 and the enter key
2. Select X to go back to Main Menu - NSX PowerOps (Not "Connections Profiles")

NSX-PowerOps Tool for Documentation Tasks

![NSX-PowerOps Main Menu > Connection Profiles](image1)

![NSX-PowerOps Main Menu > Documentation Tasks](image2)
Current location will require that last step was successful to ensure toolset is connected to "Default Connection"

If for any reason it is not connected to the "NSX PowerOps Main Menu" then please select X again. Please do not Select Q for quit as it may require Proctor assistance to get connected again for this step

1. Notice Displayed "NSX PowerOps Main Menu"

**PowerOps Documentation Tools**

1. **Choose 4** as we will be doing the task of PowerOps Documentation Tools (Other choices are available but not focused on in this lab)
Validate NSX PowerOps Documentation Location

1. Notice the documentation will be created in the location as stated "C: \ nsx-powerops\nsx-powerops-master\report" as shown illustration

Create DFW2Excel

NSX PowerOps Main Menu - PowerOps Documentation Tools
NOTE: After Selecting #4 in previous step you are now in the selection for Documentation Tools

1. Choice for Lab is to now Select #6 as we will create excel document around this small environment pertaining to Security
2. Notice activity and success of the selection

**Validate Created DFW2Excel**

![Validate Created DFW2Excel Image]

Review NSX-PowerOps Generated Excel Document with Focus on Security Findings

1. Notice that the sample location as was generated by this report *(This location will slightly vary depending on your time of execution)*
2. Notice Generated Excel Document to review

![Excel Document Image]

**Open to Review DFW2Excel**

1. [Open Excel Generated report](#) *(Excel installed for this lab)*

---

Page 263
Review DFW2Excel

1. **Review Environment summary** (Multiple tabs to review but this was just an example as you can review more if time allows during lab)
Module 6 Conclusion

Congratulations on completing Module 6!

You've finished Module 6

If you are looking for additional information on NSX Troubleshooting please review all items in this lab and then be willing to reach out to your local VMware Sales Team whom can contact specialists to meet your expectations. Ask your local Sales team about an NSX Technical Account Specialist.

If you are looking for additional information on NSX Routing capabilities and configuration, then please review the NSX 6.4.x Documentation Center via the URL below:

- Go to https://tinyurl.com/y9fe6w8v

Proceed to any module below which interests you the most:

Lab Module List:

- **Module 1 - Service Composer and DFW Overview** (45 minutes) - Basic - This module will cover the Distributed Firewall and Service Composer creating firewall rules between a 3-tier application.
- **Module 2 - Collapse 3-Tier Application Feature Walk-Through** (15 minutes) - Basic - This module will walk you through the basics of migrating a 3-tier application to a collapsed single tier architecture.
- **Module 3 - Intelligent Grouping** (30 minutes) - Basic - This module will help understand how NSX can help secure applications and virtual machines using dynamic inclusion with security groups.
- **Module 4 - User Based Security with a Jump Box** (45 minutes) - Basic - This module will demonstrate the capabilities of the Identity Based Firewall feature and how it can provide security with Active Directory integration.
- **Module 5 - Application Rule Manager** (45 minutes) - Basic - This module will cover application micro segmentation.
- **Module 6 - NSX Troubleshooting & Maintenance** (30 minutes) - Basic - This module will cover NSX troubleshooting & Backups with vRNI & Example NSX PowerOPs tasks.

Lab Captain:

- **Module (1-6) James Emmons, Staff Technical Account Manager / NSX Technical Account Specialist, United States**
How to End Lab

To end the lab click on the END button.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1903-02-NET

Version: 20190914-211416