# Table of Contents

Lab Overview - HOL-1803-02-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 ......................... 39
  Security Groups Overview ......................................................................................................... 54
  Security Policy Overview .......................................................................................................... 59
  Review of Service Composer Canvas ....................................................................................... 69
  Module 1 - Conclusion ............................................................................................................... 77

Module 2 - Collapse 3-Tier Application Feature Walk-Through (15 minutes) ............ 79
  Securing Collapsed Architectures with NSX's Distributed Firewall Capability ..................... 80
  Module 2 - Conclusion .............................................................................................................. 117

Module 3 - Intelligent Grouping (30 minutes) ................................................................. 119
  Intelligent Grouping ................................................................................................................ 120
  Log on to the End of Support Virtual Machines ...................................................................... 121
  Security Group Creation .......................................................................................................... 129
  Limit VM Access .................................................................................................................... 135
  Verify Limited Access from Windows XP VMs ...................................................................... 149
  Module 3 Conclusion ............................................................................................................... 153

Module 4 - User Based Security with a Jump Box (45 minutes) ............................... 155
  User Based Security in a Jump Box Scenario ......................................................................... 156
  Explore Link between NSX and Active Directory .................................................................. 157
  NSX Guest Introspection .......................................................................................................... 166
  Use Security Objects based on AD Groups ............................................................................ 172
  Define Internal Application Firewall Rules ............................................................................ 188
  Testing User Identity Based Rules ......................................................................................... 194
  Module 4 Conclusion ............................................................................................................... 205

Module 5 - NSX Application Rule Manager (30 minutes) ........................................... 207
  Module 5 Application Rule Manager ...................................................................................... 208
  Application Microsegmentation ............................................................................................. 209
  Module 5 Conclusion ............................................................................................................... 235
Lab Overview -
HOL-1803-02-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.

Lab Captains:

- Module 1 - Chris Cousins, Sr. Systems Engineer, USA
- Module 2 - Chris Cousins, Sr. Systems Engineer, USA
- Module 3 - Chris Cousins, Sr. Systems Engineer, USA
- Module 4 - Chris Cousins, Sr. Systems Engineer, USA

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
- Review the Service Composer Canvas as an interface to show the mapping of Security Policies to Security Groups

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.

**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-1803-01-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.

[Click here to skip to Improved IP Discovery Mechanism for Virtual Machines and SpoofGuard module](#)

**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 via the icon on the desktop labeled, **Google Chrome**.

**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@vsphere.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

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

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**

![Database Table]

You should get back data that passed from the web tier to the app-01a vm and finally queried the db-01a vm.
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**.

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.

Change the default firewall policy from Allow to Block

![vSphere Web Client](image)

**Firewall**

Configuration | Saved Configurations | Settings
---|---|---
NSXManager: | 192.108.110.42 | 

- Flow Monitoring & Traceflow Rules - Disabled By Default (Rule 1)
- Default Section Layer3 (Rule 1 - 4)
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. 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 the Last Default Rule

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 on rule 5. This will bring up a pencil sign that allows you to see the choices for this field.

1. Click on the Pencil icon.
Change the Last Default Rule Action from Allow to Block

Click the drop-down arrow and select the **Block** action

1. **Click Save**

**Publish the Default Rule changes**

This rule set has unused changes. Click on Publish Changes button to start deploying or click Save Changes to save this configuration.

You will notice a green bar appears announcing that you now need to choose either to Publish Changes, Revert Changes or Save Changes. Publish pushes to the DFW. Revert cancels your edits. Save Changes allows you to save and publish later.

1. **Select Publish Change** to save your block rule.
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 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 **New Security Group** icon

**New Security Group - Web**

1. 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.

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. On the far right of the "Flow Monitoring & Trace Flow Rules-Disabled by Default (Rule 1)" row click on Add Section which looks like a folder

Add New Rule Section for 3-Tier Application

1. Name the section "3-tier App"
2. Select Add above
3. Click Save

Add Rule to New Section

1. On the row for the new "3-tier App" section click on the Add rule icon which is a green plus-sign.
Edit New Rule name

1. Click the Drop down arrow to open the rule
2. Hover to the upper right corner of the "Name" field until a pencil icon appears, then click on the pencil

Edit New Rule name cont

1. Enter "Ext to Web" for the name
2. Click Save

Set Rule Source and Destination

Source: Leave the Rule Source set to any.

1. Hover the mouse pointer in the Destination field and select the Destination pencil sign.
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 OK

Destination:

Edit Service

1. Again hover in the Service field and click on the pencil sign.
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. Note: Repeat the above steps 1-3 to find and add SSH. (You will see later in the module that we need SSH.)
5. Click OK

Note: This will cause the green bar with the option to publish or revert changes.

DO NOT Publish yet, as you have more rules to make.
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 opening the pencil sign beside rule ID 1
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
2. Click the pencil to edit.

Create Second Rule Destination field: Choose Logical Network

In the first rule you used the Web-tier security group as the destination. You could proceed with the remaining rules in the same fashion. But as you see 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 you can use existing virtual
datacenter objects for your rules rather having to start from scratch. Here you will use a VXLAN Logical Switch as the destination. This allows you to create 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 AppTier-Logical_Switch**
3. **Click on the top arrow** to move the object to the right
4. **Click OK**

**Create Second Rule Service**

1. **Hover** over the Service Field and **click the pencil** to edit.
Create Second Rule Service Field: New Service

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

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

Repeating the 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**

![Image of vsphere Web Client window with HOL - Customer Database highlighted]

**External Customer Database**

Accessed via: web-01a

<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>
<tr>
<td>8</td>
<td>Frobozz Magic Co.</td>
<td>Zork</td>
<td>$112.9 billion</td>
</tr>
<tr>
<td>9</td>
<td>Warbucks Industries</td>
<td>Lil' Orphan Annie</td>
<td>$61.5 billion</td>
</tr>
</tbody>
</table>

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

1. `ping -c 2 172.16.10.12`
   
   PING 172.16.10.12 (172.16.10.12) 50(84) bytes of data.
   
   --- 172.16.10.12 ping statistics ---
   
   2 packets transmitted, 0 received, 100% packet loss, time 11000ms

2. `ping -c 2 172.16.20.11`
   
   PING 172.16.20.11 (172.16.20.11) 50(84) bytes of data.
   
   --- 172.16.20.11 ping statistics ---
   
   2 packets transmitted, 0 received, 100% packet loss, time 11000ms

3. `ping -c 2 172.16.30.11`
   
   PING 172.16.30.11 (172.16.30.11) 50(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

```
ping -c 2 172.16.10.12
```

app-01a

```
ping -c 2 172.16.20.11
```

db-01a

```
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.
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

You will need to set the Default Rule back to Allow to proceed to the next Module.

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 Settings

Click on the browser tab for the vSphere Web Client

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

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

**Enable IP address discovery via ARP Snooping**

1. Click **Change**

**Change IP detection type to ARP Snooping**

Now we will enable IP address discovery with "ARP Snooping"

1. Check **ARP Snooping**
2. Click **OK**
Edit Default SpoofGuard Policy

1. Click on **Default Policy**
2. Click on **Pencil to edit**

Enable SpoofGuard

1. Click the **Radio button** for **Enabled**
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 to continue.
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
1. Enter "linux" into the Filter
2. Select the **linux-01a** VM
3. Click the **Blue 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

<table>
<thead>
<tr>
<th>Logical Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NSX Manager:</strong> 192.168.110.42</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Virtual Wire ID</strong></td>
</tr>
<tr>
<td>virtualwire-5</td>
</tr>
<tr>
<td>virtualwire-9</td>
</tr>
<tr>
<td>virtualwire-10</td>
</tr>
<tr>
<td>virtualwire-8</td>
</tr>
<tr>
<td>virtualwire-6</td>
</tr>
<tr>
<td><strong>virtualwire-12</strong></td>
</tr>
<tr>
<td>virtualwire-11</td>
</tr>
<tr>
<td>virtualwire-4</td>
</tr>
</tbody>
</table>
1. **Double-click** the new `Linux_Logical_Switch` to view the associated virtual machines.

**View Related Virtual Machines**

![Virtual Machines view](image1)

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

**Open Console to linux-01a VM**

![Console access](image2)

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

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

![Remote Console](image)

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**

![Ifconfig](image)

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**

```bash
ping -c 2 192.168.120.1
```

--- 192.168.120.1 ping statistics ---
2 packets transmitted, 0 received 100% packet loss, time 1243ms

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

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
3. Pick Active Virtual NICs in the View dropdown
4. Enter "lin" and press enter to filter for linux-01a

Notice that the Source Field denotes TOFUARP (Trust On First Use ARP) for the address 192.168.120.115.

Approve Linux-01a new IP Address

- Click Approve

Note: we may have to scroll to the right to view the Approve action
Publish IP Approval

- Click on Publish Changes

View Active Virtual NICs Since Last Published

1. Select **Active Virtual NICs Since Last Published** from the drop down menu

Note: linux-01a is no longer listed because we have approved the IP address for use by that VM, and no activity has originated from the VM since the approval.

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 name VM1

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.
Create the Web Security Group

1. Click the Security Groups tab in Services Composer.
2. Click the New Security Group icon.
3. Enter "Web Security Group" in the Name dialog box.
4. 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**.

---

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**.
View Membership

1. Click the **number** in the **Virtual Machine column** associated with the new **Web Security Group**.

Note: There should **6** in the Virtual Machine column for the Web Security Group, including all VMs with "WEB" in their name, without consideration for capitalization, or IP networks.

2. Click the **X** in the upper right hand corner of the dialog box to close it.
Security Policy Overview

NSX Security Policies can be a collection of the following service configurations, Firewall rules, Endpoint services, 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 the Security Policies tab in the Service Composer panel
2. Click the Create Security Policy icon
3. Type in "Block Web-to-Web Traffic" in the Name field
4. Click Firewall Rules in the left panel
Create a New Firewall Rule

1. Click the Green Plus icon to add a New Firewall Rule
2. Type in "Block Web-to-Web Traffic" in the Name field
3. Select Block from the Action list
4. Click Change... to the right of the Destination: Any
Firewall Rule - Select Destination

1. Select **Policy's Security Group** at the top of the list of options
2. Click **OK**

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.
Click OK

1. Click **OK**
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
3. Select the **Web Security Group**
4. Click **OK**
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 the Firewall Rules have a 1 in the column

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

Next we will 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.
Review of Service Composer Canvas

Service Composer offers a canvas view displaying all security groups within the selected NSX Manager. The view also displays details such as members of each security group as well as the security policy applied on it.

This topic introduces Service Composer by walking you through a partially configured system so that you can visualize the mappings between security groups and security policy objects at a high level from the canvas view.

Graphical View of Service Composer Canvas

1. Click Service Composer
2. Click Canvas

All security groups within the selected NSX Manager (that are not contained within another security group) are displayed along with the policies applied on them. The NSX Manager drop-down lists all NSX Managers on which the currently logged in user has a role assigned.

Each rectangular box in the canvas represents a security group and the icons within the box represent security group members and details about the security policy mapped to the security group.
Applied Security Policy

A number next to each icon indicates the number of instances - for example, the number 1 next to the **Security Policy** icon indicates that a policy is mapped to that **Security Group**.

**Nested Security Groups**

This icon **Security Groups** nested within the main security group. In your Security Group there are no nested groups.
1. Click the **Virtual Machine icon** in the bottom left hand corner of the Canvas.
2. **Close the window**.

Virtual machines that are currently part of the main security group as well as nested security groups. If we had any virtual machines with services errors, we could click on the **Errors tab** to see those virtual machines.
Effective Security Policies mapped to the Security Group

1. Click the **Security Policy icon** in the top right hand corner of the Canvas.

Optional Actions:

- You can create a new security policy by clicking the **Create Security Policy icon**. The newly created security policy object is automatically mapped to the security group.
- Map additional security policies to the security group by clicking the **Apply Security Policy icon**.

2. **Close the window.**

Effective Guest Introspection services

1. Click **Guest Introspection Services icon** to display services associated with the security policy mapped to the security group.
Suppose you have two policies applied to a security group and both have the same category Endpoint service configured. The effective service count in this case will be 1 (since the second lower priority service is overridden).

Note: Guest Introspection Service failures, if any, are indicated in the Errors tab. Clicking the Errors icon displays the issues.

2. Close the Window.

Effective Firewall rules

1. Click the Firewall rules icon to display firewall rules associated with the security policy mapped to the security group.
2. Close the window.
Effective Network Introspection services

1. Click the **Network Introspection Services icon** to display the services associated with the security policy mapped to the security group.

   Note: Again, Network Introspection Service failures, if any, are indicated in the **Errors** tab. Clicking the **Errors icon** displays the issues.

2. **Close the window.**

Search Security Groups

1. Enter "hr" in the search field in the top right corner of the Canvas window to display only the security groups with "hr" in their names.
View Security Group Hierarchy

1. Click the **Top Level icon** at the top left of the window
2. Click the **Internal Services**

This will allow us to see the security group hierarchy, and if a security group contains nested security groups

**View Parent Security Group services**

The top bar displays the name of the parent security group and the icons in the bar display the total number of security policies, endpoint services, firewall services, and network introspection services applicable to the parent group.
1. We can navigate back up to the top level by clicking the blue **Go up one level arrow icon** in the top left part of the window.

**Smooth Zoom In and Out of Canvas View**

You can zoom in and out of the canvas view smoothly by moving the zoom slider on the top right corner of the window. The Navigator box shows a zoomed out view of the entire canvas. If the canvas is much bigger than what fits on your screen, it will show a box around the area that is actually visible and you can move it to change the section of the canvas that is being displayed.
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. Right-click on Block Web-to-Web Traffic row
4. Select the Delete option. When prompted "Remove security policy?", click Yes
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 6.3 Documentation Center via the URL below:

- Go to https://tinyurl.com/zwch3gh

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.

Lab Captain:

- Module 1 Chris Cousins, Sr. Systems Engineer, United States.
- Module 2 Chris Cousins, Sr. Systems Engineer, United States.
- Module 3 Chris Cousins, Sr. Systems Engineer, United States.
- Module 4 Chris Cousins, Sr. Systems Engineer, 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**

![Collapsed Network Topology Diagram]

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

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@vsphere.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 - 5004).
View Connected Virtual Machines

1. Click the **Virtual Machines** selection.

You should see 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.

Validate you are accessing the Financial Department Cost Centers Database. You should receive data from fin-web-01a.
1. Open a **New Tab** in Chrome.
2. Click on the **HR DB App** bookmark.

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

1. Welcome to Photon 1.0 x86
2. fin-web-01a login: root
   Password: 
   root@fin-web-01a
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**

```
root@fin-web-01a ~ ]# ping -c 3 hr-web-01a
PING hr-web-01a.corp.local (172.16.60.10): 64 bytes of data.
64 bytes from hr-web-01a.corp.local (172.16.60.10): icmp_seq=1 ttl=64 time=7.45 ms
64 bytes from hr-web-01a.corp.local (172.16.60.10): icmp_seq=2 ttl=64 time=0.574 ms
64 bytes from hr-web-01a.corp.local (172.16.60.10): icmp_seq=3 ttl=64 time=1.090 ms
--- hr-web-01a.corp.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 301ms
rtt min/avg/max/mdev = 0.46772/0.93277/4.327/2.262 ms

root@fin-web-01a ~ ]# ping -c 3 hr-db-01a
PING hr-db-01a.corp.local (172.16.60.12): 56 bytes of data.
56 bytes from hr-db-01a.corp.local (172.16.60.12): icmp_seq=1 ttl=64 time=5.85 ms
56 bytes from hr-db-01a.corp.local (172.16.60.12): icmp_seq=2 ttl=64 time=0.929 ms
56 bytes from hr-db-01a.corp.local (172.16.60.12): icmp_seq=3 ttl=64 time=0.847 ms
--- hr-db-01a.corp.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.847/2.345/5.857/2.345 ms
```

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 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!"

**Test ping between HR VM to Finance App VMs**

Welcome to Photon 1.0 (x86_64) - Kernel 4.4.8-esx (tty1)
hr-db-01a login: root
Password:
```
root@hr-db-01a [ ~ ]# ping -c 3 fin-app-01a
PING fin-app-01a.corp.local (172.16.60.21) 56(84) bytes of data.
64 bytes from fin-app-01a.corp.local (172.16.60.21): icmp_seq=1 ttl=64 time=13.8 ms
64 bytes from fin-app-01a.corp.local (172.16.60.21): icmp_seq=2 ttl=64 time=0.83 Zs
64 bytes from fin-app-01a.corp.local (172.16.60.21): icmp_seq=3 ttl=64 time=1.44 ms
--- fin-app-01a.corp.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2549ms
rtt min/avg/max/mdev = 0.832/13.806/5.976 ms
```
```
root@hr-db-01a [ ~ ]# ping -c 3 fin-db-01a
PING fin-db-01a.corp.local (172.16.60.22) 56(84) bytes of data.
64 bytes from fin-db-01a.corp.local (172.16.60.22): icmp_seq=1 ttl=64 time=15.3 ms
64 bytes from fin-db-01a.corp.local (172.16.60.22): icmp_seq=2 ttl=64 time=0.53 Zs
64 bytes from fin-db-01a.corp.local (172.16.60.22): icmp_seq=3 ttl=64 time=0.533 ms
--- fin-db-01a.corp.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2754ms
rtt min/avg/max/mdev = 0.533/5.479/15.368/6.952 ms
```

We have verified HR and Finance application VMs can communicate with each other. To enable application isolation on the collapsed application tier, we will now configure the Distributed Firewall, and Security Groups 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** browser icon on the Taskbar.

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 **Folder with the Green Plus** icon in the top row of the Firewall Configuration rules.

---

Access the Firewall Configuration

1. Click the **Firewall** from the Navigator menu on the left.

Add a New Section

1. Click the **Folder with the Green Plus** 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 section above button.
3. Click Save.

Note: DO NOT PUBLISH CHANGES YET.

Create a New Firewall Rule

1. Click the Green plus icon on the right side of section title of our new Collapsed App Tier Rules to add a new firewall rule.

Open up New Rule
1. Click the "twistie" to drop down the **Collapsed App Tier Rules** section.
2. Hover over the right side of the **Name** box to click the **pencil** icon to edit the name of the new rule.

**Name Block HR to Finance Traffic rule**

![Image of Rule 1 - Edit Name]

1. Enter "**Block HR to Finance Traffic**" in the Rule Name field.
2. Click **Save**.

**Edit Source Object**

![Image of Collapsed App Tier Rules]

1. Click the edit or "**pencil**" icon to edit the Source Object.
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.
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 OK.

Edit Destination Object

1. Click the edit or Pencil icon to edit the Destination Object
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.
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

1. Verify the new **Finance App** security group has been added to the **Selected Objects**.
2. Click **OK**.
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.

   Validate that you see all VMs with "hr" in the name listed, like in the image above.

2. 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.

   Validate you see all VMs with "fin" in the name listed, like in the image above.

2. 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 Pencil icon 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 **Green Plus** icon of the **Collapsed App Tier Rules** section to add a new rule.
Edit Rule Name

1. Hover over the right side of the Name box to click the pencil icon 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.
2. Click Save.

Edit Source Object

1. Click the edit or "pencil" icon to 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 **Blue Arrow** icon to move the object to the **Selected Objects** list.
4. Click **OK**.

Edit Destination Object

1. Click the **Pencil** icon 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 **Blue Arrow** icon to move the object to the **Selected Objects** list.
4. Click **OK**.

Edit Action Settings

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

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

Publish Changes

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

Verify Collapsed App Tier Rules

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Rule ID</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Block Finance to HR Traffic</td>
<td>1008</td>
<td>Fin...</td>
<td>HR...</td>
<td>any</td>
<td>Blo...</td>
</tr>
<tr>
<td>2</td>
<td>Block HR to Finance Traffic</td>
<td>1007</td>
<td>HR...</td>
<td>Fin...</td>
<td>any</td>
<td>Blo...</td>
</tr>
</tbody>
</table>
1. Click the **twistie** to drop down the **Collapsed App Tier Rules** section.
2. 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.

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**

![Ping Command Output]

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.
Test ping between Finance App VMs

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**

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

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

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

The **100% success rate** indicates that 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 "HR-Medical Enrollment".
2. Click the Refresh button.

Validate you are accessing the Medical Enrollment Database.

Return Remote Console to HR DB VM

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

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

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

   ```bash
   # 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`

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

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

   ```bash
   # ping -c 3 hr-app-01
   ```

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 browser tab.

**Deleted Collapsed App Tier Section**

1. Click the Red "X" on the right hand side of the Collapsed App Tier Rules section to delete the entire section.

**Confirm Deletion of rule section**

1. Click Yes to proceed with the removal of the rule section.

**Publish Changes**

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 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, 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 6.3 Documentation Center via the URL below:

- Go to [https://tinyurl.com/zwch3gh](https://tinyurl.com/zwch3gh)

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.

Lab Captain:
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 an Operating Systems that is 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.
- 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 - Chris Cousins, Sr. Systems Engineer, 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

![Login to 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@vsphere.local** into User name
2. Type in **VMware1!** into Password
3. Click **Login**

1. Clicking on the **Push-Pins** will allow task panes to collapse and provide more viewing space to the main pane. You can also collapse the left-hand pane to gain the maximum space.
Log on to EOS Virtual Machines

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

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

login Credentials

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

Launch Mozilla Browser from desktop.

1. Click **Customer DB-App** link to launch internal application.
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

The control console VM exists outside of the virtual environment we are using for this lab. As such it represents a service external to our environment. We will use the control center IP address 192.168.110.10 to represent Internet services.

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.

```
ping 192.168.110.10
```

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 EOS OSes and secure them using policy enforcement.

Create Security Group

1. Click the vSphere Web Client browser tab.
2. Click the HOME icon.

1. Click the **vSphere Web Client** browser tab.
2. Click the **HOME** icon.
3. Select **Networking & Security**.
1. Click on **Service Composer**.
Create Security Group

1. Select the **Security Groups** Tab.
2. Click **New Security Group**.
New Security Group

1. Name type: Windows XP EOS.
2. Click Next.
Define Dynamic membership

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.

Move your mouse over the Virtual Machines column. It should indicate 1.

1. Click the number "1" to display the name of the VM in the Security Group.
2. Click the "X" to close the window.
Limit VM Access

We will now apply rules to limit VM external access.

Apply Policy

Go to Service Composer.

1. Select the "Windows XP EOS" Security Group we created previously.
2. Click the "Apply Policy" icon.
New Security Policy

1. Click **New Security Policy**

Create security policy

1. Type Name: **Security Policy Internal Only Access**.
2. Click **Firewall Rules**.
Creating Firewall Rules

1. Click **New Firewall Rule**.
Configure 1st Firewall Rule

1. Name: **Access Internal Resources**
2. Action: **Allow**
3. Source: **Policy's Security Group**
4. Destination: Click **Change**
In order to make this Lab easier to configure the Internal Services Security Group was premade and contains VMs that are apart of the internal applications. We are creating rules that will allow the EOS XP VMs to access these Internal Services but not to access external services (i.e. the internet).

1. Select: "Select Security Groups".
3. Click OK.
Verify Firewall rule settings

Verify settings:
Service: **Any**
State: **Enabled**
Log: **Do not log**

1. Click **OK**.
Verify Firewall Rule

1. Click **Finish**.
Add Additional Firewall Rule

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.

1. Click **Firewall** to access the firewall rules.
Edit Section Name

On the Firewall configuration tab.

1. Click the Add Section icon on the Flow Monitoring Rule section
2. Type "Internal Services to Internal Services" as the Section Name
3. Verify Add section Below is selected
4. Click Save

Publish Changes

1. Click Publish Changes.
Add rules to the New Section

1. Click **Add Rule**.
2. **Click to expand the rules section**.

Edit Firewall Rule Name

1. Hover and Click the **Pencil Icon** to Edit the Firewall Name.
2. **Type the rule name: App to App**.
3. Click **Save**.
Select the Source.

1. Click the pencil icon in the Source column.
2. Select Security Group as the Object Type.
3. Select the Internal Services security group.
4. Click the arrow to add it to Selected Objects.
5. Click Ok.
Select the Destination

1. Click the pencil Icon in the Destination column.
2. Select Security Group as the Object Type.
3. Select the Internal Services security group.
4. Click the arrow to add it to Selected Objects.
5. Click Ok.
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**

Verify 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**.
2. Click the **Pencil Icon** on the Action Column of the Default Rule.
3. Select **Block** as the action.
4. Click **Save**.

**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-01a

1. Click the browser tab for "win-xp-01a".
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-01a** desktop.
2. In the Command Prompt, enter: `ping 192.168.110.10`
3. Verify that external access to the Control Center is now **blocked**.

Now we can see that win-xp-01a 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

1. Expand the Default Section Layer3.
2. Hover and Click the pencil on the Action column of the Default Rule.
3. Select the Allow Action.
4. Click Save.

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 6.3 Documentation Center via the URL below:

- Go to [https://tinyurl.com/zwch3gh](https://tinyurl.com/zwch3gh)

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.

Lab Captain:

- Module 1 Chris Cousins, Sr. Systems Engineer, United States.
- Module 2 Chris Cousins, Sr. Systems Engineer, United States.
- Module 3 Chris Cousins, Sr. Systems Engineer, United States.
- Module 4 Chris Cousins, Sr. Systems Engineer, United States.
- Module 5 Chris Cousins, Sr. Systems Engineer, 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 two 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.
- Add Application Rules for Internal Applications.
- Verify and Test AD Based Rules.

Lab Captain:

Module 4  Chris Cousins, Sr. Systems Engineer, 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

- 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:

(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@vsphere.local** into User name
2. Type in **VMware1!** into Password
3. Click **Login**

Explore Link between NSX and Active Directory

1. Click on **Home** icon
2. Click on **Networking & Security**
Select NSX Manager

On the left go down to the NSX Managers. Notice it denotes only one.

1. **Click on NSX Managers.**

Choose NSX Manager
1. **Click on 192.168.110.42.**

**Explore Domain Connector**

1. **Click on Manage tab.**
2. **Click on Domains tab.**
3. **Click on corp.local.**
4. **Click on Pencil to edit.**

Notice that the table has an entry. This is partially-configured for another lab module but you will step through the process so you have the opportunity to review how the connection was created.

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. Click Next
Provide LDAP Options

Here you will complete the configuration.

1. **Enter VMware1! for the password.**
2. **Click Next.**
Security Event Log Access Options

Here you would enter settings for the log access.

1. **Uncheck the Use Domain Credentials box**
2. **Enter administrator and VMware1! for the Credentials**
3. **Click Next**
Now you would verify all your settings.

1. **Click Finish.**

**AD Synchronization**

1. **Click the "Double-Gear".**
2. **Click the "Single-Gear"** to get updates from the AD. You should see a Success Status and the current date.

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.

Deploy Guest Introspection

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

---

**Diagram:**
- A screenshot showing a navigation menu with "Home," "Networking & Security," and other options.
- An arrow pointing from "Home" to "Networking & Security."
Service Deployments

1. Select Installation.
2. Select Service Deployments tab.
3. Click + icon to deploy Guest Introspection.

Guest Introspection deployment wizard
1. Select **Guest Introspection** service.
2. Click **Next**.
1. Select **RegionA01-COMP02**.
2. Click **Next**.

1. Leave default values.
2. Click **Next**.
1. Click **Finish**.

Wait a few minutes for the installation to complete and then confirm successful installation to the cluster.
Verify Guest Introspection installation on hosts

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

1. Expand the RegionA01-COMP02 folder.
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. Security Objects are defined to based on AD group membership and will be used to enforce security policy.

Create a Security Object based on AD Groups

1. Hover the mouse over the Home Button.
2. Click on Networking & Security.

Create New Firewall Rule Section

1. Click the Firewall link on the navigation pane.
2. Click the “Add Section” icon on the "Flow Monitoring & Traceflow Rule section"
AD-Group Firewall Rule Section

1. Name the new section **AD Based Firewall Rules**.
2. Verify **Add section below** is selected.
3. Click Save.

Add Rule Net-Admin

1. Click the **Add rule** icon on the newly created rule section.
2. Click to **Expand** the newly created rule section.
3. Click the **pencil Icon** on the **Name** column to edit the new rule.

Name Rule

1. **Type name:** Network Admin Access
2. Click Save.

### Edit Source

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 pencil sign.**
2. **Select Security Group in the Object Type pull-down.**
3. **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. Select "Entity" from the drop-down
2. Select "Belongs to"
3. Click to open "Select Entity" window
Choose AD Group

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

1. Click OK

Edit Rule Destination

1. Hover and Click Pencil Icon in the Destination Column of the new created rule.
Select the Internal Services Security Group

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

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

Verify Rule Settings.

1. Click Publish Changes.

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. Click to **Expand the AD based Rule section**
2. Click the **Add Rule** icon.

Name Rule

1. **Hover and Click the Pencil icon** in the Name column of the newly created rule.
2. Rule Name type: **Human Resources Access**.
3. **Click Save**.
Edit Source

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

1. Hover on to source field and click on the pencil sign
2. Select Security Group in the Object Type pull-down
3. 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. Select "Entity" from the drop-down
2. Select "Belongs to"
3. Click to open "Select Entity" window

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

![Security Group Creation Diagram]

1. **Click on "Finish".**
Verify Security Group Selection

1. Click OK.

Edit Rule Destination

1. Hover and Click Pencil Icon 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 **OK**.

Define Service

---

HOL-1803-02-NET
1. Hover and Click the pencil to edit Service.

**Limit the Allowed services.**

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

1. Select **Service** from 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 OK.**
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 Rule

We have created an AD based firewall rules to allow HR admins and Net admins to access the appropriate applications based on their 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.
Edit Section Name

On the Firewall configuration tab.

1. Click the Add Section icon on the "Flow Monitoring & Traceflow Rule Section"
2. Type "Internal Services to Internal Services" as the Section Name
3. Verify Add section Below is selected
4. Click Save

Publish Changes

1. Click Publish Changes.

Add rules to the New Section

1. Click Add Rule.
2. Click to expand the rules section.
Edit Firewall Rule Name

1. Click the Pencil Icon to Edit the Firewall Name
2. Type the rule name: App to App
3. Click Save.

Select the Source.
1. Click the "pencil" Icon in the Source column.
2. Select Security Group as the Object Type.
3. Select the "Internal Services" security group.
4. Click the arrow to add it to Selected Objects.
5. Click Ok.

Select the Destination

1. Click the "pencil" Icon in the Destination column.
2. Select Security Group as the Object Type.
3. Select the "Internal Services" security group.
4. Click the arrow to add it to Selected Objects.
5. Click Ok.
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 to expand the Default Firewall Rule section.
2. Click the Pencil Icon on the Action column of the Default Rule.
3. Select Block as the action.
4. Click Save.
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

Expand the containers "RegionA01" and "Discovered virtual machines" to find win12-jump.

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!** (be sure to include "." after the "!" mark)
6. **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".

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

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
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! (be sure to add "." after "!" mark)
3. **Click on the arrow.**

**Open Firefox 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 AppConfigration 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 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.

If you are looking for additional information on NSX Identity Based Firewall capabilities and configuration, then please review the NSX 6.3 Documentation Center via the URL below:

- Go to [https://tinyurl.com/zwch3gh](https://tinyurl.com/zwch3gh)

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.

Lab Captain:

- Module 1 Chris Cousins, Systems Engineer, United States.
- Module 2 Chris Cousins, Systems Engineer, United States.
- Module 3 Chris Cousins, Systems Engineer, United States.
- Module 4 Chris Cousins, Systems Engineer, United States.
- Module 5 Chris Cousins, Systems Engineer, United States.
How to End Lab

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

Lab Captain:

Module 5 - Chris Cousins, Sr. Systems Engineer, United States
Application Microsegmentation

Launch Chrome Browser and vSphere Web Client

1. Double-click on Chrome icon on the desktop

Login to the vSphere Web Client

User name: administrator@vsphere.local
Password: ********

Login
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@vsphere.local** in to User name
2. Type in **VMware1!** into Password
3. Click **Login**

**Explore Application Rule Manager**

1. Select **Home**
2. Select **Networking & Security**
Select Flow Monitoring

1. Select **Flow Monitoring**

Start New Session for HR_App

1. Select **Application Rule Manager** tab
2. Click **Start New Session** to start collecting application flow data.
Select HR_DB_App Virtual Machines

1. Session Name: HR_DB_App.
2. Select Virtual Machine in the Object Type drop-down menu.
3. Type hr into the Search field.
4. Select hr-web-01a.corp.local, hr-db-01a.corp.local, and hr-app-01a.corp.local.
5. Click on the right arrow.
6. Click OK.
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. To generate some flow data:

1. Open a Putty session and select hr-web-01a.corp.local
2. In the command line, type `ping -c 2 172.16.60.12`
3. Open the Command Prompt on the Main Console
4. `ping 172.16.60.10`

```
ping -c 2 172.16.60.12

ping 172.16.60.10
```
Create More Traffic Flows - HTTPS

1. Open a new Chrome browser tab
2. Click on the HR DB App bookmark
3. Refresh the page several times.

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

1. After three minutes, click Stop.
2. Click Yes to confirm.

### Review Flow Data

![Flow Monitoring Console]

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.

### Start Session for Finance_DB_App

![Session Configuration]

1. Click Start New Session
Select Finance_App Virtual Machines

1. Session Name: Finance_DB_App.
2. Select Virtual Machine in the Object Type drop-down menu.
3. Type fin into the Search field.
5. Click on the right arrow
6. Click OK.
Finance_App Data Collection

Application Rule Manager is now collecting flow data from the three Finance_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. To generate flow data, open a new Chrome browser tab and click on the Finance_DB App bookmark and refresh the page several times. Within three minutes, you will see Flows in the Flow Monitoring console. The number of flows will vary in each lab.

1. Click **Stop**
2. Click **Yes**

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

**Review Sources**

1. Click on **Source** to review vnics being monitored.
Review Flow Duration

1. Click on **Flows** to review collection time and duration.

Start Flow Analysis for Finance_DB_App

1. Click **Analyze** to being analyzing the collected flow data.
Start Flow Analysis for HR_App

When the data analysis is complete for Finance_DB_App:

1. Select HR_DB_App in the Session drop down menu
2. Click **Analyze**

Verify Data Analysis

1. Verify **Analysis Complete** has green checkmark. This indicates data analysis was successful.
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_App Firewall Rules**

We will use the information ARM has given us to microsegment virtual machines within and between HR_DB_App & Finance_DB_App. Let's see if hr-web-01a can communicate with hr-db-01a.
1. Open a Putty session for hr-web-01a.corp.local.
2. Click hr-db-01a.corp.local in the Destination column to retrieve its IP address.
3. Here we can see the IP address 172.16.60.12 as well as the Vnic information.
4. Ping 172.16.60.12. You should see a successful ping with no packet loss.

```bash
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 three-tiered virtual machines.

**New Firewall Rules**

1. Select the flow with Source (192.168.110.10), Destination (hr-web-01a.corp.local) and Service (SSH).
2. Click the Gear icon
3. Select Create Firewall Rule
Control Center to HR_Web

1. Name: **Control Center to HR_Web**
2. Click **Select** across from Service
Select Services

1. Enter https in the search field.
2. Select HTTPS.
3. Click right arrow.
4. Confirm SSH and HTTPS are selected.
5. Click OK.
1. Confirm your configuration matches the image and click **OK**
Configure HR_Web to HR_App Firewall Rule

1. Select the row that lists hr-app-01a as the Destination.
2. Click the Actions gear and select **Create Firewall Rule**.
New Firewall Rule: HR_Web to HR_App

1. Name: **HR_Web to HR_App**
2. Leave everything else as default and click **OK**
Configure New Firewall Rule: HR_App to HR_DB

1. Select the row with hr-db-01a as the Destination.
2. Click the Gear icon and select Create Firewall Rule.
3. Do NOT select the row with ICMP Echo as the Service.
New Firewall Rule: HR_App to HR_DB

Publish Firewall Rules
1. Under Flow Details, select the **Firewall Rules** tab. Here we can see the firewall rules you just created.
2. Firewall rules can also be **Edited and Deleted** from this view.
3. Click **Publish**

**Enter Name**

![Enter Name Image]

1. Section Name: HR_DB_App
2. Select **Default Section Layer 3**

**Review HR_DB_App Firewall Rule**

![Review HR_DB_App Firewall Rule Image]

1. Select **Firewall** in the Navigator panel
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 unsecure traffic has been blocked.

**Edit Default FW Rule**

![Edit Default FW Rule](image)
1. Under the Default Rule, click on the **Pencil** icon to edit the rule.
2. Action: **Block**
3. Click **Save**

![Publish Changes](image)

1. **Publish Changes**

**Verify HR_DB_App is working**

![HR Employee Salary Database](image)

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**.
Open Command Prompt

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.

**Open Putty**

```
root@hr-web-01a [ ~ ]# ping -c 2 172.16.60.12
PING 172.16.60.12 (172.16.60.12) 56(84) bytes of data.
^C
172.16.60.12 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1154ms

root@hr-web-01a [ ~ ]#
```

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!
Module 5 Conclusion

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 6.3 Documentation Center via the URL below:

- Go to [https://tinyurl.com/zwch3gh](https://tinyurl.com/zwch3gh)

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.

Lab Captain:

- Module 1 Chris Cousins, Sr. Systems Engineer, United States.
- Module 2 Chris Cousins, Sr. Systems Engineer, United States.
- Module 3 Chris Cousins, Sr. Systems Engineer, United States.
- Module 4 Chris Cousins, Sr. Systems Engineer, 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-1803-02-NET

Version: 20180215-205024