Table of Contents

Lab Overview - HOL-2003-91-NET - VMware NSX for vSphere Lightning Lab ............ 2
  Introduction ............................................................................................................. 3
  Flow Monitoring ..................................................................................................... 6
  Traceflow ................................................................................................................ 17
  Lightning Lab Conclusion ....................................................................................... 30
  Appendix - Lab Guidance ...................................................................................... 31
Lab Overview - HOL-2003-91-NET - VMware NSX for vSphere Lightning Lab
Introduction

Welcome to the NSX for vSphere Lightning Lab

We have developed Lightning Labs to help you learn about VMware products in small segments of time. In this lab we will use native NSX tools to learn how to troubleshoot and have additional visibility into the virtual environment with tools like Traceflow and Flow monitoring.

Lab Captains:

• Jennifer Schmidt, NSX Solutions Architect, United States
• Frank Snyder, Senior Cloud Solutions Engineer, United States

This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

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


Below are the lab modules included in the complete VMware NSX for vSphere: Getting Started lab:

• Module 1 - NSX Manager Installation and Configuration
• Module 2 - Distributed Networking
• Module 3 - Edge Services
• Module 4 - Distributed Firewall and Microsegmentation
• Module 5 - Operations and Visibility

If you have never taken a lab, view the Appendix - Lab Guidance to see best practices and tips on how to use the lab environment console.
Notice to User about this Lightening Lab

This Lightning Lab is a subsection of the HOL-2003-01 lab: VMware NSX for vSphere - Getting started. Therefore it is necessary to run a script to get your lab environment configured properly for this lightening lab. Please follow the instructions to prepare the lab.

To run the 2003-91.ps1 script use the following procedure:

1. On your desktop Right-Click on 2003-91.ps1
2. Click **Run with PowerShell**

A Powershell window will pop up and run the necessary commands. Please wait for this script to finish and the window to close before continuing.

**Execute the 2003-91.ps1 Script**
Flow Monitoring

Flow Monitoring is a traffic analysis tool that provides a detailed view of the traffic to and from virtual machines. When flow monitoring is enabled, its output defines which machines are exchanging data and over which application. This data includes the number of sessions and packets transmitted per session. Session details include sources, destinations, applications, and ports being used. Session details can be used to create firewall allow or block rules.

Flow Monitoring can thus be used as a forensic tool to detect rogue services and examine inbound and outbound sessions.

Launch Google Chrome

![Google Chrome](image)

**NOTE**: Please ensure you have executed the 2009-91.ps1 script from the previous steps before continuing with this lab.

1. Open **Google Chrome** browser from the taskbar or the desktop of main console.

Navigate to vCenter - Region A

![vCenter Login](image)

1. If the page does not automatically default to the vSphere Web Client (HTML) page click on the **Region A | RegionA vCenter (HTML)** link in the bookmarks bar.
Log in to vSphere Web Client

If you are not already logged in to the vSphere Web Client:

1. Click the check box next to **Use Windows session authentication**.
2. Click **Login**.
Navigate to Networking and Security

1. Click the **Menu** drop-down.
2. Select **Networking and Security**.
Navigate to Firewall

1. Select **Firewall** on the left hand side.
2. Click the "+" to expand the section **Flow Monitoring & Traceflow Rules**.
3. Click the "+" to expand the section **Default Section Layer3**.
4. Verify the **Flow Monitoring and Traceflow Rule** has the following properties:
   - Enabled = toggle button is green
   - Source = web-01a.corp.local
   - Destination = web-02a.corp.local, app-01a.corp.local
   - Service = Any
   - Action = Block

5. Verify the **Default Rule** is set to **Allow**.

We first need to verify the presence of the distributed firewall rule that was created with the 2003-91.ps script that will block communication between **web-01a.corp.local (172.16.10.11)** and **app-01a.corp.local (172.16.20.11)** virtual machines. This will allow us to test Flow Monitoring and show the difference between an allowed and blocked flow.
Navigate to Flow Monitoring

1. In the Networking and Security tab click on **Flow Monitoring**.
2. Click the **Select vNIC** link to select a virtual machine network interface card to monitor.

When using the HTML Client, only the Live Flow tab is visible for Flow Monitoring. Live Flow displays live flows of a selected vNIC from the virtual infrastructure.
Select The Virtual Machine

1. In the search field type **web-01** and press enter.
2. Click on the **web-01a_corp.local** virtual machine.
3. Click on the **right arrow**.
Select The vNIC

1. Click the radio button to select **web-01a_corp.local - Network adapter 1**.
2. Click **OK** to confirm.

Start Live Flow Monitoring

1. Click on **Start** to start monitoring flows to and from the vNIC.
2. Optionally, you can change the Refresh Rate by clicking on the drop down menu and selecting a new refresh rate.

**Note**: Proceed to the next steps to generate live traffic flow.

When traffic flows through the vNIC, flow entries will be highlighted in different colors:
- Green - These are new and active flows.
- Yellow - These are existing flows that have changed their state.
- Red - These are flows that have been terminated.

Flows will appear for X number of seconds depending on the refresh rate that has been selected, by default this is every 5 seconds.

### Open A New Browser Tab

1. Click on the **new tab** icon to open a new tab on your web browser.

### Open Customer DB App

1. Click on the Customer DB-App bookmark, which will eventually display a 504 Gateway Time-out webpage because we blocked all access between web-01a.corp.local (172.16.10.11) and app-01a.corp.local (172.16.20.11).
2. Return to the vSphere Web Client tab where we should see some flows.
Viewing Active and Blocked Flows

1. Flows are showing active flows from the **Main Console (192.168.110.10)**, which is where the Chrome browser is running, to **web-01a.corp.local (172.16.10.11)**.

2. The selected red flow is showing a blocked flow from **web-01a.corp.local (172.16.10.11)** to **app-01a.corp.local (172.16.20.11)** as this is being blocked by the NSX distributed firewall.

Note **Rule ID 1005** associated with the blocked flow; this is the distributed firewall rule **Flow Monitoring and Traceflow Test rule** we verified in an earlier step.

Refresh The Customer DB App Web Page

1. Go back to the **Customer DB App** browser tab.
2. Click on the browser **refresh** button.
3. Switch back to the **vSphere Web Client** browser tab to continue observing live flows.
Filtering Flows

We have the ability to filter flows based on source or destination IP addresses. This allows us to easily focus on flows of interest and ignore all the unnecessary ones.

1. While monitoring a vNIC, click on the Apply filter button.
2. Select either Source IP or Destination IP and enter that address in the IP Address field.
3. Click Apply.

This is just to display functionality, no need to add any filters.

When finished exploring Flow Monitoring, continue to the next step to stop flow monitoring.

Stop Flow Monitoring
1. Click the **Stop** button to stop Flow Monitoring. Switching to another tab in Networking & Security would accomplish the same task.
Traceflow

Traceflow is a feature that improves operational visibility and troubleshooting of NSX deployments in virtual environments. Traceflow injects a packet into a vNIC of a virtual machine, which has no reliance on the guest operating system, and follows it through the various network overlay components and distributed firewall rules all the way to the destination virtual machine. Traceflow supports both L2 and L3 destinations and enables administrators to quickly identify problems and pinpoint issues in the NSX data path.

In this lesson we will perform a Traceflow between two virtual machines and analyze the results of dropped and successful traces.

Verify Firewall Rule

The first step that we need to complete is to verify that the Distributed Firewall rule that will block communication between web-01a.corp.local (172.16.10.11) and web-02a.corp.local (172.16.10.12) is currently enabled and set to BLOCK. This will allow us to see a dropped Traceflow between the two virtual machines on the same L2 segment due to a firewall rule.
Navigate to Networking and Security

1. Click on the Menu drop-down.
Navigate to the Distributed Firewall

1. Click on Firewall.
2. Click on the + to expand the section called Flow Monitoring & Traceflow Rules.
3. Verify the toggle switch is green which ensures the Flow Monitoring & Traceflow Rule firewall rule is enabled.
4. Verify that the Source is set to web-01a and the Destination field includes web-02a and app-01a and that the Service is Any.
5. Verify that the action is set to Block.
Navigate to Traceflow

1. Under Tools click on **Traceflow**.
2. Under **Traffic Type** drop down menu there are options to select Unicast, L2 Multicast of L2 Broadcast traffic to simulate. Leave the option set as **Unicast**.
Select the Source Virtual Machine

1. Click on **Select** link next to Source.
2. In the filter field type **web-01** and press enter.
3. Click on the right arrow next to virtual machine **web-01a_corp.local**, which will be the source of the Traceflow.
Select the Source vNIC

1. Select the radio button for **web-01a_corp.local - Network adapter 1**. This will be the source of the packet.
2. Click **OK** to confirm the selection.
1. Click on the **Select** link next to the Destination.
The options are to perform a L2 or L3 Traceflow based on destination IP or MAC address or to select a particular virtual machine. We are going to select the web-02 virtual machine.

1. Click the radio button to **Select Destination vNIC**.
2. In the filter field type **web-02** and press enter.
3. Click on the **right arrow** next to virtual machine **web-02a_corp.local**, which will be the destination of the Traceflow.
Select the Destination vNIC

1. Select the radio button for **web-02a_corp.local - Network Adapter 1**. This will be the destination of the packet.
2. Click **OK** to confirm the selection.
Configure Advanced Options

We can configure additional settings for the packet injected into the Source vNIC under **Advanced Options**. Additional settings include Protocol, which can be either ICMP, TCP or UDP, Timeout, Frame Size, and TTL. Additional options are presented based on the protocol selected. In this example we will trace a TCP packet with Destination Port 80 and TCP SYN Flag set.

1. Click on the arrow next to **Advanced Options**.
2. Change the **Protocol** to **TCP**.
3. Set the **Destination Port** to **80**.
4. Select **SYN** as the TCP Flag.
5. Click **Trace** to inject the packet.

Review Traceflow Results

1. Once the trace completes, the result will display that the packet was **Dropped**.
2. We can follow the sequence and see that the packet was injected into the vNIC, received by the firewall and then dropped by **Rule - 1005**, which we verified earlier.

Note that the packet was dropped at the source VM firewall without traversing the infrastructure. If this was unexpected behavior then we could investigate rule 1005 to check if it should be in place or not.
Allow The Traceflow Distributed Firewall Rule

In the next steps we will set the Distributed Firewall rule to allow communication from web-01a.corp.local (172.16.10.11) to web-02a.corp.local (172.16.10.11) and perform Traceflow again to see a successful packet delivery.

Navigate to Firewall

1. Click on **Firewall**.
2. Click on the + to expand the section called **Flow Monitoring & Traceflow Rules**.
3. Set the **Flow Monitoring & Traceflow Rule** firewall rule Action to **Allow**. (Click on Block and select Allow from the drop-down)
4. Click **Publish** to push the firewall change down to the hypervisors.
5. Verify that the publish operation completed successfully (Please note the date of your publish will not be identical to the screenshot).

Perform a Traceflow

1. Click on **Traceflow**.
2. **Trace Parameters** from the previous trace attempt should still be in place. If not, repeat the steps to set the following parameters:
Traffic Type: **Unicast**
Source: **web-01a_corp.local**
Source vNIC: **web-01a_corp.local - Network Adapter 1**
Destination: **Select Destination vNIC**
Destination: **web-02a_corp.local**
Destination vNIC: **web-02a_corp.local - Network Adapter 1**
Advanced Options - Protocol: **TCP**
Advanced Options - Destination Port: **80**
Advanced Options - TCP Flags: **SYN**

3. Click **Trace**.

**Review Traceflow Results**

1. Once the trace completes, we should see the end result as **Delivered**.
2. We can follow the packet and see that it was injected into the vNIC, passed through the distributed firewall on egress, encapsulated and delivered to the receiving host, and then passed through the distributed firewall on ingress.

Note that you may need to scroll down to see the full Traceflow information.
Filtering Results

1. It is also possible to filter the results based on Observation Type, Component Type, Component Name and Host by clicking on the filter icon in the top right of the Trace Result section.
2. Select the appropriate filter criteria, such as Component Type: Firewall.
3. Click Apply to only display firewall-specific Traceflow components.
Lightning Lab Conclusion

In this module we focused on Flow Control and Traceflow. Flow Monitoring can be used as a forensic tool to detect rogue services and examine inbound and outbound sessions. Traceflow is a feature that improves operational visibility and troubleshooting of NSX deployments in virtual environments.

You have finished the Lightning Lab!

Congratulations on finishing the Lightning Lab.

If you are looking for additional information on deploying NSX, please review the NSX 6.4 Documentation Center via the URL below:

https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/index.html

Below are the lab modules included in the complete VMware NSX for vSphere - Getting Started Lab (HOL-2003-01-NET)

Lab Module List:

• Module 1 - NSX Manager Installation and Configuration
• Module 2 - Distributed Networking
• Module 3 - Edge Services
• Module 4 - Distributed Firewall and Mircosegmentation
• Module 5 - Operations and Visibility
• Module 6 - NSX-V and vRealize Network Insight

How to End Lab

To end your lab click on the END button.
Appendix - Lab Guidance

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**

![On-Screen Keyboard with @ key highlighted]

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

**Activation Prompt or Watermark**

![Watermark indicating Windows is not activated]

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**

![Screen shot showing Lab Status]

Please check to see that your lab has 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.

Click here to return to the [VMware Cloud on AWS - Introduction](#)
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-2003-91-NET

Version: 20191106-095828