# Table of Contents

Lab Overview - HOL-1941-01-NET - Secure Horizon with Trend Micro and NSX ........... 2
  Lab Guidance .................................................................................................................................. 3
Module 1 - Installation and Configuration of Trend Deep Security (30 minutes) .......... 9
  Introduction ....................................................................................................................................... 10
  Hands-on Labs Interactive Simulation: Trend Micro Deep Security ........................................ 11
  Conclusion ........................................................................................................................................ 12
Module 2 -Protecting Horizon Desktops with NSX and Trend Micro Deep Security (45 minutes) ........................................................................................................................................ 13
  Module 2 Introduction .................................................................................................................... 14
  Ensure that Trend Micro is running properly .................................................................................. 15
  Protecting Horizon Desktops with NSX and Trend Micro Deep Security .................................... 21
  Conclusion ........................................................................................................................................ 44
Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep
  Security (30 Minutes) ..................................................................................................................... 45
  Module 3 Introduction .................................................................................................................... 46
  Ensure that Trend Micro is running properly .................................................................................. 47
  Protecting Web Servers against exploits with NSX and Trend Micro Deep
  Security ............................................................................................................................................. 53
  Module 3 Summary ....................................................................................................................... 65
Module 4 - Securing internal access to Horizon View environment using NSX load
  balancing and DFW (45 Minutes) ...................................................................................................... 66
  Module 4 Introduction .................................................................................................................... 67
  Securing internal access using VMware NSX Load Balancing and DFW ................................. 69
  Module 4 Summary ....................................................................................................................... 94
Module 5 - Securing external access using VMware Horizon access servers and DFW (45 Minutes) ................................................................................................................................. 95
  Module 5 introduction ................................................................................................................... 96
  Securing external access using VMware Horizon access servers ............................................. 99
  Module 5 Summary ....................................................................................................................... 129
Lab Overview - HOL-1941-01-NET - Secure Horizon with Trend Micro and NSX
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.

This lab will demonstrate how VMware End User Computing and NSX Security solutions can provide a secure desktop experience, doing so while maximizing operational efficiencies automated security policy delivery and redundant internal and external access.

Lab Module List:

- Module 1 - Installation and Configuration of Trend Deep Security
- Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security
- Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security
- Module 4 - Securing and protecting internal access using VMware NSX Load balancing
- Module 5 - Securing and protecting external access using VMware NSX Load balancing

Lab Captains:

- Kevin Moats, Staff Technical Account Manager, 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

Wait for “Lab Status” to change to green “Ready”
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 - Installation and Configuration of Trend Deep Security (30 minutes)
Introduction

This Module contains the following lessons:

- Lesson 1 In this Hands-on Labs Interactive Simulation, we will take a look at installing and configuring Deep Security with vCenter and NSX. This will include adding the vCenter connector and NSX as well as configuring the security policies within NSX to be used by Deep Security.
Hands-on Labs Interactive Simulation: Trend Micro Deep Security

This part of the lab is presented as a **Hands-on Labs Interactive Simulation**. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. [Click here to open the installation simulation](#). It will open in a new browser window or tab.
2. When finished, click the "return to lab" link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.
Conclusion

You have now seen what it takes to install and configure Trend's Deep Security with vCenter and NSX. This included adding the vCenter connector and NSX as well as configuring the security policies within NSX to be used by Deep Security.

Congratulations on completing Module 1.

Proceed to any module below which interests you most.

- **Module 1 - Installation and configuration of Trend Deep Security** (30 minutes) (Basic) In this module we'll go over the installation and configuration of the Trend Deep Security platform.
- **Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 2 we will go over how we can use Horizon in concert with NSX and Trend Micro to protect the end user.
- **Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 3 we will go over how you can protect Web Servers with NSX and Trend
- **Module 4 - Securing and protecting internal access using NSX load balancing** (30 Minutes) (Advanced) In Module 4 we'll show how we can leverage NSX load balancing
- **Module 5 - Securing and protecting external access using VMware Horizon access servers** (45 Minutes) (Advanced) In Module 5 we'll explore ways to protect external access to our environment.

Lab Captain:

Kevin Moats Staff TAM United States

How to End Lab

To end your lab click on the END button.
Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security (45 minutes)
Module 2 Introduction

In module two we are going to take a look at the ability of Trend Micro Deep Security to detect a virus on a Windows 10 virtual desktop. This detection will leverage VMware NSX using a firewall rule to block all traffic to and from the VM’s. In a production environment, we could implement more advanced NSX firewall rules to allow an anti-malware server the ability to access the infected machine and remediate the threat. This functionality could be leveraged further by utilizing vSphere API's to capture the current state of the virtual machine just after infection for further investigation.
Ensure that Trend Micro is running properly

Due to the limited resources and virtualization nesting of the Hands on Labs environment not all services are always deployed successfully when a lab is launched. The next six steps will guide you through the process to verify guest introspection services are healthy before continuing on with your lab.

Launch Chrome

1. Click Google Chrome Icon

Log into the vCSA

1. Check the Use Windows session authentication box
2. Click the Login button

Alternate credentials if needed:

User: administrator@corp.local
Password: VMware1!
Navigate to Networking and Security

1. Click **Home**
2. Click **Networking and Security**
Navigate to NSX Installation section

1. Click **Installation and Upgrade**

**View Service Deployments**

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Installation Status</th>
<th>Service Status</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Introspection</td>
<td>6.4.1.848880</td>
<td>Failed</td>
<td>Unknown</td>
<td>Details</td>
</tr>
<tr>
<td>Trend Micro Deep Security</td>
<td>11.0</td>
<td>Succeeded</td>
<td>Up</td>
<td>Details</td>
</tr>
</tbody>
</table>
If the Installation status shows "Succeeded" and Service Status shows "Up" skip the next step and continue with your lab.

1. Click the **Service Deployments** tab.
2. Note the Installation Status, if it is in a **Failed Status** continue to the next step.

### Resolve the Failed Installation

1. Click the **Resolve** link.
2. **WAIT** for about two minutes before moving on to the next step.
Refresh the vSphere Client to verify Guest Introspection services are resolved

1. Click the refresh Icon.
2. If the status is still "Failed" or the Service Status is "Warning" repeat the resolve action and refresh again.

It will usually take two separate resolve actions to correct the issue however three resolve actions may be needed. Please wait for at least 60 seconds between resolve actions.
Example of a healthy environment

1. Once the Installation status reports **Succeeded** and Service status reports **Up** move on to the rest of your lab.
Protecting Horizon Desktops with NSX and Trend Micro Deep Security

Launch Google Chrome

1. Double click `google chrome` from the Main Console desktop.

Launch Trend Micro Deep Security

1. Click to open a new tab
2. Click Trend folder
3. Click Trend Micro Deep Security from the menu bar

Log into Trend Micro Deep Security

1. Username: **admin**
2. Password: **VMware1!**
3. Click **Sign in.**

**Trend Micro Deep Security Main screen**

1. From the main screen select **Computers.**

**View the managed machine**
1. 1. Use the scroll bar to scroll down and find "Win10-View-01a.corp.local".  
2. Notice that the "Win10-View-01a.corp.local" machine shows "managed online".

Open a new incognito window in Chrome.

![Chrome incognito window](image)

1. Click the three dots in the top right of Chrome.  
2. Open a new incognito window in Chrome.

Switch back to the non-incognito mode chrome session

![Chrome non-incognito session](image)

1. Click the non-incognito mode chrome session

Launch Horizon External Access URL

![Horizon External Access](image)
1. Click the **Open a new Tab**.
2. Launch **Horizon External Access** URL.

### Use Horizon HTML Access

The VMware Horizon Client offers better performance and features.

1. Select **VMware Horizon HTML Access**.
Log into Horizon

Log into Horizon with the following credentials.

1. username: **qeuser**
2. password: **VMware1!**
3. Select **Login**
Select Windows-10

1. Select **Windows-10** desktop.

Open the temp-shortcut

1. From the desktop double click the **temp-Shortcut** folder

Copy the eicar.com file

1. Right click on **eicar.com** and select **Copy**
EICAR.com is the European Institute of Computer Anti-virus Research's Standard Anti-Malware Test file is a special 'dummy' virus file which we will now use to test the correct operation of our Trend Micro Deep Security along with NSX rulesets. (For purposes of this test the "Temp" directory has been excluded from Trend's detection)

1. Right click the **eicar.com** file
2. Select **copy**.

**Try to infect our VM**

Let's see what happens when we try to infect our desktop with this virus file.

1. **Click** anywhere on the desktop.
2. **Right click** on the desktop.
3. Select **Paste**.

**Malware detected**

Notice that the eicar file will not be permitted to be pasted to the desktop and will be detected as malicious code.
Malware detection message may appear.

Disconnected message

A firewall rule will block all traffic to and from the desktop. This will cause your session to terminate and if you try to reconnect to the desktop you'll be unable to at this point. (It may take a couple of minutes for this to be processed) Let's investigate further.

Open the vCenter Web Client

Let's log into our vCenter and see what has happened to our VM

1. Click to open a new tab.
2. Launch RegionA vCenter web interface.
Log in to the VMware Web Client

1. Check the **Use Windows session authentication** check box.
2. Click **Login**.

Alternate credentials if needed:

User name: **administrator@corp.local**
Password: **VMware1!**

Search for the Win10 Desktop

1. In the search bar type in **Win10**
2. Select **Win 10-View-01a**
Review the Win10-View01a VM

1. Click on the Win10-View-01a summary tab.
2. Note that the VM has been tagged with "ANTI_VIRUS.VirusFound.threat=medium" tag.

Trend picked up the Virus, next let's take a look at what policy's in NSX changed connectivity to the machine.
View Firewall rules

1. Click on the **Home** button.
2. From the dropdown select **Networking & Security**.

Open Service Composer

1. Select **Service Composer**.
View Security Groups

1. Click on **Security Group** tab.
2. Quarantine Group **radio button**.
3. Click **Edit**.

Notice the name of the VM in the Group. We can now verify that our Win10-View-01a VM has indeed been **caught by this NSX Firewall rule** due to the virus file we tried copying to the View desktop.

4. Click the "x" to close the window.
Explore group membership settings

1. Click Define dynamic membership.
2. Note that the membership criteria requires a vm to have a Security tag including **ANTI_VIRUS**.
3. Click the X to close the window.
Explore firewall settings

1. Click **Firewall**
2. Expand **Trend Quarantine** firewall group
3. Use the **scroll bar** to Explore firewall settings in Rule ID 1007 and 1008:

   **Verify Win10-View-01a is included in the Quarantine group**
1. Click the Quarantine Group listed in rule 1007 or 1008.
2. Verify Win10-View-01a is included.

Go back to the Trend Deep Security Chrome session


(Log back in if you have been timed out.)

username: admin
password: VMware1!

Click Sign in

Trend Micro Deep Security Main screen

1. From the main screen select computers.
Find the Windows 10 machine

1. In the search Window type **Win10**
2. Press **Enter**
3. **Double click** Win10-View-01a.corp.local.

View Anti-Malware detection

1. From the WIN10-VIEW-01A.corp.local system select **Anti-Malware**.
View Anti-Malware Events

1. Click on the **Anti-Malware Events** Tab.
2. Note that the Eicar file is listed as a *quarantined file*. This tells us that our file was quarantined and remediated.
3. Close the **WIN10-VIEW-01A.corp.local** Tab.
Rescan the Windows 10 VM

1. Right Click WIN10-VIEW-01A.corp.local in Trend.
2. Select Actions.
3. Select Full Scan for Malware (allow 60 seconds or so for this to complete)
View NSX Security tag was removed

Go back to the vSphere Web Client Tab in Google Chrome.

Type **Win10** in the search field.

1. Click on **Win10-View-01a**
2. Click on **Summary tab**
3. **Verify** Security tag was removed automatically.

Verify your connection to the Horizon desktop works once again

1. **Switch back to your VMware Horizon Tab in the incognito mode Chrome session**
Connect to your Windows-10

1. Double click the **Windows-10** Icon.

Select VMware Horizon HTML Access

1. Select VMware Horizon HTML Access
Log into Horizon with the following credentials.

1. Username: **quser**
2. Password: **VMware1!**
3. Select **Login**
Select the Windows-10 Desktop

1. Select the **Windows-10** Desktop
Access to the desktop.

Notice that we once again have access to our Windows 10 desktop which means we effectively cleaned the virus and the NSX rules put the machine back on the production network! Great job.
Conclusion

In Module 2 we've seen how we can leverage both NSX and Trend Micro Deep Security together to detect and quarantine a Horizon desktop. We then showed how after remediating the threat in Trend we were able to automatically detect that the VM was clean with NSX and place it back out of the quarantine group and the system is back and ready for use. This automated workflow is a huge advantage enabling organizations to quickly quarantine and remediate threats.

Proceed to any module below which interests you most.

- **Module 1 - Installation and configuration of Trend Deep Security** (30 minutes) (Basic) In this module we'll go over the installation and configuration of the Trend Deep Security platform.
- **Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 2 we will go over how we can use Horizon in concert with NSX and Trend Micro to protect the end user.
- **Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 3 we will go over how you can protect Web Servers with NSX and Trend
- **Module 4 - Securing and protecting internal access using NSX load balancing** (30 Minutes) (Advanced) In Module 4 we'll show how we can leverage NSX load balancing
- **Module 5 - Securing and protecting external access using VMware Horizon access servers** (45 Minutes) (Advanced) In Module 5 we'll explore ways to protect external access to our environment.

Lab Captains:

Kevin Moats Staff TAM United States
Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security (30 Minutes)
Module 3 Introduction

In module three we are going to demonstrate a Heartbeat exploit attack utilizing a heartbleed Python script. Once we have demonstrated that the Web server is vulnerable we will automatically protect it with agentless intrusion prevention services utilizing Trend Micro Deep Security in conjunction with VMware NSX.

This Module contains the following lessons:

- Lesson 1: Attack a web server with the heartbeat vulnerability
- Lesson 2: Automatically set intrusion prevention policy on a Web Server
- Lesson 3: Verify exploit is blocked with agentless intrusion prevention services
Ensure that Trend Micro is running properly

Due to the limited resources and virtualization nesting of the Hands on Labs environment not all services are always deployed successfully when a lab is launched. The next six steps will guide you through the process to verify guest introspection services are healthy before continuing on with your lab.

Launch Chrome

1. Click Google Chrome Icon

Log into the vCSA

1. Check the Use Windows session authentication box
2. Click the Login button

Alternate credentials if needed:

User: administrator@corp.local
Password: VMware1!
Navigate to Networking and Security

1. Click **Home**
2. Click **Networking and Security**
Navigate to NSX Installation section

1. Click Installation and Upgrade

View Service Deployments

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Installation Status</th>
<th>Service Status</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest Introspection</td>
<td>6.4.1.848907</td>
<td>Failed</td>
<td>Unknown</td>
<td>Region Details</td>
</tr>
<tr>
<td>Trend Micro Deep Security</td>
<td>11.0</td>
<td>Succeeded</td>
<td>Up</td>
<td>Region Details</td>
</tr>
</tbody>
</table>
If the Installation status shows "Succeeded" and Service Status shows "Up" skip the next step and continue with your lab.

1. Click the Service Deployments tab.
2. Note the Installation Status, if it is in a Failed Status continue to the next step.

Resolve the Failed Installation

1. Click the Resolve link.
2. \textbf{WAIT} for about two minutes before moving on to the next step.
Refresh the vSphere Client to verify Guest Introspection services are resolved

1. Click the refresh Icon.
2. If the status is still "Failed" or the Service Status is "Warning" repeat the resolve action and refresh again.

It will usually take two separate resolve actions to correct the issue however three resolve actions may be needed. Please wait for at least 60 seconds between resolve actions.
### Example of a healthy environment

- **Service**: Guest Introspection
  - **Version**: 6.4.1.8481357
  - **Installation Status**: Succeeded
  - **Service Status**: Up

- **Service**: Trend Micro Deep Security
  - **Version**: 11.0
  - **Installation Status**: Succeeded
  - **Service Status**: Up

1. Once the Installation status reports **Succeeded** and Service status reports **Up**, move on to the rest of your lab.
Protecting Web Servers against exploits with NSX and Trend Micro Deep Security

Launch a new tab and open DVWA

1. In Chrome, click to open a **new tab**
2. Click the **DVWA** folder
3. Launch the **Damn Vulnerable Web App**

Log into the DVWA site

1. username: **admin**
2. Password: **password**
3. select **Login**
This login is to cache the username and password "securely" into RAM over SSL

**Minimize Chrome to access the Heartbleed script**

1. In Chrome, click the **minimize** button.

1. Right click the **Heartbleed** shortcut.
2. Click **open**.

**Launch the Heartbleed script**
Observe the "server is vulnerable" message

1. Use the scroll bar to scroll up to the top of the data
2. Note that the script displays that the server is vulnerable

View the SSL memory dump

1. Scroll through the memory dump and you should be able to view the "secure" user name and password we input into the DVWA interface
Launch the trend deep security manager interface

1. In Chrome, open a **new Tab**
2. Click the **Trend** folder
3. Click the **Trend Micro Deep Security Manager** Shortcut

Log into Trend Micro Deep Security

1. Username: **admin**
2. Password: **VMware1!**
3. Click **Sign In**
Navagate to the Web-01a.corp.local computer

1. Click **Computers**
2. Type **Web-01a** in the search box and **press enter**.
3. Verify the computer is in a **managed** state
4. Double click **Web-01a.corp.local**

**View assigned policy**

1. **Policy**: None
1. Notice that that policy shows as **None** applied

**Close the Web-01a properties box**

1. Click the **Close** icon to Close the Web-01a properties box (do not close the Trend tab)

**Launch the vSphere Web Client**

1. In Chrome, click to open a **new tab**
2. Click **RegionA folder**
3. Click **RegionA vCenter** shortcut
Log in to vCenter

1. **Check** the Use Windows session authentication **checkbox**.
2. Click **Login**

Alternate credentials if needed:

Username: **administrator@vsphere.local**

Password: **VMware1!**

Navigate to VM's and Templates

1. Click **Home**
2. Click **VMs and Templates**
1. Click the arrow to expand the Datacenter folders.
2. Click the arrow to expand the Dev Web Servers folder.

Move Web-01a from "Dev Web Servers" to "Prod Web Servers"

1. Drag and drop Web-01a from "Dev Web Servers" to "Prod Web Servers"
Verify that Web-01a moved to the proper folder

1. Verify that Web-01a is now in the "Prod Web Servers" folder

Change focus to the Trend deep security interface tab

1. Click to open Trend Micro Deep Security tab

Open the Web-01a computer object

1. Double click the Web-01a object
View assigned policy

1. Observe that the Web-01a object now has the **Prod Web Servers Policy** applied.

Close the Web-01a properties box

1. Click the **Close icon** to Close the Web-01a properties box (do not close the Trend tab).
Minimize Chrome

1. Click the **Minimize** button

Launch the Heartbleed script again

1. Right Click the **Heartbleed shortcut**
2. Click **Open**
1. Notice that the server now reports as "**Likely not vulnerable**" and there is no memory dump available.

Congratulations!!! You have successfully protected the Web server from a Heartbleed attack without patching the server.
Module 3 Summary

In module three we demonstrated a Heartbeat exploit attack utilizing a heartbleed Python script. Once we demonstrated that the Web server was vulnerable we automatically protected it with agentless intrusion prevention services utilizing Trend Micro Deep Security in conjunction with VMware NSX.

Proceed to any module below which interests you most.

- **Module 1 - Installation and configuration of Trend Deep Security** (30 minutes) (Basic) In this module we'll go over the installation and configuration of the Trend Deep Security platform.
- **Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 2 we will go over how we can use Horizon in concert with NSX and Trend Micro to protect the end user.
- **Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 3 we will go over how you can protect Web Servers with NSX and Trend
- **Module 4 - Securing and protecting internal access using NSX load balancing** (30 Minutes) (Advanced) In Module 4 we'll show how we can leverage NSX load balancing
- **Module 5 - Securing and protecting external access using VMware Horizon access servers** (45 Minutes) (Advanced) In Module 5 we'll explore ways to protect external access to our environment.

Lab Captain:

Kevin Moats Staff TAM United States

How to End Lab

To end your lab click on the **END** button.
Module 4 - Securing internal access to Horizon View environment using NSX load balancing and DFW (45 Minutes)
Module 4 Introduction

In module four we are going to demonstrate access to two load balanced Horizon connection brokers through a NSX load balancer. We will use a Windows 10 virtual machine configured on an internal corporate network to demonstrate a connection to a Windows 10 Horizon managed virtual machine through a redundant pair of Horizon connection brokers. This connection will use a single connection name space and SSL certificate presented by the NSX Load Balancer.

This Module contains the following lessons:

- Lesson 1: Connection to a Horizon hosted virtual machine through a NSX load balancer
- Lesson 2: Exploring the NSX load balancing configuration
- Lesson 3: Verify redundant connection server used for Horizon View connection

Module 4 Topology

The key components are outlined here.
1. External endpoint
2. Distributed Firewall
3. Endpoint on an internal secure network
4. Target horizon virtual desktop
5. Load balancing services
6. Connection Server 1
7. Connection Server 2
Securing internal access using VMware NSX Load Balancing and DFW

In this module you will connect to an internal Windows 10 desktop through one of two redundant Horizon connection servers, verify redundancy and explore the NSX configuration.

Connect to the Win10-internal desktop

1. Double Click the Internal Desktop Icon.

Log in will happen automatically

If the session does not automatically log in, log in as Administrator using the following credentials:

1. Verify user: corp\administrator
2. Type Password: VMware1!
3. Click OK.
Check your desktop, then Launch the VMware Horizon Client

Based on the Hand on Labs environment you will be using the Win10-internal virtual machine as a desktop endpoint. This would normally be a physical device located on an internal trusted corporate network.

1. Validate that you are connected to the **Win10-internal desktop** and that you are connected to the **172.16.30.0 subnet**
2. Double click the **VMware Horizon Client** to launch it.
Double Click the cloud icon to connect to the "view-internal" Horizon infrastructure and your virtual desktop.

![VMware Horizon Client](image)

The View-internal.corp.local name space will connect you to one of the redundant Horizon connection servers through a NSX load balancer.

1. Double click the `view-internal.corp.local` icon.

**Log in**

![Login](image)

Log in as `qeuser` using the following credentials:

1. User name: `qeuser`
2. Password: `VMware1!`
3. Domain: **CORP.**
4. Click **Login.**

**Connect to your virtual desktop**

1. Double click the **Windows-10** Icon
Verify connection to Horizon hosted virtual machine

You are now connected to your Windows 10 Virtual machine through one of two redundant connection servers, HVCS-01a or HVCS-02a

1. Verify you are connected to **Win10-View-01a**.
Disconnect from the Win10-View-01a Desktop session

1. Click **options**.
2. Click **Disconnect**.

**Confirm disconnect**

1. Click **OK**

**Minimize the RDP session**

1. Click the minimize button.
Explore NSX load balancing configuration

In this lesson we will explore the NSX load balancing configuration and force a connection server failure.

Launch the VMware Web client

1. Launch Chrome from your Main console machine.

Log in to the VMware Web Client
1. Check the Use Windows session authentication check box.
2. Click Login.

Alternate credentials:

User name administrator@corp.local
Password VMware1

Navigate to networking and Security

1. Click the Home button.
2. Click on Networking & Security.
Open NSX Edges

1. Click on **NSX Edges**.

Open the view-internal Load Balancer

1. **Double Click** the view-internal-LoadBalancer edge gateway.
Open the view-internal application profile

1. Click the **manage** tab.
2. Click on the **Load Balancer** tab.
3. Select **Application profiles**.
4. Click the **edit** icon.
Explore the Application Profile for Horizon View

1. Notice that the Application profile is set to HTTPS and is using a certificate assigned at the load balancer in termination mode with the name view-internal.corp.local

2. Once complete Click Cancel (note: you may need to maximize your chrome window and drag the configuration widow up to access the cancel button)
Open the Horizon View service monitor

1. Select service monitoring.
2. Highlight the HVCS monitor-4.
3. Click the Edit icon.
Explore the HVCS service monitor settings

1. Notice that the monitor is set to HTTPS and is configured to detect a /portal page.
2. Once complete Click Cancel (note: you may need to maximize your chrome window and drag the configuration widow up to access the cancel button)
Explore the pool statistics

1. Select the **Pools** section.
2. Click on **Show Pool statistics**.
3. Click on **Pool-2**.
4. At this point both servers should show as **UP**. (Note: Due to the nature of Hands on labs one server may be down.)

If both servers show as up please move to the next step, if one server shows down this completes the module and shows that even with one connection server **UP** the connection was still successful. Please move on to the next module or end your lab.
Close the Pool statistics window

1. Click the X button.

Find the connection server virtual machine.

Proceed with this step only if both connection servers show as UP in the load balanced Pool Status.

1. **Type** the connection server name HVCS-01a into the search box.
2. Click on the **connection server name**.
Power off the selected connection server to simulate a failure

1. Right click the connection server.
2. Hover over Power.
3. Click Power Off.

Confirm power off of virtual machine

1. Click Yes.
Navigate back to networking and Security

1. Click the **Home button**.
2. Click on **Networking & Security**.
Open NSX Edges again

1. Click on NSX Edges.

Open the view-internal Load Balancer again

1. Double Click the view-internal-LoadBalancer edge gateway.
Explore the pool statistics after failure

1. Select the **Pools** section.
2. Click on **Show Pool statistics**.
3. Click on **Pool-1**.
4. At this point HVCS-01a will show as **DOWN**.
Close the Pool statistics window

1. Click the X button.

Verify redundant connection server used for Horizon View connection

Verify redundant connection server used for Horizon View connection.

Return to the RDP session

1. Click the open RDP session

Relaunch the Horizon View Client

1. Double Click the Horizon Client
Double Click the cloud icon to connect to the "view-internal" Horizon infrastructure and your virtual desktop.

The View-internal.corp.local name space will connect you to the remaining redundant Horizon connection server through the edge gateway we just explored.

1. Double click the **view-internal.corp.local** icon

**Log in**

Logon as Dr. Melissa Null using the following credentials:

1. User name: **qeuser**
2. Password: **VMware1!**
3. Domain: **CORP**
4. Click **Login**
Connect to your Windows-10 desktop

1. Double click the **Windows-10** icon.

Verify connection to Horizon hosted virtual machine
You are once again connected to your Win10-View-01a Virtual machine, now through the redundant connection server

1. Verify you are one again connected to **Win10-View-01a**

**Disconnect from the Win10-View-01a Desktop session**

1. Click **options**
2. Click **Disconnect**

**Confirm disconnect**

Click **OK**

**Close the RDP session**
1. Click the X to close the RDP session

Confirm the RDP session disconnect

![RDP Session Disconnect Confirmation]

1. Click OK

Power the Connection server back on for module 5

If you plan to move on to module 5 you will need to power the connection server back on that was powered down in a previous step. If you do not plan to move on to module 5 you can end your lab.

Return to the vSphere Web Client

![vSphere Web Client]  

1. Click the vSphere Web Client tab

Find the connection server virtual machine

![Connection Server Search]

1. Type the connection server name you powered down in a previous step. (HVCS-01a or HVCS-02a)  
2. Click on the connection server name.
Power on the selected connection server

1. **Right click** the connection server.
2. **Hover over Power.**
3. Click **Power On.**
Module 4 Summary

In module four we demonstrated access to two load balanced Horizon connection brokers through a NSX load balancer. We also simulated a failure of one Horizon connection server and verified redundancy. This redundancy is key when designing a virtual desktop environment for production use.

Proceed to any module below which interests you most.

- **Module 1 - Installation and configuration of Trend Deep Security** (30 minutes) (Basic) In this module we'll go over the installation and configuration of the Trend Deep Security platform.
- **Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 2 we will go over how we can use Horizon in concert with NSX and Trend Micro to protect the end user.
- **Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 3 we will go over how you can protect Web Servers with NSX and Trend
- **Module 4 - Securing and protecting internal access using NSX load balancing** (30 Minutes) (Advanced) In Module 4 we'll show how we can leverage NSX load balancing
- **Module 5 - Securing and protecting external access using VMware Horizon access servers** (45 Minutes) (Advanced) In Module 5 we'll explore ways to protect external access to our environment.

Lab Captain:

Kevin Moats Staff TAM United States

How to End Lab

To end your lab click on the END button.
Module 5 - Securing external access using VMware Horizon access servers and DFW (45 Minutes)
Module 5 introduction

In module five we are going to demonstrate access to two Horizon View Access servers through a NSX load balancer. We will simulate an external firewall protected connection to a Windows 10 Horizon managed virtual machine through a redundant pair of Horizon Access servers. The connection will use a single connection name space. The Access Point functions as a secure gateway for users who want to access Horizon 7 desktops and applications from outside the corporate firewall.

This Module contains the following lessons:

- Lesson 1: Verify external access to internal protected network is secure
- Lesson 2: Exploring the NSX firewall configuration
- Lesson 3: Connection to a Horizon hosted virtual machine through a NSX edge gateway to a protected internal network.
- Lesson 4: Explore the Horizon Access Server load balancer configuration

Module 5 topology

The key components are outlined here.

1. External endpoint
2. Load balancing services
3. Distributed firewall
4. Endpoint on an internal secure network
5. Target Horizon virtual machine
6. Redundant connection servers
7. Redundant access point

**Access point configuration**

1. Access point HVAP-01a is paired to Connection Server HVCS-01a
2. Access point HVAP-02a is paired to Connection Server HVCS-02a
VMware Horizon 7 Network Ports
Securing external access using VMware Horizon access servers

In this module we are going to demonstrate HTML Blast access to an internal Windows 10 vm using load balanced Horizon View Access servers paired to connection servers.

Lesson 1: Verify external access to internal protected network is secure

Launch **Google Chrome** from your Main Console

Attempt to connect to the "view-internal.corp.local" Horizon infrastructure.

1. Click on the **Horizon folder**.
2. Click the **Horizon Internal access** shortcut.
1. After approximately 24 seconds this connection will timeout and fail. This is by design, the browser is attempting to connect to the internal name space `view-internal.corp.local` and is being blocked by the Distributed firewall and ESG.
Launch the command prompt

1. From the task bar click the **command prompt icon**

Determine what resource the view-internal.corp.local name space is mapped to

1. At the command prompt type the following and press enter

```plaintext
ping view-internal.corp.local
```

2. Note that the target is 172.16.60.100
The reason the timeout is occurring is because there is a distributed firewall rule blocking TCP 443 authentication access between our source machine and the view-internal load balancer for Horizon View services. (Note, ICMP is allowed in the entire environment, this is why ping works however the Web page is blocked)

1. Source machine
2. Destination Load balancing services
3. Distributed firewall rule
Close the command prompt window

1. Click the X button

Lesson 2: Exploring the NSX firewall configuration

In this lesson we will explore the Distributed firewall rules blocking the access.

Launch the VMware Web client

1. Open a new tab from Chrome on your Main console machine

Launch the vSphere Web Client

1. Click the vSphere Web (Flash) shortcut
Log in to the VMware Web Client

1. **Check** the Use Windows session authentication **check box**.
2. Click **Login**.

Alternate credentials:

Input user name **administrator@corp.local**

Input password **VMware1!**
Navigate to networking and Security

1. Click the **Home button**
2. Click on **Networking and security**
Open the distributed firewall

1. Click on **Firewall**
2. Scroll the **bottom scroll bar** all the way to the **right**
3. Scroll the **inside scroll bar** all the way to the **bottom**
Locate the block rules section

1. **Scroll** the **bottom scroll bar** back to the **left**
2. **Expand** the Block rules section
1. Feel free to explore the BlockView rule settings and note the firewall rule settings below (Note: you will need to use the bottom scroll bar to view all of the rule settings)

Rule = BlockView
Source = Main Console
Destination = View internal load balancer
Service = Any
Action = Block
Disable Block View rule

1. Click the green sliders next to rule 18 and 19 to turn them gray.
2. Click Publish Changes.
Connect to the view-internal.corp.local name space from the external network

1. Change focus back to the view-internal tab.
2. Click refresh button.
Verify that the Page now displays

The View-internal.corp.local name space will connect you to one of the redundant Horizon connection servers through a NSX load balancer.

1. Verify that the **VMware Horizon** landing page is accessible
2. In module four we explored the use of the view-internal.copr.local namespace from an internal desktop. There is no need to move forward and log in at this time.

Return focus to the Web Client Tab
1. Click the **vSphere Web Client** Tab

**Re-enable rules 18 and 19**

1. Click the **gray sliders next to rule 18 and 19** to turn them green
2. Click **Publish Changes**

**Lesson 3: Connection to a Horizon hosted virtual machine through a NSX edge gateway to a protected internal network.**

In this lesson we will connect to an internal vm through a load balanced Horizon View Secure Access point.
Open a Chrome incognito window

1. Click the **three dots** in the top right of the Chrome window.
2. Click the **New incognito window**.

Launch the view-external.corp.local web page

1. Click the **Horizon folder**
2. Launch the **Horizon External Access** shortcut
Access the VMware Horizon HTML interface

1. Click on the **VMware Horizon HTML Access** link

Log in to VMware Horizon

1. Type user **qeuser**
2. Type password **VMware1!**
3. Click **Login**
Launch the Windows-10 pool

1. Click the **Windows-10** icon
Verify you are connected to Win10-View-01a

You are now connected through a tunneled Blast session, refer to the topology diagram for more information

1. Verify you are connected to the Win10-View-01a virtual machine
Launch a command window

1. Click the **circle** in the windows task bar.
2. Type **cmd** and press **enter**.

Verify you are connected through HVAP-01a

1. Type **netstat** and press **enter**
2. **Note** that we are connected through **172.16.70.20**, this is a Horizon access gateway server HVAP-02a acting as a proxy for the blast connection.

Move on to Lesson 4 to learn more about the Horizon access point servers and how they are configured.
Close the Horizon Chrome session

1. Click the X button to close.

Lesson 4: Explore the Horizon Access Server load balancer configuration

In lesson 4 we will explore the Horizon view access point configuration

A Horizon View Access Point functions as a secure gateway for users who want to access Horizon 7 desktops and applications from outside the corporate firewall.

Access Point appliances typically reside within a DMZ and act as a proxy host for connections inside your company’s trusted network. This design provides an additional layer of security by shielding View virtual desktops, application hosts, and View Connection Server instances from the public-facing Internet.

This configuration utilizes a NSX load balancer to target two redundant Access Points that are in turn paired with two redundant connection servers. Refer to the topology diagrams below.
Lesson 4 Topology

The key components are outlined here.

1. External endpoint
2. Load balancing services
3. Distributed firewall
4. Endpoint on an internal secure network
5. Target Horizon virtual machine
6. Redundant connection servers
7. Redundant access point
1. The Access point appliance is placed between the DMZ and the internal secure connection servers to proxy View connections from external networks.
Access point connection server pairing

1. Access point HVAP-01a is paired to Connection Server HVCS-01a
2. Access point HVAP-02a is paired to Connection Server HVCS-02a

Launch the vSphere Web client

1. **Launch Chrome** from your Main console machine
Log in to the VMware Web Client

1. **Check** the Use Windows session authentication checkbox.
2. Click **Login**

Alternate credentials if needed:

Input user name **administrator@corp.local**

Input password **VMware1!**
Navigate to networking and Security

1. Click the **Home button**
2. Click on **Networking and security**

Open the perimeter-Gateway-01 ESG

1. Click **NSX Edges**
2. Double Click **edge-3 Perimeter-Gateway-01**
Open the view-external application profile

1. Click the **manage** tab
2. Click on the **Load Balancer** tab
3. Select **Application profiles**
4. Click the **edit** icon
Explore the Application Profile for Horizon View

1. Notice that the Application profile is set to HTTPS and is using SSL passthrough
2. Once complete Click **Cancel** *(note: you may need to drag the configuration widow up to access the cancel button)*
Open the Access point service monitor

1. Select service monitoring
2. Highlight the view-external-auth monitor-4
3. Click the Edit icon
Explore the view-external service monitor settings

1. Notice that the monitor is set to HTTPS and is configured to detect a /portal page
2. Once complete Click Cancel (note: you may need to drag the configuration widow up to access the cancel button)
Explore the pool statistics

1. Select the **Pools** section
2. Click on **Show Pool statistics**
3. Click on **Pool-1**
4. Notice that there are two access servers configured to receive requests.
Module 5 Summary

In module five we demonstrated access to two load balanced Horizon access servers through a NSX load balancer. We also explored the firewall configuration required to secure external connections to a Horizon View environment. This secure external HTML access enables internal applications to be securely delivered for production environments.

Proceed to any module below which interests you most.

- **Module 1 - Installation and configuration of Trend Deep Security** (30 minutes) (Basic) In this module we'll go over the installation and configuration of the Trend Deep Security platform.
- **Module 2 - Protecting Horizon Desktops with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 2 we will go over how we can use Horizon in concert with NSX and Trend Micro to protect the end user.
- **Module 3 - Protecting Web Servers against exploits with NSX and Trend Micro Deep Security** (45 minutes) (Advanced) In Module 3 we will go over how you can protect Web Servers with NSX and Trend
- **Module 4 - Securing and protecting internal access using NSX load balancing** (30 Minutes) (Advanced) In Module 4 we'll show how we can leverage NSX load balancing
- **Module 5 - Securing and protecting external access using VMware Horizon access servers** (45 Minutes) (Advanced) In Module 5 we'll explore ways to protect external access to our environment.

Lab Captain:

Kevin Moats Staff TAM United States

How to End Lab

To end your 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-1941-01-NET

Version: 20181114-024553