VMware NSX-T Data Center: Install, Configure, Manage [V3.0]

Lab Manual

NSX-T Data Center 3.0

VMware® Education Services
VMware, Inc.
www.vmware.com/education

VMware NSX-T Data Center: Install, Configure, Manage [V3.0]

Lab Manual

NSX-T Data Center 3.0

Part Number EDU-EN-NSXTICM3-LAB (14-MAY-2021)

Typographical Conventions

The following typographical conventions are used in this course.

Conventions	Usage and Examples
`Monospace`	Identifies command names, command options, parameters, code fragments, error messages, filenames, folder names, directory names, and path names: • Run the `esxtop` command. • … found in the `/var/log/messages` file.
`Monospace Bold`	Identifies user inputs: • Enter **`ipconfig /release`**.
Boldface	Identifies user interface controls: • Click the **Configuration** tab.
Italic	Identifies book titles: • *vSphere Virtual Machine Administration*
< >	Indicates placeholder variables: • <ESXi_host_name> • … the `Settings/<Your_Name>.txt` file

Contents

Lab 1 Introduction to Labs

Lab Environment: Key Knowledge Points

The lab environment in which you work is highlighted by the Lab Environment topology map.

You must be aware of the following items that impact the NSX-T Data Center 3.0 ICM lab performance:

- You access and manage the lab environment from the student desktop.
- The student desktop resides on the Management network (SA-Management), and you can start deploying the various NSX-T Data Center fabric items from here.
- A vCenter Server system and NSX Manager instance are predeployed with two clusters that are populated with various virtual machines.
- At various points in the labs, you are directed to copy and paste information for later use.

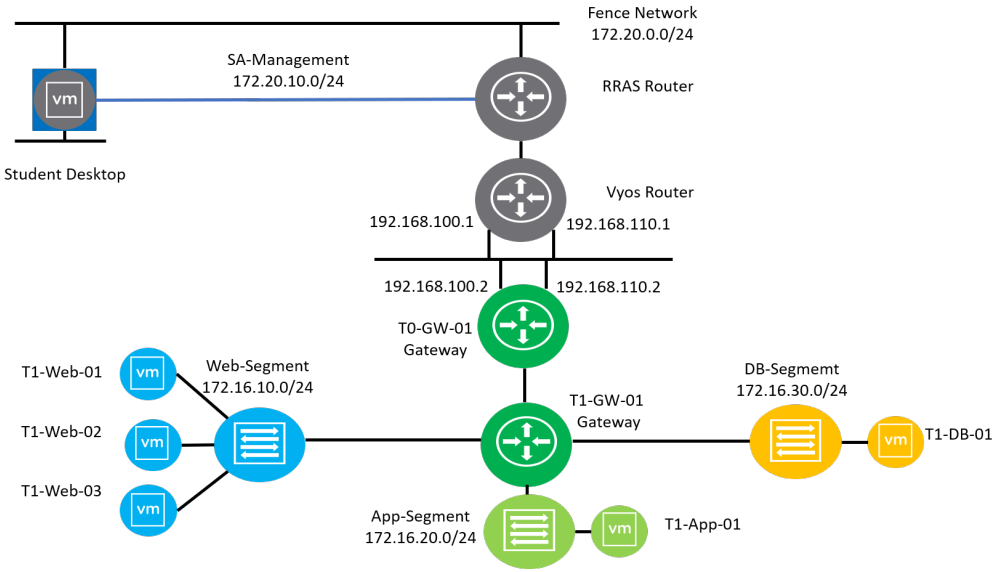
  a. When you initially access the student desktop, right-click the **Start** button, select **Run**> **Notepad**, and add the useful information to the file.

     - Password used on many occasions: `VMware1!VMware1!`
     - User Name for the vSphere Client: `administrator@vsphere.local`

  b. Save the file to your desktop and name it as `Lab-notes`.

Lab Environment Topology Map

You can view the topology map periodically while configuring the NSX-T Data Center environment.



Lab 2 Reviewing the Configuration of the Predeployed NSX Manager Instance

Objective and Tasks

Verify the NSX Manager appliance settings:

1. Access Your Lab Environment
2. Prepare for the Lab
3. Verify the vCenter Server and the ESXi Hosts Licensing
4. Verify the NSX Manager Configuration and Licensing
5. Use the NSXCLI to Review the NSX Manager Cluster Information
6. Register vCenter Server as a Compute Manager

In this lab environment, you use a single-node NSX cluster. In a production environment, a three-node cluster must be deployed to provide redundancy and high availability.

Task 1: Access the Lab Environment

You access and manage the lab environment from the student desktop. The system assigned to you serves as an end-user terminal.

1. Verify that you are successfully logged in to the student desktop.

   If not, log in to your student desktop by entering `vclass\administrator` as the username and `VMware1!` as the password.

Task 2: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. On your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.

      Use Chrome as your primary browser, unless specified otherwise.

   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.

   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.

2. Log in to the NSX UI.
   a. Open another tab in Chrome.

   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.

   c. If the `Your connection is not private` message appears, click **ADVANCED** and click the **Proceed to sa-nsxmgr-01.vclass.local (unsafe)** link.

   d. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 3: Verify the vCenter Server and the ESXi Hosts Licensing

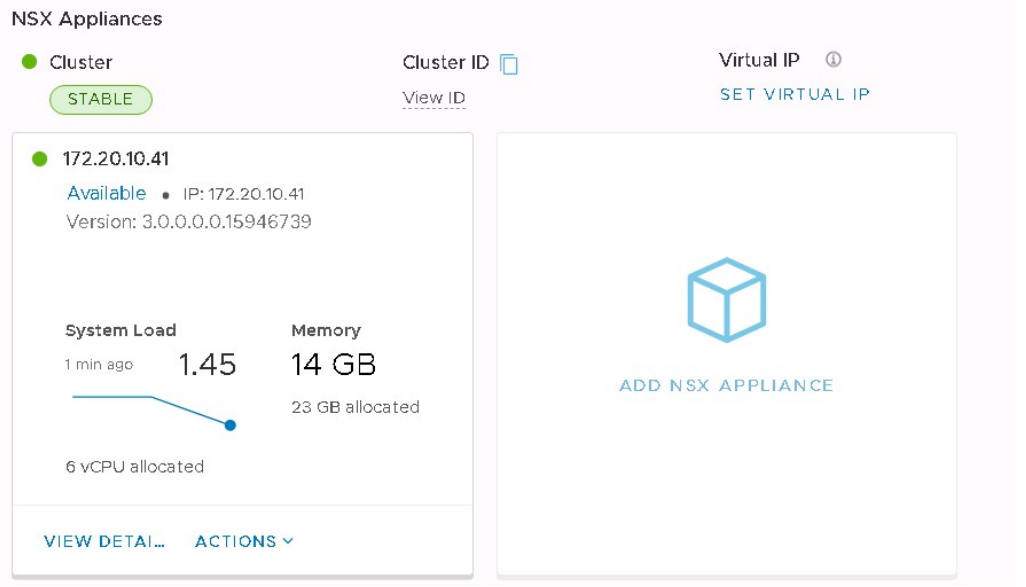
You verify the licenses of the vCenter Server and ESXi hosts.

1. In the vSphere Client UI, select **Administration** from the Menu drop-down menu**.**
2. In the Navigator pane, click **Licenses.**
3. Verify that the vCenter Server license is valid.
    a. In the middle pane, click the **Assets** tab.
    b. Click the **vCenter Server Systems** tab and view the license expiration date.
4. If the license is not valid, assign a vCenter Server license key to the vCenter Server instance.
    a. Follow this link to retrieve the vCenter Server license key.
    b. With your vCenter Server instance selected, click **Assign License**.
    c. Navigate to the **NEW LICENSE** tab.
    d. In the **License key** text box, enter or paste the vCenter Server license key.
    e. Review the expiration date and license capacity.
    f. Click **OK.**
5. Verify that the ESXi hosts licenses are valid.
    a. In the center pane, click the **Assets** tab.
    b. Click the **Hosts** tab and view the license expiration dates.
6. If the licenses are not valid, assign a license key to all ESXi hosts.
    a. Follow this link to retrieve the ESXi host license key.
    b. Select all ESXi hosts in the list.
    c. Click **Assign License**.
    d. At the `Perform this action on 5 objects?` prompt, click **YES**.
    e. Navigate to the **NEW LICENSE** tab.
    f. In the **License key** text box, enter or paste the license key**.**
    g. Review the expiration date and license capacity.
    h. Click **OK.**

Task 4: Verify the NSX Manager Configuration and Licensing

You examine the configuration and licensing information of the predeployed NSX Manager appliance.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Appliances**.
2. Under NSX Appliances**,** view the information of the predeployed NSX Manager instance (172.20.10.41), including the IP address, NSX version, cluster status, and resource utilization.



   Information appears for only one NSX Manager node because you use a single-node cluster in this lab.

   For now, you can safely ignore the following alert *"A compute manager is required to deploy an appliance. To add a computer manager, visit the COMPUTE MANAGERS page"*. You will add a computer manager in an upcoming task in this lab.

3. Verify the license of NSX Manager by clicking **System** > **Settings** > **Licenses**.

   Two valid licenses should be assigned to NSX Manager.

   If not, follow this link to retrieve the NSX Manager license key.

Task 5: Use the NSXCLI to Review the NSX Management Cluster Information

You use the NSXCLI to review the configuration and status information of the NSX cluster.

1. On your student desktop, open the MTPuTTY application from the system tray.
2. Double-click **sa-nsxmgr-01** to open a console connection.
3. If a PuTTY security alert appears, click **Yes** to proceed.
4. Disable the command-line timeout.
   ```
   set cli-timeout 0
   ```
5. View the status of the NSX cluster.

   ```
   get cluster status
   ```

   This command returns the status for each of the roles in the NSX cluster, including Policy, Manager, and Controller. The cluster for each of these components is STABLE.

   NOTE

   In this lab, you use a single-node NSX cluster.

Task 6: Register vCenter Server as a Compute Manager

You configure vCenter Server as a compute manager.

1. If not open already , open a new tab in your browser and click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
2. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Compute Managers** and click **+ADD**.
3. On the New Compute Manager page, provide the configuration details.

Option	Action
Name	Enter **`sa-vcsa-01.vclass.local`**.
FQDN or IP Address	Enter **`172.20.10.94`**.
Username	Enter **`administrator@vsphere.local`**.
Password	Enter **`VMware1!`**.
SHA-256 Thumbprint	Leave the text box blank.

   Leave the default values for all the other options.

4. Click **ADD.**
5. When the `Thumbprint is Missing` message appears, click **ADD** to use the server's default thumbprint.
6. Click **Refresh** at the bottom of the display to update the contents.

   The registration status appears as Registered and the connection status appears as Up.

7. Verify that the version of vCenter Server is 7.0.0.

Lab 3 (Simulation) Deploying a Three-Node NSX Management Cluster

Objective and Tasks

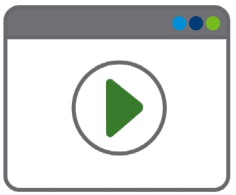
Deploy a three-node NSX Management cluster from the NSX UI:

1. Prepare for the Lab
2. Deploy the Second NSX Manager
3. Deploy the Third NSX Manager
4. Review the NSX Management Cluster Information from the NSX UI
5. Review the NSX Management Cluster Information from the NSX CLI

From your local desktop, go to https://vmware.bravais.com/s/8KkvsPi341xTZR1i8PRV to open the simulation.

IMPORTANT

This is a simulation. Do NOT perform these steps in your actual lab environment.



IMPORTANT

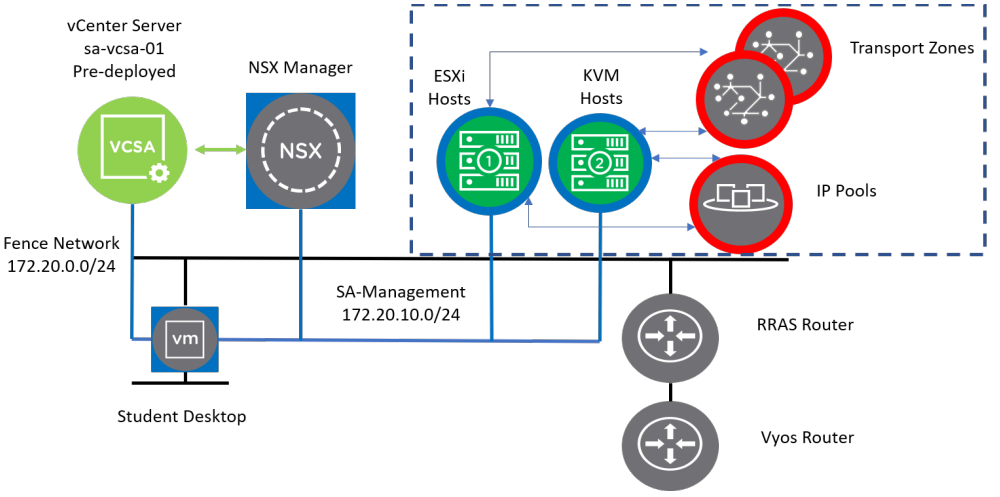
Do not refresh, navigate away from, or minimize the browser tab hosting the simulation. These actions might pause the simulation and the simulation might not progress.

Lab 4 Preparing the NSX Infrastructure

Objective and Tasks

Deploy transport zones, create IP pools, and prepare hosts for use by NSX:

1. Prepare for the Lab
2. Create Transport Zones
3. Create IP Pools
4. Prepare the ESXi Hosts
5. Prepare the KVM Hosts



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. From your student desktop, open Chrome.
2. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
3. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create Transport Zones

You create an overlay transport zone and a VLAN transport zone.

1. Create an overlay transport zone.
   a. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Transport Zones** and click **+ADD.**
   b. In the New Transport Zone window, create a transport zone.

Option	Action
Name	Enter **`PROD-Overlay-TZ`**.
Switch Name	Enter **`PROD-Overlay-NVDS`**.
Traffic Type	Click **Overlay** (default).
Uplink Teaming Policy Name	Leave the text box blank.

   c. Click **ADD.**

      A new transport zone appears.

2. Create a VLAN-based transport zone to communicate with the nonoverlay networks that are external to NSX-T Data Center.
   a. Click **+ADD**.
   b. In the New Transport Zone window, create a transport zone.

Option	Action
Name	Enter **`PROD-VLAN-TZ`**.
Switch Name	Enter **`PROD-VLAN-NVDS`**.
Traffic Type	Select **VLAN**.
Uplink Teaming Policy Name	Leave the text box blank.

   c. Click **ADD.**

      A new transport zone appears.

Task 3: Create IP Pools

You create an IP pool for assigning IP addresses to the NSX transport nodes.

1. On the NSX UI Home page, navigate to **Networking** > **IP Management** > **IP Address Pools** and click **ADD IP ADDRESS POOL**.
2. Provide the configuration details in the ADD IP ADDRESS POOL window.
   a. Enter **`VTEP-IP-Pool`** in the **Name** text box.
   b. Enter **`IP Pool for ESXi, KVM, and Edge`** in the **Description** text box.
   c. Click **Set** under Subnets and select **ADD SUBNET** > **IP Ranges**.
   d. In the **IP Ranges/Block** text box, enter **`172.20.11.151-172.20.11.170`** and click **Add item(s)**.
   e. In the **CIDR** text box, enter **`172.20.11.0/24`**.
   f. In the **Gateway IP** text box, enter **`172.20.11.10`**.
   g. Click **ADD** on the ADD SUBNETS page.
3. Click **APPLY** on the Set Subnets page.
4. Click **SAVE**.

Task 4: Prepare the ESXi Hosts

You prepare the ESXi hosts to participate in the virtual networking and security functions offered by NSX-T Data Center.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Nodes** > **Host Transport Nodes**.
2. From the **Managed by** drop-down menu, select **sa-vcsa-01.vclass.local.**

   Two clusters appear: SA-Management-Edge and SA-Compute-01.
3. Expand the **SA-Compute-01** cluster view.

   The NSX Configuration status of the hosts appears as Not Configured and the Node Status is Not Available.
4. Select the **SA-Compute-01** check box and click **CONFIGURE NSX.**
5. In the NSX Installation dialog box, click **Create New Transport Node Profile**.
6. Provide the required details in the Add Transport Node Profile page.

Option	Action
Name	Enter **`ESXi-TN-Profile`**.
Type	Select **N-VDS (default).**
Mode	Select **Standard (All hosts) (default).**
Name (Node Switch)	Enter **`PROD-Overlay-NVDS`**.
Transport Zone	Select **PROD-Overlay-TZ.**
NIOC Profile	Select **nsx-default-nioc-hostswitch-profile.**
Uplink Profile	Select **nsx-default-uplink-hostswitch-profile.**
LLDP Profile	Select **LLDP [Send Packet Disabled]**.
IP Assignment	Select **Use IP Pool**.
IP Pool	Select **VTEP-IP-Pool**.
Teaming Policy Switch Mapping	Enter **`vmnic4`** next to uplink-1 (active).

   Leave the default values for all other settings.
7. Click **ADD**.

8. In the NSX Installation window, click **APPLY.**

   The autoinstall process starts.

   The process might take approximately 5 minutes to complete.

9. When the installation completes, verify that NSX is installed on the hosts and the status of the SA-Compute-01 cluster nodes is Up.

   You might need to click **REFRESH** at the bottom to refresh the page.

Task 5: Prepare the KVM Hosts

You prepare the kernel-based virtual machine (KVM) hosts to participate in the NSX virtual networking and security functions.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Nodes** > **Host Transport Nodes**.
2. Add the sa-kvm-01 KVM host to NSX.
   a. From the **Managed by** drop-down menu, select **None: Standalone Hosts.**
   b. Click **+ADD.**
   c. Provide the configuration details in the Add Transport Node-Host Details page.

Option	Action
Name	Enter **`sa-kvm-01.vclass.local.`**
IP Addresses	Enter **`172.20.10.151`**.
Operating System	Select **Ubuntu KVM.**
Username	Enter **`vmware`**.
Password	Enter **`VMware1!`**.
SHA-256 Thumbprint	Leave the text box blank.

   d. Click **Next.**
   e. When the `Thumbprint is missing` message appears, click **ADD.**
   f. In the Add Transport Node wizard, click **Next**.

g. In the Configure NSX window, provide the configuration details.

Option	Action
N-VDS Creation	Select **NSX Created (default).**
Mode	Select **Standard (All hosts) (default).**
Name (Node Switch)	Enter **`PROD-Overlay-NVDS`**.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-default-uplink-hostswitch-profile.**
LLDP Profile	Select **LLDP [Send Packet Disabled].**
IP Assignment	Select **Use IP Pool.**
IP Pool	Select **VTEP-IP-Pool.**
Teaming Policy Switch Mapping	Enter **`eth1`** next to uplink-1 (active).

Ignore the `Host running on OS other than ESXi/Windows Server will need third party package installed to display physical NICs` message.

h. Click **FINISH** and the NSX Install process starts.

This process might take approximately 5 minutes to complete.

3. Add the sa-kvm-02 KVM host to NSX.

a. From the **Managed by** drop-down menu, select **None: Standalone Hosts.**

b. Click **+ADD.**

c. Provide the configuration details in the Add Transport Node-Host Details page.

Option	Action
Name	Enter **`sa-kvm-02.vclass.local.`**
IP Addresses	Enter **`172.20.10.152`**.
Operating System	Select **Ubuntu KVM.**
Username	Enter **`vmware`**.
Password	Enter **`VMware1!`**.
SHA-256 Thumbprint	Leave the text box blank.

d. Click **Next.**

e. When the `Thumbprint is missing` message appears, click **ADD.**

f. In the Add Transport Node wizard, click **Next**.

g. In the Configure NSX window, provide the configuration details:

Option	Action
N-VDS Creation	Select **NSX Created (default).**
Mode	Select **Standard (All hosts) (default).**
Name (Node Switch)	Enter **`PROD-Overlay-NVDS`**.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-default-uplink-hostswitch-profile.**
LLDP Profile	Select **LLDP [Send Packet Disabled].**
IP Assignment	Select **Use IP Pool.**
IP Pool	Select **VTEP-IP-Pool.**
Teaming Policy Switch Mapping	Enter **`eth1`** next to uplink-1 (active).

You can safely ignore the message: `Host running on OS other than ESXi/Windows Server will need third party package installed to display physical NICs.`

h. Click **FINISH** and the NSX Install process starts.

This process might take approximately 5 minutes to complete.

4. Verify that the configuration state appears as Success and the node status appears as Up for the two KVM hosts.

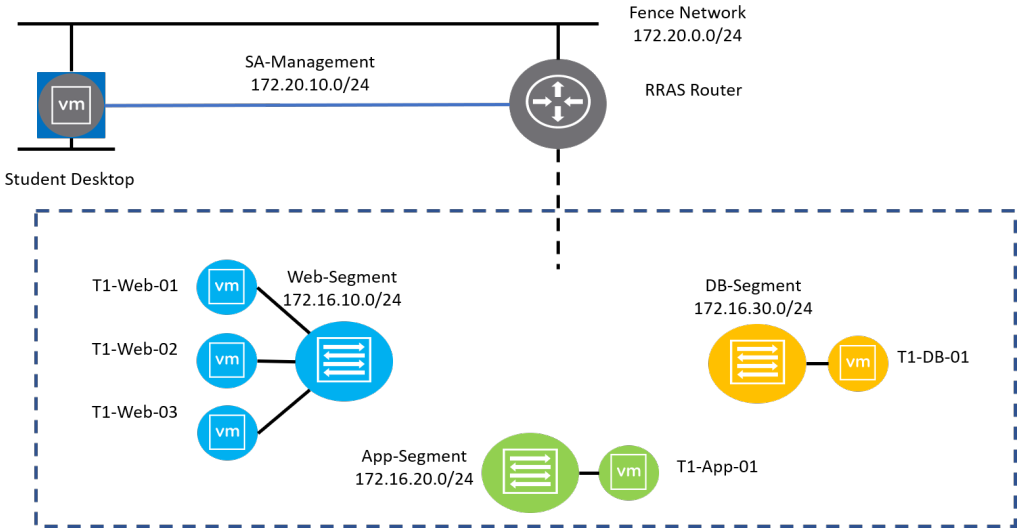
   You might need to refresh the page to update the status of the installation.

Lab 5 Configuring Segments

Objective and Tasks

Create segments for VMs residing on the ESXi and KVM hosts:

1. Prepare for the Lab
2. Create Segments
3. Attach VMs to Segments
4. Test Layer 2 Connectivity and Verify the Configuration of Segments



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create Segments

You create three segments to provide L2 connectivity.

1. Create a segment named Web-Segment.
   a. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments.**
   b. Click **ADD SEGMENT** and configure the segment.

Option	Action
Segment Name	Enter **`Web-Segment`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.10.1/24`**.

   Leave the default values for all the other options.
   c. Click **SAVE**.
   d. When the message to continue segment configuration appears, click **NO**.

2. Create a segment named App-Segment.
   a. Click **ADD SEGMENT** and configure the segment.

Option	Action
Segment Name	Enter **`App-Segment`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.20.1/24`**.

   Leave the default values for all the other options.
   b. Click **SAVE**.
   c. When the message to continue segment configuration appears, click **NO**.
3. Create a segment named DB-Segment.
   a. Click **ADD SEGMENT** and configure the segment.

Option	Action
Segment Name	Enter **`DB-Segment`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.30.1/24`**.

   Leave the default values for all the other options.
   b. Click **SAVE**.
   c. When the message to continue segment configuration appears, click **NO**.
4. Verify that the three segments are created successfully and the Status is Up.
5. On the vSphere Client Home page, click **Menu > Networking.**
6. Verify that the three newly created segments are listed under SA-Datacenter.

Task 3: Attach VMs to Segments

You attach VMs running on the ESXi hosts and KVM hosts to their corresponding segments.

1. In the navigator pane of the vSphere Client, click the **Hosts and Clusters** tab and expand the view of **SA-Datacenter** > **SA-Compute-01.**
2. Add T1-Web-01 to the Web-Segment segment.
    a. Right-click **T1-Web-01** and select **Edit Settings.**
    b. From the **Network adapter 1** drop-down menu, select **Browse**, select **Web-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**
3. Add T1-Web-02 to the Web-Segment segment.
    a. Right-click **T1-Web-02** and select **Edit Settings.**
    b. From the **Network adapter 1** drop-down menu, select **Browse**, select **Web-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**
4. Add T1-App-01 to the App-Segment segment.
    a. Right-click **T1-App-01** and select **Edit Settings.**
    b. From the **Network adapter 1** drop-down menu, select **Browse**, select **App-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**

5. Power on T1-DB-01 on the sa-kvm-01 host.
   a. Open MTPuTTY and double-click the **SA-KVM-01** connection.
   b. Switch the user to root.

      ```
      sudo -s
      ```

   c. Check the status of the VMs running on the SA-KVM-01 host.

      ```
      virsh list --all
      ```

      The T1-DB-01 VM is in the shutoff state.

   d. Power on the VM.

      ```
      virsh start T1-DB-01
      ```

   e. Verify that T1-DB-01 is powered on.

      ```
      virsh list --all
      ```

6. Attach T1-DB-01 to the DB-Segment segment.
   a. At the SA-KVM-01 command prompt, view the UUID (shown as `interfaceid`) that is associated with T1-DB-01.

      ```
      virsh dumpxml T1-DB-01 | grep interfaceid
      ```

   b. Copy and paste the UUID to a Notepad file so that it can be used in a future step.

      In this example, the UUID associated with T1-DB-01 is 57601300-2e82-48c4-8c27-1e961ac70e81.

   c. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments**, click the vertical ellipsis icon next to DB-Segment, and select **Edit**.
   d. Under Ports, click **Set** and click **ADD SEGMENT PORT**.

      The Set Segment Ports window appears.

   e. Provide the details in the Set Segment Ports window.

Option	Action
Name	Enter **`DB01-Segment-Port`**.
ID	Copy and paste the ID (numbers between the single quotes) from the Notepad file.

   f. Click **SAVE.**
   g. Click **CLOSE.**
   h. Click **CLOSE EDITING**.

7. Power on T1-Web-03 on the sa-kvm-02 host.
   a. Open MTPuTTY and double-click the **SA-KVM-02** connection.
   b. Switch the user to root.

      ```
      sudo -s
      ```

   c. Check the status of the VMs running on the SA-KVM-02 host.

      ```
      virsh list --all
      ```

   d. Power on the VM.

      ```
      virsh start T1-Web-03
      ```

   e. Verify that T1-Web-03 is powered on.

      ```
      virsh list --all
      ```

8. Attach T1-Web-03 to the Web-Segment segment.
   a. At the SA-KVM-02 command prompt, view the UUID (shown as `interfaceid`) associated with T1-Web-03.

      ```
      virsh dumpxml T1-Web-03 | grep interfaceid
      ```

   b. Copy and paste the UUID to a Notepad file so that it can be used in a future step.

      In this example, the UUID associated with T1-Web-03 is 57601300-2e82-48c4-8c27-1e961ac70e79.

   c. On the NSX UI Home page, click **Networking** > **Connectivity** > **Segments**, click the vertical ellipsis icon next to Web-Segment, and select **Edit**.
   d. Under Ports, click **2**, and click **ADD SEGMENT PORT**.

      If the number of ports configured does not appear, click the **REFRESH** button.

   e. Provide the details in the Set Segment Ports window.

Option	Action
Name	Enter **`Web03-Segment-Port`**.
ID	Copy and paste the ID (numbers between the single quotes) from the Notepad file.

   f. Click **SAVE.**
   g. Click **CLOSE.**
   h. Click **CLOSE EDITING**.

Task 4: Test Layer 2 Connectivity and Verify the Configuration of Segments

You verify the information about segments from the NSX Manager instance and the data plane.

1. Open a console connection to T1-Web-01.
   a. On the vSphere Client Home page, click **Hosts and Clusters.**
   b. In the Navigator pane, click **T1-Web-01** and select **Launch Web Console.**
   c. When the web console window opens, click in the window and press enter to activate the screen.
   d. Enter **root** as the user name and **VMware1!** as the password.
2. Ping the T1-Web-02 (172.16.10.12) VM which resides on an ESXi host.

   ```
   ping -c 3 172.16.10.12
   ```

   Your ping should be successful.
3. Ping the T1-Web-03 (172.16.10.13) VM which resides on a KVM host.

   ```
   ping -c 3 172.16.10.13
   ```

   Your ping should be successful.
4. Retrieve the UUID information for each segment.
   a. Use MTPuTTY to connect to sa-nsxmgr-01.
   b. Retrieve information for the segments.

      ```
      get logical-switches
      ```

      ```
      sa-nsxmgr-01> get logical-switches
      VNI UUID Name
      69633 20d91369-b964-4ff6-a8a9-f8c263dc7213 App-Segment
      69632 8fd97015-4bdc-47eb-ad98-d67608f82e75 Web-Segment
      69634 4fa53e28-3923-4d6f-865c-5736e0e1d02a DB-Segment
      ```

   c. Record the UUID value for Web-Segment in a Notepad file.

      ```
      69632 8fd97015-4bdc-47eb-ad98-d67608f82e75 Web-Segment
      ```

      The UUIDs in your lab environment might be different.
5. Retrieve the Tunnel Endpoint (TEP) information for Web-Segment.

   ```
   get logical-switch <Web-Segment_UUID> vtep
   ```

   The sample output shows the TEPs connected to the Web-Segment.

   ```
   sa-nsxmgr-01> get logical-switch 8fd97015-4bdc-47eb-ad98-
   d67608f82e75 vtep
   ```

6. Retrieve the MAC table information for Web-Segment.

   ```
   get logical-switch <Web-Segment_UUID> mac
   ```

   ```
   sa-nsxmgr-01> get logical-switch 8fd97015-4bdc-47eb-ad98-
   d67608f82e75 mac
   ```

7. Retrieve the ARP table information for Web-Segment.

   ```
   get logical-switch <Web-Segment_UUID> arp
   ```

   ```
   sa-nsxmgr-01> get logical-switch 8fd97015-4bdc-47eb-ad98-
   d67608f82e75 arp
   ```

   If your Address Resolution Protocol (ARP) table is empty, initiate a ping between the Web-Segment VMs.

8. Retrieve information about the established host connections on Web-Segment.

   ```
   get logical-switch <Web-Segment_UUID> ports
   ```

   ```
   sa-nsxmgr-01> get logical-switch 8fd97015-4bdc-47eb-ad98-
   d67608f82e75 ports
   ```

9. Use MTPuTTY to connect to the sa-esxi-04 host.

10. Access the `nsxcli` command line.

    ```
    nsxcli
    ```

11. Retrieve the segment information from the sa-esxi-04 host.

    ```
    get logical-switches
    ```

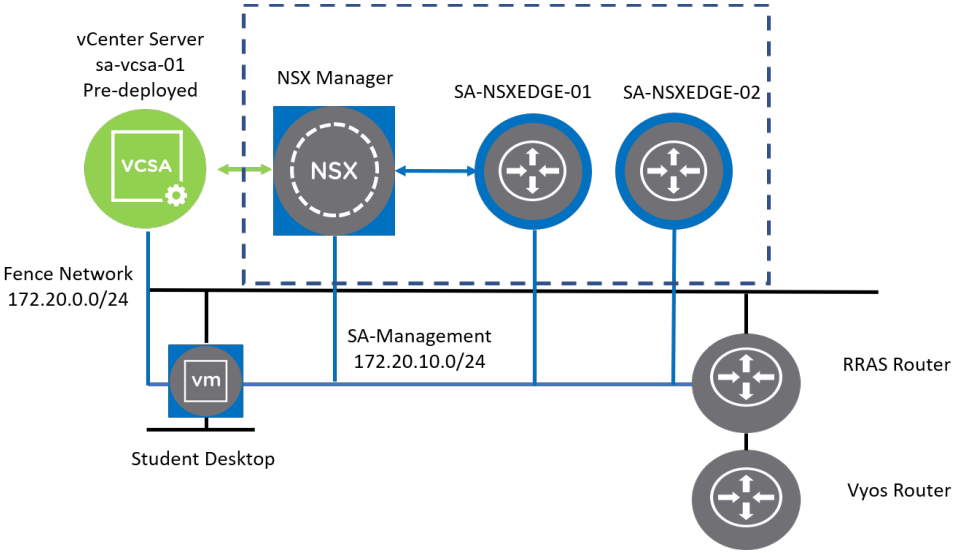
```
sa-esxi-04.vclass.local> get logical-switches
Logical Switches Summary
------------------------------------------------------------

Overlay Kernel Entry
============================================================
VNI DVS name VIF num
69632 PROD-Overlay-NVDS 1
69633 PROD-Overlay-NVDS 1

Overlay LCP Entry
============================================================
VNI Logical Switch UUID Name
69632 8fd97015-4bdc-47eb-ad98-d67608f82e75 Web-Segment
69633 20d91369-b964-4ff6-a8a9-f8c263dc7213 App-Segment

VLAN Backed Entry
============================================================
Logical Switch UUID VLAN ID
```

Lab 6 Deploying and Configuring NSX Edge Nodes

Objective and Tasks

Deploy NSX Edge nodes and configure them as transport nodes:

1. Prepare for the Lab
2. Deploy Two NSX Edge Nodes
3. Configure an Edge Cluster



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. On your student desktop, log in to the vSphere Web Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Deploy Two NSX Edge Nodes

You deploy NSX Edge nodes on ESXi hosts to perform routing and other Layer 3 networking functionality.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Nodes** > **Edge Transport Nodes**.
2. Click **+ADD EDGE VM.**
3. Provide the configuration details in the Add Edge VM window.

Option	Action
Name	Enter **`sa-nsxedge-01`**.
Host name/FQDN	Enter **`sa-nsxedge-01.vclass.local`**.
Form Factor	Click **Medium** (default).

4. Click **NEXT.**
5. On the Credentials page, enter **`VMware1!VMware1!`** as the CLI password and the system root password.
6. Click the **Allow SSH Login** and **Allow Root SSH Login** toggles to display Yes.
7. Click **NEXT.**

8. On the Configure Deployment page, provide the configuration details.

Option	Action
Compute Manager	Select **sa-vcsa-01.vclass.local.**
Cluster	Select **SA-Management-Edge.**
Resource Pool	Leave the text box blank.
Host	Leave the text box blank.
Datastore	Select **SA-Shared-02-Remote.**

9. Click **NEXT.**
10. On the Configure Node Settings page, provide the configuration details.

Option	Action
IP Assignment	Select **Static.**
Management IP	Enter **`172.20.10.61/24`**.
Default Gateway	Enter **`172.20.10.10`**.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management,** and click **SAVE**.
Search Domain Names	Enter **`vclass.local`**.
DNS Servers	Enter **`172.20.10.10`**.
NTP Servers	Enter **`172.20.10.10`**.

11. Click **NEXT.**

12. On the Configure NSX page, provide the configuration details.

Option	Action
Edge Switch Name	Enter **PROD-Overlay-NVDS.**
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
IP Assignment	Select **Use IP Pool.**
IP Pool	Select **VTEP-IP-Pool.**
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Overlay**, and click **SAVE**.

13. On the Configure NSX page, click **+ ADD SWITCH** and provide the configuration details.

    You might need to scroll up the page.

Option	Action
Edge Switch Name	Enter **PROD-VLAN-NVDS.**
Transport Zone	Select **PROD-VLAN-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Uplinks**, and click **SAVE**.

14. Click **FINISH**.

    The Edge deployment might take several minutes to complete. The deployment status displays various values, for example, Node Not Ready, which is only temporary**.**

    Wait for the configuration status to appear as Success and the status as Up. You can click **REFRESH** occasionally.

15. On the NSX UI Home page, navigate to **System Configuration** > **Fabric** > **Nodes** > **Edge Transport Nodes** , click **+ADD EDGE VM**, and provide the configuration details to deploy the second edge node.

    a. In the Name and Description window, enter the details.

Option	Action
Name	Enter **`sa-nsxedge-02`**.
Host name/FQDN	Enter **`sa-nsxedge-02.vclass.local`**.
Form Factor	Click **Medium** (default).

    b. In the Credentials window, enter **`VMware1!VMware1!`** as the CLI password and the system root password.

    c. Click the **Allow SSH Login** and **Allow Root SSH Login** toggles to display Yes.

    d. On the Configure Deployment window, enter the details.

Option	Action
Compute Manager	Select **sa-vcsa-01.vclass.local.**
Cluster	Select **SA-Management-Edge.**
Resource Pool	Leave the text box blank.
Host	Leave the text box blank.
Datastore	Select **SA-Shared-02-Remote.**

e. On the Configure Node Settings window, enter the details.

Option	Action
IP Assignment	Select **Static.**
Management IP	Enter **`172.20.10.62/24`**.
Default Gateway	Enter **`172.20.10.10`**.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management**, and click **SAVE**.
Search Domain Names	Enter **`vclass.local`**.
DNS Servers	Enter **`172.20.10.10`**.
NTP Servers	Enter **`172.20.10.10`**.

f. On the Configure NSX window, enter the details.

Option	Action
Edge Switch Name	Enter **`PROD-Overlay-NVDS.`**
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
IP Assignment	Select **Use IP Pool.**
IP Pool	Select **VTEP-IP-Pool.**
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Overlay**, and click **SAVE**.

g. On the Configure NSX page, click **+ ADD SWITCH** and provide the configuration details.

Option	Action
Edge Switch Name	Enter **`PROD-VLAN-NVDS`**.
Transport Zone	Select **PROD-VLAN-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Uplinks**, and click **SAVE**.

h. Click **FINISH**.

The Edge deployment might take several minutes to complete. The deployment status displays various temporary values, for example, Node Not Ready**.**

Wait for the configuration state to appear as Success and the node status as Up. You can click **REFRESH** occasionally.

16. Verify that the two edge nodes are deployed and listed on the Edge VM list.

The configuration state appears as Success and the node status appears as Up**.**

Task 3: Configure an Edge Cluster

You create an NSX Edge cluster and add the two NSX Edge nodes to the cluster.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Nodes** > **Edge Clusters**.
2. Click **+ADD**.
3. Provide the configuration details in the Add Edge Cluster window.

Option	Action
Name	Enter **`Edge-Cluster-01`**.
Edge Cluster Profile	Select **nsx-default-edge-high-availability-profile** (default).
Member Type	Select **Edge Node** (default).

4. In the **Available (2)** pane, select both **sa-nsxedge-01** and **sa-nsxedge-02** and click the right arrow to move them to the Selected (0) pane.

5. Click **ADD.**
6. Verify that Edge-Cluster-01 appears in the Edge Cluster list.

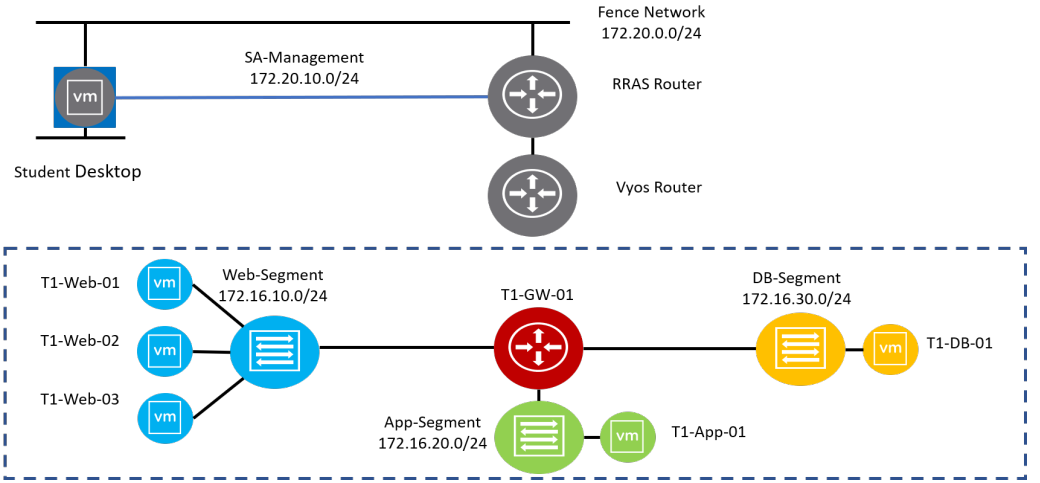
   Click **REFRESH** if Edge-Cluster-01 does not appear after a few seconds.
7. Click **2** in the Edge Transport Nodes column and verify that sa-nsxedge-01 and sa-nsxedge-02 appear in the list.

Lab 7 Configuring the Tier-1 Gateway

Objective and Tasks

Create and configure a Tier-1 gateway for East-West L3 connectivity:

1. Prepare for the Lab
2. Create a Tier-1 Gateway
3. Connect Segments to the Tier-1 Gateway
4. Test East-West L3 Connectivity



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. On your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create a Tier-1 Gateway

You create a Tier-1 gateway to provide east-west connectivity.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-1 Gateways**.
2. Click **ADD TIER-1 GATEWAY**.
3. Provide the configuration details in the ADD TIER-1 GATEWAY window.

Option	Action
Tier-1 Gateway Name	Enter **`T1-GW-01`**.
Linked Tier-0 Gateway	Leave the text box blank because the Tier-0 gateway is not yet created.
Edge Cluster	Leave the text box blank because services are not required at this point.

4. Scroll to the lower portion of the T1-GW-01 gateway, click the expand button next to **Route Advertisement**, and select the options.
   - Turn on the **All Static Routes** toggle.
   - Turn on the **All Connected Segments & Service Ports** toggle.
5. Click **SAVE.**

6. When a message prompts you to continue editing the Tier-1 gateway, click **NO**.

Task 3: Connect Segments to the Tier-1 Gateway

You connect the Web, App, and DB segments to the Tier-1 Gateway.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments**.
2. Click the vertical ellipsis icon next to Web-Segment and select **Edit**.
   a. Select **T1-GW-01** from the **Connectivity** drop-down menu.
   b. Click **SAVE** and click **CLOSE EDITING**.
3. Click the vertical ellipsis icon next to App-Segment and select **Edit**.
   a. Select **T1-GW-01** from the **Connectivity** drop-down menu.
   b. Click **SAVE** and click **CLOSE EDITING**.
4. Click the vertical ellipsis icon next to DB-Segment and select **Edit**.
   a. Select **T1-GW-01** from the **Connectivity** drop-down menu.
   b. Click **SAVE** and click **CLOSE EDITING**.

Task 4: Test East-West L3 Connectivity

You verify east-west connectivity among the tenant networks.

1. In the vSphere Client, open a web console to T1-Web-01.
2. If not already logged in, enter **`root`** as the user name and **`VMware1!`** as the password.
3. From T1-Web-01, verify that you can reach the virtual machines in App-Segment and DB-Segment.

   `ping -c 3 172.16.20.11` (T1-App-01)

   `ping -c 3 172.16.30.11` (T1-DB-01)

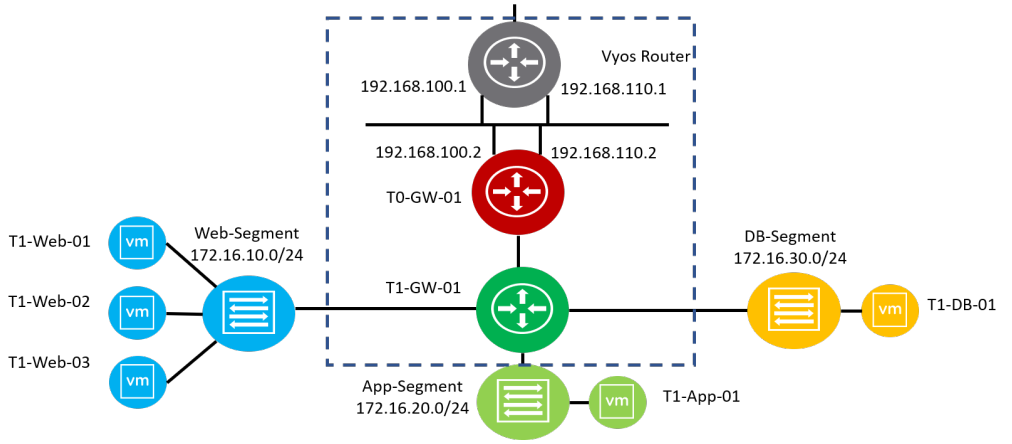
   Both pings should be successful. If the pings fail, verify that both virtual machines are powered on.

Lab 8 Configuring the Tier-0 Gateway

Objective and Tasks

Create a Tier-0 gateway and configure the north-south end-to-end connectivity:

1. Prepare for the Lab
2. Create Uplink Segments
3. Create a Tier-0 Gateway
4. Connect the Tier-0 and Tier-1 Gateways
5. Test the End-to-End Connectivity



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. From your student desktop, open Chrome.
2. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
3. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create Uplink Segments

You create segments for the two uplinks used by the Tier-0 gateway to connect to the upstream router.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments** and click **ADD SEGMENT**.
2. Configure the segment.

Option	Action
Segment Name	Enter **`T0-GW-01-Uplink-1`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **0** and click **Add Item(s)**.

3. Click **SAVE**.
4. When a message prompts you to continue configuring the segment, click **NO**.
5. Click **ADD SEGMENT** to create another segment for the second uplink.

6. Configure the segment.

Option	Action
Segment Name	Enter **`T0-GW-01-Uplink-2`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **0** and click **Add Item(s)**.

7. Click **SAVE**.
8. When a message prompts you to continue configuring the segment, click **NO**.
9. Verify that the two segments for the Tier-0 Gateway uplinks appear in the Segments list.

Task 3: Create a Tier-0 Gateway

You create a Tier-0 gateway.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-0 Gateways**.
2. Click **ADD GATEWAY** > **Tier-0**.
3. Configure the Tier-0 gateway.

Option	Action
Tier-0 Gateway Name	Enter **`T0-GW-01`**.
HA Mode	Select **Active Active.**
Edge Cluster	Select **Edge-Cluster-01.**

4. Click **SAVE.**
5. When a message prompts you to continue editing this Tier-0 gateway, click **YES**.
6. Scroll to the lower portion of the T0-GW-01 gateway, click the expand button next to ROUTE RE-DISTRIBUTION, and click **Set**.

7. Set route redistribution.
    a. Click **ADD ROUTE RE-DISTRIBUTION.**
    b. Enter **`T0-GW-01 Route Re-distribution`** in the **Name** text box.
    c. Click **Set** under Route Re-distribution.
    d. Select the **Static Routes** and the **Connected Interfaces & Segments** check boxes under Tier-0 Subnets on the Set Route Re-distribution page.

        When you select the **Connected Interfaces & Segments** check box, all related options in that category are selected.
    e. Select the **Static Routes** and the **Connected Interfaces & Segments** check boxes under Advertised Tier-1 Subnets on the Set Route Re-distribution page.

        When you select the **Connected Interfaces & Segments** check box, all related options in that category are selected.
    f. Click **APPLY** and **ADD**.
8. Click **APPLY**.
9. Verify that the **Route Re-distribution Status** toggle is turned on.
10. Click **SAVE**.
11. Click the expand button next to INTERFACES and click **Set**.
12. In the Set Interfaces page, click **ADD INTERFACE**.
    a. Configure the interface.

Option	Action
Name	Enter **`T0-GW-01-Uplink-1`**.
Type	Select **External** (default).
IP Address / Mask	Enter **`192.168.100.2/24`** and click **Add Item(s)**.
Connected To(Segment)	Select **T0-GW-01-Uplink-1.**
Edge Node	Select **sa-nsxedge-01.**

    b. Click **SAVE**.

13. In the Set Interfaces page, click **ADD INTERFACE**.
    a. Enter the configuration information for the interface.

Option	Action
Name	Enter **`T0-GW-01-Uplink-2`**.
Type	Select **External** (default).
IP Address / Mask	Enter **`192.168.110.2/24`** and click **Add Item(s)**.
Connected To(Segment)	Select **T0-GW-01-Uplink-2.**
Edge Node	Select **sa-nsxedge-02.**

    b. Click **SAVE** and click **CLOSE**.
14. Click the expand button next to BGP and enter **`100`** in the **Local AS** text box.
15. Click **Set** next to BGP Neighbors.
16. Add BGP neighbors.
    a. Click **ADD BGP NEIGHBOR** and enter the configuration information.

Option	Action
IP Address	Enter **`192.168.100.1`**.
Remote AS number	Enter **`200`**.
Source Addresses	Select **192.168.100.2**.

    b. Click **SAVE.**
    c. Click **ADD BGP NEIGHBOR** and enter the configuration information.

Option	Action
IP Address	Enter **`192.168.110.1`**.
Remote AS number	Enter **`200`**.
Source Addresses	Select **192.168.110.2**.

    d. Click **SAVE.**
    e. Click **CLOSE.**

f. Click **SAVE** and **CLOSE EDITING**.

Task 4: Connect the Tier-0 and Tier-1 Gateways

You connect the Tier-1 gateway to the Tier-0 gateway for north-south routing.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-1 Gateways**.
2. Click the vertical ellipsis icon next to the T1-GW-01 gateway and select **Edit.**
3. On the T1-GW-01 edit page, select **T0-GW-01** from the **Linked Tier-0 Gateway** drop-down menu.
4. Click **SAVE** and click **CLOSE EDITING**.

Task 5: Test the End-to-End Connectivity

You test the connectivity from your student desktop to tenant VMs to verify that end-to-end routing is working. In the lab environment, routing was preconfigured on your student desktop, the RRAS server, and the VyOS router.

1. To verify connectivity, ping from the console of any tenant VM (T1-Web-01, T1-App-01, T1-DB-01, and so on) to the 192.168.100.1 gateway.

   ```
   ping -c 3 192.168.100.1
   ```

   ```
   ping -c 3 192.168.110.1
   ```

   Your pings should be successful.

2. Use the command prompt of your student desktop to verify that you can reach all the tenant VMs.

   ```
   ping 172.16.10.11
   ```

   ```
   ping 172.16.20.11
   ```

   ```
   ping 172.16.30.11
   ```

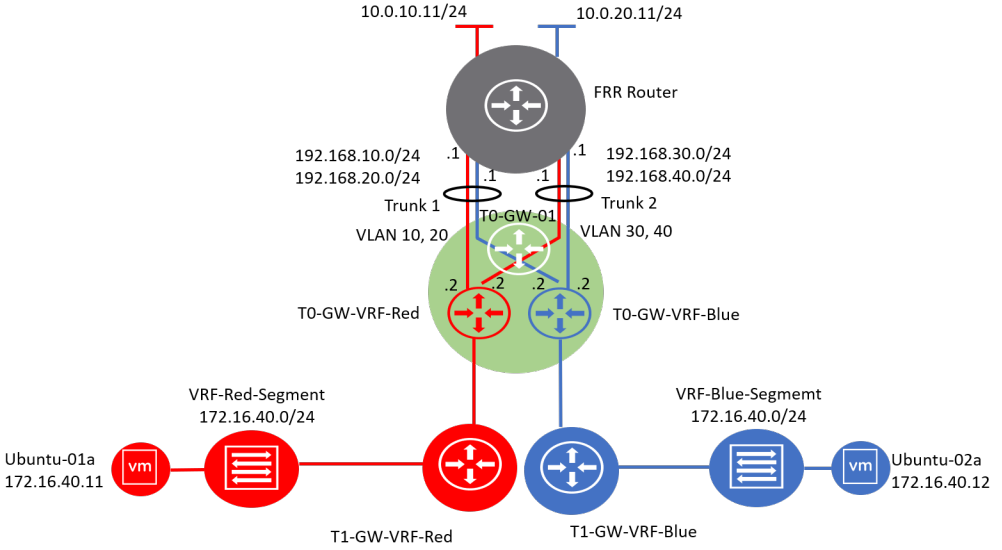
   You should be able to ping from your student desktop to any of the tenant networks, which verifies that the north-south routing is working properly.

Lab 9 Configuring VRF Lite

Objective and Tasks

Configure and verify the VRF Lite functionality to isolate routing domains:

1. Prepare for the Lab
2. Create the Uplink Trunk Segments
3. Deploy and Configure the VRF Gateways
4. Deploy and Connect the Tier-1 Gateways to the VRF Gateways
5. Create and Connect Segments to the Tier-1 Gateways
6. Attach VMs to Segments on Each VRF
7. Test the VRF End-to-End Connectivity
8. Review the Routing Tables in Each VRF
9. Verify the Routing Isolation Between VRFs



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure > vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center > SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create the Uplink Trunk Segments

You create the uplink trunk segments that are connected to the uplink interfaces of each VRF gateway.

1. In the NSX UI, navigate to **Networking** > **Connectivity** > **Segments** > **SEGMENTS**.
2. Click **ADD SEGMENT.**
3. When the Segment wizard appears, configure the uplink trunk segment for the VRF Gateways Uplink-1 interfaces.

Option	Action
Segment Name	Enter **`Uplink-Trunk-1.`**
Connectivity	Select **None.**
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **`10,20`** and click **Add Item(s).**

   Leave the default values for all the other options.

4. Click **SAVE** and click **NO** at the `Want to continue configuring this Segment?` prompt.
5. Click **ADD SEGMENT** and configure the uplink trunk segment for Uplink-2 interfaces.

Option	Action
Segment Name	Enter **`Uplink-Trunk-2.`**
Connectivity	Select **None.**
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **`30,40`** and click **Add Item(s).**

6. Click **SAVE** and click **NO** at the `Want to continue configuring this Segment?` prompt.

Task 3: Deploy and Configure the VRF Gateways

You deploy one VRF gateway for each VRF. You select T0-GW-01 as the default Tier-0 gateway to connect the VRF gateways.

1. In the NSX UI, navigate to **Networking** > **Connectivity** > **Tier-0 Gateways**.
2. Deploy a VRF gateway for VRF Red.
   a. Click **ADD GATEWAY** and select **VRF** from the drop-down menu to deploy the first VRF gateway.
   b. When the VRF Gateway wizard appears, configure the VRF gateway for VRF Red.

Option	Action
Tier-0 Gateway Name	Enter **`T0-GW-VRF-Red.`**
Connect to Tier-0 Gateway	Select **T0-GW-01** from the drop-down menu.

   c. Click **SAVE** and click **YES** at the `Want to continue configuring this Tier-0 Gateway?` prompt**.**
3. Configure uplink interfaces for VRF Red.
   a. Expand **INTERFACES** and click **Set.**
   b. When the Set Interfaces window appears, click **ADD INTERFACE.**
   c. Configure the first uplink interface for the T0-GW-VRF-Red VRF gateway in the ADD INTERFACE wizard.

Option	Action
Name	Enter **`T0-GW-VRF-Red-Uplink-1`**.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.10.2/24`** and click **Add Item(s)**.
Connected To (Segment)	Select **Uplink-Trunk-1** from the drop-down menu.
Edge Node	Select **sa-nsxedge-01** from the drop-down menu.
Access VLAN ID	Enter **`10`**.

   Leave the default values for all the other options.
   d. Click **SAVE.**

e. Click **ADD INTERFACE.**

f. Configure the second uplink interface for the T0-GW-VRF-Red VRF gateway in the ADD INTERFACE wizard.

Option	Action
Name	Enter **`T0-GW-VRF-Red-Uplink-2`**.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.30.2/24`** and click **Add Item(s)**.
Connected To (Segment)	Select **Uplink-Trunk-2** from the drop-down menu.
Edge Node	Select **sa-nsxedge-02** from the drop-down menu.
Access VLAN ID	Enter **`30`**.

Leave the default values for all the other options.

g. Click **SAVE** and click **CLOSE** to finish configuring the interfaces**.**

4. Configure BGP for VRF Red.

a. Click the expand button next to BGP.

b. Turn on the **BGP** toggle and click **SAVE**.

c. Click **Set** on the right of BGP Neighbors.

d. When the Set BGP Neighbors window appears, click **ADD BGP NEIGHBOR** and set up the peering with the upstream router.

Option	Action
IP Address	Enter **`192.168.10.1`**.
Remote AS number	Enter **`10`**.
Source Addresses	Select **`192.168.10.2`**.
Route Filter	Click **Set**, click **ADD ROUTE FILTER**, click **ADD** for the IPv4 address family, and click **Apply**.

e. Click **SAVE** to finish configuring the first neighbor.

f. Click **ADD BGP NEIGHBOR** and set up the second peering with the upstream router.

Option	Action
IP Address	Enter **192.168.30.1**.
Remote AS number	Enter **10**.
Source Addresses	Select **192.168.30.2**.
Route Filter	Click **Set**, click **ADD ROUTE FILTER**, click **ADD** for the IPv4 address family, and click **Apply**.

g. Click **SAVE** and click **CLOSE** to finish the BGP configuration.

5. Scroll to the lower portion of the T0-GW-VRF-Red gateway, click the expand button next to ROUTE RE-DISTRIBUTION, and click **Set**.
6. Set route redistribution.
   a. Click **ADD ROUTE RE-DISTRIBUTION.**
   b. Enter **T0-GW-VRF-Red Route Re-Distribution** in the **Name** text box.
   c. Click **Set** under Route Re-distribution.
   d. Select the **Connected Interfaces & Segments** check box under Tier-0 Subnets on the Set Route Re-distribution page.

      When you select the **Connected Interfaces & Segments** check box, all the related check boxes are selected.

   e. Select the **Connected Interfaces & Segments** check box under Advertised Tier-1 Subnets on the Set Route Re-distribution page

      When you select the **Connected Interfaces & Segments** check box, all the related check boxes are selected.

   f. Click **APPLY** and **ADD**.
7. Click **APPLY**.
8. Verify that the **Route Re-distribution Status** toggle is turned on and click **SAVE.**
9. Click **CLOSE EDITING** to finish configuring the VRF gateway configuration for VRF Red.

10. Deploy a VRF gateway for VRF Blue.
    a. Click **ADD GATEWAY** and select **VRF** from the drop-down menu to deploy the second VRF gateway.
    b. When the VRF Gateway wizard appears, configure the VRF gateway for VRF Blue.

Option	Action
Tier-0 Gateway Name	Enter **`T0-GW-VRF-Blue.`**
Connect to Tier-0 Gateway	Select **T0-GW-01** from the drop-down menu.

    c. Click **SAVE** and click **YES** at the `Want to continue configuring this Tier-0 Gateway?` prompt.
11. Configure the uplink interfaces for VRF Blue.
    a. Expand **INTERFACES** and click **Set.**
    b. When the Set Interfaces window appears, click **ADD INTERFACE.**
    c. Configure the first uplink interface for the T0-GW-VRF-Blue VRF gateway from the ADD INTERFACE wizard.

Option	Action
Name	Enter **`T0-GW-VRF-Blue-Uplink-1`**.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.20.2/24`** and click **Add Item(s)**.
Connected To (Segment)	Select **Uplink-Trunk-1** from the drop-down menu.
Edge Node	Select **sa-nsxedge-01** from the drop-down menu.
Access VLAN ID	Enter **`20`**.

    Leave the default values for all the other options.
    d. Click **SAVE**
    e. Click **ADD INTERFACE**

f. Configure the second uplink interface for the T0-GW-VRF-Blue VRF gateway in the ADD INTERFACE wizard.

Option	Action
Name	Enter **`T0-GW-VRF-Blue-Uplink-2`**.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.40.2/24`** and click **Add Item(s)**.
Connected To (Segment)	Select **Uplink-Trunk-2** from the drop-down menu.
Edge Node	Select **sa-nsxedge-02** from the drop-down menu.
Access VLAN ID	Enter **`40`**.

Leave the default values for all the other options.

g. Click **SAVE** and click **CLOSE** to finish configuring the interfaces**.**

12. Configure a BGP for VRF Blue.

a. Click the expand button next to BGP.

b. Turn on the **BGP** toggle and click **SAVE**.

c. Click **Set** on the right of BGP Neighbors.

d. When the Set BGP Neighbors window appears, click **ADD BGP NEIGHBOR** and set up the peering with the upstream router.

Option	Action
IP Address	Enter **`192.168.20.1`**.
Remote AS number	Enter **`20`**.
Source Addresses	Select **`192.168.20.2`**.
Route Filter	Click **Set**, click **ADD ROUTE FILTER**, click **ADD** for the IPv4 address family and click **Apply**.

e. Click **SAVE** to finish configuring the first neighbor.

f. Click **ADD BGP NEIGHBOR** and set up the second peering with the upstream router.

Option	Action
IP Address	Enter **192.168.40.1**.
Remote AS number	Enter **20**.
Source Addresses	Select **192.168.40.2**.
Route Filter	Click **Set**, click **ADD ROUTE FILTER**, click **ADD** for the IPv4 address family and click **Apply**.

g. Click **SAVE** and click **CLOSE** to finish configuring the BGP.

13. Scroll to the lower portion of the T0-GW-VRF-Blue gateway, click the expand button next to ROUTE RE-DISTRIBUTION, and click **Set**.
14. Set route redistribution.
    a. Click **ADD ROUTE RE-DISTRIBUTION.**
    b. Enter **T0-GW-VRF-Blue Route Re-Distribution** in the **Name** text box.
    c. Click **Set** under Route Re-distribution.
    d. Select the **Connected Interfaces & Segments** check box under Tier-0 Subnets on the Set Route Re-distribution page.

       When you select the **Connected Interfaces & Segments** check box, all the related check boxes are selected.

    e. Select the **Connected Interfaces & Segments** check box under Advertised Tier-1 Subnets on the Set Route Re-distribution page.

       When you select the **Connected Interfaces & Segments** check box, all the related check boxes are selected.

    f. Click **APPLY** and **ADD**.
15. Click **APPLY**.
16. Verify that the **Route Re-distribution Status** toggle is turned on and click **SAVE**.
17. Click **CLOSE EDITING** to finish the VRF gateway configuration for VRF Blue.

Task 4: Deploy and Connect the Tier-1 Gateways to the VRF Gateways

You deploy one Tier-1 gateway for each VRF by selecting the corresponding VRF gateway to connect.

1. In the NSX UI, navigate to **Networking** > **Connectivity** > **Tier-1 Gateways**.
2. Click **ADD TIER-1 GATEWAY** to add the Tier-1 gateway connected to VRF Red.
3. Configure the Tier-1 gateway in the ADD TIER-1 GATEWAY window for VRF Red.

Option	Action
Tier-1 Gateway Name	Enter **`T1-GW-VRF-Red`**.
Linked Tier-0 Gateway	Select **T0-GW-VRF-Red.**
Edge Cluster	Leave blank because no services are required for this lab.

4. Click **SAVE** and click **YES** at the `Want to continue configuring the Tier-1 Gateway?` prompt.
5. Scroll to the lower portion of the Tier-1 configuration wizard, click the expand button next to Route Advertisement, and select the options.
6. Turn on the **All Static Routes** and **All Connected Segments & Service Ports** toggles.
7. Click **SAVE** and click **CLOSE EDITING**.
8. Click **ADD TIER-1 GATEWAY** to add the Tier-1 gateway connected to VRF Blue.
9. Configure the Tier-1 gateway in the ADD TIER-1 GATEWAY window for VRF Blue.

Option	Action
Tier-1 Gateway Name	Enter **`T1-GW-VRF-Blue`**.
Linked Tier-0 Gateway	Select **T0-GW-VRF-Blue.**
Edge Cluster	Leave blank because no services are required for this lab.

10. Click **SAVE** and click **YES** at the `Want to continue configuring the Tier-1 Gateway?` prompt.
11. Scroll to the lower portion of the Tier-1 configuration wizard, click the expand button next to Route Advertisement, and select the options.
12. Turn on the **All Static Routes** and **All Connected Segments & Service Ports** toggles.

13. Click **SAVE** and click **CLOSE EDITING**.

Task 5: Create and Connect Segments to the Tier-1 Gateways

You create one segment for each VRF and connect it to the corresponding Tier-1 gateway. Each segment uses the same subnet in this lab to verify the routing isolation between VRFs.

1. Create a segment named VRF-Red-Segment.
   a. In the NSX UI, navigate to **Networking > Connectivity > Segments.**
   b. Click **ADD SEGMENT** and configure the segment.

Option	Action
Segment Name	Enter **`VRF-Red-Segment`**.
Connectivity	Select **T1-GW-VRF-Red**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.40.1/24`** in the text box for IPv4.

   Leave the default values for all the other options.
   c. Click **SAVE**.
   d. When the message to continue segment configuration appears, click **NO**.
2. Create a segment named VRF-Blue-Segment.
   a. In the NSX UI, navigate to **Networking** > **Connectivity** > **Segments**.
   b. Click **ADD SEGMENT** and configure the segment.

Option	Action
Segment Name	Enter **`VRF-Blue-Segment`**.
Connectivity	Select **T1-GW-VRF-Blue**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.40.1/24`** in the text box for IPv4.

   Leave the default values for all the other options.
   c. Click **SAVE**.
   d. When the message to continue segment configuration appears, click **NO**.

3. On the vSphere Client home page, click the **Networking** tab**.**
4. Verify that the two newly created segments are listed under SA-Datacenter.

Task 6: Attach VMs to Segments on Each VRF

You attach VMs to segments created for each VRF.

1. In the navigator pane of the vSphere Client, click the **Hosts and Clusters** tab and expand the **SA-Datacenter** > **SA-Compute-01** view**.**
2. Add Ubuntu-01a to the VRF-Red-Segment segment.
    a. Right-click **Ubuntu-01a** and select **Edit Settings.**
    b. In the **Network adapter 1** drop-down menu, click **Browse**, select **VRF-Red-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**
3. Add Ubuntu-02a to the VRF-Blue-Segment segment.
    a. Right-click **Ubuntu-02a** and select **Edit Settings.**
    b. In the **Network adapter 1** drop-down menu, click **Browse**, select **VRF-Blue-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**

Task 7: Test the VRF End-to-End Connectivity

You test the connectivity from VMs, which are connected to segments, to the remote networks. These remote networks are preconfigured in each VRF. You verify that the end-to-end connectivity is working. In the lab environment, routing was preconfigured in the upstream FRR router SA-FRR-01.

1. Open a console connection to the Ubuntu-01a VM.
   a. In the Navigator pane, click **Ubuntu-01a** and select **Launch Web Console.**
   b. When the web console window opens, click in the window and press Enter to activate the screen.
   c. Enter **vmware** as the user name and **VMware1!** as the password.
2. Verify connectivity in VRF Red by pinging from the Ubuntu-01a VM console to the 10.0.10.11 IP in the remote network 10.0.10.0/24, which is routed through the upstream FRR router.

   ```
   ping -c 3 10.0.10.11
   ```

   The pings are successful.
3. Verify the route that the packets follow in VRF Red to reach the remote IP 10.0.10.11 by running the `traceroute` command from the Ubuntu-01a console.

   ```
   traceroute -n 10.0.10.11
   ```

   The hops T1-GW-VRF-Red and T0-GW-VRF-Red should appear in the traceroute before reaching remote IP 10.0.10.11.
4. Open a console connection to the Ubuntu-02a VM.
   a. In the Navigator pane, click **Ubuntu-02a** and select **Launch Web Console.**
   b. When the web console window opens, click in the window and press Enter to activate the screen.
   c. Enter **vmware** as the user name and **VMware1!** as the password.
5. Verify the connectivity in VRF Blue by pinging from the Ubuntu-02a VM console to IP 10.0.20.11 in the remote network 10.0.20.0/24, which is routed through the upstream FRR router.

   ```
   ping -c 3 10.0.20.11
   ```

   The pings are successful.

6. Verify the route that the packets follow in VRF Blue to reach the remote IP 10.0.20.11 by running the `traceroute` command from the Ubuntu-02a console.

   ```
   traceroute -n 10.0.20.11
   ```

   The hops T1-GW-VRF-Blue and T0-GW-VRF-Blue should appear in the traceroute before reaching remote IP 10.0.20.11.

Task 8: Review the Routing Tables in Each VRF

You review the routing tables in each VRF.

1. Use SSH to connect to the sa-nsxedge-01 edge node.
   a. From MTPuTTY, connect to sa-nsxedge-01.
   b. If a PuTTY security alert appears, click **Yes**.
   c. Disable the command-line timeout.

      ```
      set cli-timeout 0
      ```

2. List the logical routers in the sa-nsxedge-01 by running the `get logical-routers` command in the console.

   ```
   get logical-routers
   ```

   The VRF ID for the SR-VRF-T0-GW-VRF-Red logical router is 6. The VRF ID might be different in your lab environment.

3. Enter into the VRF context for the SR-VRF-T0-GW-VRF-Red logical router.

   ```
   vrf 6
   ```

   The prompt changes to `sa-nsxedge-01(tier0_vrf_sr)`.

4. Verify the routing table for VRF Red.

   ```
   get route
   ```

   All the routes in the VRF, including Tier0-Connected, Tier1-Connected, and BGP types, appear.

5. Verify the BGP neighbor status for VRF Red.

   ```
   get bgp neighbor summary
   ```

   The 192.168.10.1 neighbor in AS 10 appears and its state is Established.

   NOTE

   You obtain 192.168.30.1 neighbor if you run the same command in the sa-nsxedge-02 edge node.

6. Exit the VRF context in the edge prompt.

   ```
   exit
   ```

   The prompt changes to `sa-nsxedge-01`.

7. List the logical routers in sa-nsxedge-01 by running the `get logical-routers` command in the console.

   ```
   get logical-routers
   ```

   The VRF ID for the SR-VRF-T0-GW-VRF-Blue logical router is 7. The VRF ID might be different in your lab environment.

8. Enter the SR-VRF-T0-GW-VRF-Blue logical router into the vrf context.

   ```
   vrf 7
   ```

   The prompt changes to `sa-nsxedge-01(tier0_vrf_sr)`.

9. Verify the routing table for VRF Blue.

   ```
   get route
   ```

   All the routes in the VRF, including Tier0-Connected, Tier1-Connected, and BGP types, must appear.

   NOTE

   The 172.16.40.0/24 network also appears in the VRF Red routing table in an earlier step. VMs in different VRFs can be connected to overlapping networks.

10. Verify the BGP neighbor status for VRF Blue.

    ```
    get bgp neighbor summary
    ```

    The 192.168.20.1 neighbor must appear in AS 20 and its state should be Established.

    NOTE

    You obtain the 192.168.40.1 neighbor if you run the same command in the sa-nsxedge-02 edge node.

11. Exit the VRF context and return to the edge prompt.

    ```
    exit
    ```

    The prompt changes to `sa-nsxedge-01`.

Task 9: Verify the Routing Isolation Between VRFs

You verify the lack of connectivity between VMs that are connected to segments in different VRFs. You verify that remote networks are only accessible from their VRF.

1. Verify the lack of connectivity between VMs connected to different VRFs even though they are using the same 172.16.40.0/24 subnet address.

    a. If not already open, open a vSphere Client console connection to Ubuntu-01a.

Ubuntu-01a VM has the 172.16.40.11 IP.

    b. Ping the Ubuntu-02a VM IP 172.16.40.12.

    ```
    ping -c 3 172.16.40.12
    ```

    The pings are not successful.

2. Verify the lack of connectivity from the Ubuntu-01a VM in VRF Red to the 10.0.20.0/24 remote network IP in VRF Blue by pinging from the Ubuntu-01a console to the 10.0.20.11 remote network IP.

    ```
    ping -c 3 10.0.20.11
    ```

    The pings are not successful.

3. Verify the lack of connectivity in the other direction by pinging from the Ubuntu-02a VM to the Ubuntu-01a VM IP 172.16.40.11.

   a. If not already open, open a vSphere Client console connection to Ubuntu-02a.

      Ubuntu-02a VM has the 172.16.40.12 IP.

   b. Ping the Ubuntu-02a VM IP 172.16.40.11.

      ```
      ping -c 3 172.16.40.11
      ```

      The pings are not successful.

4. Verify the lack of connectivity from the Ubuntu-02a VM in VRF Blue to the 10.0.10.0/24 remote network IP in VRF Red by pinging from the Ubuntu-02a console to the 10.0.10.11 remote network IP.

   ```
   ping -c 3 10.0.10.11
   ```

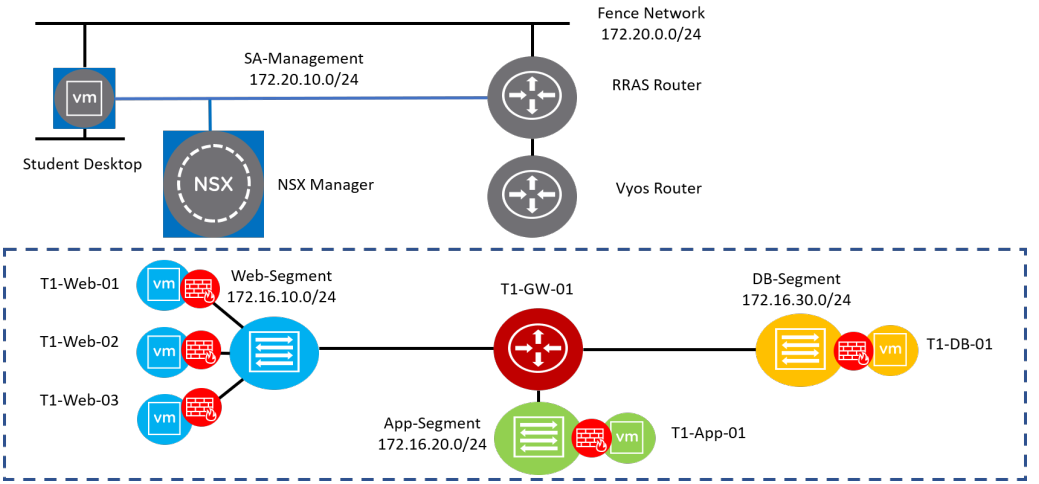
   The pings are not successful.

Lab 10 Configuring the NSX Distributed Firewall

Objective and Tasks

Create NSX distributed firewall rules to allow or deny the application traffic:

1. Prepare for the Lab
2. Test the IP Connectivity
3. Create Security Groups
4. Create Distributed Firewall Rules
5. Test the IP Connectivity After the Firewall Rule Creation
6. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. From your student desktop, open Chrome.
2. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
3. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.

Task 2: Test the IP Connectivity

You test various types of connections, including ICMP, HTTP, and MySQL. You should have full accessibility because the default firewall rule is Allow.

1. Use MTPuTTY (located in the toolbar of the student desktop) to open an SSH console to T1-Web-01.
2. If the PuTTY security alert appears, click **Yes**.
3. Test the ICMP reachability.

   `ping -c 2 172.16.10.12` (T1-Web-02)

   `ping -c 2 172.16.10.13` (T1-Web-03)

   `ping -c 2 172.16.20.11` (T1-App-01)

   `ping -c 2 172.16.30.11` (T1-DB-01)

   All pings should be successful. If the pings fail, verify that all virtual machines are powered on.
4. Test the HTTP access.
   a. From the T1-Web-01 console, request an HTTP webpage from T1-App-01.

      ```
      curl http://172.16.20.11
      ```

   b. Verify that an HTTP response is returned from T1-App-01.
5. Test the MySQL access.
   a. Use MTPuTTY to open an SSH console to T1-App-01.
   b. Connect to the SQL database and enter **VMware1!** when prompted for the password.

      ```
      mysql -u root -h 172.16.30.11 -p
      ```

   c. Verify that the MySQL prompt is available to query the database.
   d. Enter **quit** to exit.

Task 3: Create Security Groups

You create three dynamic security groups and one static security group for the future definition of firewall rules.

1. On the NSX UI Home page, navigate to **Inventory** > **Groups**.
2. Add a group.
    a. Click **ADD GROUP**.
    b. Enter **`Web-Servers`** as the name.
    c. Click **Set Members** under Compute Members and click **+ADD CRITERIA**.
    d. Under Criteria 1, enter the configuration values.
        - First entry: Virtual Machine
        - Second entry: Name
        - Third entry: Contains
        - Fourth entry: web
    e. Click **APPLY** and click **SAVE.**
3. Click the **View Members** link for the Web-Servers group and verify that all the three web VMs (T1-Web-01, T1-Web-02, and T1-Web-03) are listed.
4. Click **CLOSE.**
5. Add a group.
    a. Click **ADD GROUP**.
    b. Enter **`App-Servers`** as the name.
    c. Click **Set Members** under Compute Members and click **+ADD CRITERIA**.
    d. Under Criteria 1, enter the configuration values.
        - First entry: Virtual Machine
        - Second entry: Name
        - Third entry: Contains
        - Fourth entry: app
    e. Click **APPLY** and click **SAVE.**
6. Click the **View Members** link for the App-Servers group and verify that the T1-App-01 VM is listed.
7. Click **CLOSE.**

8. Add a group.
    a. Click **ADD GROUP**.
    b. Enter **`DB-Servers`** as the name.
    c. Click **Set Members** under Compute Members and click **+ADD CRITERIA**.
    d. Under Criteria 1, enter the configuration values.
        - First entry: Virtual Machine
        - Second entry: Name
        - Third entry: Contains
        - Fourth entry: db
    e. Click **APPLY** and click **SAVE.**
9. Click the **View Members** link for the DB-Servers group and verify that the T1-DB-01 VM is listed.
10. Click **CLOSE.**
11. Add a group.
    a. Click **ADD GROUP**.
    b. Enter **`3-Tier`** as the name.
    c. Click **Set Members** under Compute Members.
    d. Navigate to the **Members** tab.
    e. Select **Virtual Machines** from the category drop-down menu.
    f. Find and select **T1-Web-01**, **T1-Web-02**, **T1-Web-03**, **T1-App-01**, and **T1-DB-01**.
    g. Click **APPLY** and click **SAVE.**
12. Click the **View Members** link for the 3-Tier group and verify that all VMs for the 3-tier application are listed.
13. Click **CLOSE.**

Task 4: Create Distributed Firewall Rules

You create distributed firewall rules to manage traffic between applications.

1. In the NSX UI, navigate to **Security** > **East West Security** > **Distributed Firewall**.
2. Click **CATEGORY SPECIFIC RULES** and click the **APPLICATION** tab.
3. Click **+ADD POLICY**.
4. After the row for the new policy appears, enter **`3-TIER POLICY`** as the name.
5. Configure the Applied To field for 3-TIER POLICY so that it applies only to the 3-Tier group.
   a. In the 3-TIER POLICY, point to the **DFW** text box next to the Applied To field.
   b. Click the pencil button**.**
   c. Click **Groups**, select the **3-Tier** check box, and click **APPLY.**
6. Click the vertical ellipsis icon near 3-TIER POLICY and select **Add Rule** to add three distributed firewall rules.

   IMPORTANT

   You must perform this step thrice to add three new distributed firewall rules under 3-TIER POLICY.

   ---

7. On the first row, configure the rule.
   - Name: Enter **`Allow Web Traffic`**.
   - Sources: Select the **Web-Servers** check box and click **APPLY.**
   - Destinations: Select the **App-Servers** check box and click **APPLY.**
   - Services: Select the **HTTP** check box and click **APPLY.**
   - Profiles: Leave **None** (default) selected.
   - Applied To: Click **Groups**, select the **3-Tier** check box, and click **APPLY.**
   - Action: Leave **Allow** (default) selected.

   Leave the default values for all the other settings.

8. On the second row, configure the rule.
    - Name: Enter **`Allow MySQL Traffic`**.
    - Sources: Select the **App-Servers** check box and click **APPLY.**
    - Destinations: Select the **DB-Servers** check box and click **APPLY.**
    - Services: Select the **MySQL** check box and click **APPLY.**
    - Profiles: Leave **None** (default) selected.
    - Applied To: Click **Groups**, select the **3-Tier** check box, and click **APPLY.**
    - Action: Leave **Allow** (default) selected.

    Leave the default values for the other settings.
9. On the third row, configure the rule.
    - Name: Enter **`Drop All Other Traffic`**.
    - Sources: Select the **3-Tier** check box and click **APPLY.**
    - Destinations: Select the **3-Tier** check box and click **APPLY.**
    - Services: Leave **Any** (default) selected.
    - Profiles: Leave **None** (default) selected.
    - Applied To: Click **Groups**, select the **3-Tier** check box, and click **APPLY.**
    - Action: Select **Drop** from the drop-down menu.

    Leave the default value for all other settings.
10. Navigate to the top-right corner of the screen and click **PUBLISH**.

Task 5: Test the IP Connectivity After the Firewall Rule Creation

You test the connectivity between applications to verify that the distributed firewall rules were successfully applied.

1. Use MTPuTTY to open an SSH console to T1-Web-01.
2. Test the ICMP reachability.

   `ping -c 2 172.16.10.12` (T1-Web-02)

   `ping -c 2 172.16.10.13` (T1-Web-03)

   `ping -c 2 172.16.20.11` (T1-App-01)

   `ping -c 2 172.16.30.11` (T1-DB-01)

   All pings fail because you configured a rule to drop all traffic that is not explicitly allowed between the Web, App, and DB VMs.
3. Test the HTTP access.
   a. From the T1-Web-01 console, request an HTTP webpage from T1-App-01.

      `curl http://172.16.20.11`

   b. Verify that an HTTP response is returned from T1-App-01.
4. Test the SQL access.
   a. Use MTPuTTY to open an SSH console to T1-App-01.
   b. Connect to the SQL database and enter **`VMware1!`** when prompted for the password.

      `mysql -u root -h 172.16.30.11 -p`

   c. Verify that the MySQL prompt is available to query the database.
   d. Enter **`quit`** to exit.
5. From the T1-App-01 console, attempt to open an SSH session to T1-DB-01 to verify that only MySQL traffic is allowed between T1-App-01 and T1-DB-01.

   `ssh 172.16.30.11`

   The connection times out eventually. If you do not want to wait, press Ctrl+C to exit.

Task 6: Prepare for the Next Lab

You disable all user-created distributed firewall rules.

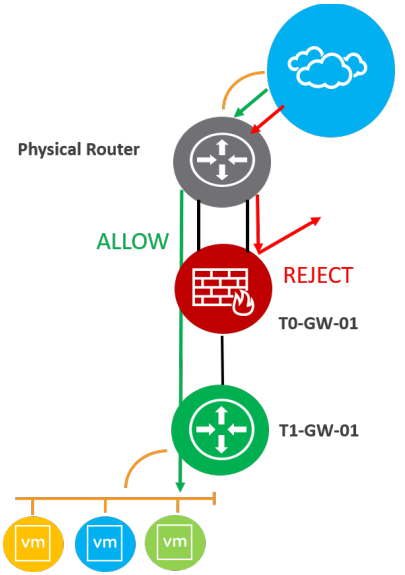
1. On the NSX UI Home page, navigate to **Security** > **East West Security** > **Distributed Firewall** > **CATEGORY SPECIFIC RULES** > **APPLICATION**.
2. Click the vertical ellipsis icon near 3-TIER POLICY and select **Disable All Rules.**
3. Click **PUBLISH.**

Lab 11 Configuring the NSX Gateway Firewall

Objective and Tasks

Configure and test the NSX gateway firewall rules to control north-south traffic:

1. Prepare for the Lab
2. Test SSH Connectivity
3. Configure a Gateway Firewall Rule to Block External SSH Requests
4. Test the Effect of the Configured Gateway Firewall Rule
5. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Test SSH Connectivity

You verify that the SSH connections are successful.

1. Use MTPuTTY on your student desktop to open the preconfigured SSH connections to T1-Web-01, T1-App-01, and T1-DB-01.
2. From the T1-Web-01 MTPuTTY connection, use SSH to connect to T1-App-01.
   a. Establish an SSH connection.

      ```
      ssh 172.16.20.11
      ```

   b. Log in with VMware1! as the password.
   c. Terminate the SSH connection.

      ```
      exit
      ```

Task 3: Configure a Gateway Firewall Rule to Block External SSH Requests

You configure a gateway firewall rule to block SSH requests from external networks.

1. On the NSX UI Home page, navigate to **Security** > **North South Security** > **Gateway Firewall** > **GATEWAY SPECIFIC RULES**.
2. From the **Gateway** drop-down menu, select **T0-GW-01**.
3. Click **+ ADD POLICY.**
4. When the row for the new policy appears, enter **`SSH TRAFFIC`** as the name.
5. Click the vertical ellipsis icon near the SSH TRAFFIC policy and select **Add Rule**.
6. Configure the rule.
   - Name: Enter **`Block SSH`**.
   - Sources: Leave **Any** (default) selected.
   - Destinations: Select the **3-Tier** check box and click **APPLY.**
   - Services: Select the **SSH** check box in the Set Services page and click **APPLY.**
   - Profiles: Leave **None** (default) selected.
   - Applied To: Select the **T0-GW-01-Uplink-1** and **T0-GW-01-Uplink-2** check boxes and click **APPLY**.
   - Action: Select **Reject** from the drop-down menu.
7. Click **PUBLISH**.

Task 4: Test the Effect of the Configured Gateway Firewall Rule

You verify that the gateway firewall rule successfully blocks the SSH traffic.

1. Open MTPuTTY from the student desktop and try to connect to T1-Web-01, T1-App-01, and T1-DB-01.

   Your connections fail.

2. Close the PuTTY connection attempts by clicking **OK** and **Close**.

3. From T1-Web-01, open an SSH connection to T1-App-01.

   a. In the vSphere Client UI, launch a web console to T1-Web-01.

   b. Establish an SSH connection.

      ```
      ssh 172.16.20.11
      ```

   c. Log in with VMware1! as the password.

      The connection should be successful because the gateway firewall rule that you configured does not affect the east-west traffic.

   d. Terminate the SSH connection.

      ```
      exit
      ```

Task 5: Prepare for the Next Lab

You disable the gateway firewall rule.

1. On the NSX UI Home page, navigate to **Security** > **North South Firewall** > **Gateway Firewall** > **GATEWAY SPECIFIC RULES**.

2. Verify that **T0-GW-01** is selected from the **Gateway** drop-down menu.

3. Click the vertical ellipsis icon near the SSH TRAFFIC policy and select **Disable All Rules.**

4. Click **PUBLISH.**

5. Open MTPuTTY from the desktop and connect to T1-Web-01, T1-App-01, and T1-DB-01.

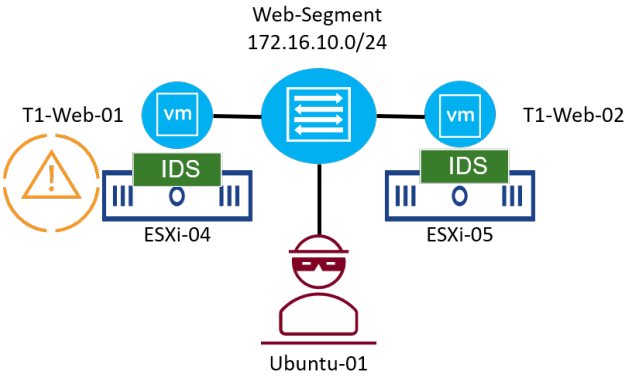
6. Verify that SSH connections are allowed from the external network.

Lab 12 Configuring Distributed Intrusion Detection

Objective and Tasks

Configure Distributed Intrusion Detection and analyze the malicious traffic:

1. Prepare for the Lab
2. Download the Intrusion Detection Signatures
3. Enable Distributed Intrusion Detection for a vSphere Cluster
4. Create an Intrusion Detection Profile
5. Configure the Intrusion Detection Rules
6. Generate the Malicious East-West Traffic
7. Analyze the Intrusion Detection Events



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Download the Intrusion Detection Signatures

You configure NSX Manager to automatically download Intrusion Detection signatures from a third-party repository.

1. On the NSX UI Home page, navigate to **Security** > **East West Security** > **Distributed IDS.**
2. When the message to start with the NSX Intrusion Detection System appears, click **GET STARTED**.
3. Navigate to the **SETTINGS** tab.
4. Under Intrusion Detection Signatures, verify the current version of the IDS signatures and the last time they were downloaded.
5. In the Intrusion Detection Signatures section, select the **Auto Update new versions (recommended)** check box.

IMPORTANT

If a message indicates that a new update is available, do not click the Update Now link. If you click the link, the lab works, but the number of IDS events that you see might differ.

Task 3: Enable Distributed Intrusion Detection for a vSphere Cluster

You enable Distributed Intrusion Detection for the SA-Compute-01 vSphere cluster.

1. On the **SETTINGS** tab, navigate to **Enable Intrusion Detection for Cluster(s)**.
2. Select the **SA-Compute-01** check box and click **ENABLE.**
3. When the `Are you sure you want to enable intrusion detection for selected clusters?` message appears, click **YES** and verify that the status is changed to Enabled.

Task 4: Create an Intrusion Detection Profile

You create a custom Intrusion Detection profile that includes all critical signatures.

1. On the NSX UI Home page, navigate to **Security** > **East West Security** > **Distributed IDS** > **PROFILES**.
2. Click **ADD IDS PROFILE**.

   The IDS Profile wizard appears.
3. Configure the IDS profile.

Option	Action
Name	Enter **`Critical_High_IDS_Profile`**.
Description	Enter **`IDS Profile for critical and high signatures`**.
Severities to Include	Select the **Critical** and **High** check boxes.

   Leave all other options at their default values.
4. Click **SAVE.**
5. Verify that Success appears as the status for Critical_High_IDS_Profile.

Task 5: Configure the Intrusion Detection Rules

You configure Intrusion Detection rules to detect east-west malicious traffic.

1. On the NSX UI Home page, navigate to **Security** > **East West Security** > **Distributed IDS** > **RULES**.
2. Click **+ADD POLICY**.

   A row appears for the new policy.
3. Enter **`IDS Policy`** as the name of the policy.
4. Click the vertical ellipsis icon near IDS Policy and select **Add Rule.**

   A row appears for the new rule.
5. Configure the new rule.
   - Name: IDS Rule
   - Sources: Any
   - Destinations: Any
   - Services: Any
   - IDS Profile: Critical_High_IDS_Profile
   - Applied To: DFW
   - Action: Detect
6. Navigate to the top-right corner of the screen and click **PUBLISH**.

   Success appears as the realization status for the IDS policy.

Task 6: Generate the Malicious East-West Traffic

You use tcpreplay to generate the malicious east-west traffic.

1. In the vSphere Client, navigate to the **Hosts and Clusters** tab.
2. Connect the Ubuntu-01 virtual machine to the Web-Segment segment.
   a. Right-click **Ubuntu-01a** and select **Edit Settings.**
   b. In the **Network adapter 1** drop-down menu, click **Browse**, select **Web-Segment**, and click **OK.**
   c. Verify that the **Connected** check box is selected.
   d. Click **OK.**
3. In the vSphere Client, open a web console to Ubuntu-01a.
4. Log in with the vmware/VMware1! credentials.
5. Access the root mode.

   ```
   sudo -s
   ```

   Use **VMware1!** as the password.
6. Change the IP address of Ubuntu-01a.
   a. Change the IP address to 172.16.10.14/24.
   ```
   ifconfig ens160 172.16.10.14 netmask 255.255.255.0
   ```
   b. Verify the IP address change.
   ```
   ifconfig ens160
   ```
7. Change the default gateway of Ubuntu-01a.
   a. Change the default gateway to 172.16.10.1.
   ```
   route add default gw 172.16.10.1
   ```
   b. Verify the default gateway change.
   ```
   route
   ```
8. Navigate to the **/home/vmware** folder.

   ```
   cd /home/vmware
   ```
9. Use a `.pcap` file to replay an intrusion detection attempt.

   ```
   tcpreplay -i ens160
   cryptolocker_9CBB128E8211A7CD00729C159815CB1C.pcap
   ```

   The replay of the packet capture file might take a few minutes.

Task 7: Analyze the Intrusion Detection Events

You examine the Intrusion Detection events dashboard.

1. On the NSX UI Home page, navigate to **Security** > **East West Security** > **Distributed IDS** > **EVENTS**.

   At least two critical events appear in the histogram.

   If the events do not appear, refresh your browser.

2. Point to each of the red dots to gather additional information about each intrusion, including its severity, type, total number of attempts, and when it was first launched.

3. Navigate to the bottom of the dashboard and expand one of the critical events that was logged.

4. Review additional information about the attack, including the attacker and target information, the protocol used, and its associated IDS rule.

5. Click the **View Intrusion History** link to obtain specific details about each occurrence of the attack.

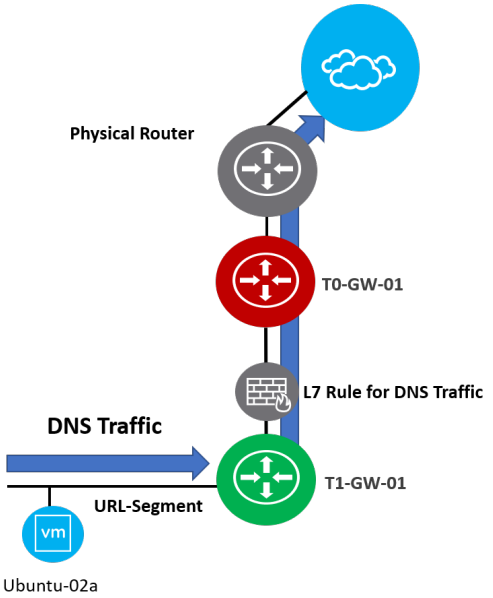
6. Click **CLOSE** to exit.

Lab 13 Analyzing Web Traffic with URL Analysis

Objective and Tasks

Configure URL Analysis and analyze traffic for external websites:

1. Prepare for the Lab
2. Configure the Tier-1 Gateway to Use Layer 7 Firewall Rules
3. Create a Segment
4. Enable URL Analysis
5. Configure Custom Context Profiles for URL Analysis
6. Create a Layer 7 Rule for DNS Traffic
7. Generate Traffic for External Websites
8. Review the URL Analysis Dashboard
9. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Configure the Tier-1 Gateway to Use Layer 7 Firewall Rules

You associate an edge cluster to the Tier-1 gateway to allow the context-aware configuration or Layer 7 gateway firewall rules.

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-1 Gateways**.
2. Click the vertical ellipsis icon next to T1-GW-01 and select **Edit.**
3. Select **Edge-Cluster-01** from the **Edge Cluster** drop-down menu.
4. Click **SAVE.**
5. Click **CLOSE EDITING.**

Task 3: Create a Segment

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments** and click **ADD SEGMENT**.
2. Provide the configuration details in the ADD SEGMENT window.

Option	Action
Segment Name	Enter **`URL-Segment`**.
Connectivity	Select **T1-GW-01**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.60.1/24`**

   Leave the default values for all other options.

3. Click **SAVE.**
4. When the `Want to continue this Segment` message appears, click **No**.
5. Verify that URL-Segment is successfully created.

Task 4: Enable URL Analysis

You enable URL Analysis on the Edge-Cluster-01 NSX Edge cluster.

1. From the NSX UI, navigate to **Security** > **North South Security** > **URL Analysis**.
2. When the `Start the NSX URL Analysis` message appears, click **GET STARTED**.
3. Navigate to the **Settings** tab.
4. Find the Edge-Cluster-01 NSX Edge Cluster and turn on the **URL Analysis State** toggle.
5. Click **YES** when asked to confirm enable.
6. Verify that the URL Analysis state is changed to Enabled.
7. Expand **Edge-Cluster-01** and verify that the Connection Status for both NSX Edge nodes is Up.

   The Connection Status might take up to 5 minutes to change. Click the **REFRESH** arrow next to Connection Status periodically to update the status.

Task 5: Configure Custom Context Profiles for URL Analysis

You create three custom context profiles to filter the web traffic.

1. On the **Settings** tab, find the Edge-Cluster-01 NSX Edge cluster and click **Set** under the Profiles option.

   The Context Profile wizard appears
2. Click **ADD CONTEXT PROFILE.**
3. Configure a new context profile for social network websites.
   a. Enter **SOCIAL** in the **Name** text box.
   b. Click **Set**
   c. Select **ADD ATTRIBUTE** > **URL Category**.
   d. Select **Social Network** from the **Attribute Name/Values** drop-down menu.
   e. Click **ADD** and click **APPLY.**
4. Click **SAVE**.
5. Click **ADD CONTEXT PROFILE.**

6. Configure a new context profile for search engines.
    a. Enter **SEARCH** in the Name text box.
    b. Click **Set**.
    c. Select **ADD ATTRIBUTE** > **URL Category**.
    d. Select **Search Engines** from the **Attribute Name/Values** drop-down menu.
    e. Click **ADD** and click **APPLY.**
7. Click **SAVE**.
8. Click **ADD CONTEXT PROFILE.**
9. Configure a new context profile for sports websites.
    a. Enter **SPORTS** in the **Name** text box.
    b. Click **Set**.
    c. Select **ADD ATTRIBUTE** > **URL Category**.
    d. Select **Sports** from the **Attribute Name/Values** drop-down menu.
    e. Click **ADD** and click **APPLY.**
10. Click **SAVE** and **APPLY.**

Task 6: Create a Layer 7 Rule for DNS Traffic

You configure a Layer 7 firewall rule on the Tier-1 gateway uplink to capture DNS traffic.

1. In the NSX UI, navigate to **Security** > **North South Security** > **Gateway Firewall > GATEWAY SPECIFIC RULES**.
2. From the **Gateway** drop-down menu, select **T1-GW-01**.
3. Click **+ ADD POLICY.**
4. When the row for the new policy appears, enter **`URL POLICY`** as the name.
5. Click the vertical ellipsis icon near URL POLICY and select **Add Rule**.
6. Configure the rule.
   - Name: Enter **`URL Rule`**.
   - Sources: Leave **Any** (default) selected.
   - Destinations: Leave **Any** (default) selected.
   - Services: Select the **DNS-UDP** and **DNS** check boxes in the Set Services page and click **APPLY.**
   - Profiles: Select the **DNS** check box in the Select Context Profile page and click **APPLY.**
   - Applied To: Select the **T1-GW-01** check box and click **APPLY**.
   - Action: Leave **Allow** (default) selected.
7. Click **PUBLISH**.

Task 7: Generate Traffic for External Websites

You generate web traffic to different types of websites from the Ubuntu-02 virtual machine.

1. In the vSphere Client, navigate to the **Hosts and Clusters** tab.
2. Connect the Ubuntu-02a virtual machine to the URL-Analysis segment.
   a. Right-click **Ubuntu-02a** and select **Edit Settings.**
   b. From the **Network adapter 1** drop-down menu, select **URL-Segment.**
   c. Verify that the **Connected** check box is selected.
   d. Click **OK.**
3. In the vSphere Client, open a web console to Ubuntu-02a.
4. Log in with the vmware/VMware1! credentials.
5. Access the root mode.

   ```
   sudo -s
   ```

   Use VMware1! as the password.
6. Change the IP address of Ubuntu-02a.
   a. Change the IP address to 172.16.60.12/24.
      ```
      ifconfig ens160 172.16.60.12 netmask 255.255.255.0
      ```
   b. Verify the IP address change.
      ```
      ifconfig ens160
      ```
7. Change the default gateway of Ubuntu-02a.
   a. Change the default gateway to 172.16.60.1.
      ```
      route add default gw 172.16.60.1
      ```
   b. Verify the default gateway change.
      ```
      route -n
      ```
8. Verify the DNS configuration for Ubuntu-02a.

   ```
   cat /etc/resolv.conf
   ```

   The DNS server is 172.20.10.10
9. Generate traffic for social media sites.

   ```
   ping -c5 www.facebook.com
   ping -c5 www.linkedin.com
   ```

10. Generate traffic for search engines.

```
ping -c5 www.google.com
```

11. Generate traffic for sports sites.

```
ping -c5 www.espn.com
```

Task 8: Review the URL Analysis Dashboard

You examine the URL Analysis dashboard to get insights about the accessed websites.

1. From the NSX UI, navigate to **Security** > **North South Security** > **URL Analysis** > **URLs.**

   The URL Analysis dashboard displays the accessed URLs classified by reputation score and category. At least three different categories appear in the dashboard.

   Results might take up to 5 minutes to appear. Click the **REFRESH** link at the top-right of the page to see the most recent results.

2. Navigate to the bottom of the dashboard and review additional information about each visited URL, including its reputation score, domain name, category, and session count.

Task 9: Prepare for the Next Lab

You disable the Layer 7 gateway firewall rule.

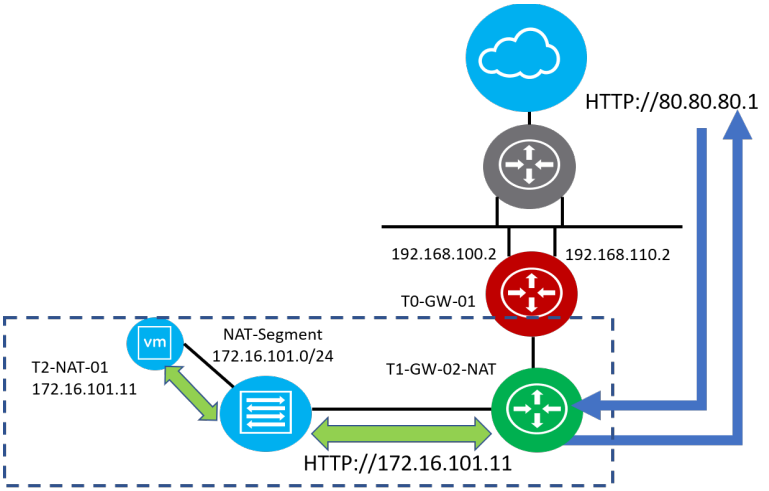
1. On the NSX UI Home page, navigate to **Security** > **North South Security** > **Gateway Firewall** > **GATEWAY SPECIFIC RULES**.
2. Verify that **T1-GW-01** is selected from the **Gateway** drop-down menu.
3. Click the vertical ellipsis icon near URL POLICY and select **Disable All Rules.**
4. Click **PUBLISH.**

Lab 14 Configuring Network Address Translation

Objective and Tasks

Configure source and destination network address translation rules on the Tier-1 gateway:

1. Prepare for the Lab
2. Create a Tier-1 Gateway for Network Address Translation
3. Create a Segment
4. Attach a VM to the NAT-Segment
5. Configure NAT
6. Configure NAT Route Redistribution
7. Verify the IP Connectivity



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Create a Tier-1 Gateway for Network Address Translation

You create a Tier-1 gateway to support network address translation (NAT).

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-1 Gateways** and click **ADD TIER-1 GATEWAY.**
2. Provide the configuration details in the ADD TIER-1 GATEWAY window.

Option	Action
Tier-1 Gateway Name	Enter **`T1-GW-02-NAT`**.
Linked Tier-0 Gateway	Select **T0-GW-01**.
Edge Cluster	Select **Edge-Cluster-01**.
Fail Over	Leave **Non Preemptive** (default) selected.
Route Advertisement	Turn on the **All Static Routes**, **All Connected Segments & Service Ports**, and **All NAT IPs** toggles.

   Leave the default values selected for all other options.

3. Click **SAVE.**
4. If a message prompts you to continue editing the Tier-1 gateway, click **NO**.
5. Verify that the NAT gateway appears in the Tier-1 Gateway list and the status is Success.

Task 3: Create a Segment

1. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments** and click **ADD SEGMENT**.
2. Provide the configuration details in the ADD SEGMENT window.

Option	Action
Segment Name	Enter **`NAT-Segment`**.
Connectivity	Select **T1-GW-02-NAT**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.101.1/24`**

   Leave the default values for all other options.
3. Click **SAVE.**
4. When the `Want to continue this Segment` message appears, click **No**.
5. Verify that NAT-Segment is successfully created.

Task 4: Attach a VM to the NAT-Segment

You attach the T2-NAT-01 VM to the newly created NAT-LS segment.

1. In the vSphere Client UI, select **Hosts and Clusters** from the **Menu** drop-down menu**.**
2. Right-click the **T2-NAT-01** VM and select **Edit Settings.**
3. In the **Network adapter 1** drop-down menu, click **Browse**, select **NAT-Segment**, and click **OK.**
4. Verify that the **Connected** check box is selected.
5. Click **OK.**

Task 5: Configure NAT

You configure the source and destination NAT rules on the Tier-1 NAT gateway.

1. On the NSX UI Home page, navigate to **Networking > Network Services > NAT**.
2. Select **T1-GW-02-NAT** from the **Gateway** drop-down menu.
3. Click **ADD NAT RULE**.
4. Provide the configuration details in the ADD NAT RULE window.

Option	Action
Name	Enter **`SNAT-Rule`**.
Action	Select **SNAT**.
Source	Enter **`172.16.101.11.`**
Destination	Leave blank.
Translated	Enter **`80.80.80.1`**.
Firewall	Select **Bypass**.

   Leave the default values for all other options.

5. Click **SAVE.**
6. Verify that the SNAT rule appears in the list.
7. Verify that T1-GW-02-NAT is still selected in the **Gateway** drop-down menu and click **ADD NAT RULE** again.

8. Provide the configuration details in the New NAT Rule window.

Option	Action
Name	Enter **DNAT-Rule**.
Action	Select **DNAT**.
Source	Leave blank.
Destination	Enter **80.80.80.1**.
Translated	Enter **172.16.101.11.**
Firewall	Select **Bypass**.

   Leave the default values for all other options.

9. Click **SAVE.**
10. Verify that the DNAT rule appears in the list.

Task 6: Configure NAT Route Redistribution

You verify route redistribution in the NAT network to the upstream VyOS router.

1. Use MTPuTTY to connect to sa-vyos-01 and verify that the 172.16.101.0/24 route is advertised by entering **`show ip route`**.

```
vmware@sa-vyos-01> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O
- OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 172.20.10.10, eth0
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 19:14:19
  *                       via 192.168.110.2, eth2, 19:14:19
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 19:14:19
  *                       via 192.168.110.2, eth2, 19:14:19
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 19:14:19
  *                       via 192.168.110.2, eth2, 19:14:19
B>* 172.16.101.0/24 [20/0] via 192.168.100.2, eth2, 00:08:27
  *                        via 192.168.110.2, eth2, 00:08:27
C>* 172.20.10.0/24 is directly connected, eth0
C>* 172.20.11.0/24 is directly connected, eth1
C>* 192.168.100.0/24 is directly connected, eth2
C>* 192.168.110.0/24 is directly connected, eth2
```

2. On the Tier-0 Gateway, redistribute the NAT route (80.80.80.1/32) so that the upstream router learns about it.
   a. On the NSX UI Home page, navigate to **Networking > Connectivity > Tier-0 Gateways**.
   b. Click the vertical ellipsis icon next to T0-GW-01 and select **Edit** from the menu.
   c. Click the expand button next to ROUTE RE-DISTRIBUTION and click the current count value, **1.**
   d. Click the vertical ellipsis icon next to T0-GW-01 Route Re-distribution and select **Edit** from the menu.
   e. On the T0-GW-01 Route Re-distribution, click the current count value, **4.**
   f. Select the **NAT IP** check box under Advertised Tier-1 Subnets.
   g. Click **APPLY.**
   The ROUTE RE-DISTRIBUTION count is set to 5.
   h. Click **ADD** and **APPLY.**

3. Click **SAVE** and click **CLOSE EDITING**.
4. Switch back to the MTPuTTY connection for sa-vyos-01 and enter **`show ip route`** again to verify that 80.80.80.1/32 appears.

```
vmware@sa-vyos-01> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O
- OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route

S>* 0.0.0.0/0 [1/0] via 172.20.10.10, eth0
B>* 80.80.80.1/32 [20/0] via 192.168.100.2, eth2, 00:29:15
  *                      via 192.168.110.2, eth2, 00:29:15
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2, 20:15:56
  *                       via 192.168.110.2, eth2, 20:15:56
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2, 20:15:56
  *                       via 192.168.110.2, eth2, 20:15:56
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2, 20:15:56
  *                       via 192.168.110.2, eth2, 20:15:56
B>* 172.16.101.0/24 [20/0] via 192.168.100.2, eth2, 01:10:04
  *                        via 192.168.110.2, eth2, 01:10:04
C>* 172.20.10.0/24 is directly connected, eth0
C>* 172.20.11.0/24 is directly connected, eth1
C>* 192.168.100.0/24 is directly connected, eth2
C>* 192.168.110.0/24 is directly connected, eth2
```

Task 7: Verify the IP Connectivity

You test the connectivity to the NAT network.

1. From MTPuTTY, connect to sa-nsxedge-01.
2. Retrieve gateway instances and identify the virtual routing and forwarding (VRF) instance context for SR-T0-GW-01.

   ```
   get logical-routers
   ```

   ```
   sa-nsxedge-01> get logical-routers
   Logical Router
   UUID                                   VRF    LR-ID  Name
   Type                        Ports
   736a80e3-23f6-5a2d-81d6-bbefb2786666   0      0
   TUNNEL                      3
   90dbc567-26d2-4010-9f98-519d9f2802c3   1      3      SR-T0-GW-
   01                          SERVICE_ROUTER_TIER0       7
   a949fe00-5d14-4ce7-9af1-a5bce157d75f   3      2      DR-T0-GW-
   01                          DISTRIBUTED_ROUTER_TIER0   5
   bd4b7bc2-8800-432e-844a-a646057edb03   4      1      DR-T1-GW-
   01                          DISTRIBUTED_ROUTER_TIER1   7
   2eb670da-f124-4c2f-b1bf-b77c174ac2b5   5      9      SR-VRF-T0-
   GW-VRF-Red                 VRF_SERVICE_ROUTER_TIER0   5
   298ce52a-a221-4440-9057-61147b01f55e   6      14     SR-VRF-T0-
   GW-VRF-Blue                VRF_SERVICE_ROUTER_TIER0   5
   01da2dfd-3270-4e32-b7ac-fe046ce7c5ed   7      17     DR-T1-GW-
   VRF-Red                     DISTRIBUTED_ROUTER_TIER1   5
   a2b1cbe8-844a-4ffc-a139-aa6bf61ce9bf   8      7      DR-VRF-T0-
   GW-VRF-Red                 VRF_DISTRIBUTED_ROUTER_TIER0 4
   0ee4a285-58eb-4e02-ba33-77c04132246e   9      18     DR-T1-GW-
   VRF-Blue                    DISTRIBUTED_ROUTER_TIER1   5
   10d4bdb0-df81-4c82-965c-5dedcefd71f0   10     12     DR-VRF-T0-
   GW-VRF-Blue                VRF_DISTRIBUTED_ROUTER_TIER0 4
   ba44be1f-ee5e-4876-8851-a15fbe5aa808   11     20     SR-T1-GW-
   02-NAT                      SERVICE_ROUTER_TIER1       5
   2d78b3f7-08e2-4f55-85e7-f362a303e2fa   12     19     DR-T1-GW-
   02-NAT                      DISTRIBUTED_ROUTER_TIER1   4
   ```

   In the command output, the VRF ID for SR-T0-GW-01 is 1. The VRF ID in your lab might be different.

3. Access the VRF for SR-T0-GW-01 and view the routing table of the Tier-0 SR.

```
vrf 1
get route
```

```
sa-nsxedge-01> vrf 1
sa-nsxedge-01(tier0_sr)> get route

Flags: t0c - Tier0-Connected, t0s - Tier0-Static, b - BGP,
t0n - Tier0-NAT, t1s - Tier1-Static, t1c - Tier1-Connected,
t1n: Tier1-NAT, t1l: Tier1-LB VIP, t1ls: Tier1-LB SNAT,
t1d: Tier1-DNS FORWARDER, t1ipsec: Tier1-IPSec, isr: Inter-SR,
> - selected route, * - FIB route

Total number of routes: 20

b  > * 0.0.0.0/0 [20/0] via 192.168.100.1, uplink-273, 20:34:38
t1n> * 80.80.80.1/32 [3/0] via 100.64.240.7, downlink-348,
01:21:05
t0c> * 100.64.240.0/31 is directly connected, linked-287,
20:33:51
t0c> * 100.64.240.6/31 is directly connected, downlink-348,
01:29:47
t0c> * 169.254.0.0/25 is directly connected, downlink-274,
20:33:51
isr> * 169.254.0.128/25 is directly connected, inter-sr-271,
20:40:04
t1c> * 172.16.10.0/24 [3/0] via 100.64.240.1, linked-287,
20:33:44
t1c> * 172.16.20.0/24 [3/0] via 100.64.240.1, linked-287,
20:33:44
t1c> * 172.16.30.0/24 [3/0] via 100.64.240.1, linked-287,
20:33:44
t1c> * 172.16.101.0/24 [3/0] via 100.64.240.7, downlink-348,
01:27:58
b  > * 172.20.10.0/24 [20/66] via 192.168.100.1, uplink-273,
20:34:37
b  > * 172.20.11.0/24 [20/66] via 192.168.100.1, uplink-273,
20:34:37
t0c> * 192.168.100.0/24 is directly connected, uplink-273,
20:40:04
isr> * 192.168.100.2/32 unreachable (blackhole), 20:40:01
b  > * 192.168.110.0/24 [20/66] via 192.168.100.1, uplink-273,
20:34:37
isr> * 192.168.110.2/32 [200/0] via 169.254.0.131, inter-sr-
271, 11:44:09
```

```
t0c> * fcb7:309d:a277:c800::/64 is directly connected, linked-
287, 20:33:51
t0c> * fcb7:309d:a277:c803::/64 is directly connected,
downlink-348, 01:29:47
t0c> * fe80::/64 is directly connected, downlink-274, 20:33:51
isr> * ff00::/8 is directly connected, inter-sr-271, 20:40:04
```

4. From your student desktop, open a browser window and either enter **`http://80.80.80.1`** or click the **NAT Web Server** bookmark.

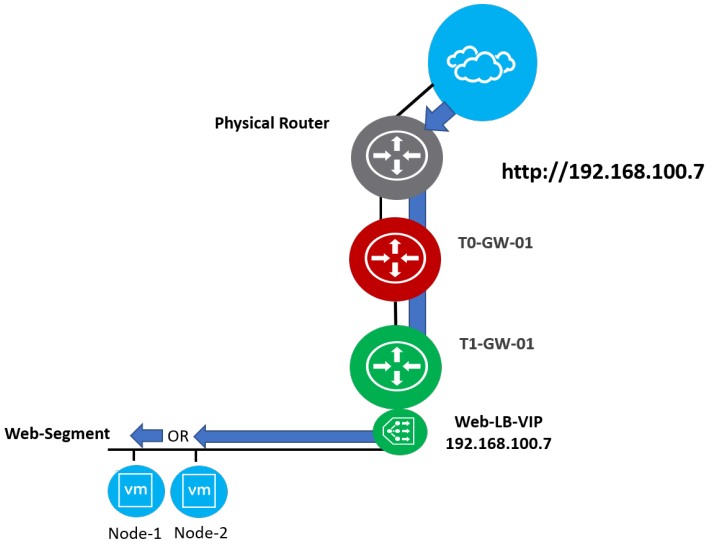
   A test page appears indicating that your NAT is successful.

Lab 15 Configuring Load Balancing

Objective and Tasks

Configure load balancing on the Tier-1 gateway to distribute web traffic:

1. Prepare for the Lab
2. Test the Connectivity to Web Servers
3. Create a Load Balancer
4. Configure Route Advertisement and Route Redistribution for the Virtual IP
5. Prepare for the Next Lab



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure > vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center > SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Test the Connectivity to Web Servers

You verify the end-to-end connectivity from your student desktop to the web servers.

1. On your student desktop, open a command prompt window.
2. Ping the two web servers and verify that the pings are successful.

   ```
   ping 172.16.10.11
   ping 172.16.10.12
   ```

3. On your student desktop, open a browser tab and verify that you can access the two web servers.

   ```
   http://172.16.10.11
   http://172.16.10.12
   ```

   Do not proceed to the next task if you cannot access the two web servers.

Task 3: Create a Load Balancer

You create a load balancer and attach it to the Tier-1 gateway.

1. On the NSX UI Home page, navigate to **Networking > Network Services > Load Balancing > LOAD BALANCERS**.
2. Create a load balancer.
   a. Click **ADD LOAD BALANCER** and provide the configuration details.

Option	Action
Name	Enter **`Web-LB.`**
Size	Select **Small**.
Attachment	Select **T1-GW-01.**

   Leave the default values for all the other settings.

   b. Click **SAVE**.

   c. When the message to continue the load balancer configuration appears, click **YES**.

   d. On the Load Balancer options page, click **Set Virtual Servers** under VIRTUAL SERVERS.

3. Click **ADD VIRTUAL SERVER > L4 TCP** to create a virtual server.

Option	Action
Name	Enter **`Web-VirtualServer.`**
IP Address	Enter **`192.168.100.7`**.
Ports	Enter **80** and click **Add Item**.
Server Pool	Click the vertical ellipsis icon next to the field and select **Create New**

4. Create a server pool for the web servers.

   a. Provide the configuration details on the Create Server Pool page.

Option	Action
Name	Enter **`Web-Pool.`**
Algorithm	Leave **Round Robin** (default) selected.
Description	Enter **`Server pool for web servers.`**
SNAT Translation Mode	Leave **Automap** (default) selected.
Members/Group	Click **Select Members.**

   b. On the Configure Server Pool Members page, click **ADD MEMBER** under Enter individual members to add two web server nodes (T1-Web-01 and T1-Web-02) to the pool member list.

Option	Action
Name	Enter **`Node-1`**.
IP	Enter **`172.16.10.11`**.
Port	Enter **`80`**.
Weight	Leave **1** (default) selected.
State	Leave **Enabled** (default) selected.
Backup Member	Leave **Disabled** (default) selected.

   c. Click **SAVE**.

d. Click **ADD MEMBER** and enter the configuration details for the second member.

Option	Action
Name	Enter **Node-2**.
IP	Enter **172.16.10.12**.
Port	Enter **80**.
Weight	Leave **1** (default) selected.
State	Leave **Enabled** (default) selected.
Backup Member	Leave **Disabled** (default) selected.

e. Click **SAVE**.

f. Click **APPLY.**

g. On the Create Server Pool page, click **SAVE**.

h. On the Set Virtual Servers page, click **SAVE** and **CLOSE**.

i. On the LOAD BALANCERS tab, click **SAVE**.

5. Click the **SERVER POOLS** tab and verify that the newly created Web-Pool appears in the server pool list.

6. Click the **VIRTUAL SERVERS** tab and verify that the newly created Web-VirtualServer appears in the virtual server list.

7. Click the **LOAD BALANCERS** tab and verify that the Web-LB load balancer is attached to the T1-GW-01 gateway and its status is Success.

Task 4: Configure Route Advertisement and Route Redistribution for the Virtual IP

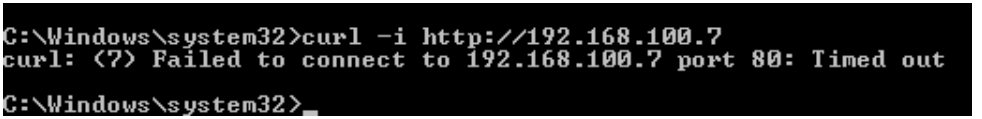
You advertise the load balancer's virtual IP (VIP) and verify that the HTTP traffic is handled by both web servers in a round-robin method.

1. Use Chrome to access the load balancer VIP.
   a. From your student desktop, open a Chrome browser window and try to access the load balancer's VIP address http://192.168.100.7.
   b. Verify that the website cannot be reached.

      The website cannot be reached because the load balancer's VIP is not advertised and is unknown to the external clients.
2. Use `curl` to verify access to the load balancer VIP.
   a. From your student desktop, open the Command Prompt window and access the load balancer's VIP address.

      ```
      curl -i http://192.168.100.7
      ```
   b. Verify that the website cannot be reached.

      The website cannot be reached because the load balancer's VIP is not advertised and is unknown to the external clients.

3. Configure the T1-GW-01 gateway to advertise the VIP route.
   a. On the NSX UI Home page, navigate to **Networking > Connectivity > Tier-1 Gateways.**
   b. Click the vertical ellipsis icon next to T1-GW-01 and select **Edit.**
   c. Expand the **Route Advertisement** option.
   d. In the Edit Route Advertisement Configuration window, enable **All LB VIP Routes.**
4. Click **SAVE** and click **CLOSE EDITING**.

5. Configure the T0-GW-01 gateway to redistribute the VIP route to the upstream VyOS router.
    a. Select **Tier-0 Gateways > T0-GW-01**.
    b. Click the vertical ellipsis next to T0-GW-01 and select **Edit**.
    c. Expand **ROUTE RE-DISTRIBUTION** and click the **Route Re-distribution** number.
    d. Click the vertical ellipsis icon next to **T0-GW-01 Route Re-distribution** and select **Edit** from the menu.
    e. On the T0-GW-01 Route Re-distribution, click the current count **value 5**.
    f. Select the Advertised Tier-1 Subnets > **LB VIP** check box.
    g. Click **APPLY.**
    The ROUTE RE-DISTRIBUTION count is set to 6.
    h. Click **ADD** and **APPLY.**
6. Click **SAVE** and click **CLOSE EDITING**.
7. Use **Firefox** to verify the access to the load balancer VIP.
    a. From the student desktop, open a Firefox browser and access the VIP address by using http://192.168.100.7.

        The webpage appears.
    b. Refresh the browser display to verify that both back-end web servers are being used (as a result of the configured round-robin method).

        The client's HTTP requests alternate between T1-Web-01 and T1-Web-02.

        Due to the browser cache behavior, you might need to press Ctrl+F5 (force refresh) to see the traffic being load balanced between the two web servers.

8. Use `curl` to verify access to the load balancer VIP.

   a. From the student desktop, open a Command Prompt window and access the load balancer's VIP address.

      ```
      curl -i http://192.168.100.7
      ```

      The webpage should appear.

   b. Run the same `curl` command again to verify that both back-end web servers are being used in a round-robin method.

```
C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Date: Wed, 23 Jan 2019 22:23:53 GMT
Server: Apache/2.2.12 (Linux/SUSE)
Last-Modified: Tue, 28 Aug 2018 14:18:17 GMT
ETag: "16f4-75-5747f835afc40"
Accept-Ranges: bytes
Content-Length: 117
Content-Type: text/html

<html>
<head>
<title>NSX-T Data Center Labs</title>
</head>
<body>
<b>Web-Server-02 172.16.10.12</b>
</body>
</html>

C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Date: Wed, 23 Jan 2019 22:24:35 GMT
Server: Apache/2.2.12 (Linux/SUSE)
Last-Modified: Tue, 28 Aug 2018 14:20:50 GMT
ETag: "4b69-75-5747f8c799480"
Accept-Ranges: bytes
Content-Length: 117
Content-Type: text/html

<html>
<head>
<title>NSX-T Data Center Labs</title>
</head>
<body>
<b>Web-Server-01 172.16.10.11</b>
</body>
</html>

C:\Windows\system32>
```

Task 5: Prepare for the Next Lab

You disable the load balancer and detach the Web-LB load balancer from the T1-GW-01 gateway.

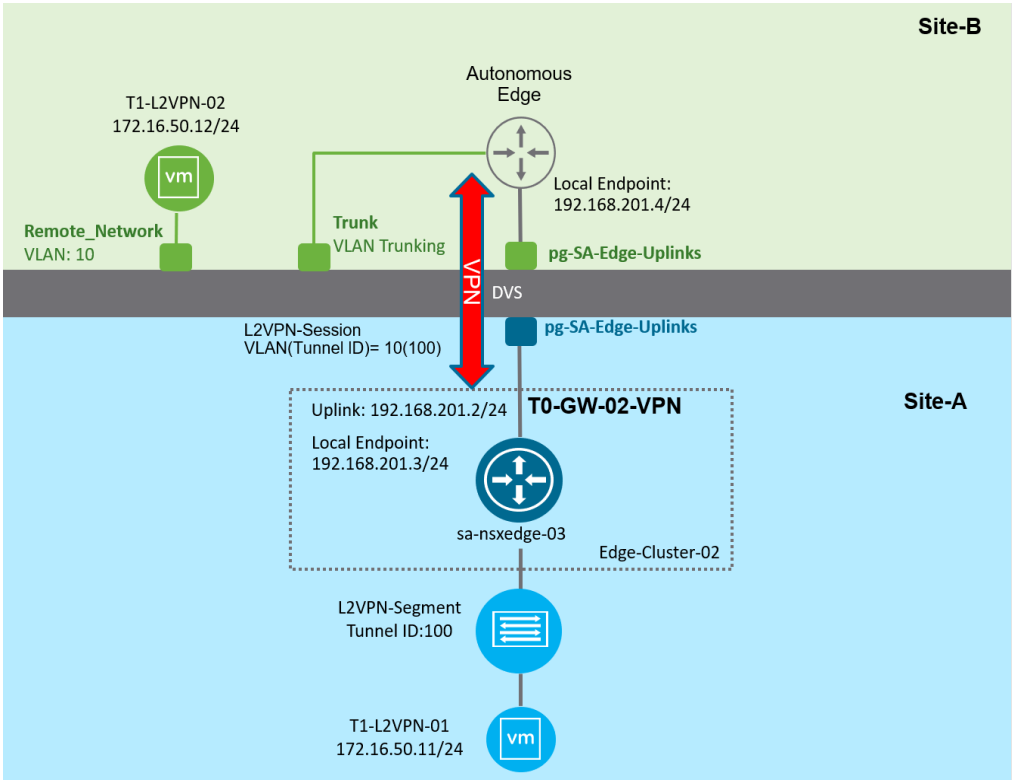
1. Navigate to **Networking > Network Services** > **Load Balancing > LOAD BALANCERS.**
2. Click the vertical ellipsis next to Web-LB and select **Edit**.
3. Turn off the **Admin State** toggle to display Disabled.
4. Clear the Attachment option by clicking the X beside T1-GW-01.
5. Click **SAVE.**

Lab 16 Deploying Virtual Private Networks

Objective and Tasks

Configure the VPN tunnel and verify the operation:

1. Prepare for the Lab
2. Deploy a New NSX Edge Node to Support the VPN Deployment
3. Configure a New Edge Cluster
4. Deploy and Configure a New Tier-0 Gateway and Segments for VPN Support
5. Create an IPSec VPN Service
6. Create an L2 VPN Server and Session
7. Configure a Predeployed Autonomous Edge as an L2 VPN Client
8. Verify the Operation of the VPN Setup



Task 1: Prepare for the Lab

You log in to the vSphere Client UI and the NSX UI.

1. From your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere Infrastructure** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. On the login page, enter **`administrator@vsphere.local`** as the user name and **`VMware1!`** as the password.
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX-T Data Center > SA-NSXMGR-01** bookmark.
   c. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Deploy a New NSX Edge Node to Support the VPN Deployment

You deploy a new NSX Edge node to configure VPN tunnels.

1. On the NSX UI Home page, navigate to **System > Configuration > Fabric > Nodes > Edge Transport Nodes**.
2. Click **+ADD EDGE VM.**
3. Provide the configuration details in the Add Edge VM window.

Option	Action
Name	Enter **`sa-nsxedge-03`**.
Host name/FQDN	Enter **`sa-nsxedge-03.vclass.local`**.
Form Factor	Leave **Medium** (default) selected.

4. Click **NEXT.**
5. On the Credentials page, enter **`VMware1!VMware1!`** as the CLI password and the system root password.
6. Click the **Allow SSH Login** and **Allow Root SSH Login** toggles to display Yes.
7. Click **NEXT.**
8. On the Configure Deployment page, provide the configuration details.

Option	Action
Compute Manager	Select **sa-vcsa-01.vclass.local.**
Cluster	Select **SA-Management-Edge.**
Resource Pool	Leave blank.
Host	Leave blank.
Datastore	Select **SA-Shared-02-Remote.**

9. Click **NEXT.**

10. On the Configure Node Settings page, provide the configuration details.

Option	Action
IP Assignment	Select **Static.**
Management IP	Enter **`172.20.10.63/24`**.
Default Gateway	Enter **`172.20.10.10`**.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management**, and click **SAVE**.
Search Domain Names	Enter **`vclass.local`**.
DNS Servers	Enter **`172.20.10.10`**.
NTP Servers	Enter **`172.20.10.10`**.

11. Click **NEXT.**
12. On the Configure NSX page, provide the configuration details.

Option	Action
Edge Switch Name	Enter **`PROD-Overlay-NVDS.`**
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile**.
IP Assignment	Select **Use IP Pool**.
IP Pool	Select **VTEP-IP-Pool**.
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Overlay**, and click **SAVE**.

13. On the Configure NSX page, click **+ ADD SWITCH** and provide the configuration details.

    You might need to scroll up.

Option	Action
Edge Switch Name	Enter **PROD-VLAN-NVDS .**
Transport Zone	Select **PROD-VLAN-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
Teaming Policy Switch Mapping - DPDK Fastpath Interfaces for uplink-1 (active)	Click the **Select Interface** link, select **pg-SA-Edge-Uplinks**, and click **SAVE**.

14. Click **FINISH**.

    NOTE

    The edge deployment might take several minutes to complete. The deployment status displays various temporary values, for example, Node Not Ready**.**

    Wait until the configuration state displays Success and the node status is Up. You might need to click **REFRESH** occasionally.

15. Verify that the edge node is deployed and listed in the Edge VM list.

    The configuration state appears as Success and the node status is Up.

Task 3: Configure a New Edge Cluster

You create an NSX Edge cluster and add the NSX Edge node to the cluster.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Nodes** > **Edge Clusters**.
2. Click **+ADD**.
3. Provide the configuration details in the Add Edge Cluster window.

Option	Action
Name	Enter **`Edge-Cluster-02`**.
Edge Cluster Profile	Leave **nsx-default-edge-high-availability-profile** (default) selected.
Member Type	Leave **Edge Node** (default) selected.

4. In the Available (1) pane, select **sa-nsxedge-03** and click the right arrow to move it to the Selected (0) pane.
5. Click **ADD.**

Task 4: Deploy and Configure a New Tier-0 Gateway and Segments for VPN Support

You deploy and configure a new Tier-0 gateway and segments for VPN support.

1. Create a segment for the Tier-0 gateway uplink.
   a. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Segments**.
   b. Click **ADD SEGMENT** and provide the configuration details.

Option	Action
Segment Name	Enter **`T0-GW-02-VPN-Uplink`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **0** and click **Add Item(s)**.

   Leave the default values for all the other options.
   c. Click **SAVE**.
   d. When a prompt to continue segment configuration appears, click **NO**.
2. Click **ADD SEGMENT** again to create another segment.
   a. Enter the configuration information for the new segment.

Option	Action
Segment Name	Enter **`L2VPN-Segment`**.
Connectivity	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Leave blank.

   Leave the default values for all the other options.
   b. Click **SAVE.**
   c. When prompted to continue editing the segment, click **NO**.
3. On the NSX UI Home page, navigate to **Networking** > **Connectivity** > **Tier-0 Gateways**.

4. Click **ADD GATEWAY** > **Tier-0**.
5. Provide the configuration details for the Tier-0 gateway.

Option	Action
Tier-0 Gateway Name	Enter **`T0-GW-02-VPN`**.
HA Mode	Select **Active Standby.**
Fail Over	Select **Preemptive.**
Edge Cluster	Select **Edge-Cluster-02.**
Preferred Edge	Select **sa-nsxedge-03.**

6. Click **SAVE.**
7. When the prompt to continue configuring this Tier-0 gateway appears, click **YES**.
8. Scroll to the lower portion of the T0-GW-02-VPN gateway, click the expand button next to ROUTE RE-DISTRIBUTION, and click **Set**.
    a. Click **ADD ROUTE RE-DISTRIBUTION.**
    b. Enter **`T0-GW-02-VPN Route Re-distribution`** in the Name text box.
    c. Click **Set** under Route Re-distribution.
    d. On the Set Route Redistribution page, leave all the check boxes deselected under Advertised Tier-1 Subnets.
    e. On the Set Route Redistribution page, select the **Static Routes** and **Connected Interfaces & Segments** check boxes under Tier-0 Subnets.
    f. Click **APPLY** and **ADD.**
9. Click **APPLY.**
10. Verify that the **Route Re-distribution Status** toggle is turned on.
11. Click **SAVE.**
12. Click the expand button next to INTERFACES and click **Set**.

13. In the Set Interfaces page, click **ADD INTERFACE**.
    a. Configure the interface.

Option	Action
Name	Enter **`T0-GW-02-VPN-Uplink`**.
Type	Leave **External** (default) selected.
IP Address / Mask	Enter **`192.168.201.2/24`** and click **Add Item(s)**.
Connected To(Segment)	Select **T0-GW-02-VPN-Uplink.**
Edge Node	Select **sa-nsxedge-03.**

    b. Click **SAVE**.
14. Click **CLOSE** and click **CLOSE EDITING**.

    Wait for the new Tier-0 gateway status to appear as Successful. You might need to click **REFRESH** periodically while waiting.

Task 5: Create an IPSec VPN Service

You create and configure an IPSec VPN Service.

1. On the NSX UI Home page, navigate to **Networking** > **Network Services** > **VPN** > **VPN SERVICES.**
2. Click **ADD SERVICE** > **IPSec**.
3. Enter the configuration information for the new VPN service.

Option	Action
Name	Enter **`IPSec-for-L2VPN.`**
Tier-0/Tier-1 Gateway	Select **T0-GW-02-VPN.**

   Leave the default values for all the other options.
4. Click **SAVE**.
5. When you are prompted to continue configuring this VPN service, click **NO**.

Task 6: Create an L2 VPN Server and Session

You create an L2 VPN server and session for the VPN network.

1. Create an L2 VPN server.
   a. On the **VPN SERVICES** tab, click **ADD SERVICE** > **L2 VPN Server**.
   b. Enter the configuration information for the new L2 VPN server.

Option	Action
Name	Enter **`L2VPN-Server.`**
Tier-0/Tier-1 Gateway	Select **T0-GW-02-VPN.**

   Leave the default values for all the other options.
   c. Click **SAVE**.
   d. When you are prompted to continue configuring this VPN service, click **YES**.
2. Click the expand button next to SESSIONS, click **Add Sessions**, and click **ADD L2 VPN SESSION**.
3. Configure the session.
   a. Enter **`L2VPN-Session`** as the name.
   b. Click the vertical ellipsis icon next to Local Endpoint/IP and select **Add Local Endpoint.**

Option	Action
Name	Enter **`L2VPN-Endpoint.`**
VPN Service	Select **IPSec-for-L2VPN** (default).
IP Address	Enter **`192.168.201.3.`**
Local ID	Enter **`192.168.201.3.`**

   c. Click **SAVE**.

d. On the ADD L2 VPN SESSION page, continue configuring the session.

Option	Action
Remote IP	Enter **192.168.201.4.**
Pre-shared Key	Enter **VMware1!.**
Tunnel Interface	Enter **169.1.1.1/24.**
Remote ID	Enter **192.168.201.4.**

e. Click **SAVE**.

f. When you are prompted to continue configuring this L2 VPN session, click **NO**.

4. Click **CLOSE** and click **CLOSE EDITING**.

5. Click the **L2 VPN SESSIONS** tab and verify that the session was created.

NOTE

The L2VPN session status appears as either Down or In Progress until you configure the Autonomous Edge as an L2 VPN client and an active session is running.

6. Acquire the peer code for the L2 VPN session.

a. On the **L2 VPN SESSIONS** tab, click the expand button next to L2-VPN-Session.

b. Click **DOWNLOAD CONFIG**.

The `Download Config has PSK information in it` warning appears.

c. Click **YES**.

d. The file is saved as `L2VPNSession_L2VPN-Session_config.txt` in the `Downloads` folder on your student desktop.

7. Navigate to **Networking** > **Connectivity** > **Segments** and add the newly created VPN session information to the L2VPN-Segment.
   a. Click the vertical ellipsis icon next to L2VPN-Segment and select **Edit** from the menu.
   b. Provide the configuration details.

Option	Action
L2 VPN	Select **L2VPN-Session.**
VPN Tunnel ID	Enter **100.**

   c. Click **SAVE** and click **CLOSE EDITING**.

Task 7: Configure a Predeployed Autonomous Edge as an L2 VPN Client

You configure a predeployed Autonomous Edge appliance as an L2 VPN client.

1. Open a web browser and click the **NSX-T Data Center** > **NSX Autonomous Edge** bookmark.
2. If the `Your connection is not private` message appears, click **ADVANCED** and click the **Proceed to 172.20.10.70 (unsafe)** link.
3. On the login page, enter **admin** as the user name and **VMware1!VMware1!** as the password.
4. Navigate to the **PORT** tab and click **ADD PORT.**
5. Configure the new port.

Option	Action
Port Name	Enter **L2VPN-Port**.
Subnet	Leave blank.
VLAN	Enter **10.**
Exit Interface	Select **eth3.**

6. Click **SAVE.**
7. Navigate to the **L2VPN** tab and click **ADD SESSION.**

8. Configure the L2VPN client session.

Option	Action
Session Name	Enter **L2VPN-Client-Session.**
Admin Status	Select **ENABLED** (default).
Local IP	Enter **192.168.201.4.**
Remote IP	Enter **192.168.201.3.**

9. Obtain and paste the peer code.
   a. Use Notepad to open the `L2VPNSession_L2VPN-Session_config.txt` file in the `Downloads` folder on your student desktop.
   b. Select **Format** > **Word Wrap**.
   c. Copy the string after the `peer_code` text. Be sure to copy only the text without the quotes.
   d. Paste the code in the **Peer Code** text box.
10. Click **SAVE.**
11. On the **L2VPN** tab, click **ATTACH PORT.**
12. Configure the port attachment.

Option	Action
Session	Select **L2VPN-Client-Session.**
Port	Select **name: L2VPN-Port vlan:10.**
Tunnel ID	Enter **100.**

13. Click **ATTACH.**
14. On the **L2VPN** tab, verify that the status for L2VPN-Client-Session changes to UP.

Task 8: Verify the Operation of the VPN Setup

You verify the proper operation of the VPN tunnel deployed by opening consoles into the two L2VPN VMs and using ping to reach across the VPN.

1. In the NSX UI, navigate to **Networking** > **Network Services** > **VPN** > **L2 VPN SESSIONS.**
2. Verify that the status of the L2VPN-Session is Success**.**

   You might need to refresh the status to view the most recent information.
3. Click the Information icon beside the status for L2VPN-Session to display additional information about the tunnel status.

   Both the tunnel and IKE status should be Up.
4. In the vSphere Client inventory, verify the connectivity.
   a. Right-click the **T1-L2VPN-01** virtual machine and select **Edit Settings**
   b. In the **Network adapter 1** drop-down menu, click **Browse**, select **L2VPN-Segment**, and click **OK**.
   c. Verify that **Connected** is selected and click **OK**.
5. Verify that both the NSX Autonomous Edge (Auto-Edge-01) and the T1-L2VPN-02 virtual machines reside on sa-esxi-01.vclass.local.

   Otherwise, use vSphere vMotion to migrate these VMs.
6. Verify that the T1-L2VPN-02 virtual machine is connected to Remote_Network.
   a. In the vSphere Client inventory, right-click **T1-L2VPN-02** and select **Edit Settings**.
   b. Verify that Network adapter 1 has the Remote_Network value.

      Otherwise, click **Browse**, select **Remote_Network** from the drop-down menu, and click **OK.**
7. In the vSphere Client, open a web console to T1-L2VPN-01.
8. Log in to the T1-L2VPN-01 VM with vmware as the user name and VMware1! as the password .
   a. Verify connectivity with T1-L2VPN-02.

      ```
      ping -c 3 172.16.50.12
      ```

      The ping should complete successfully.
9. Return to the vSphere Client and open a web console to T1-L2VPN-02.

10. Log in to T1-L2VPN-02 VM with vmware as the user name and VMware1! as the password.
    a. Verify bidirectional connectivity from T1-L2VPN-02 to T1-L2VPN-01.

       ```
       ping -c 3 172.16.50.11
       ```

       The ping should also complete successfully. You have now verified bidirectional communication between the two VMs at the end of the VPN tunnel.

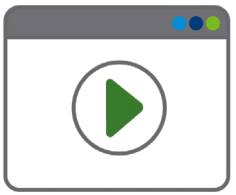
Lab 17 (Simulation) Using NSX Intelligence to Gain Security Insights

Objective and Tasks

Visualize traffic flows and generate recommendations to secure NSX.

1. Deploy the NSX Intelligence Appliance
2. Check the Health Status of NSX Intelligence
3. Generate Traffic Flows
4. Visualize Traffic Flows
5. Generate Security Recommendations
6. Publish Security Recommendations

From your local desktop, go to https://vmware.bravais.com/s/cI5BgTRekegJER3oVUfJ to open the simulation.



IMPORTANT

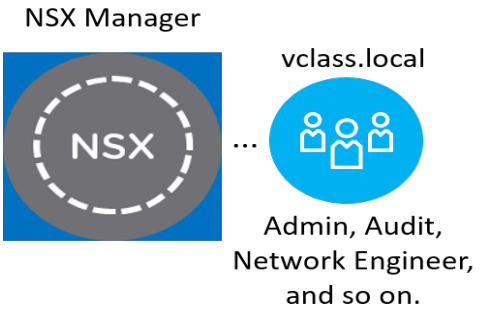
Do not refresh, navigate away from, or minimize the browser tab hosting the simulation. These actions might pause the simulation and the simulation might not progress.

Lab 18 Managing Users and Roles

Objective and Tasks

Integrate NSX Manager with Active Directory over LDAP:

1. Prepare for the Lab
2. Add an Active Directory Domain as an Identity Source
3. Assign NSX Roles to Domain Users and Test Permissions



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. From your student desktop, open Chrome.
2. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
3. On the login page, enter **`admin`** as the user name and **`VMware1!VMware1!`** as the password.

Task 2: Add an Active Directory Domain as an Identity Source

You use LDAP to add an Active Directory Domain to NSX Manager.

1. On the NSX UI Home page, navigate to **System** > **Settings** > **Users and Roles** and click the **LDAP** tab.
2. Click **ADD IDENTITY SOURCE.**
3. Configure the new identity source.

Option	Action
Name	Enter **`VCLASS`**.
Domain Name	Enter **`vclass.local`**.
Type	Select **Active Directory over LDAP** (default).
Base DN	Enter **`CN=Users,DC=vclass,DC=local`**.
LDAP Servers	Click the **Set** link.

4. When the Set LDAP Server window appears, click **ADD LDAP SERVER**.
5. Configure the LDAP server.

Option	Action
Hostname/IP	Enter **`DC.vclass.local`**.
LDAP Protocol	Select **LDAP** (default).
Type	Enter **`389.`** (default).
Bind Identity	Enter **`administrator@vclass.local`**.
Password	Enter **`VMware1!`**.

   Leave all other settings at their default values.
6. Click the **Check Status** link and verify that the connection status is Successful.
7. Click **ADD** and click **APPLY.**
8. Click **SAVE.**

9. Click the **Check Status** link and verify that the connection status is Successful.

Task 3: Assign NSX Roles to Domain Users and Test Permissions

You assign an NSX role to an Active Directory domain user and verify the user's permissions.

1. On the NSX UI home page, navigate to **System** > **Settings** > **Users and Roles** and click the **USERS** tab.
2. Click **ADD** and select **Role Assignment for LDAP.**
3. When the role assignment window appears, select **VCLASS** in the **Search Domain** drop-down menu.
4. Enter **`jdoe`** in the **Users/User Group Name** box and select the **jdoe@vclass.local** user.
5. In the Roles pane, select **Network Engineer** from the **Roles** drop-down menu .
6. Click **SAVE**.
7. At the upper-right corner of the NSX UI, click the **admin** user and select **Log out.**
8. Log in to the NSX UI at https://sa-nsxmgr-01.vclass.local as jdoe.
   a. Click the **NSX-T Data Center** > **SA-NSXMGR-01** bookmark.
   b. Enter **`jdoe@vclass.local`** as the user name and enter **`VMware1!`** as the password.
   c. Click **LOG IN.**
9. In the upper-right corner of the NSX UI, verify that you are logged in as jdoe@vclass.local.
10. Navigate to **Networking** > **Connectivity** > **Tier-1 Gateways** and verify that the **ADD TIER-1 GATEWAY** option is available.

    The availability of the option indicates that users with the Network Engineer role have permissions to configure Tier-1 gateways.
11. Navigate to **Security** > **East West Security** > **Distributed Firewall**.
12. Click **CATEGORY SPECIFIC RULES** and click the **APPLICATION** tab.
13. Click **+ADD POLICY**.

    The unavailable option indicates that users with the Network Engineer role do not have permissions to configure distributed firewall policies or rules.
14. In the upper-right corner of the NSX UI, click the **jdoe@vclass.local** user and select **Log out.**